Sujet élaboré par une cellule pédagogique nationale

EXAMEN PROFESSIONNEL DE PROMOTION INTERNE D'INGÉNIEUR TERRITORIAL

SESSION 2020

ÉPREUVE DE PROJET OU ÉTUDE

ÉPREUVE D'ADMISSIBILITÉ :

L'établissement d'un projet ou étude portant sur l'une des options choisie par le candidat, au moment de son inscription.

Durée : 4 heures
Coefficient : 5

SPÉCIALITÉ : INFORMATIQUE ET SYSTÈMES D'INFORMATION

OPTION : SYSTÈMES D'INFORMATION ET DE COMMUNICATION

À LIRE ATTENTIVEMENT AVANT DE TRAITER LE SUJET :

- Vous ne devez faire apparaître aucun signe distinctif dans votre copie, ni votre nom ou un nom fictif, ni initiales, ni votre numéro de convocation, ni le nom de votre collectivité employeur, de la commune où vous résidez ou du lieu de la salle d'examen où vous composez, ni nom de collectivité fictif non indiqué dans le sujet, ni signature ou paraphe.
- Sauf consignes particulières figurant dans le sujet, vous devez impérativement utiliser une seule et même couleur non effaçable pour écrire et/ou souligner. Seule l'encre noire ou l'encre bleue est autorisée. L'utilisation de plus d'une couleur, d'une couleur non autorisée, d'un surligneur pourra être considérée comme un signe distinctif.
- Le non-respect des règles ci-dessus peut entraîner l'annulation de la copie par le jury.
- Les feuilles de brouillon ne seront en aucun cas prises en compte.

Ce sujet comprend 50 pages dont 1 annexe.

Il appartient au candidat de vérifier que le document comprend le nombre de pages indiqué.
S'il est incomplet, en avertir le surveillant.

- Vous répondrez aux questions suivantes dans l'ordre qui vous convient, en indiquant impérativement leur numéro.
- Vous répondrez aux questions à l'aide des documents et de vos connaissances.
- Des réponses rédigées sont attendues et peuvent être accompagnées si besoin de tableaux, graphiques, schémas …

Ingénieur territorial, vous avez été recruté en tant que chargé de mission au sein de la Direction des Systèmes d'Information (DSI) de la communauté d'agglomération d'INGECO. Cette collectivité compte 500 agents répartis sur un territoire composé de 25 communes mutualisées pour 75 000 habitants. La DSI est composée de 2 pôles : le pôle développement du Système d'Information (SI) qui participe au développement des projets d'équipements (logiciels et matériels pour la collectivité) et le pôle technique ayant la responsabilité de la disponibilité du SI et du traitement des demandes quotidiennes des agents.

Le Directeur Général des Services (DGS) a chargé la DSI de la mise en œuvre du télétravail au sein de la collectivité au côté de la Direction des Ressources Humaines (DRH), des finances et instances paritaires.
Un référent télétravail a été désigné. Il réfère directement au DGS. En tant que Chef de projet, vous travaillez en collaboration avec ce référent télétravail pour le déploiement informatique.

À l'aide des documents et de l'annexe, le DGS vous demande de répondre aux questions suivantes :

Question 1 (3 points)

Détaillez dans une note de service adressée à votre DSI ce qui distingue le télétravail des autres formes de travail telles que : le nomadisme, le travail à distance... Vous en préciserez les usages possibles dans la collectivité et les enjeux pour la DSI en termes de matériel et d'infrastructure informatique.

Question 2 (5 points)

a) Décrivez la méthodologie de projet proposée en précisant les groupes et acteurs permettant de mener la mise en œuvre du télétravail au sein de la collectivité. (2 points)

b) Pour chaque axe thématique de ce projet, donnez tous les éléments à aborder en groupe de travail tant au niveau organisationnel que technique. (3 points)

Question 3 (6 points)

a) Décrivez les différentes architectures techniques permettant aux agents d'accéder au système d'information. (3 points)

b) Développez les bénéfices et inconvénients de ces solutions techniques. (3 points)

Question 4 (6 points)

a) Indiquez comment concilier l'accès à distance du SI et les impératifs de sécurité. (3 points)

b) Décrivez et détaillez les principes de l'architecture technique à développer afin de sécuriser le SI. (3 points)

Liste des documents :

Document 1 : « Le télétravail dans la fonction publique » – Anne Le Mouëllic – *lagazettedescommunes.com* – Janvier 2017 – 2 pages

Document 2 : « Comment mettre en place le télétravail ? » – *cdg80.fr* – Octobre 2019 – 3 pages

Document 3 : « Charte du télétravail à Bordeaux Métropole » – Christophe Weiss – *bordeaux-metropole.fr* – Janvier 2017 – 8 pages

Document 4 : « Guide télétravail : Guide d'accompagnement de la mise en œuvre du télétravail dans la fonction publique » – *fonction-publique.gouv.fr* – Mai 2016 – 2 pages

Document 5 : « Décret n° 2016-151 du 11 février 2016 relatif aux conditions et modalités de mise en œuvre du télétravail dans la fonction publique et la magistrature » – *legifrance.gouv.fr* – Septembre 2019 – 5 pages

Document 6 : « Les collectivités territoriales face à la cybercriminalité : Fiche 11 Les organes de la sécurité » – Association nationale des directeurs et directeurs adjoints des centres de gestion – *cdg43.fr* – 2016 – 9 pages

Document 7 : « 3 risques de sécurité IT à gérer pour protéger les ressources des télétravailleurs sans impacter leur productivité » – *undernews.fr* – Avril 2019 – 2 pages

Document 8 : « Quand le télétravail modifie le travail de l'encadrement » – Martine Doriac – *lagazettedescommunes.com* – Décembre 2012 – 3 pages

Document 9 : « Les pratiques des collectivités territoriales en matière de développement du télétravail pour leurs agents » – *Extrait étude du CNFPT* – Décembre 2013 – 2 pages

Document 10 : « Les pratiques des collectivités territoriales en matière de développement du télétravail pour leurs agents : Conditions techniques et financières de mise en œuvre » – *Extrait étude du CNFPT* – Décembre 2013 – 1 page

Document 11 : « Sécuriser l'accès aux systèmes d'information de la collectivité depuis les mobiles personnels » – *lagazettedescommunes.com* – Octobre 2015 – 7 pages

Liste des annexes :

Annexe 1 : « Présentation de la Communauté d'Agglomération d'INGECO » – *INGECO* – 2019 – 2 pages

Documents reproduits avec l'autorisation du C.F.C.

Certains documents peuvent comporter des renvois à des notes ou à des documents non fournis car non indispensables à la compréhension du sujet.

STATUT DE LA FONCTION PUBLIQUE

Le télétravail dans la fonction publique

Anne Le Mouëllic | Fiches de droit pratique | Publié le 07/03/2016 | Mis à jour le 11/01/2017

Un décret du 11 février fixe les conditions et les modalités de mise en œuvre du télétravail dans la fonction publique.

Définition

Le télétravail désigne toute forme d'organisation du travail dans laquelle les fonctions qui auraient pu être exercées par un agent dans les locaux de son employeur sont réalisées hors de ces locaux, de façon régulière et volontaire, en utilisant les technologies de l'information et de la communication.

Modalités

Le télétravail est organisé au domicile de l'agent ou, éventuellement, dans des locaux professionnels distincts de ceux de son employeur public et de son lieu d'affectation. Le décret fixe un temps de présence sur le lieu d'affectation qui ne peut être inférieur à deux jours par semaine. Le nombre de jours de télétravail ne peut donc être supérieur à trois par semaine. A la demande des agents dont l'état de santé le justifie et après avis du médecin de prévention ou du médecin du travail, il peut être dérogé pour six mois maximum à ces seuils. Cette dérogation est renouvelable une fois, après avis médical.

Les agents exerçant leurs fonctions en télétravail bénéficient des mêmes droits et des mêmes obligations que les agents exerçant sur leur lieu d'affectation. L'employeur prend en charge les coûts découlant directement de l'exercice des fonctions en télétravail, notamment le coût des matériels, des logiciels, des abonnements, des communications et des outils ainsi que de la maintenance de ceux-ci. A noter, les périodes d'astreintes ne constituent pas du télétravail.

Procédure

L'exercice des fonctions en télétravail est accordé sur demande écrite de l'agent. Celle-ci précise les modalités d'organisation souhaitées, notamment les jours de la semaine travaillés sous cette forme ainsi que le ou les lieux d'exercice. Le chef de service, l'autorité territoriale ou l'autorité investie du pouvoir de nomination apprécie la compatibilité de la demande avec la nature des activités exercées, l'intérêt du service et, lorsque le télétravail est organisé au domicile de l'agent, la conformité des installations aux spécifications techniques. Le refus opposé à une demande initiale ou de renouvellement de télétravail formulé par un agent exerçant des activités éligibles ainsi que l'interruption du télétravail à l'initiative de l'administration doivent être précédés d'un entretien et motivés.

Autorisation

L'autorisation a une durée d'un an maximum. Elle peut être renouvelée par décision expresse, après entretien avec le supérieur hiérarchique direct et sur avis de ce dernier. En cas de changement de fonctions, l'agent intéressé doit présenter une nouvelle demande. L'autorisation peut prévoir une période d'adaptation de trois mois maximum.

Réversibilité

En dehors de la période d'adaptation, il peut être mis fin à cette forme d'organisation du travail, à tout moment et par écrit, à l'initiative de l'administration ou de l'agent, moyennant un délai de préavis de deux mois. Dans le cas où il est mis fin à l'autorisation de télétravail à l'initiative de l'administration, le délai de préavis peut être réduit, en cas de nécessité du service dûment motivée.

Acte

L'acte autorisant l'exercice des fonctions en télétravail doit mentionner les fonctions de l'agent exercées en télétravail, le lieu ou les lieux d'exercice, la date de prise d'effet de l'exercice des fonctions en télétravail et sa durée, ainsi que le cas échéant, la période d'adaptation et sa durée. Il doit aussi préciser les jours de référence travaillés sous forme de télétravail et sur site, compte tenu du cycle de travail applicable à l'agent, ainsi que les plages horaires durant lesquelles l'agent en télétravail est à la disposition de son employeur et peut être joint, en référence au cycle de travail de l'agent ou aux amplitudes horaires de travail habituelles.

Notification

Lors de la notification de l'acte autorisant le télétravail, le chef de service doit remettre à l'agent un document d'information indiquant la nature et le fonctionnement des dispositifs de contrôle et de comptabilisation du temps de travail, ainsi que la nature des équipements mis à la disposition de l'agent, leurs conditions d'installation et de restitution, les conditions d'utilisation, de renouvellement et de maintenance de ces équipements mais aussi, la fourniture par l'employeur d'un service d'appui technique. Le chef de service doit remettre à l'agent un document rappelant ses droits et ses obligations en matière de temps de travail et d'hygiène et de sécurité.

REFERENCES

- Loi n° 2012-347 du 12 mars 2012 relative à l'accès à l'emploi titulaire et à l'amélioration des conditions d'emploi des agents contractuels dans la fonction publique, art. 133.
- Décret n° 2016-151 du 11 février 2016 relatif aux conditions et modalités de mise en œuvre du télétravail dans la fonction publique et la magistrature.

Comment mettre en place le télétravail ?

CONTEXTE
Bien connu du secteur privé, le télétravail restait confidentiel dans le secteur public et s'il était mis en place il l'était de manière informelle, faute de cadre juridique. La loi Sauvadet du 12 mars 2012 lui en a donné un et le décret n°2016-151 du 11 février 2016 est venu en préciser les modalités d'application.
Cette nouvelle organisation du travail vise essentiellement à permettre de mieux concilier vie professionnelle et personnelle, il permet ainsi de constituer une réponse pour les agents qui rencontrent les problématiques suivantes :

- chargés de famille, en congé maladie ou parental ;
- en situation de handicap ;
- de trajets ;
- des restrictions médicales.

Le télétravail peut constituer également une réponse en cas de crises graves : pandémies, intempéries ou autres situations exceptionnelles (pics de pollution, grève dans les transports...), dans ce cas, il peut être mis en œuvre à titre exceptionnel.
Comment le mettre en place ?

EN PRATIQUE :

ETAPE 1 : définir le projet
L'introduction du télétravail au sein d'une structure suppose, au préalable, de définir les contours de ce projet :
Pourquoi mettre en place le télétravail ? définir la finalité
Sous quelle forme ?
Le télétravail peut se présenter sous quatre formes différentes, il peut être mis en place :

- à domicile : l'agent travaille chez lui de façon exclusive ou en partie
- de manière nomade : l'agent conserve son poste de travail physique dans la structure mais dispose des outils pour lui permettre de travailler dans n'importe quel lieu
- par le télécentre : l'agent travaille à distance de son équipe dans un lieu ou sont présents des agents d'autres structures
- par le travail en réseau : l'agent est localisé dans un site géographique relevant de la structure mais il dépend d'un manager localisé dans un autre site

Il est important de définir les formes autorisées de télétravail.

Définir les activités concernées
Le télétravail n'est pas compatible avec tous les métiers d'une collectivité, il convient de maintenir l'obligation de continuité du service public en définissant dans la délibération les postes qui sont compatibles avec une organisation télétravaillée et en s'assurant que les effectifs présents dans la structure soient suffisants pour la bonne organisation du service (définir un pourcentage obligatoire de personnel présent dans la structure).

Délimiter les bénéficiaires
Le télétravail est une modalité d'organisation du travail exigeante, les agents qui souhaitent travailler de cette manière doivent être rigoureux, autonomes, motivés, être en capacité de gérer leur travail seul et à gérer leur temps de travail. Ces compétences doivent être validées notamment dans le cadre de la procédure d'entretien professionnel.

Préciser les règles à respecter en matière de :

- sécurité des systèmes d'information et de protection des données ;
- temps de travail, hygiène, sécurité et de prévention des risques.

Arrêter les modalités de prise en charge par l'employeur des équipements nécessaires et des coûts directs découlant de l'exercice du télétravail (matériels, logiciels, abonnements, communications, maintenance...) ; de contrôle et de comptabilisation du temps de travail ; de formation aux outils nécessaires et les durées d'autorisation d'exercice du travail selon cette modalité.

ETAPE 2 : présenter le projet en comité technique (CT) et adopter une délibération

Le décret prévoir qu'une délibération doit être adoptée, après avis du CT, elle reprend les modalités de mise en œuvre du télétravail : les activités éligibles au télétravail, les conditions en prise en charge des coûts directs, les modalités de comptabilisation et de contrôle des temps de travail (cf étape 1).

ETAPE 3 : informer le CHSCT

Le comité d'hygiène, de sécurité et des conditions de travail (CHSCT) est informé de l'avis rendu par le CT sur la délibération relative au télétravail, une délégation du CHSCT peut réaliser une visite au domicile de l'agent avec son accord dûment recueilli par écrit.

ETAPE 4 : formaliser l'engagement individuel par écrit

Le télétravail revêt un caractère volontaire pour l'agent concerné aussi une demande écrite doit être effectuée par l'agent qui souhaite exercer ses fonctions dans le cadre du télétravail.
Le refus de la part de l'autorité territoriale à une demande initiale doit être motivé et faire l'objet d'un entretien préalable.
En cas d'accord pour passer à une organisation télétravaillée, une période d'adaptation de 3 mois maximum peut être aménagée pendant laquelle chaque partie peut y mettre fin par écrit en respectant un préavis d'un mois.
L'autorisation de télétravailler est accordée pour une période d'un an maximum renouvelable et l'engagement entre l'agent concerné et son autorité territoriale est formalisé par un arrêté individuel pour les fonctionnaires ou par la conclusion d'un avenant pour les agents contractuels.
Dans cet acte, sont fixées les conditions d'application à l'agent de la délibération instituant le télétravail dans la structure, telles que :

- les fonctions de l'agent concernées par le télétravail ;
- le lieu d'exercice du télétravail et les jours consacrés à celui-ci (la quotité de travail ouverte au télétravail est plafonnée à trois jours par semaine et le temps de présence sur le lieu d'affectation ne peut être inférieur à deux jours par semaine, ce seuil pouvant être apprécié sur une base mensuelle. Toutefois, une dérogation est possible en considération de l'état de santé de l'agent après avis du médecin de prévention).
- la date de prise d'effet de la situation de télétravail et, le cas échéant, sa durée et une période d'adaptation ;
- les plages horaires durant lesquelles l'agent en situation de télétravail est à la disposition de son employeur et ses horaires de travail lorsqu'il est sur son lieu de travail.
- De plus, l'acte individuel doit comporter les annexes suivantes :
- un document d'information de portée générale définissant les conditions d'application du télétravail à sa situation professionnelle : la nature et le fonctionnement des dispositifs de contrôle et de comptabilisation du temps de travail ; la nature des équipements mis à disposition de l'agent, les conditions d'installation, de restitution...

- une synthèse des droits et obligations de l'agent en matière de temps de travail et d'hygiène et de sécurité. Dans ce cadre, les risques liés au poste en télétravail doivent être pris en compte dans le document unique d'évaluation des risques.
- une copie de la délibération instituant le télétravail dans la collectivité.

L'organisation du télétravail ne prend effet qu'à compter de la date de notification de l'arrêté ou de l'avenant précité et de ses annexes.
La possibilité de mettre fin au télétravail doit être mentionnée dans l'acte, celle-ci peut intervenir à tout moment, par écrit, à l'initiative de l'agent ou de l'administration et sous réserve de respecter un délai de prévenance de deux mois pouvant être ramené éventuellement à un mois en cas de nécessité de service. La décision doit obligatoirement être motivée.

ETAPE 5 : réaliser un bilan annuel du télétravail
Le télétravail fait l'objet d'un bilan annuel présenté aux comités techniques et CHSCT compétents (article 9 du décret n°2016-151 du 16 février 2016).

NOTRE CONSEIL :

- Lorsqu'un emploi est éligible au télétravail, indiquez cette spécificité sur la fiche de poste diffusée via la bourse de l'emploi et publiée par le Centre de Gestion (cf fiche élaborer les fiches de poste).
- Pensez à définir dans la délibération de mise en œuvre du télétravail des critères d'éligibilité à cette organisation du travail qui permettront de justifier les éventuels refus de passage en télétravail et permettront ainsi d'éviter le sentiment d'arbitraire ou de favoritisme.

ERREURS A EVITER :

- Il ne faut pas considérer le télétravail comme un droit ou une obligation, la démarche de l'agent doit être volontaire et ce mode d'organisation ne saurait constituer une faveur ou une sanction.
- Veillez à respecter la vie privée de l'agent ayant une organisation télétravaillée en identifiant des plages horaires spécifiques pour être joint, ouvrir une ligne téléphonique particulière ou à ce que les systèmes de surveillance soient proportionnés à l'activité de l'agent.
- Soyez vigilant à éviter l'isolement de l'agent, le télétravail présente le risque de couper le lien social entre l'agent et son service.

FOIRE AUX QUESTIONS :

Comment s'organise la visite médicale du télétravailleur ?
La délibération et l'acte d'engagement entre la collectivité et l'agent doivent prévoir les modalités d'intervention du service technique, des membres du CHSCT et du médecin de prévention à son domicile, son accord doit être recueilli par écrit lorsqu'une visite à domicile est nécessaire.

Le médecin de prévention est habilité à donner son avis sur l'aménagement du poste du télétravailleur à son domicile, une visite médicale spécifique au télétravail peut être prévue à la demande de l'agent ou à celle de l'administration sous réserve d'avoir obtenu l'accord **préalable par écrit de l'agent.**

DOCUMENT 3

« Charte du télétravail à Bordeaux Métropole » – Christophe Weiss – *bordeaux-metropole.fr* – Janvier 2017

Charte du télétravail à Bordeaux Métropole

Préambule

Le télétravail est encore très peu développé dans la fonction publique (2 % des agents), contre 16 % dans le privé, et jusqu'à plus de 30 % dans certains pays à économie comparable.

Le télétravail répond à plusieurs finalités recherchées par Bordeaux Métropole :

- Il permet une qualité de vie au travail, une efficacité professionnelle et une meilleure articulation entre la vie professionnelle et la vie privée.
- Il participe à la modernisation de l'administration en innovant dans les modes de travail et en promouvant le management par objectifs, qui se traduit par la confiance et la responsabilisation. Il développe l'implication au travail.
- Il participe aussi d'une démarche de développement durable : limitation des déplacements pendulaires, des risques d'accidents de trajet, réduction des gaz à effets de serre.

Cadre juridique

L'accord interprofessionnel du 19 juillet 2005 définit les conditions du télétravail. Il est complété par l'arrêté du 30 mai 2006.

L'article 133 de la Loi du 12 mars 2012 autorise l'exercice des fonctions des agents publics en télétravail. Il indique que cet exercice est accordé à la demande de l'agent et après acceptation du chef de service. Il précise qu'il peut y être mis fin à tout moment, sous réserve d'un délai de prévenance. Enfin, il rappelle que les agents télétravailleurs bénéficient des mêmes droits que les agents en fonction dans les locaux de l'employeur.

Le décret du 11 février 2016 fixe les conditions d'organisation de cette modalité de travail.

Les conditions générales du dispositif sont définies au sein de la présente charte.

Ce document de cadrage doit être complété par le protocole individuel que chaque agent télétravailleur signera avec son encadrant direct.

Première partie
Définition et principes généraux du télétravail

Article 1 : Définition

Le télétravail est une forme d'organisation et/ou de réalisation du travail, utilisant les technologies de l'information et dans laquelle un travail, qui aurait pu être réalisé dans le bureau habituellement occupé par l'agent, est effectué ailleurs de façon régulière.

Article 2 – Principes généraux

- Volontariat : le télétravail revêt un caractère volontaire. Il ne peut être imposé à l'agent par l'administration. De même, il ne peut pas être obtenu par l'agent sans l'accord de son supérieur hiérarchique.

- Réversibilité : la situation de télétravail est réversible. À tout moment, chacune des parties peut y mettre fin, sous réserve du respect d'un délai de préavis dont la durée est fixée par l'organisation.

- Maintien des droits et obligations : le télétravailleur bénéficie des mêmes droits et avantages légaux que ceux applicables à ses collègues en situation comparable travaillant dans leur bureau. Il est soumis aux mêmes obligations.

- Protection des données : il incombe à l'employeur de prendre, dans le respect des prescriptions de la Commission Nationale de l'Informatique et des Libertés (CNIL), les mesures qui s'imposent pour assurer la protection des données utilisées et traitées par le télétravailleur à des fins professionnelles.

- Respect de la vie privée : l'employeur est tenu de respecter la vie privée du télétravailleur. À cet effet, il fixe en concertation avec celui-ci les plages horaires pendant lesquelles il peut le contacter.

Deuxième partie
Modalités du télétravail à Bordeaux Métropole

Article 3 : Entrée en vigueur du télétravail

Par principe, le télétravailleur s'engage sur une durée d'un an, reconductible, après évocation lors de l'entretien annuel d'évaluation. Les agents n'ont donc pas à candidater de nouveau chaque année.

Toutefois, dès lors que l'agent change de poste et/ou d'encadrant, son télétravail devra être examiné de nouveau.

A tout moment, chaque partie peut décider de mettre fin au télétravail. L'abandon du télétravail, qu'il soit le fait de l'agent ou du chef de service, doit être formulé par écrit à l'autre partie signataire du protocole d'accord, en respectant un délai d'un mois avant le terme souhaité. Il est applicable sans autre délai ni formalité. Ce préavis pourra être supprimé si l'intérêt du service exige une cessation immédiate de l'activité en télétravail.

Article 4 : Contractualisation agent/Bordeaux Métropole

Les conditions individuelles du télétravail sont fixées par un protocole individuel entre l'agent et son supérieur hiérarchique direct. Ce protocole sera validé par la signature du directeur concerné.

Il porte, notamment, sur les missions, activités ou tâches à réaliser, le ou les jours télé travaillés, le lieu de télétravail, les plages horaires…

Une fiche de suivi permettra de faire le lien entre le télétravailleur et son encadrant. Cette fiche détaillera les objectifs précis, qui seront fixés pour une période donnée, ainsi que les tâches et missions que l'agent devra réaliser. Pour chaque objectif, mission, tâche une date de début et une date de fin seront fixées conjointement par le chef de service et l'agent. Chaque objectif, mission, tâche fera l'objet d'une évaluation, l'encadrant devant préciser s'il a été réalisé dans les temps et conformément aux attendus.

Article 5 : Descriptif de la procédure de candidature

Chaque année, un appel à candidature sera ouvert pendant un mois.

L'agent télétravailleur devra répondre au questionnaire d'auto-évaluation avant de postuler au télétravail. Ce document lui est personnel. Ensuite, il remplira une fiche de candidature et sollicitera un entretien auprès de son encadrant. Cet entretien est obligatoire et ne peut être refusé par l'encadrant. Il est différent de l'entretien annuel d'évaluation.

Ce dernier devra prendre une décision écrite et motivée d'accord ou de refus de la demande de télétravail :

- Si la candidature est validée par le N+1, le dossier papier suit la chaîne hiérarchique de validation jusqu'au Directeur général, puis est envoyé à la direction qui traite le télétravail.

- Si la candidature n'est pas validée, le refus écrit doit être motivé et le dossier papier est envoyé à la Direction qui traite le télétravail. Une copie est remise à l'agent demandeur. L'agent peut demander un entretien à son N+ 2.
- En cas de refus motivé exprimé par un supérieur hiérarchique autre que le N+1, le dossier devra être retourné à la direction qui traite le télétravail. Une copie est remise à l'agent demandeur du télétravail.

Les demandes de télétravail seront ensuite recensées par la direction en charge du dossier :

- si le nombre de demandes n'entraîne pas un dépassement du quota annuel de télétravailleurs, fixé annuellement en amont de l'appel à candidature par le Comité de direction générale (Codir), la liste des candidats est validée par ce dernier.

- si le nombre de demandes entraîne un dépassement du quota annuel de télétravailleurs, la liste des candidats sera arbitrée et validée par le Codir.

Article 6 : Télétravail pour raison médicale

Les demandes de télétravail pour raison médicale pourront être traitées tout au long de l'année.

Les agents concernés devront consulter les médecins de travail qui émettront un avis. Ces derniers pourront proposer un aménagement de poste fondé sur un télétravail. L'avis du médecin personnel de l'agent ne sera pas pris en compte.

Un entretien devra être réalisé avec le chef de service, qui donnera ou non son accord. Tout refus devra être motivé par écrit.

Toutefois, le télétravail est exclusif de l'arrêt maladie et l'agent en situation de travail doit être apte à exercer les tâches qui lui sont confiées.

Article 7 : Champ d'application du télétravail aux agents de l'établissement

Toutes les missions ne sont pas compatibles avec le télétravail. Les fonctions opérationnelles (collecte des déchets, voirie, parcs et jardins…) ou celles nécessitant une relation de proximité ou une présence physique sont exclues du dispositif.
En revanche, les tâches administratives d'expertise, d'étude, de rédaction (…) peuvent être réalisées à distance.

La possibilité de candidater est ouverte à tous les agents concernés, dès lors qu'ils ont plus d'un an d'ancienneté dans l'institution, quelles que soient leur fonction, exceptés les agents occupant des fonctions de chef de service, chef de mission, directeur, directeur de mission, adjoint à un directeur général ou un emploi fonctionnel.

Il appartient aux responsables hiérarchiques directs, saisis par un agent d'une demande, de définir et d'expliquer quels sont les postes non télétravaillables, c'est-à-dire ceux des agents dont les missions nécessitent une présence physique indispensable à la réalisation de leur mission.

La limite du nombre de télétravailleurs par entité de travail est laissée à l'appréciation de l'encadrant direct et/ou du directeur.

Les critères, qui prévaudront pour arbitrer si besoin les candidatures, s'appuieront sur les critères d'accessibilité et d'éligibilité déterminés dans la délibération du 16 décembre 2016.

L'agent doit être apte au travail durant les périodes de télétravail.

Article 8 : Critère d'éligibilité technique

L'éligibilité technique au télétravail en fonction du lieu choisi :

- soit l'agent souhaite télétravailler sur un site métropolitain, il dispose alors d'un bureau et de l'équipement technique nécessaire (connexions à son poste de travail identiques à celles du bureau).

- soit l'agent choisit de télétravailler à domicile, en tiers-lieu ou dans une commune partenaire et doit disposer d'une connexion ADSL d'au moins 1 mégabit de débit aux heures de bureau. Il aura accès à sa boîte aux lettres électronique et à des espaces de travail collaboratifs via Cubetcites, au réseau et à l'Intranet. La liste des applicatifs métiers disponibles sera diffusée tous les ans en amont de l'appel à candidature.

Article 9 : Forme du télétravail

La forme pendulaire du télétravail est retenue, afin d'éviter l'isolement du télétravailleur et de conserver un fonctionnement collectif. Le télétravailleur fera ainsi des horaires de bureau.

Le nombre de jour de télétravail autorisé :

Agents à temps complet	1 jour tous les 15 jours 1 jour toutes les semaines 2 jours toutes les semaines
Agents à 90%	1 jour tous les 15 jours 0,5 jour par semaine (jour du temps partiel) 1,5 jours par semaine
Agents à 80%	1 jour toutes les semaines

Le seuil du nombre de jour de télétravail par semaine s'apprécie sur une base mensuelle.

Une période de 3 mois maximum d'adaptation peut être prévue.

Le télétravail est exclusif du dispositif du temps de travail aménagé (semaine en 4,5 jours ou deux semaines en 9 jours).

Une journée de télétravail est d'une durée de 7 heures 15 minutes. Les jours télétravaillés ne peuvent pas faire l'objet d'acquisition d'heures supplémentaires au titre du régime de RTT.

Les jours de télétravail sont fixes. Néanmoins, en cas d'obligation de service et avec l'accord de la hiérarchie, ils peuvent être reportés sur un autre jour.

Toutefois, ils ne se rattrapent pas s'ils tombent sur un jour férié ou pendant un jour de congé.

En cas d'impossibilité de télétravailler le jour prévu, l'agent doit se rendre sur son lieu de travail et badger le cas échéant.

Article 10 : Lieu du télétravail

Le télétravail s'effectue au domicile de l'agent ou dans un site métropolitain, ou sur un tiers-lieu ou dans une commune partenaire.

L'agent conserve sa résidence administrative pour les jours non télétravaillés.

Pour les périodes de télétravail, la résidence administrative est celle de la commune d'implantation du lieu de télétravail.

L'agent n'effectuera pas de déplacements le(s) jour(s) où il télétravaille.

Il devra s'assurer de disposer à domicile d'un espace permettant de travailler dans de bonnes conditions.

Article 11 : Horaires de travail

Les horaires de travail de l'agent sont précisés dans le protocole individuel.

Si l'agent choisit le télétravail à domicile, il ne peut être contacté pour son activité en dehors des horaires fixés.

L'agent doit être joignable sur une plage fixe de 7 heures 15 minutes dans la journée de télétravail, en fonction des modalités déterminées dans le protocole.

L'agent n'a pas d'activités personnelles et/ou familiales dans les créneaux horaires de télétravail. Il se consacre exclusivement à son activité professionnelle.

Ainsi le télétravail est exclusif de la garde d'enfant.

Article 12 : Équipement du télétravailleur

1 – Informatique

L'établissement met à la disposition du télétravailleur à domicile un ordinateur portable, paramétré par le service informatique, que le télétravailleur s'engage à utiliser dans le respect de la charte

d’usage du système d’information de Bordeaux Métropole. Des séances de formation peuvent être dispensées lors de la remise.

Bordeaux Métropole met à la disposition du télétravailleur sur site un poste fixe avec les applicatifs métiers qui lui sont nécessaires.

Seuls les ordinateurs métropolitains sont aptes à se connecter à l’ensemble des systèmes informatiques. L'utilisation d'un ordinateur personnel est interdite.

Les imprimantes et périphériques personnels ne sont pas pris en compte et ne peuvent être installés pour des raisons techniques et de sécurité.

En cas de panne ou de dysfonctionnement, l’agent en télétravail bénéficie d’un accès à la hotline informatique. Il doit pour cela contacter le 10 aux heures ouvrées depuis le site ou le 05 56 99 89 10 depuis son domicile. La hotline est apte à répondre à la majorité des problèmes et dans le cas où une intervention technique serait nécessaire, elle sera réalisée sur le lieu de travail habituel de l’agent.

L’agent télétravailleur est responsable du matériel mis à sa disposition.

2 – Téléphonie

Le télétravailleur sur site métropolitain fera un transfert de sa ligne professionnelle sur sa ligne personnelle. Il continue ainsi d’être joignable sur son numéro professionnel pendant son temps de télétravail.

Le télétravailleur à domicile ou en tiers-lieux disposera d'un outil de téléphonie.

Article 13 : Sensibilisation du télétravailleur et de son supérieur hiérarchique

Au moment de la mise en œuvre du télétravail, l'agent et son encadrant qui ne l'ont pas déjà fait suivront une session de sensibilisation, qui leur permettra d’appréhender la démarche et les spécificités du télétravail.

Article 14 : Organisation du télétravail

Les missions, activités ou tâches qui sont effectuées dans les périodes de télétravail, ainsi que les modalités de liaison, sont définies par le supérieur hiérarchique, après échange avec l’agent.

Elles sont inscrites dans la fiche de poste de l’agent et actées dans le protocole individuel.

Article 15 : Maintien des droits et obligations

Le télétravailleur bénéficie des mêmes garanties et droits que tout autre agent :

- il conserve son régime de rémunération
- l’ensemble des droits liés à son statut (titulaires, non-titulaires) est maintenu : déroulement de carrière, congés, formation, représentation syndicale, évaluation…

- il peut prétendre au versement de l'indemnité de panier pour les jours télé travaillés. Le recensement de cette indemnité sera assuré par le supérieur hiérarchique via l'état des éléments variables de paie.

Il est également soumis aux mêmes obligations que tout autre agent. Il doit respecter la charte informatique et les différentes règles de sécurité de l'information, édictées par l'établissement.
Il doit également respecter le règlement intérieur de Bordeaux Métropole.

Article 16 : Accidents liés au travail

L'établissement prend en charge les accidents de service et du travail survenus au télétravailleur, dans les mêmes conditions réglementaires que celles qui s'appliquent aux autres agents.

Dans ce cadre, il appartient au télétravailleur d'apporter la preuve de l'accident et de sa relation avec le service. Sur la base de la déclaration de l'accident (lieu, heure, activité, circonstances) l'employeur juge de l'imputabilité ou non au service.

Si l'imputabilité au service est reconnue, l'accident est pris en charge par Bordeaux Métropole.

Article 17 : Assurances

Bordeaux Métropole prend en charge les dommages subis par les biens de toute nature mis à disposition du télétravailleur dans le cadre de son activité professionnelle.

Les dommages causés aux tiers sont pris en charge par l'établissement s'ils résultent directement de l'exercice du travail ou s'ils sont causés par les biens qu'il met à la disposition du télétravailleur.

Si les dommages résultent d'une faute personnelle détachable du service, la responsabilité de Bordeaux Métropole n'est pas engagée ou si la responsabilité de l'établissement est recherchée, cette dernière peut se retourner contre le télétravailleur.

Par ailleurs, le télétravailleur à domicile s'engage à signaler sa situation à son assureur.

Il sera demandé aux télétravailleurs à domicile un certificat d'assurance logement.

Article 18 : Indemnisation

Une indemnisation forfaitaire de 60 euros par an est attribuée au télétravailleur à domicile. Elle a pour objet de compenser les frais occasionnés par le télétravail.

Article 19 : Suivi du télétravail

Le suivi mensuel des activités réalisées en télétravail est précisé dans le protocole individuel.

Le télétravailleur s'engage à participer au bilan annuel d'évaluation en remplissant les tableaux demandés et en renseignant le questionnaire annuel sur sa situation de télétravail.

DOCUMENT 4

« Guide télétravail : Guide d'accompagnement de la mise en œuvre du télétravail dans la fonction publique » – *fonction-publique.gouv.fr* – Mai 2016

Ce qu'est le télétravail

Article 2 du décret n°2016-151

« Le télétravail désigne toute forme d'organisation du travail dans laquelle les fonctions qui auraient pu être exercées par un agent dans les locaux de son employeur sont réalisées hors de ces locaux de façon régulière et volontaire en utilisant les technologies de l'information et de la communication »

Cette définition appelle plusieurs observations :

- Le télétravail dans la fonction publique ne s'entend donc pas comme une notion différente du télétravail dans le secteur privé, même si les modalités d'exercice peuvent être différentes. Les termes posés à l'article 2 du décret reprennent, en effet, quasiment à l'identique ceux qui figurent à l'article L.1222-9 du Code du travail.

- Le fait, pour un agent, de travailler en dehors des locaux de son employeur ne suffit pas à lui conférer la qualité d'agent en télétravail. Encore faut-il qu'il s'agisse d'une pratique régulière nécessitant l'usage des technologies de l'information et de la communication.

- Le caractère régulier du télétravail ne signifie pas que les tâches de l'agent doivent être réalisées, dans leur totalité, en dehors des locaux de l'employeur. L'article 3 du décret plafonne, en effet, la quotité de travail ouverte au télétravail à trois jours par semaine, sauf, à leur demande, pour les agents dont l'état de santé le justifie, après avis du médecin de prévention ou du médecin de travail.

- Un agent qui exerce ses fonctions en télétravail ne doit pas être assimilé aux autres agents qui peuvent également être absents du bureau (au titre des congés, d'une autorisation de travail à temps partiel, d'une formation ou encore d'un congé maladie), car, contrairement à lui, ces derniers sont déchargés de toute obligation professionnelle.

Article 133 de la loi n°2012-347 du 12 mars 2012

« Les fonctionnaires relevant de la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires peuvent exercer leurs fonctions dans le cadre du télétravail tel qu'il est défini au premier alinéa de l'article L. 1222-9 du code du travail. L'exercice des fonctions en télétravail est accordé à la demande du fonctionnaire et après accord du chef de service. Il peut y être mis fin à tout moment, sous réserve d'un délai de prévenance. Les fonctionnaires télétravailleurs bénéficient des droits prévus par la législation et la réglementation applicables aux agents exerçant leurs fonctions dans les locaux de leur employeur public.

Le présent article est applicable aux agents publics non fonctionnaires et aux magistrats.

Un décret en Conseil d'Etat fixe, après concertation avec les organisations syndicales représentatives de la fonction publique, les conditions d'application du présent article, notamment en ce qui concerne les modalités d'organisation du télétravail et les conditions dans lesquelles la commission administrative paritaire compétente peut être saisie par le fonctionnaire intéressé en cas de refus opposé à sa demande de télétravail.»

Et ce qu'il n'est pas

Le télétravail ne constitue toutefois qu'une forme d'organisation du travail parmi d'autres modalités existantes auxquelles il n'a pas vocation à se substituer.

Dans ce contexte, il semble donc utile de distinguer le télétravail des autres modalités les plus courantes d'organisation du travail à distance, notamment :

- du travail en tiers lieu statutaire, qui est exercé par des agents dotés d'un statut particulier et jouissant d'une forte autonomie (par exemple, les magistrats et les personnels des corps d'inspection) ;
- du nomadisme, qui est pratiqué par les agents dont les activités s'exercent, par nature, en dehors des locaux de l'employeur (par exemple, les activités de contrôle) ;
- du travail en réseau ou en site distant, ainsi désigné parce que l'agent exerce ses activités dans des locaux relevant de l'autorité de son employeur mais sur un site distinct de celui d'une partie de sa hiérarchie et de ses collègues ;
- du travail à distance dans le cadre du plan de continuité des activités, qui répond au besoin de maintenir un niveau minimal d'activité en cas de survenance d'événements exceptionnels (par exemple, intempéries, pandémies ou encore terrorisme) ;
- de l'astreinte : la période d'astreinte ne constitue pas pour l'agent du télétravail, tout comme l'éventuelle intervention réalisée depuis son domicile pendant la période d'astreinte si celle-ci est comptabilisée comme du temps de travail effectif.

Article 2 du décret n° 2016-151

« Les périodes d'astreintes mentionnées à l'article 5 du décret du 25 août 2000 [temps de travail dans la fonction publique de l'Etat], *à l'article 5 du décret du 12 juillet 2001* [temps de travail dans la fonction publique territoriale] *et à l'article 20 du décret du 4 janvier 2002* [temps de travail dans la fonction publique hospitalière] *ne constituent pas du télétravail au sens du présent décret »*

Exemple

Un agent est en télétravail trois jours par semaine (lundi, jeudi, vendredi).

Il effectue une astreinte le samedi et le dimanche et réalise une intervention à raison de deux heures le dimanche.

Ni la période d'astreinte, ni celle de l'intervention ne constituent du télétravail.

Par ailleurs, seule l'intervention de deux heures est comptabilisée comme du temps de travail effectif. Elle s'ajoute alors au temps de travail comptabilisé à la fois au titre du télétravail et du travail réalisé sur site.

Décret n° 2016-151 du 11 février 2016 relatif aux conditions et modalités de mise en œuvre du télétravail dans la fonçtion publique et la magistrature

NOR: RDFF1519812D
Version consolidée au 23 septembre 2019

Le Premier ministre,
Sur le rapport de la ministre de la décentralisation et de la fonction publique,
Vu le code du travail, notamment son article R. 4121-1 ;
Vu la loi n° 83-634 du 13 juillet 1983 modifiée portant droits et obligations des fonctionnaires, notamment son article 8 bis, ensemble la loi n° 84-16 du 11 janvier 1984 modifiée portant dispositions statutaires relatives à la fonction publique de l'Etat, la loi n° 84-53 du 26 janvier 1984 modifiée portant dispositions statutaires relatives à la fonction publique territoriale et la loi n° 86-33 du 9 janvier 1986 modifiée portant dispositions statutaires relatives à la fonction publique hospitalière ;
Vu la loi n° 2012-347 du 12 mars 2012 modifiée relative à l'accès à l'emploi titulaire et à l'amélioration des conditions d'emploi des agents contractuels dans la fonction publique, à la lutte contre les discriminations et portant diverses dispositions relatives à la fonction publique, notamment son article 133 ;
Vu l'ordonnance n° 58-1270 du 22 décembre 1958 modifiée portant loi organique relative au statut de la magistrature ;
Vu le décret n° 82-451 du 28 mai 1982 modifié relatif aux commissions administratives paritaires ;
Vu le décret n° 82-453 du 28 mai 1982 modifié relatif à l'hygiène et à la sécurité du travail ainsi qu'à la prévention médicale dans la fonction publique ;
Vu le décret n° 85-603 du 10 juin 1985 modifié relatif à l'hygiène et à la sécurité du travail ainsi qu'à la médecine professionnelle et préventive dans la fonction publique territoriale ;
Vu le décret n° 86-83 du 17 janvier 1986 modifié relatif aux dispositions générales applicables aux agents contractuels de l'Etat pris pour l'application de l'article 7 de la loi n° 84-16 du 11 janvier 1984 portant dispositions statutaires relatives à la fonction publique de l'Etat ;
Vu le décret n° 88-145 du 15 février 1988 modifié pris pour l'application de l'article 136 de la loi du 26 janvier 1984 modifiée portant dispositions statutaires relatives à la fonction publique territoriale et relatif aux agents non titulaires de la fonction publique territoriale ;
Vu le décret n° 91-155 du 6 février 1991 modifié relatif aux dispositions générales applicables aux agents contractuels des établissements mentionnés à l'article 2 de la loi n° 86-33 du 9 janvier 1986 modifiée portant dispositions statutaires relatives à la fonction publique hospitalière ;
Vu le décret n° 2000-815 du 25 août 2000 modifié relatif à l'aménagement et à la réduction du temps de travail dans la fonction publique de l'Etat et dans la magistrature ;
Vu le décret n° 2001-623 du 12 juillet 2001 modifié pris pour l'application de l'article 7-1 de la loi n° 84-53 du 26 janvier 1984 et relatif à l'aménagement et à la réduction du temps de travail dans la fonction publique territoriale ;
Vu le décret n° 2002-9 du 4 janvier 2002 modifié relatif au temps de travail et à l'organisation du travail dans les établissements mentionnés à l'article 2 de la loi n° 86-33 du 9 janvier 1986 portant dispositions statutaires relatives à la fonction publique hospitalière ;
Vu l'avis du Conseil commun de la fonction publique en date du 24 septembre 2015 ;
Vu l'avis du Conseil national d'évaluation des normes du 10 septembre 2015 ;
Le Conseil d'Etat (section de l'administration) entendu,
Décrète :

Article 1

Les dispositions du présent décret s'appliquent aux fonctionnaires et aux agents publics non fonctionnaires régis par la loi du 13 juillet 1983 susvisée et aux magistrats de l'ordre judiciaire régis par l'ordonnance du 22 décembre 1958 susvisée.

Article 2

Le télétravail désigne toute forme d'organisation du travail dans laquelle les fonctions qui auraient pu être exercées par un agent dans les locaux de son employeur sont réalisées hors de ces locaux de façon régulière et volontaire en utilisant les technologies de l'information et de la communication.
Le télétravail est organisé au domicile de l'agent ou, éventuellement, dans des locaux professionnels distincts de ceux de son employeur public et de son lieu d'affectation.
Les périodes d'astreintes mentionnées à l'article 5 du décret du 25 août 2000 susvisé, à l'article 5 du décret du 12 juillet 2001 susvisé et à l'article 20 du décret du 4 janvier 2002 susvisé ne constituent pas du télétravail au sens du présent décret.

Article 3

La quotité des fonctions pouvant être exercées sous la forme du télétravail ne peut être supérieure à trois jours par semaine. Le temps de présence sur le lieu d'affectation ne peut être inférieur à deux jours par semaine.
Les seuils définis au premier alinéa peuvent s'apprécier sur une base mensuelle.

Article 4

Modifié par Décret n°2019-637 du 25 juin 2019 - art. 1

A la demande des agents dont l'état de santé, le handicap ou l'état de grossesse le justifient et après avis du médecin de prévention ou du médecin du travail, il peut être dérogé pour six mois maximum aux conditions fixées par l'article 3. Cette dérogation est renouvelable une fois par période d'autorisation du télétravail, après avis du médecin de prévention ou du médecin du travail.

Article 5

Modifié par Décret n°2019-637 du 25 juin 2019 - art. 2

L'exercice des fonctions en télétravail est accordé sur demande écrite de l'agent. Celle-ci précise les modalités d'organisation souhaitées, notamment les jours de la semaine travaillés sous cette forme ainsi que le ou les lieux d'exercice.

Le chef de service, l'autorité territoriale ou l'autorité investie du pouvoir de nomination apprécie la compatibilité de la demande avec la nature des activités exercées, l'intérêt du service et, lorsque le télétravail est organisé au domicile de l'agent, la conformité des installations aux spécifications techniques précisées par l'employeur.

Dans le cas où la demande est formulée par un agent en situation de handicap, le chef de service, l'autorité territoriale ou l'autorité investie du pouvoir de nomination doit mettre en œuvre sur le lieu de télétravail de l'agent les aménagements de poste nécessaires.

La durée de l'autorisation est d'un an maximum. L'autorisation peut être renouvelée par décision expresse, après entretien avec le supérieur hiérarchique direct et sur avis de ce dernier. En cas de changement de fonctions, l'agent intéressé doit présenter une nouvelle demande.

L'autorisation peut prévoir une période d'adaptation de trois mois maximum.

En dehors de la période d'adaptation prévue à l'alinéa précédent, il peut être mis fin à cette forme d'organisation du travail, à tout moment et par écrit, à l'initiative de l'administration ou de l'agent, moyennant un délai de prévenance de deux mois. Dans le cas où il est mis fin à l'autorisation de télétravail à l'initiative de l'administration, le délai de prévenance peut être réduit en cas de nécessité du service dûment motivée. Pendant la période d'adaptation, ce délai est ramené à un mois.

Le refus opposé à une demande initiale ou de renouvellement de télétravail formulée par un agent exerçant des activités éligibles fixées par l'un des actes mentionnés à l'article 7 ainsi que l'interruption du télétravail à l'initiative de l'administration doivent être précédés d'un entretien et motivés.

Article 6

Les agents exerçant leurs fonctions en télétravail bénéficient des mêmes droits et obligations que les agents exerçant sur leur lieu d'affectation.
L'employeur prend en charge les coûts découlant directement de l'exercice des fonctions en télétravail, notamment le coût des matériels, logiciels, abonnements, communications et outils ainsi que de la maintenance de ceux-ci.

Article 7

I. - Un arrêté ministériel pour la fonction publique de l'Etat, une délibération de l'organe délibérant pour la fonction publique territoriale, une décision de l'autorité investie du pouvoir de nomination pour la fonction publique hospitalière, pris après avis du comité technique ou du comité consultatif national compétent, fixe :
1° Les activités éligibles au télétravail ;
2° La liste et la localisation des locaux professionnels éventuellement mis à disposition par l'administration pour l'exercice des fonctions en télétravail, le nombre de postes de travail qui y sont disponibles et leurs équipements ;
3° Les règles à respecter en matière de sécurité des systèmes d'information et de protection des données ;
4° Les règles à respecter en matière de temps de travail, de sécurité et de protection de la santé ;
5° Les modalités d'accès des institutions compétentes sur le lieu d'exercice du télétravail afin de s'assurer de la bonne application des règles applicables en matière d'hygiène et de sécurité ;
6° Les modalités de contrôle et de comptabilisation du temps de travail ;
7° Les modalités de prise en charge, par l'employeur, des coûts découlant directement de l'exercice du télétravail, notamment ceux des matériels, logiciels, abonnements, communications et outils ainsi que de la maintenance de ceux-ci ;
8° Les modalités de formation aux équipements et outils nécessaires à l'exercice du télétravail ;
9° La durée de l'autorisation mentionnée à l'article 5 si elle est inférieure à un an.
II. - Dans les directions départementales interministérielles, les conditions de mise en œuvre du télétravail prévues au I font l'objet d'un arrêté du Premier ministre, pris après avis du comité technique des directions départementales interministérielles.
III. - Les modalités de mise en œuvre du télétravail fixées aux 1° à 9° du I sont précisées en tant que de besoin, dans chaque service ou établissement, après consultation du comité technique ou du comité consultatif national compétent.
IV. - Les comités d'hygiène, de sécurité et des conditions de travail compétents et la commission des conditions de travail commune aux personnels de direction de la fonction publique hospitalière sont informés des avis rendus par les comités techniques ou les comités consultatifs nationaux en application du présent article.

Article 8

I. - L'acte autorisant l'exercice des fonctions en télétravail mentionne :
1° Les fonctions de l'agent exercées en télétravail ;
2° Le lieu ou les lieux d'exercice en télétravail ;
3° Les jours de référence travaillés, d'une part, sous forme de télétravail et, d'autre part, sur site, compte tenu du cycle de travail applicable à l'agent, ainsi que les plages horaires durant lesquelles l'agent exerçant ses activités en télétravail est à la disposition de son employeur et peut être joint, par référence au cycle de travail de l'agent ou aux amplitudes horaires de travail habituelles ;
4° La date de prise d'effet de l'exercice des fonctions en télétravail et sa durée ;
5° Le cas échéant, la période d'adaptation prévue à l'article 5 et sa durée.
II. - Lors de la notification de l'acte mentionné au I, le chef de service remet à l'agent intéressé :
1° Un document d'information indiquant les conditions d'application à sa situation professionnelle de l'exercice des fonctions en télétravail, notamment :
a) La nature et le fonctionnement des dispositifs de contrôle et de comptabilisation du temps de travail ;
b) La nature des équipements mis à disposition de l'agent exerçant ses activités en télétravail et leurs conditions d'installation et de restitution, les conditions d'utilisation, de renouvellement et de maintenance de ces équipements et de fourniture, par l'employeur, d'un service d'appui technique ;
2° Une copie des règles mentionnées à l'article 7 et un document rappelant ses droits et obligations en matière de temps de travail et d'hygiène et de sécurité.

Article 9

Le télétravail fait l'objet d'un bilan annuel présenté aux comités techniques et aux comités d'hygiène, de sécurité et des conditions de travail compétents.
Les risques liés aux postes en télétravail sont pris en compte dans le document mentionné à l'article R. 4121-1 du code du travail.

Article 10

Dans la fonction publique de l'Etat, la commission administrative paritaire ou la commission consultative paritaire compétentes peuvent être saisies, par l'agent intéressé, du refus opposé à une demande initiale ou de renouvellement de télétravail formulée par celui-ci pour l'exercice d'activités éligibles fixées par l'un des actes mentionnés à l'article 7 ainsi que de l'interruption du télétravail à l'initiative de l'administration, dans les conditions prévues respectivement par le décret n° 82-451 du 28 mai 1982 susvisé et le décret du 17 janvier 1986 susvisé.

Article 11

A modifié les dispositions suivantes :

- Modifie Décret n°82-453 du 28 mai 1982 - art. 52 (V)

Article 12

A modifié les dispositions suivantes :

- Modifie Décret n°85-603 du 10 juin 1985 - art. 40 (V)

Article 13

Les dispositions du second alinéa de l'article 9 ne sont pas applicables à Mayotte.

Article 14

Le ministre des affaires étrangères et du développement international, la ministre de l'écologie, du développement durable et de l'énergie, la ministre de l'éducation nationale, de l'enseignement supérieur et de la recherche, le garde des sceaux, ministre de la justice, le ministre des finances et des comptes publics, le ministre de la défense, la ministre des affaires sociales, de la santé et des droits des femmes, la ministre du travail, de l'emploi, de la formation professionnelle et du dialogue social, le ministre de l'intérieur, le ministre de l'agriculture, de l'agroalimentaire et de la forêt, porte-parole du Gouvernement, le ministre de l'économie, de l'industrie et du numérique, la ministre du logement, de l'égalité des territoires et de la ruralité, la ministre de la décentralisation et de la fonction publique, la ministre de la culture et de la communication, le ministre de la ville, de la jeunesse et des sports et la ministre des outre-mer sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au Journal officiel de la République française.

Fait le 11 février 2016.

Manuel Valls

Par le Premier ministre :

La ministre de la décentralisation et de la fonction publique,

Marylise Lebranchu

Le ministre des affaires étrangères et du développement international,

Laurent Fabius

La ministre de l'écologie, du développement durable et de l'énergie,

Ségolène Royal

La ministre de l'éducation nationale, de l'enseignement supérieur et de la recherche,

Najat Vallaud-Belkacem

Le garde des sceaux, ministre de la justice,

Jean-Jacques Urvoas

Le ministre des finances et des comptes publics,

Michel Sapin

Le ministre de la défense,

Jean-Yves Le Drian

La ministre des affaires sociales, de la santé et des droits des femmes,

Marisol Touraine

La ministre du travail, de l'emploi, de la formation professionnelle et du dialogue social,

Myriam El Khomri

Le ministre de l'intérieur,

Bernard Cazeneuve

Le ministre de l'agriculture, de l'agroalimentaire et de la forêt, porte-parole du Gouvernement,

Stéphane Le Foll

Le ministre de l'économie, de l'industrie et du numérique,

Emmanuel Macron

La ministre du logement, de l'égalité des territoires et de la ruralité,

Sylvia Pinel

La ministre de la culture et de la communication,

Fleur Pellerin

Le ministre de la ville, de la jeunesse et des sports,

Patrick Kanner

La ministre des outre-mer,

George Pau-Langevin

Fiche n° 11
LES ORGANES DE LA SÉCURITÉ

Bien que l'aspect organisationnel dans la gestion de notre sécurité au quotidien soit adopté, la protection de notre information a besoin de s'appuyer sur des outils techniques qui vont nous permettre de répondre aux grands enjeux de la sécurité qui sont, la disponibilité, l'intégrité et la confidentialité.

Dans cette fiche, il sera abordé la définition des enjeux de sécurité, ainsi que des dispositifs de protection que l'on peut trouver entre le poste utilisateur et l'internet.

1. *Les enjeux de la sécurité*

La sécurité informatique est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. Il convient d'identifier les exigences fondamentales en sécurité informatique. Celles-ci caractérisent ce à quoi s'attendent les utilisateurs de systèmes informatiques en regard de la sécurité :

- Disponibilité : demande que l'information sur le système soit disponible aux personnes autorisées et au bon moment.
- Confidentialité : demande que l'information sur le système ne puisse être accédée que par les personnes autorisées.
- Intégrité : demande que l'information sur le système ne puisse être modifiée que par les personnes autorisées et habilitées.

Pour les organes nécessaires à la protection, il en existe 2 types :

- Des solutions couvrant la sécurité des accès,
- Des solutions couvrant la sécurité des contenus.

2. *Postes de travail*

Quand on évoque la sécurité d'un poste de travail, il vient naturellement à l'esprit « antivirus », outil indispensable qui ne couvre aujourd'hui qu'environ 45 % des menaces. Ci-après, sont présentés les organes à mettre en place pour protéger plus efficacement son poste.

L'antivirus

Ce dispositif repose principalement sur des bases de signature, sortes de vaccins pour ne pas laisser s'installer une maladie connue. Les virus étant apparus, il y a bien longtemps, les bases de signature sont colossales. De fait, il est fréquent de trouver des antivirus qui ne contiennent que des bases récentes, ce qui permet aux personnes mal attentionnées d'utiliser de vieux virus et ainsi passer cette barrière de protection pourtant à jour.

L'antimalware

Le malware est un type de virus doté d'une intelligence ne visant pas seulement la corruption de l'ordinateur mais également la prise de contrôle de ce dernier. Il cherche en conséquence à s'installer sur la machine, à y résider longtemps et si possible, se propager aux ordinateurs voisins ou distants.

Parmi les plus connus :

- Les vers : virus capables de se propager au travers du réseau,
- Les chevaux de troie (ou troyens) : virus qui permettent de créer une faille dans le système pour s'y introduire et y résider,
- Les spywares : logiciels espions destinés à recueillir de l'information (frappes clavier, copies d'écrans…),
- Les cryptolockers : programmes qui chiffrent le contenu des disques locaux ou réseau. Ils sont souvent accompagnés d'une demande de rançon afin que le pirate vous fournisse la clé pour déchiffrer les disques. On les appelle aussi des ransonwares.

Il existe des solutions de protection contre ces menaces. Cela se matérialise aussi bien par des logiciels à implémenter sur les postes que des dispositifs à placer au niveau du réseau.

Le pare-feu (firewall) personnel

Il a pour objectif principal de contrôler l'accès au réseau des applications installées sur l'ordinateur. Il permet de contrôler des programmes nuisibles (comme les chevaux de troie) ouvrant une brèche dans le système afin de permettre une prise en main à distance de la machine par un individu (ou un robot) à des fins malveillantes.

Ce dispositif est efficace mais nécessite des compétences pour sa gestion, notamment au niveau de la mise en place et du suivi des règles d'accès.

Le contrôle des périphériques

Le blocage des périphériques (clés USB, cartes mémoires, smartphone…) est aussi une mesure importante dans la protection du poste de travail. Les logiciels pour en assurer la gestion sont préconisés car ils permettent de ne pas tout interdire et de laisser un accès aux périphériques autorisés.
Un grand nombre de menaces étant véhiculées par ce biais, il est important de prendre cette mesure en considération même si parfois elle fait grincer des dents les utilisateurs.

Le chiffrement

Principalement utilisées sur les ordinateurs portables et les postes VIP, les solutions de chiffrement empêchent la lecture des données présentes sur le disque si la personne souhaitant y accéder ne possède pas la clé de déchiffrement. Cette solution était initialement lourde à mettre en œuvre. On la trouve aujourd'hui de façon native dans les systèmes Windows (à partir de Windows 7 Enterprise) via l'application « Bitlocker » et sur les machines elles-mêmes qui embarquent des puces Trusted Platform Module (TPM) qui est un composant matériel installé sur de nombreux ordinateurs récents.

BitLocker fournit donc une protection supplémentaire lorsqu'il est utilisé avec cette puce.

En conclusion, il est vrai que toute cette liste de composants peut s'avérer inquiétante. Mais depuis quelques années, les fournisseurs d'antivirus se sont orientés vers des solutions complètes que l'on trouve souvent sous le nom « Endpoint Security ». Elles comprennent une suite de logiciels permettant de réduire considérablement la surface d'exposition aux menaces.

Il est bon de rappeler aussi que les menaces exploitent des failles et que souvent les brèches sont béantes. Il faut alors adopter une bonne hygiène en limitant les droits d'accès aux postes (notamment les droits administrateurs), en verrouillant sa session lorsqu'on n'est pas devant son poste, en passant régulièrement les mises à jour (Windows, Adobe, Java…), et surtout en mettant un mot de passe renforcé qui ne doit être stocké que dans votre mémoire.

3. *Le réseau*

On parle souvent de la sécurité à la frontière du réseau et d'internet. En conséquence, la sécurité du réseau interne (LAN ou Intranet) est souvent négligée.

Les organes principaux des réseaux internes sont composés de commutateurs (souvent appelés switch) sur lesquels sont raccordés chacun des composants du système d'information (PC, copieurs, imprimantes, serveurs…). Il est dès lors très important d'y implémenter de la sécurité afin que ni personne, ni un équipement ne puisse s'y connecter sans avoir une autorisation. On peut implémenter des restrictions d'accès par « mac adress » qui est un identifiant matériel unique, ou bien par des protocoles d'authentification de type 802.1q. Il est important aussi de segmenter son réseau en zones (VLAN) et de contrôler les accès entre ces zones. Cette segmentation augmente la sécurité du réseau mais aussi ses performances.

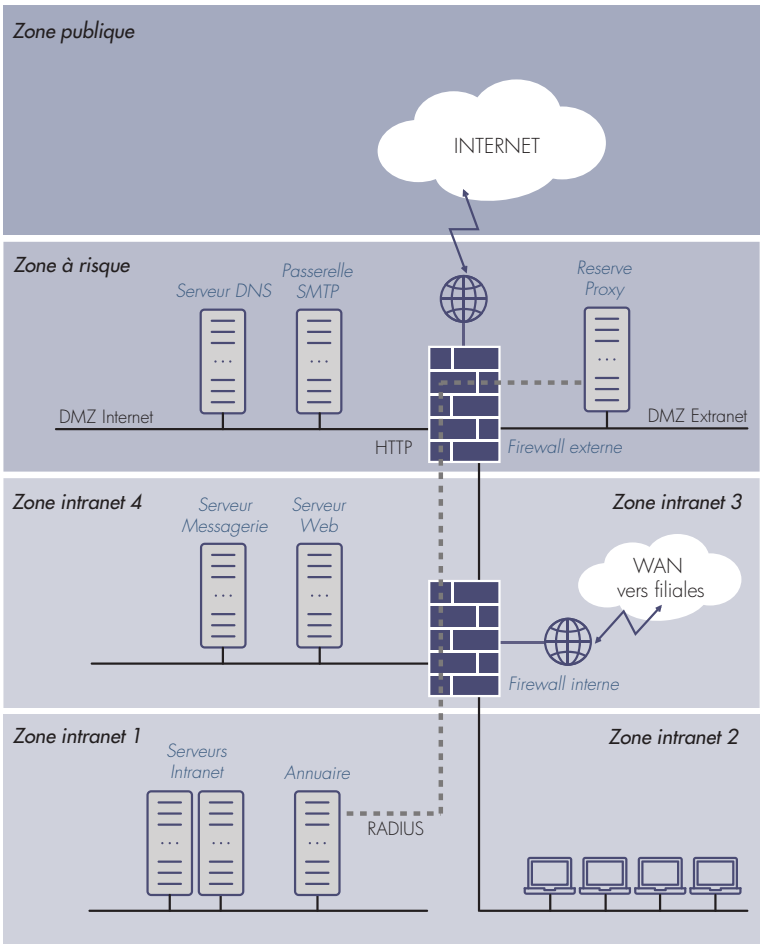
3.1. *Sécurité Internet (frontière réseau interne et réseau public)*

3.1.1. Les systèmes de pare-feu (Firewall)

C'est un système permettant de protéger le réseau interne contre les intrusions provenant d'un réseau tiers (notamment Internet). Il filtre les paquets de données échangés entre ces 2 réseaux. Il agit comme une passerelle filtrante, dans laquelle on enregistre des règles basées sur des autorisations (ou des noms autorisés) de communications entre différentes adresses (IP) via certains canaux que l'on appelle des ports comme http par exemple. Les firewalls ont évolué ces 10 dernières années vers des versions plus intelligentes visant à embarquer des fonctions supplémentaires de sécurité comme les UTM (Antivirus de flux, Proxy, Antimalware…) ou encore à appliquer des règles au niveau des utilisateurs et des applications, les « Nexgen Firewall »).

Beaucoup de flux traversent ces firewall. Aussi, afin d'accroître la protection du réseau interne, on crée sur ces pare-feux des zones démilitarisées (DMZ), que l'on utilise lorsque des machines précises du réseau doivent êtres accédées depuis l'extérieur, comme les serveurs de messagerie ou les serveurs Web. Cette zone accessible va alors servir de zone tampon dans laquelle seront analysés les flux. S'ils sont légitimes, alors seuls les firewalls seront habilités à envoyer l'information au serveur destinataire (comme par exemple le serveur de messagerie.)

Exemple d'une architecture sécurisée



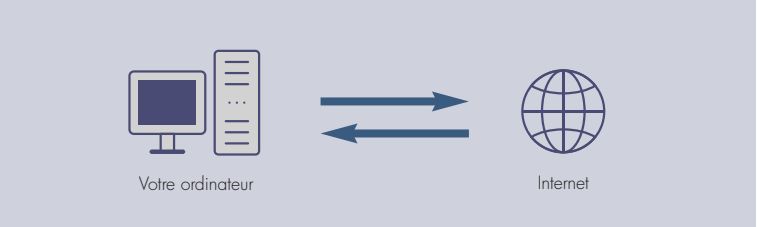
3.1.2. Les serveurs mandataires et mandataires inverses (Proxy et Reverses Proxy)

Ce sont des machines faisant fonction d'intermédiaire entre votre poste situé sur le réseau et internet. Ils sont principalement utilisés pour la navigation internet. On parle alors de proxy web ou proxy http.

Analogie

Imaginons que vous souhaitez acheter du pain, mais que vous ne voulez pas vous rendre à la boulangerie. Vous envoyez alors votre enfant remplir cette tâche. Il devient votre mandataire. Cependant, il va falloir qu'il paye pour vous, donc vous devrez lui fournir des informations confidentielles (code CB…), ce qui implique que vous ayez une grande confiance en lui pour que non seulement il remplisse sa tâche mais aussi, qu'il ne vide pas la boulangerie en achetant un kilo de bonbons. Votre enfant a en quelque sorte joué le rôle de proxy.

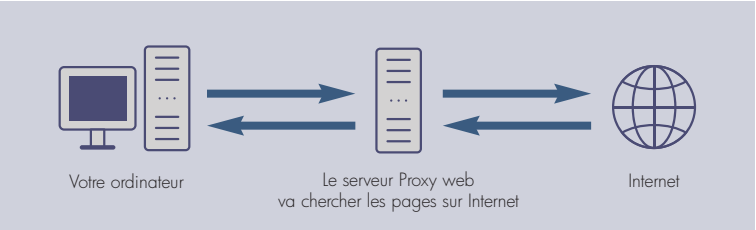
Lorsque vous surfez sur Internet, votre ordinateur est directement connecté. C'est lui qui va chercher les pages comme dans le schéma ci-dessous :



L'inconvénient principal de ce fonctionnement est que votre ordinateur est directement exposé sur Internet.

Si maintenant, on place un serveur proxy entre votre ordinateur et Internet, on obtient le schéma suivant :

→ votre ordinateur est connecté au serveur proxy,
→ et c'est lui qui est connecté à Internet.
→ vous demandez des pages à ce serveur,
→ il va chercher les pages demandées sur Internet
→ et vous renvoie les pages demandées.



Principaux avantages du Proxy

- **Le surf anonyme :** ce n'est pas votre adresse qui est vue sur les sites, mais l'adresse du proxy. Vous êtes ainsi « quasiment anonyme » ou « complètement anonyme » (voir un peu plus bas).

- **La protection de votre ordinateur :** ce n'est pas vous qui êtes en première ligne sur Internet, vous êtes donc mieux protégé.

- **Le masquage de votre lieu de connexion :** le proxy peut être dans un pays différent du vôtre. Lorsqu'il se connecte à un site, c'est la géolocalisation du proxy qui est vue, pas la vôtre. Cela peut être utile sur certains sites qui filtrent les connexions suivant les lieux d'où elles proviennent.

- **Le filtrage :** comme toutes les requêtes et les réponses passent par le proxy, il est possible de filtrer ce que l'on autorise à sortir ou à entrer. C'est le cas dans de nombreuses entreprises (nous y reviendrons plus loin).

Principaux inconvénients du Proxy

Qui dit avantages, dit également inconvénients. Comme nous l'avons vu au-dessus, c'est lui qui fait l'intermédiaire entre vous et le web. Donc il voit et peut enregistrer tout ce qui circule entre votre ordinateur et le web, et cela peut être risqué ! Imaginez juste que la personne qui gère ce serveur soit mal intentionnée. Elle a accès à l'ensemble de votre historique de navigation.

Il faut donc utiliser un proxy dont vous êtes sûr, ou alors ne pas l'utiliser : c'est-à-dire mettre des exceptions à l'utilisation de celui-ci. Sur certains sites, certains préconisent absolument d'utiliser des proxys pour être cachés, mais oublient de parler de la sécurité des données confidentielles que vous envoyez sur Internet.

Sachez cependant que vous avez une obligation de conserver les traces de connexion, et que vous devrez les fournir en cas de commission rogatoire. La mise en place de ce type d'équipement nécessite aussi une déclaration à la CNIL.

Si le serveur proxy est très sollicité, il peut éventuellement mettre plus longtemps à répondre. Donc, il est possible que le surf à travers un proxy soit un peu plus lent que le surf direct sur Internet.

Le reverse Proxy quant à lui fonctionne dans l'autre sens. Il joue le rôle d'intermédiaire entre l'internaute et une ressource que vous mettriez à sa disposition comme un site internet par exemple (portail citoyen, accès portail famille…)

Analogie

Situons-nous dans un café. Si vous souhaitez une boisson, vous n'allez pas aller directement vous servir derrière le bar, vous allez demander au garçon de café de vous apporter ce que vous désirez, et c'est ce dernier qui aura accès à la zone protégée où se trouvent les boissons et la caisse. Il agira donc en mandataire inverse (ou reverse proxy).

3.1.3. Les IDS/IPS (Intrusion Detection/Protection System)

C'est un organe basé sur un mécanisme écoutant le trafic réseau de manière furtive (non détectable) afin de repérer des activités anormales ou suspectes et permettant d'avoir une action de prévention sur les risques d'intrusion. Il fonctionne avec des bases de signatures mais aussi sur des analyses comportementales.

Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions.

Ces équipements sont assez controversés car ils ont la réputation d'être très difficiles à régler (éviter les fausses alertes) et à gérer.

3.1.4. Antispam

Idéalement placé sur une zone démilitarisée, il fonctionne comme un proxy visant à protéger la messagerie de la collectivité contre les spam (pourriels) et les virus. Certaines solutions sont aussi embarquées sur les logiciels de messagerie eux-mêmes.

La technologie anti-spam moderne couvre un large éventail de filtres, de scanners et d'autres types d'applications. Certains services anti-spam fonctionnent à partir d'une méthode statistique (signatures), tandis que d'autres utilisent des méthodes heuristiques ou des algorithmes prédictifs. Pour trier le courrier de manière sophistiquée, les fournisseurs de service anti-spam peuvent surveiller les signatures électroniques, les adresses IP (blacklist de spammer) ou autres données, ce qui réduit le spam ; idéalement à placer sur le relais SMTP en DMZ, pour une plus grande efficacité.

Conclusion

Dans cette fiche, ont été décrits les organes principaux liés à la sécurité, mais il en existe bien d'autres (WAF, SandBox…) répondant à des menaces plus précises. Autant d'organes qu'il faudra maintenir à jour pour conserver leur efficacité.

Ces dispositifs sont techniques, mais une bonne partie de la sécurité repose sur une bonne appréciation des risques et une bonne hygiène informatique. Vous pourrez trouver bon nombre de mesures organisationnelles dans le guide d'hygiène informatique publié par l'ANSSI.

http://www.ssi.gouv.fr/uploads/IMG/pdf/guide_hygiene_informatique_anssi.pdf

Sources : Blog Orange, ANSSI, Technopedia, culture informatique

3 risques de sécurité IT à gérer pour protéger les ressources des télétravailleurs sans impacter leur productivité

3 risques de sécurité IT à gérer pour protéger les ressources des télétravailleurs sans impacter leur productivité

Un marché de l'emploi tendu, la globalisation de la technologie… de nombreux facteurs continuent d'alimenter cette tendance qui veut que les effectifs soient plus mobiles, qu'ils apprécient de travailler de chez eux et soient en demande de nouvelles solutions de cybersécurité. Selon le Gartner, « d'ici à 2020, les entreprises qui adopteront la culture du 'libre choix des conditions de travail' augmenteront leur taux de rétention des salariés de plus de 10%. »

Or, si le télétravail revêt de nombreux avantages, il rend aussi la gestion de la sécurité IT bien plus complexe. Comment les entreprises peuvent-elles fournir aux télétravailleurs les outils dont ils ont besoin pour être productifs sans exposer l'entreprise à des cyber-risques démesurés ?

Trois principaux défis se posent aux organisations qui souhaitent que leurs équipes distantes demeurent productives et protégées :

1. Les salariés distants se connectent généralement aux ressources internes via un VPN directement ou en mode hébergé via des ressources cloud. Ces employés sont généralement cachés derrière leurs routeurs domestiques qui emploient des technologies de type NAT pour isoler le réseau. Toutefois, cela crée un problème de routage réseau pour les solutions traditionnelles d'administration et de sécurité IT.

Les solutions de cybersécurité d'entreprise ne peuvent pas avoir directement accès aux salariés distants pour leur adresser les mises à jour ou interroger les systèmes. Le principal défi de cybersécurité pour les salariés distants réside donc dans les terminaux qui ne sont plus routables, ni atteignables et impossibles à adresser à partir d'un réseau d'entreprise traditionnel aux fins d'analyse et de support car ils ne sont, de fait, pas sur le réseau d'entreprise traditionnel. Ceci crée une faille de la sécurité des accès à distance qui peut être initiée par les ressources IT contre l'utilisateur final.

2. Les salariés distants obéissent généralement à l'une de ces deux règles : ressources IT fournies par l'entreprise ou Bring Your Own Device (BYOD). S'il est possible de renforcer et de contrôler les ressources déployées en entreprise, les terminaux personnels sont eux souvent partagés et leur sécurité échappe à la vigilance. Les entreprises peinent à gérer les dispositifs des utilisateurs avec les solutions MDM (mobile device management) ou EMM (enterprise mobility management) et une technologie qui n'isole les applications et les données des utilisateurs que sur un appareil.

Les équipes IT ne peuvent tout simplement pas renforcer les terminaux appartenant à leurs salariés ni gouverner les opérations de ces appareils avec la même rigueur que pour un système déployé en entreprise. Si le principe BYOD n'a plus rien de nouveau, les entreprises peinent toujours à l'instaurer sans introduire de risques inutiles. La méthodologie que choisit l'entreprise doit trouver le juste équilibre entre coût, risque et facilité d'utilisation, sans réelle préférence claire à donner.

3. Le troisième défi de sécurisation des télétravailleurs concerne les contrôles fondamentaux de cybersécurité comme les évaluations de vulnérabilité, la gestion des correctifs et les antivirus. De façon traditionnelle, ces trois aspects procèdent de scanners réseau, d'agents et de services pour l'exécution des différentes fonctions et supposent une connectivité avec les serveurs sur site. Les technologies cloud facilitent la gestion de ces bases de la sécurité, mais beaucoup d'entreprises ne sont pas suffisamment matures pour les adopter au profit de leurs salariés distants. Toutefois, les entreprises ayant des effectifs distants devraient envisager le cloud. Celui-ci offre des ressources universelles, hors d'un datacenter traditionnel, auxquelles les terminaux distants peuvent se connecter en toute sécurité pour adopter des méthodologies, comme celles de géolocalisation et d'authentification bifactorielle, afin de rajouter des couches de sécurité supplémentaires.

Conseil : les bonnes pratiques de sécurité pour les effectifs distants

Les équipes IT qui doivent protéger la sécurité de leurs effectifs distants ont intérêt à continuer de s'informer sur les conditions d'acceptation des nouvelles technologies, des méthodologies et des workflows facilitant la mise en œuvre des meilleures pratiques de cybersécurité. Ceci inclut l'utilisation de solutions MDM/EMM, notamment via le cloud, et la surveillance des données et des workflows pour empêcher toute compromission.

Les équipes IT devraient innover en ce qui concerne leur approche de la connectivité. Nous vivons à l'ère du cellulaire et du haut débit, avec une évolution de la bande passante vers la 5G. Le vol de quantités massives de données peut se produire en quelques minutes au moyen de technologies sans fil ; il faut donc s'équiper de nouvelles techniques pour se prémunir contre ces menaces. Le risque émane aussi bien d'un salarié distant qui copie les données depuis les ressources internes que de cybercriminels qui compromettent le système d'un salarié distant et s'en servent comme tête de pont.

Les équipes IT doivent tenir compte des rôles qu'assument les salariés distants, ainsi que des risques correspondants pour les données et les systèmes. Ce n'est qu'ainsi que les entreprises peuvent élaborer une stratégie en faveur de la productivité de leurs équipes, tout en gérant prudemment les cyber-risques, avec la bonne combinaison de technologies et pratiques modernes de sécurité.

Quand le télétravail modifie le travail de l'encadrement

• *Par Martine Doriac*

« La relation reste une relation de travail. Elle exige, pour le manager, de passer d'une vision unidirectionnelle à celle de l'animateur de communauté, avec des liens qui se tissent dans des temporalités différentes, le manager donnant la cohésion », a souligné Alex Lepriol, consultant de Décision Publique, dans son introduction sur les enjeux managériaux du travail distant, qui bouscule les frontières des organisations.

Cinq risques, relevés par le rapport du Conseil d'analyse stratégique sur l'impact des TIC sur les relations de travail, sont pointés :

1. risque d'augmentation du rythme et de l'intensité du travail,
2. risque de surcharge informationnelle,
3. risque de renforcement du contrôle de l'activité et de réduction de l'autonomie,
4. risque d'affaiblissement des relations interprofessionnelles et/ou du collectif de travail (risque d'isolement),
5. risque de brouillage des frontières spatiales et temporelles entre le travail et le hors travail.

« Le trajet permet la déconnection entre les deux temps. L'outil numérique ne permet pas tout », soulignait Alex Lepriol qui formule plusieurs recommandations :

- organiser des temps de rencontres où les télétravailleurs sont présents, avec des temps d'échange individuel avec chacun,
- adopter une posture de confiance a priori,
- rassurer le télétravailleur sur le fait qu'il reste visible pour l'organisation et pour la poursuite de sa carrière (promotion).

Nouveau rôle des managers – Le consultant souligne l'importance de la constitution des équipes qui expérimentent le télétravail. Le rôle innovant et la présence des managers est selon lui déterminante, alors que le télétravail bouscule les frontières de l'organisation et comporte pour celui qui l'expérimente une mise en danger. « Il faut que les agents sachent immédiatement s'ils sont dans le vrai ou pas, que les indicateurs d'évaluation soient définis et perçus clairement pour éviter les situations d'inconfort », a-t-il recommandé.

Autre conseil pour constituer les équipes amenées à travailler sur des sites distants (télécentres par exemple) : leur adjoindre des « équipiers soleil » qui vont faire passer des éléments de tension, mettre de l'ambiance, apporter un confort relationnel et une efficacité dans le travail.

A Quimper, charte et contrat – Directrice générale des services de la ville et de l'agglomération de Quimper (1 600 agents), Béatrice Mérand confirme ce point de vue à partir de l'expérimentation en cours dans sa ville, fondée sur une approche environnementale des déplacements et des enjeux énergétiques.

A Quimper, le choix a été fait de proposer le télétravail, pas plus de deux jours par semaine (RTT comprises) aux agents vivant à plus de 20 km (300 concernés, 220 agents intéressés), et avec l'accord du chef de service.
« Cela interpelle les managers, car ils devront donner leur autorisation, donc avoir réfléchi à comment ils vont organiser ce télétravail dans leur service », précise Béatrice Mérand.

Le cadre a été défini par une charte de télétravail et un contrat d'engagement. Une vingtaine d'agents démarrent l'expérimentation fin 2012/début 2013. Mais tous les métiers qui requièrent une présence physique, nombreux dans une mairie, ne sont pas concernés.

Pour éviter que les frontières entre vie privée et professionnelle ne se brouillent la charte prévoit un volet « respect de la vie privée ». « Ce n'est pas parce qu'on travaille à domicile que l'on peut être joint à toute heure », remarque Béatrice Mérand. Un espace dédié, au domicile et une connexion haut-débit sont en outre exigés des volontaires. Des temps d'évaluation sont prévus avec la DRH. « Même si peu d'agents sont concernés, cela produit un effet de capillarité, l'idée que la collectivité peut innover, travailler différemment ».

8 à 10 000 km de trajets devraient ainsi être économisés. « Cela donne un autre regard sur les territoires ruraux périphériques, qui deviennent plus attractifs », souligne Béatrice Mérand.

Télétravail en télécentre dans le Cantal – Au conseil général du Cantal (1 200 agents), c'est une démarche pragmatique et progressive qui a été appliquée. « A notre grande surprise, au fur et à mesure que l'on a développé ce projet, il a soulevé tout un tas de questions organisationnelles et culturelles », décrit Pascal Rigault, directeur général adjoint ressources.
Ce département a lui aussi adopté pour ses agents le principe du volontariat et de l'accord du responsable de service, la règle des 20 Km et des 2 jours maximum, avec une phase d'expérimentation de 12, puis 18 et aujourd'hui 32 agents.
Mais les modalités diffèrent de celle de Quimper où les agents concernés télétravaillent depuis leur domicile.

Dans le Cantal, ils se rendent dans des télécentres implantés sur tout le territoire ou dans les 70 implantations du conseil général. Seuls ceux qui sont éloignés de ces lieux travaillent chez eux.
« Le gain du télétravail, ce n'est pas l'économie de mètres carrés ou de postes de travail. Tout se fait à budget constant. Le gain pour la collectivité est culturel et managérial. C'est un projet de conduite du changement à grande échelle. Et la nouveauté, c'est le fait que ce sont les agents eux mêmes qui en sont demandeurs », précise encore Pascal Rigault qui voit dans cette nouvelle modalité de travail un mouvement de fond amené à s'installer durablement.

« Quand vous pouvez économiser deux pleins d'essence par mois, si ce n'est plus, pour fournir un travail amélioré, le gain est réel », a-t-il assuré, parlant d'externalité positive difficile à quantifier, mais concrète.

Profil de télétravailleur – Pour pallier les risques pointés en introduction par Alex Lepriol, le DGA du Cantal a précisé le profil requis pour les télétravailleurs : « être autonomes, très rigoureux et cadrés dans sa tête pour s'astreindre à des horaires habituels de travail ».
Au conseil général du Cantal, chaque cas est analysé avec une fiche d'évaluation. Un bilan annuel, notamment des gains en qualité et niveau de vie dégagés, est prévu.
Les cadres aussi – Dans ces deux expérimentations, conduites en mode projet, les cadres peuvent eux aussi demander à télétravailler, en fonction de l'éloignement de leur domicile, comme pour les autres agents à Quimper, sur un à deux jours par mois dans le Cantal, pour une veille spécifique, une note à écrire ou pour prendre du recul sur un dossier.

Quant à l'évaluation de cette nouvelle méthode de travail, les participants à cette table-ronde recommandaient de ne pas oublier de questionner ceux qui ne sont pas en télétravail dans les services, pour identifier comment ils étaient impactés par les évolutions. Dans tous les cas, il est recommandé de mettre en place des indicateurs et moments d'échanges qui permettront de « capter » les efforts conduits.

CONSEIL GÉNÉRAL DE L'HÉRAULT (34)

DATE DE LANCEMENT DU PROJET « TÉLÉTRAVAIL » : JANVIER 2010

En 2013, le dispositif télétravail est en phase d'expérimentation. La généralisation du dispositif au sein de la collectivité est prévue en 2014.

CONTEXTE DE MISE EN ŒUVRE DU TÉLÉTRAVAIL

En 2009, une double réflexion est amorcée sur :

- La question des déplacements domicile-travail, dont le poids dans le bilan carbone de la collectivité a été mis en évidence dans une étude portant sur l'ensemble des activités du CG qui s'est engagé dans un Agenda 21 dès 2003.
- L'amélioration des conditions de travail des agents en limitant les conséquences en termes de stress, de fatigue et de risques d'accidents liés aux déplacements et en permettant une meilleure articulation vie privée / vie professionnelle. La réalisation d'une expérimentation de télétravail a été inscrite dans un protocole d'accord par les partenaires sociaux en 2009.

NOMBRE D'AGENTS EN TÉLÉTRAVAIL EN 2013

88 agents (100 agents en 3 ans sur 5 000 agents, soit 2 % des effectifs).

MODALITÉS DE TÉLÉTRAVAIL

1 à 2 jours par semaine au maximum (non cumulables et non reportables) à domicile.

MISE EN ŒUVRE DU PROJET

MODALITÉS DE PILOTAGE

- Un comité de pilotage stratégique composé de deux conseillers généraux (Vice-Président du CG, délégué aux ressources humaines, et le délégué aux TIC), du DGA, en charge du Pôle des Ressources, un représentant de chaque Pôle et les membres de l'équipe projet).
- Une équipe-projet opérationnelle pluridisciplinaire (RH, SI, juridique et politique) composée de cinq membres : Chargé de mission télétravail, Directeur des systèmes d'information, Chargé de projet informatique, Chef du service de l'Assemblée, Direction du département GRH-carrière).
- Chaque étape du projet est soumise à l'approbation des partenaires sociaux et des décideurs (groupe de direction et élus).

MODALITÉS DE DÉPLOIEMENT

Phase préparatoire (2009)	Mission préparatoire par une équipe-projet pour identifier les modalités de l'expérimentation (DSI-DRH) : examen des contraintes et des retours d'expérience.
Phase expérimentale (2010 – 2013)	• 2010 : Expérimentation auprès d'un échantillon de 20 agents ; • 2011 - 2013 : – Élargissement à une centaine d'agents (appel général à candidature) ; – Prolongation de l'expérimentation pendant un an pour consolider l'évaluation (aucune nouvelle candidature) ; • Bilan et évaluation globale de l'expérimentation.
Phase de déploiement	**Prévue en 2014**

CARACTÉRISTIQUES DU DISPOSITIF

CRITÈRES D'ÉLIGIBILITÉ À L'EXPÉRIMENTATION

1) critère d'éloignement géographique du domicile (25 km) ;

2) critère de faisabilité technique : couverture ADSL du domicile et accès distant aux logiciels métiers en fonction des logiciels utilisés par les agents ;

3) critère d'appréciation des managers : compatibilité du poste/continuité de service et savoir-être (autonomie, capacité à s'organiser, à communiquer) ;

4) critère de « situation de handicap » (ajouté en 2011).

ÉQUIPEMENT TECHNIQUE

- un système de connexion à distance pour un accès sécurisé au réseau du CG ;
- installation d'un poste de travail fixe à domicile : terminal client léger sans disque dur donnant accès aux applications standards (suite bureautique, messagerie) et applications métiers accessibles à distance ;
- une solution de téléphonie ;
- l'installation d'une ligne ADSL supplémentaire était prise en charge en première phase d'expérimentation. Cette solution a été ensuite abandonnée au profit de l'utilisation de l'ADSL résidentielle ;
- infrastructures : pare-feu avec un portail VPN SSL extranet et serveur terminal. L'accès distant s'appuie sur la technologie client-léger (TSE) permettant une exécution des programmes et une centralisation des données directement sur les serveurs.

OUTILS D'ACCOMPAGNEMENT DU DISPOSITIF

- une charte du télétravail qui précise les principes et les modalités d'exercice de l'expérimentation ;
- une fiche de candidature (faisabilité technique, avis et visas hiérarchiques) ;
- une convention tripartite (CG-encadrant-télétravailleur) de 24 mois qui précise les jours télétravaillés, le lieu de télétravail, les horaires de travail (entre 8 et 18 h) et les plages de disponibilité du télétravailleur ;
- un guide de l'expérimentation du travail à domicile à destination des agents et des managers ;
- une fiche de liaison managériale pour formaliser le suivi des tâches à accomplir en télétravail et les résultats à atteindre (activité, résultat attendu, échéance, résultat constaté, gains/difficultés liés au télétravail, observations du manager et du télétravailleur) ;
- une fiche « process » qui récapitule le « qui fait quoi » dans la mise en œuvre ;
- une formation spécifique à l'utilisation du matériel informatique sur site ou à domicile si besoin est et une visite chez le médecin de prévention.

SPÉCIFICITÉS

- intégration depuis 2011 d'un dispositif de télétravail ouvert aux encadrants plus souple (sous la forme d'un forfait mensuel de 4 jours non cumulables et non reportables de mois en mois) ;
- partenariat avec le CG du Gard pour un projet de télécentres partagés pour leurs agents à partir de l'automne 2013.

ÉVOLUTIONS DU DISPOSITIF

- à l'origine, seul le mardi et le jeudi étaient autorisés pour le télétravail. Cette obligation a été abandonnée puisque ces deux jours constituaient les seuls où les équipes pouvaient être physiquement au complet (RTT, temps partiels...) ;
- aujourd'hui, le critère kilométrique ne semble pas forcément pertinent compte tenu des difficultés de circulation en proximité et à l'intérieur de l'agglomération de Montpellier. Une réflexion est actuellement conduite pour mieux intégrer le « temps de trajet » dans l'appréciation de l'éloignement.

FICHE ACTION N°5 : CONDITIONS TECHNIQUES ET FINANCIÈRES DE MISE EN ŒUVRE

LES PRATIQUES LES PLUS FRÉQUENTES

Pré-requis techniques et juridiques

- une connexion internet à domicile dont le débit est au moins égal à 1 Mo/s ;
- un espace spécifique aménagé pour télétravailler confortablement ;
- l'accessibilité des applications métiers et de la documentation nécessaire aux activités en télétravail ;
- une déclaration faite par l'agent à son assureur de sa situation de télétravailleur ;
- la signature d'une convention de télétravail.

Accompagnement financier

- aucune prime n'est versée au télétravailleur pour qui les éventuels coûts liés au télétravail sont compensés par les gains réalisés sur les coûts de transport ;
- l'éventuelle sur-prime de l'assurance personnelle liée au télétravail est à la charge de l'agent ;
- à titre indicatif, le coût d'investissement estimé par certaines collectivités s'élève à 1 000 - 1 500 € / télétravailleur la première année, puis à 100 - 150 € /télétravailleur à partir de la seconde année.

Équipement proposé

- un ordinateur portable, parfois « recyclé » (vieux ordinateurs portables qui ne sont plus utilisés par les agents « nomades ») ;
- généralement pas de téléphone portable mais un transfert d'appel sur la ligne de l'agent ;
- la connexion Internet utilisée est généralement celle de l'agent.

LES VARIANTES ET BONNES IDÉES À RETENIR

- Un contrôle de la conformité électrique du domicile peut être réalisé. Pour éviter la visite sur le lieu de travail, des vérifications peuvent être réalisées d'après des photos fournies par l'agent.
- Un appui-conseil en ergonomie à disposition du télétravailleur auprès de ressources internes spécialisées dans la prévention des risques professionnels.
- Dans certains cas, l'allocation d'une prime (de l'ordre de 100 €) peut être octroyée au lancement pour la mise en place du télétravail ou alors de façon forfaitaire et mensuelle.
- Certains équipements nécessaires aux métiers peuvent être pris en charge (grand écran, scanner, etc.).
- Des applications de communication pour fluidifier les échanges à distance sont prioritairement déployées auprès des agents en télétravail (messagerie instantanée, webconférence, etc.).
- La virtualisation des postes (via la technologie « terminal serveur ») représente un avantage en matière de sécurisation des données, y compris avec l'utilisation de matériel personnel.

LES ENJEUX ET LES QUESTIONS À SE POSER

Quand les trajets sont souvent faits avec les véhicules personnels des agents, les économies réalisées dans le cadre du télétravail peuvent constituer un facteur de motivation important. Il ne doit pas suffire à justifier sa mise en œuvre, ni épargner une réflexion sur la compatibilité du métier avec le télétravail et les aptitudes de l'agent pour télétravailler. Cette dimension financière n'étant pas toujours abordée de manière transparente, elle peut introduire un biais dans l'analyse, en amont de la situation. Le fait de ne pas proposer d'accompagnement financier important évite également de renforcer ce biais.

la gazette.fr

FICHE PRATIQUE

Sécuriser l'accès aux systèmes d'information de la collectivité depuis les mobiles personnels

Auteur associé | Fiches pratiques techniques | Publié le 05/10/2015

L'utilisation des appareils personnels sur le lieu de travail, contribue à une prolifération de plus en plus complexe des périphériques dans les entreprises et les collectivités. La frontière entre usage professionnel et privé devient de plus en plus floue, créant un environnement de gestion et de contrôle difficile pour les directions ou directeurs des systèmes d'information (DSI). Le DSI doit ainsi trouver le bon équilibre pour permettre l'utilisation du terminal personnel dans l'environnement professionnel sans pour autant sacrifier la sécurité.

[1]L'un des aspects fondamentaux du Byod (de l'anglais « bring your own device », qui signifie apporter son propre terminal à la place de celui fourni par l'employeur), est que les utilisateurs peuvent choisir eux-mêmes le périphérique qu'ils souhaitent utiliser pour accéder au système d'information professionnel.

Dans ce domaine, il n'y a pas de normalisation, et même si 80 % du marché des mobiles est aujourd'hui dominé par Androïd, la diversité des plateformes mobiles existantes (IOS, Blackberry, Windows Phone…) pose problème aux équipes informatiques souvent en manque de ressources. C'est pour cette raison que de nombreuses directions de l'informatique et des services d'information (DSI [2]), envisagent l'acquisition d'une solution de gestion des terminaux mobiles (ou MDM [3], pour Mobile Device Management), pour les aider à faire face au Byod.

Il est à noter que bien souvent, les collectivités disposant déjà d'une flotte de mobiles d'entreprise importante possèdent déjà une solution de MDM. Il s'agit dans ce cas de valider que cette dernière permet aussi la gestion des terminaux personnels.

Fonctions de sécurité et ouverture du SI aux terminaux mobiles

L'ouverture du système d'information (SI) aux appareils mobiles impose un changement « radical » d'approche de la sécurité.

Autrefois, il suffisait de protéger le périmètre du système d'information à l'aide d'un pare-feu (firewall), puis

de s'assurer d'avoir en place les dispositifs de sécurité adaptés à chaque point d'extrémité à l'intérieur de ce périmètre. Aujourd'hui, la sécurité n'est plus aussi simple. L'accès des appareils mobiles au système d'information a considérablement changé les règles du jeu, et peut créer quelques failles sur le plan de la sécurité. En réalité, une partie du périmètre de sécurité est toujours autour de l'entreprise, mais une autre partie se situe autour de chaque utilisateur et comme chacun sait, la gestion des utilisateurs est le problème le plus complexe de la sécurité.

Il existe une frontière invisible autour de chacun des utilisateurs mobiles et celle-ci doit être sécurisée.

L'ajout d'un nouveau type de point d'extrémité au réseau de l'entreprise peut potentiellement alourdir la charge de travail de la DSI, en particulier en matière de sécurité. La technologie mobile s'accompagne de son lot de défis. Et si on associe ces menaces à la nature dispersée du périmètre de sécurité de l'entreprise, la situation devient plus inquiétante encore. Heureusement, il existe aujourd'hui un grand nombre de solutions pouvant aider à défendre les appareils, les données et les systèmes d'information si l'on est conscient des risques encourus.

Mobile Device Management (MDM)

Les solutions de MDM permettent aux DSI d'étendre leurs politiques de sécurité traditionnelles à tous les périphériques, notamment les smartphones et les tablettes quel que soit le lieu où ils se trouvent. Le DSI peut ainsi automatiser à moindre coût des tâches de gestion et de surveillance, notamment la configuration des périphériques, les mises à jour logicielles ou la sauvegarde et la restauration de données, et ce, tout en assurant la sécurité des données sensibles de l'entreprise en cas de vol, de perte ou d'utilisation abusive.

Application de la conformité et des politiques de sécurité

L'objectif d'une solution de MDM est de protéger les données de la collectivité en faisant appliquer les politiques de sécurité prédéfinies. Pour cela, des contrôles réguliers doivent veiller à ce que seuls les terminaux enregistrés et conformes puissent accéder aux données.

Certes, cela peut représenter des contraintes pour l'utilisateur, mais ce dernier doit comprendre que l'accès aux données professionnelles depuis un appareil mobile personnel implique l'acceptation totale de la stratégie de sécurité mobile définie par la collectivité. Chaque périphérique doit être enregistré dans le système pour pouvoir accéder aux données. Lorsque le terminal se connecte, le système MDM vérifie sa conformité (appareil jailbreaké [Le jailbreak, également appelé débridage, déverrouillage, ou déplombage est un processus permettant aux appareils tournant sous un système mobile d'obtenir un accès complet pour déverrouiller toutes les fonctionnalités du système d'exploitation, éliminant ainsi les restrictions et sécurités posées par les constructeurs. Une fois l'OS débridé, ses utilisateurs sont en mesure de télécharger d'autres applications, des extensions ainsi que des thèmes qui ne sont pas proposés sur la boutique d'application officielle des constructeurs], configuration du mot de passe, applications interdites, etc.).

Limitation des risques

Une solution de MDM doit servir à mettre en place des mesures d'atténuation des risques, et renforcer l'application de la politique de sécurité en matière de mobilité. Les sanctions peuvent être adaptées à la gravité de la violation. Dans les cas mineurs, une simple notification à l'utilisation peut suffire. D'autres cas méritent le blocage de l'accès aux données et aux applications.

Sécurité des données et du contenu

Une solution de MDM a pour but de permettre la protection et l'administration centralisée des périphériques mobiles de manière à protéger les données stockées sur les appareils, ainsi que celles auxquelles ceux-ci ont accès.

De nombreux systèmes d'exploitation mobiles sont dotés de fonctionnalités de sécurités intégrées telles que des restrictions, comme la désactivation de l'appareil photo par exemple. RIM, avec son Blackberry, fut le précurseur dans ce domaine avec son serveur BES (Blackberry Enterprise Server) et ses quelque 150 règles de sécurité. La solution de MDM doit aider à contrôler un grand nombre de fonctions de l'appareil afin de protéger les données.

La plupart des solutions de MDM comprennent une fonction d'effacement [5] à distance, d'importance capitale pour la sécurité des données. Elle offre la possibilité à l'administrateur de procéder à la localisation, au verrouillage et à la suppression des données contenues sur un périphérique en cas de problème.

En plus de protéger les données contenues sur les périphériques, la DSI doit connaître les manières dont les utilisateurs accèdent, transfèrent et collaborent avec les données professionnelles. Comment partagent-ils les données ? Par courriel ? Sur des sites d'échanges hébergés dans le Cloud [6] ?

Pour empêcher la fuite des données, il est nécessaire de chiffrer les données à tout moment et de protéger les périphériques contre les malwares [Logiciel programmé pour nuire à un système informatique sans le consentement de l'utilisateur]. Par sécurité, le chiffrement des données doit se faire avant le transfert vers le site d'échange dans le Cloud.

Protection Web

Le Web constitue actuellement le vecteur principal d'infection. Il est donc conseillé de s'équiper d'une sécurité mobile avec protection web, principalement pour les utilisateurs des terminaux sous Androïd. En effet, s'agissant du système d'exploitation le plus répandu, il est donc particulièrement attaqué.

Contrôle d'accès au réseau

Afin de réduire le risque de fuites de données, la solution MDM doit surveiller en permanence l'état des mobiles et l'accès au réseau. Elle doit détecter les jailbreaks, les applications sur liste noire ou les mauvais paramétrages, évaluer l'état de l'appareil, et travailler avec les éditeurs de sécurité réseau pour refuser l'accès au Wifi et/ou au VPN en cas de non-conformité d'un appareil.

Administration: un point crucial de la solution de MDM

Avec autant de périphériques différents à gérer, il est impératif de trouver une solution simple qui permette de maintenir la productivité tout en réduisant le travail des DSI.

Portail d'auto-assistance

Le portail d'auto-assistance (libre-service) réduit la charge de travail informatique et autorise les utilisateurs à effectuer de nombreuses tâches courantes eux-mêmes. Après tout, ils sont les premiers à savoir s'ils ont acheté un nouvel appareil et souhaitent l'utiliser pour le travail, ou si un appareil a été perdu ou volé. Le portail libre-service doit fournir un processus simple par étapes pour les tâches courantes : enregistrer leurs propres appareils et accepter la politique de mobilité de l'entreprise, consulter l'état de conformité de leurs appareils, localiser, verrouiller ou effacer leurs appareils et réinitialiser leur mot de passe à distance.

Configuration et maintenance

Il est important également d'évaluer la facilité d'installation, de configuration et de maintenance. Un système avec installation et configuration « over-the-air » (sans connexion physique au terminal), depuis une console Web, peut accélérer le déploiement et réduire la charge de travail.

Voici une liste des critères importants à vérifier pour évaluer la simplicité de configuration, de gestion et de maintenance de la solution MDM :

- le système peut-il assigner automatiquement des profils et des politiques à des utilisateurs ou des groupes en fonction de leur appartenance à un groupe de l'annuaire d'entreprise?
- est-ce que la solution MDM peut automatiquement rendre un appareil compatible et contrôler si un utilisateur est autorisé à accéder ou à recevoir des courriels d'entreprise?
- est-il possible de configurer tous les appareils indifféremment du système d'exploitation (IOS, Androïd et Samsung, Windows Phone) directement dans le système MDM? Ou faut-il utiliser un utilitaire de configuration séparé?
- le workflow [7] (la suite des tâches à effectuer) est-il optimisé, et avec quelle facilité est-il possible de trouver les données nécessaires pour gérer les appareils et les politiques?
- est-il possible de gérer les mobiles à tout moment, de n'importe où? (Console d'administration de type web.)

Options de déploiement

Les solutions MDM de la majorité des éditeurs peuvent se déployer de deux manières différentes, sur site on parle aussi de « On-Premises » ou en mode hébergé ou « SaaS [8] ».

Sur site, le logiciel est installé et géré par la DSI sur les serveurs en local. Au niveau sécuritaire, cette option permet de stocker toutes les données en interne.

SaaS est une solution qui permet d'effectuer toutes les tâches d'administration via une console web, sans besoin d'installer ou de mettre à jour de logiciel. Elle est installée dans le Cloud et toute l'infrastructure est gérée et administrée par un prestataire externe.

Ce point est très important à prendre en considération dans la réflexion globale de mise en place du MDM. Généralement, il dépend des politiques mises en place au sein des DSI.

Utilisation du MDM pour la gestion du Byod

Il est évident que les solutions MDM proposées par les différents acteurs du marché ne sont pas équivalentes puisqu'elles n'offrent pas toutes les mêmes fonctionnalités pour les mêmes terminaux et OS avec le même niveau de sécurité (lire encadré ci-contre).

Les terminaux Byod sont par définition la propriété de l'utilisateur et sont utilisés pour son activité personnelle. Ces terminaux ne sont donc pas connus de l'entreprise et ne sont pas sous son contrôle. Cette situation implique un certain nombre de menaces réelles pour les DSI et représente un frein à leur développement en France.

Ces menaces sont dues principalement au fait que le terminal Byod ne soit pas connu du système de gestion des mobiles de la DSI. En effet, pour que la DSI puisse contrôler la sécurité d'un terminal mobile (professionnel ou personnel), l'installation d'un agent MDM de type lourd ou léger (lire focus) sur le terminal pour assurer son enrôlement dans le système de gestion est nécessaire. Cet enrôlement assurera par la suite

à la DSI, la maîtrise du niveau de sécurité des terminaux gérés. Ces fonctions de contrôle de la sécurité ne sont pas optionnelles pour les DSI quand il s'agit de donner accès aux données et applications professionnelles. Face au besoin réel des utilisateurs du Byod, la définition d'une politique adaptée dans l'entreprise est primordiale.

La séparation du monde personnel et professionnel dans l'usage des terminaux en mode Byod est une exigence aussi bien du côté des utilisateurs (qui souhaitent conserver une vie « privée »), que pour la DSI qui doit éviter la fuite des données de l'entreprise. Cette approche de séparation des usages, personnel et professionnel, existe chez les principaux éditeurs de MDM. La création de l'étanchéité entre les deux environnements, personnel et professionnel, est assurée par la création de « container ». Après l'enregistrement dans le MDM, le terminal possède un environnement professionnel sécurisé et contrôlé par le container du MDM et un environnement personnel, libre d'utilisation complètement séparé et totalement étanche au précédent.

Les offres autour de ce principe se sont beaucoup développées et ont gagné en maturité : BlackBerry fut encore une fois le précurseur avec son système Balance, puis Samsung avec Knox, Devide racheté par Google, Workspace d'Airwatch VMware, Good, Citrix, etc.

Principales solutions MDM du marché (Source: Ibelem)

- Airwatch, une des solutions leaders à l'international, est appréciée pour la richesse de ses fonctionnalités et sa gestion de sociétés en environnement multisite.
- BlackBerry enterprise service 12, s'inscrivant dans la continuité du BlackBerry enterprise server, cette solution s'adresse prioritairement aux sociétés équipées d'un BES et d'une flotte majoritairement BlackBerry.
- Good for enterprise, très axé sur les fonctionnalités de sécurité, permet, au travers d'un véritable container, de scinder parfaitement les univers personnel et professionnel.
- MobileIron est une des solutions les plus adoptées dans le monde. Elle convient, plus particulièrement, aux sociétés qui souhaitent intégrer la solution en mode « appliance ».
- PushManager est une solution française éditée par ARIANN Software et équipe déjà de nombreuses entreprises. De par sa simplicité d'utilisation, son efficacité, la proximité de ses équipes (R&D et support basés en France), PushManager séduit plus particulièrement les sociétés du haut de marché et les collectivités locales.
- Samsung Knox renforce la sécurité des terminaux Samsung. Cette plateforme de sécurité mobile fonctionne comme un véritable container permettant de séparer de manière totalement hermétique les univers personnel et professionnel. Aujourd'hui, cette solution est complètement intégrée avec la solution de Blackberry.
- Teopad est une solution innovante de sécurisation des applications professionnelles pour smartphones et tablettes issue de technologies brevetées par Thales.
- Windows Intune permet de gérer avec une interface unique terminaux fixes et mobiles. Elle intéresse, plus particulièrement, les clients équipés de SCCM 2012 et Office 365.
- XenMobile est une solution très complète parfaitement adaptée pour les grandes entreprises ayant déjà choisie les produits Citrix concernant la virtualisation de leurs postes de travail ou de leurs serveurs. XenMobile offre un large choix de fonctionnalités modulables.

Les solutions MDM Open source

Le monde du libre a aussi quelques solutions de MDM. Elles restent cependant à ce jour très confidentielles et leur avenir est relativement incertain. Les trois solutions les plus connues sont: Talend Open MDM, Java CAPS Sun MDM Suite et OpenMDM.

Conclusion

La réalité du Byod est que les utilisateurs finaux sont prêts à renoncer à un certain niveau de contrôle de leurs mobiles personnels afin de gagner en souplesse, efficacité et productivité. En même temps, les DSI ont besoin de maintenir un niveau de contrôle pour gérer correctement le Byod et assurer la sécurité. Cela passe par exemple par la capacité à appliquer la politique de sécurité de l'entreprise, la visibilité sur les appareils qui se connectent au réseau de l'entreprise et sur les applications qui sont installées sur l'appareil, et la façon dont le contenu est accessible et partagé.

La protection des données ne s'arrête pas à la porte de la collectivité. Le chiffrement des mobiles mis en place permet de s'assurer que chaque document reste sécurisé tout en permettant aux utilisateurs de rester productifs et de collaborer en toute sécurité.

Types de MDM : approche légère vs approche lourde

Presque toutes les solutions de MDM du marché couvrent la sécurité, la gestion des périphériques et des applications et les problèmes de conformité. Cependant, on peut identifier deux types d'approches : légère ou lourde.

- Approche légère

Les éditeurs ayant choisi l'approche légère complémentent les fonctionnalités natives du périphérique. Dans ce cas, les fonctionnalités peuvent varier selon le système d'exploitation. L'avantage est que « l'agent » utilisé par l'éditeur fournit une expérience utilisateur « native ».

D'autre part, il faut noter que les fabricants de mobiles et les développeurs de systèmes d'exploitation innovent à une vitesse fulgurante. Les derniers modèles de périphériques mobiles offrent bien plus de fonctionnalités de sécurité que les prédécesseurs. Si le choix se porte sur une approche légère, il est fort probable que de nouvelles fonctionnalités apparaissent lors de chaque mise à jour. Dans ce cadre, le choix d'un éditeur « réactif », capable d'évoluer en synergie avec les périphériques et les versions des systèmes d'exploitation, est primordial.

- Approche lourde

L'approche lourde utilise la solution de « conteneur » pour isoler les applications qui accèdent aux données professionnelles depuis d'autres applications.

La messagerie, le calendrier et les contacts étant les applications mobiles les plus populaires, la plupart des fournisseurs d'applications de conteneur se concentrent principalement sur la séparation du client de messagerie, du calendrier et du carnet d'adresses.

Le choix entre ces deux approches est une question d'équilibre entre le niveau de risques que l'on considère comme acceptable et l'expérience utilisateur. L'approche conteneur est plus sécurisée mais plus contraignante pour l'utilisateur. L'interface de l'application « conteneurisée » n'est pas toujours très aboutie, et nécessite un apprentissage supplémentaire pour l'utilisateur. En revanche, le niveau de sécurité est supérieur.

ANNEXE 1

Présentation de la Communauté d'Agglomération d'INGECO – *INGECO* – 2019

La communauté d'agglomération d'INGECO a été créée en 1996.

L'EPCI s'étend sur un territoire de 25 communes mutualisées représentant 75 000 habitants.

Au gré des prises de compétences la collectivité doit recruter des agents possédant des expertises spécifiques, peu présentes sur le territoire. En conséquence, les demandes de télétravail sont de plus en plus nombreuses. Par la mise en œuvre du télétravail, INGECO souhaite notamment fidéliser ses ressources humaines.

Organisation de la Collectivité :

Les services de la collectivité sont divisés en différents Pôles, tous rattachés hiérarchiquement au Directeur Général des Services :

- Pôle Moyens composé de la DSI, DRH, Direction Finances (incluant le service marchés publics) et Juridique,
- Pôle Services à la Population intégrant les Services Petite Enfance
- Pôle Services Techniques : associant les services collectes, bâtiment, voirie et déchèteries,
- Pôle Développement Economique

Description du Système d'Information :

Le réseau local est composé de 350 postes clients et 5 serveurs physiques dont une baie de disques, hébergeant 10 serveurs virtuels : gestion financière, gestion ressources humaines et les divers applicatifs métiers permettant la gestion des compétences portées par la collectivité : environnement et collecte des ordures ménagères, développement économique, SIG, gestion des billetteries dans les structures sportives comme les piscines et culturelles comme le théâtre ...

Un intranet collaboratif a été développé en 2007 et s'est enrichi avec les années de plusieurs outils collaboratifs dématérialisés : forum, demande de congés en ligne, réservation de ressources, gestion des tickets à la DSI.

Le parc informatique est renouvelé tous les 5 ans. Il est en 2019 composé de 70 % de postes fixes et 30 % de PC portables.

Une charte informatique a été établie et communiquée aux agents à l'ouverture du réseau local à Internet en 1997. Celle-ci est méconnue des agents et n'a pas fait l'objet d'une révision depuis.

Développement de la mobilité des agents :

Si le télétravail n'a pas encore été développé, le SI s'est en partie ouvert et adapté à certaines demandes des agents et exigences de fonctionnement de la collectivité.

En effet, la collectivité dispose notamment de la compétence petite enfance : gestion des multi-accueils et relais assistantes maternelles et organise des permanences dans des lieux délocalisés. Il s'agit la plupart du temps de bureaux mis à disposition par les communes permettant d'accueillir les familles sur l'ensemble du territoire.

L'agent du service petite enfance doit alors pouvoir bénéficier des ressources informatiques afin d'exercer ses missions : logiciels et données.

Le SI s'est doté de connexions VPN permettant à ces agents de se connecter de manière sécurisée au SI d'INGECO.

Les services techniques qui œuvrent sur l'ensemble du territoire bénéficient de tablettes renforcées permettant de télécharger les anomalies terrains et mettre à jour les interventions réalisées.

Le nombre de tablettes mis à disposition des agents est trop réduit pour justifier l'acquisition au niveau de la DSI d'une plate-forme de MDM pour l'instant.