MINISTÈRE
DE L'EUROPE
ET DES AFFAIRES
ÉTRANGÈRES
Liberté
Égalité
Fraternité

DIRECTION GENERALE DE L'ADMINISTRATION
ET DE LA MODERNISATION
———
DIRECTION DES RESSOURCES HUMAINES
———
Sous-direction de la Formation et des Concours
———
Bureau des concours et examens professionnels
RH4B

CONCOURS INTERNE ET EXTERNE POUR L'ACCES A L'EMPLOI D'ATTACHE DES SYSTEMES D'INFORMATION ET DE COMMUNICATION AU TITRE DE L'ANNEE 2021

EPREUVES ECRITES D'ADMISSIBILITE – 29-30 SEPTEMBRE 2021

NOTE DE SYNTHESE

Note de synthèse, établie à partir d'un dossier à caractère scientifique et technique de quarante pages maximum permettant de vérifier les qualités d'expression, d'analyse et de synthèse du candidat dans les domaines scientifiques et techniques, ainsi que son aptitude à dégager des conclusions et à formuler des propositions.

Durée : 3 heures
Coefficient : 2
Toute note inférieure à 6 sur 20 est éliminatoire.

SUJET

Voir au verso.

Ce dossier comporte 25 pages + un sommaire (page de garde non comprise).

SUJET

La crise sanitaire a provoqué l'explosion du télétravail, posant de nombreux défis aux responsables des systèmes d'information des entreprises et des administrations.

A la demande du directeur du numérique du ministère de l'Europe et des Affaires étrangères, vous rédigerez, sur la base du dossier joint, une note faisant le point sur ces enjeux. En conclusion, vous êtes invité(e) à formuler pour le Ministère de l'Europe et des Affaires étrangères, certaines propositions que vous jugerez pertinentes.

Avertissement : La note doit pouvoir être intelligible pour une personne non spécialiste du domaine numérique. Vous veillerez également à structurer au mieux votre copie. Enfin, toute recopie, même partielle, des textes du dossier sera sanctionnée.

SOMMAIRE (25 pages)

Bulletin d'actualité CERTFR-2020-ACT-002 – 18 mars 2020

TÉLÉ-TRAVAIL : PROTÉGEZ VOS SYSTÈMES D'INFORMATION

CONTEXTE

Pour faire face à la crise sanitaire actuelle, le gouvernement demande à tous de télétravailler dès lors que cela est possible. La mise en œuvre de cette mesure nécessite pour beaucoup d'employeurs de mettre en œuvre ou de renforcer des moyens de télétravail dans l'urgence.

Ces moyens d'accès à distance augmentent l'exposition des systèmes d'information (SI) sur Internet, dans un contexte où les risques pour leur sécurité sont très élevés (cf. [1] et [2] notamment) avec les découvertes récentes de vulnérabilités critiques touchant certaines de ces solutions (cf. [3], [4], [5], [6], [7] et [8] par exemple).

Enfin, un grand nombre de fraudes se développent qui peuvent notamment affecter les personnes en situation de télétravail. Il est nécessaire de sensibiliser ses équipes à ces risques qui peuvent les affecter à titre professionnel, mais également personnel[9].

SYSTÈMES AFFECTÉS

Tout système d'information (SI), qu'il s'agisse d'un SI interne ou d'un SI hébergé en nuage (*Cloud* public ou privé) disposant d'une solution d'accès à distance en mode 'nomadisme'.

RECOMMANDATIONS

Les objectifs de ce bulletin sont de rappeler les bonnes pratiques à respecter pour limiter les risques pour la sécurité des systèmes d'information et d'expliciter les comportements à bannir.

Compte tenu de l'actualité, il est important de n'**exposer sous aucun prétexte sur Internet** les interfaces web de serveurs ***Microsoft Exchange*** qui ne sont pas au dernier niveau de correctif. Comme explicité dans le dernier bulletin d'alerte associé [3], les codes d'exploitation sont publics et des attaques sont en cours en ce moment même. Il est également important de ne pas donner un accès à vos serveurs de partage de fichiers via le protocole SMB [4].

De manière générale, si vous exposez ou devez impérativement exposer de nouveaux services sur Internet, **mettez-les à jour au plus vite** avec les derniers correctifs de sécurité et activez les mécanismes de journalisation. Dans la mesure du possible, activez l'authentification double facteur.

Pour conclure, les bonnes pratiques suivantes contribuent à limiter les risques pour les systèmes d'information :

- Appliquer les correctifs de sécurité rapidement, notamment sur les équipements et logiciels exposés sur Internet (solution VPN, solution de bureau distant, solution de messagerie, etc.) ;
- Effectuer des sauvegardes hors ligne pour vos systèmes critiques ;
- Utiliser une solution d'accès de type VPN (*Virtual Private Network*, réseau privé virtuel) propre à l'entreprise, idéalement IPsec ou TLS à défaut, pour ne pas exposer les applications directement sur Internet ;
- Mettre en œuvre des mécanismes d'authentification à double facteur pour limiter les risques d'usurpation d'identité (VPN et applications accessibles) ;
- Consulter régulièrement les journaux d'accès aux solutions exposées sur Internet pour détecter des comportements suspects.

Le bulletin du CERT-FR [10] référence notamment le guide nomadisme [11].

DOCUMENTATION

- [1] https://www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-002/
- [2] https://www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-001/
- [3] correctif de sécurité pour Microsoft Exchange : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2020-ALE-007/
- [4] correctif de sécurité pour le protocole de partage de fichier SMB de Microsoft : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2020-ALE-008/
- [5] correctif de sécurité pour Remote Desktop Gateway : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2020-ALE-005/
- [6] correctif de sécurité pour Citrix Gateway et Citrix ADC : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2020-ALE-002/
- [7] correctif de sécurité pour Microsoft Sharepoint : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2019-ALE-008/
- [8] correctif de sécurité pour les VPN : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2020-ALE-001/ et https://www.cert.ssi.gouv.fr/actualite/CERTFR-2019-ACT-008/
- [9] https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/coronavirus-covid-19-vigilance-cybersecurite
- [10] https://www.cert.ssi.gouv.fr/actualite/CERTFR-2020-ACT-001/
- [11] https://www.ssi.gouv.fr/nomadisme-numerique

RAPPEL DES AVIS ÉMIS

Dans la période du 09 au 15 mars 2020, le CERT-FR a émis les publications suivantes :

- CERTFR-2020-ALE-008 : Vulnérabilité dans l'implémentation du protocole SMB par Microsoft
- CERTFR-2020-AVI-131 : Multiples vulnérabilités dans Google Chrome OS
- CERTFR-2020-AVI-132 : [SCADA] Multiples vulnérabilités dans les produits Siemens
- CERTFR-2020-AVI-133 : Multiples vulnérabilités dans Microsoft IE

- CERTFR-2020-AVI-134 : Multiples vulnérabilités dans Microsoft Edge
- CERTFR-2020-AVI-135 : Multiples vulnérabilités dans Microsoft Office
- CERTFR-2020-AVI-136 : Multiples vulnérabilités dans Microsoft Windows
- CERTFR-2020-AVI-137 : Multiples vulnérabilités dans les produits Microsoft
- CERTFR-2020-AVI-138 : Multiples vulnérabilités dans Mozilla Firefox
- CERTFR-2020-AVI-139 : Multiples vulnérabilités dans les produits Intel
- CERTFR-2020-AVI-140 : Multiples vulnérabilités dans les produits SAP
- CERTFR-2020-AVI-141 : Vulnérabilité dans GitLab
- CERTFR-2020-AVI-142 : Multiples vulnérabilités dans Palo Alto PAN-OS
- CERTFR-2020-AVI-143 : [SCADA] Multiples vulnérabilités dans les produits Schneider Electric
- CERTFR-2020-AVI-144 : Vulnérabilité dans Xen
- CERTFR-2020-AVI-145 : Multiples vulnérabilités dans Joomla!
- CERTFR-2020-AVI-146 : Multiples vulnérabilités dans les produits Fortinet
- CERTFR-2020-AVI-147 : Multiples vulnérabilités dans le noyau Linux de Red Hat
- CERTFR-2020-AVI-148 : Multiples vulnérabilités dans le noyau Linux de SUSE
- CERTFR-2020-AVI-149 : Vulnérabilité dans implémentation du protocole SMB par Microsoft
- CERTFR-2020-AVI-150 : Multiples vulnérabilités dans les produits VMware
- CERTFR-2020-AVI-151 : Vulnérabilité dans Belden HiOS et HiSecOS

Un intrus s'invite à la réunion des ministres de la Défense de l'UE. Rigolade et embarras garantis

www.bruxelles2.eu 20 novembre 2020

Une bourde de la ministre néerlandaise

Tout commence avec une bourde monumentale. Sur son compte twitter, la ministre néerlandaise de la Défense Anlk Bijleveld — ou un membre de son équipe selon le gouvernement néerlandais — publie une photo où l'on peut voir 5 des 6 chiffres du code PIN permettant d'entrer dans la réunion Zoom. Un « *accident* » assure le ministère de la Défense. La photo a d'ailleurs été retirée entre temps. Mais Daniël Verlan, journaliste spécialisé dans le 'tech' pour le média néerlandais RTL News, a eu le temps de voir l'info…

… suivie d'une défaillance de sécurité

Le journaliste fait une copie écran et devine rapidement le chiffre manquant. D'autant que le code d'utilisateur n'est pas bien sorcier. Un simple 'admin' fonctionne. Et, tout simplement, il débarque en pleine réunion, alors que la discussion entre les ministres bat son plein.

Un petit coucou magistral en réunion

Suit alors, entre le journaliste et le chef de la diplomatie européenne, Josep Borrell, qui mène la réunion, un dialogue digne d'un film de Buñuel.

— « *Quelqu'un est entré dans le système. Il faut stopper la réunion… nous travaillons sur la scène publique là* », alerte Josep Borrell, qui tente de s'adresser directement à l'intrus.

« *Comment allez-vous ?* », l'interroge-t-il, d'un ton badin, réprimant mal un sourire. On entend quelques éclats de rire dans la réunion.

— « *Bonjour. Merci ça va bien* », répond, hilare, Daniël Verlan.

— « *Qui êtes-vous ? Vous savez que vous êtes entré dans une réunion secrète des ministres de la Défense ? Vous savez, c'est un délit hein !* » (Josep Borrell)

— « *Oui je sais. Je suis un journaliste des Pays-Bas. Je suis désolé d'avoir dérangé votre réunion. Merci de… Je vais m'en aller !* » (Daniël Verlan)

— « *Oui, ce serait mieux de partir rapidement, avant que la police arrive hein* », conclu Josep Borrell, sur un ton paternel, réprimant mal un sourire envers ce 'jeunot' impétueux qui pourrait être son petit-fils.

Une intrusion éclair…

Le journaliste assure n'être resté que quelques minutes dans la réunion, et avoir immédiatement allumé sa caméra et son micro pour que l'on puisse détecter sa présence… Mais le résultat est étonnant. « *J'ai moi-même été un peu choqué que cela fonctionne. Je ne m'attendais pas à ce qu'il n'y ait aucune autre forme de sécurité ou de validation* », affirme le journaliste sur twitter.

Avec une conséquence majeure

La suite ? Le journaliste ne la raconte pas. Mais B2 l'a appris de bonne source. La réunion a été stoppée. Et la conférence de presse du Haut représentant de l'UE a été avancée d'une petite demi-heure sur l'horaire prévu. « *Cela s'est traduit par la coupure immédiate des travaux* », a confirmé à B2 un participant à la réunion. Sans vraiment créer de dommage, selon lui. L'essentiel avait été dit. « *La réunion se terminait.* » Quoi qu'il en soit, notre collègue néerlandais a mis le doigt sur un point sensible.

Un vrai problème posé

Dans les milieux européens, l'heure n'est en effet pas à la franche rigolade. Et l'embarras face à une telle intrusion est net. « *Cela montre à quel point il faut être prudent avec ce genre de réunion. Une réunion des ministres de la Défense n'est jamais innocente* », a ainsi concédé à RTL Nieuws le premier ministre néerlandais Mark Rutte, avant d'essayer de se rassurer devant la (grosse) boulette de sa ministre. « *Le seul effet secondaire, positif, que A. Bijleveld a fait remarquer aux autres ministres, est à quel point il faut être prudent.* »

Renforcer la sécurité des communications

« *Nous avons besoin d'un renforcement très net de la sécurité des communications* », a indiqué à B2 un diplomate. Le travail « *est lancé* », précise-t-on d'ailleurs. Cette question de la sécurisation des communications internes avait d'ailleurs été abordée au plus haut niveau lors d'un Conseil européen, l'année dernière (en juin 2019). Les chefs d'État et de gouvernement (qui étaient encore 28 alors) avaient demandé aux institutions européennes de plancher sur le sujet pour renforcer la sécurité. Le chef de la diplomatie européenne Josep Borrell n'a pas dit mieux lors de la réunion, s'adressant au président du comité militaire, le général Claudio Graziano : « *Général, vous avez raison. Il faut investir dans des systèmes de communication* ».

En vidéoconférence, prière de ne pas évoquer de sujets top secrets

Par précaution d'ailleurs, lors de cette réunion (comme lors des autres réunions par vidéoconférence), plusieurs ministres ont jugé bon de ne pas aborder des sujets jugés trop confidentiels. « *Les lignes n'étaient pas sécurisées* », confirme notre interlocuteur. On évite de parler de sujets trop confidentiels. Ainsi « *on n'a pas parlé précisément de l'analyse des menaces* », un document 'classifié' des services de renseignement européens.

L'aubaine du Covid-19 pour les espions en tout genre

Chacun sait en effet que dans le cas des vidéoconférences qui se sont généralisées avec la crise du coronavirus, les possibilités de piratage ou d'écoutes sont multipliées. Les vidéoconférences sont « *une aubaine* », nous confiait ainsi il y a quelques mois, un spécialiste du domaine, pour tout ce que Bruxelles compte d'espions en tout genre (Chinois, Russes…).

performance des différentes offres. C'est pourtant le critère le plus déterminant dans le choix d'une solution. Le tableau est néanmoins appelé à évoluer, pour éventuellement intégrer de nouvelles offres, ou de nouveaux critères.

Trouver un compromis entre simplicité et sécurité

Ce nouveau comparatif fait suite à un précédent tableau, dressé par la direction générale de l'administration et de la fonction publique (DGAFP) la semaine dernière. Celui-ci, déjà dans une volonté d'aiguiller les agents publics dans le choix des outils, évaluait plusieurs solutions, dont certaines très grand public : Hangouts (Google), Skype (Microsoft) et la populaire mais controversée Zoom.

Ce premier document a néanmoins rapidement été retiré et c'est désormais celui de la Dinum qui fait foi. Là où la DGAFP référençait les 3 solutions grand public tout en mettant sérieusement en garde les agents quant à leur politique de protection des données, la DSI de l'État a préféré s'en tenir uniquement aux solutions offrant des garanties en la matière, en privilégiant notamment un hébergement des données sur le sol européen. *"Notre position est claire : il faut trouver un équilibre entre facilité d'utilisation et sécurité des données, c'est pourquoi nous ne promouvons que les solutions qui offrent un minimum de garanties de protection des données"*, fait valoir Xavier Albouy.

D'ailleurs, l'utilisation de ces outils, prévient la Dinum, ne vaut que pendant la période de crise sanitaire. *"L'outil des agents de l'État par défaut est la Webconférence de l'État, la possibilité d'utilisation ou non des autres outils après la crise n'est pas garantie et fera l'objet d'une réévaluation"*, indique le site Web de la direction. Pour l'heure, si rien ne permet de dire que la doctrine de l'État en matière d'outils numériques s'assouplira dans la durée, après la crise, cette dernière aura en tout cas eu le mérite de confronter les administrations et leurs agents à la réalité du travail à distance, et à ses implications en termes d'organisation comme d'outils.

Un sac à dos numérique : l'État veut parer ses agents pour le télétravail

www.clubic.com 30 août 2020

Une très grande partie des agents de l'État ne disposent toujours pas du matériel et plus globalement des moyens nécessaires pour se connecter à distance à leur poste de travail. Un retard qui pousse les pouvoirs publics à annoncer des mesures.

Crise de coronavirus oblige, les agents de l'État, comme les salariés du secteur privé, ont été contraints de rapidement s'adapter pour maintenir un certain service à destination des administrés pour les uns, et des clients pour les autres. Au niveau de l'État, ce fut bien compliqué ces derniers mois. Jeudi, la direction interministérielle du numérique (DINUM) a donné une conférence de presse durant laquelle elle a annoncé la création d'un « *sac à dos numérique* », pour préparer l'avenir.

85% des agents sous-équipés pour le télétravail

Il s'agit, pour la DINUM, de proposer un ensemble de services qui accompagneront les agents publics de l'Administration sur le chemin du télétravail. 85% des agents de l'État n'ont en effet pas les moyens de se connecter à distance à leur poste de travail.

« *On s'est retrouvé du jour au lendemain avec quelques centaines de milliers d'agents chez eux, là où les réseaux et les plateformes d'accès à distance étaient plutôt dimensionnés pour quelques dizaines de milliers de connexions simultanées* », a expliqué Nadi Bou Hanna, le directeur interministériel du numérique, au moment d'évoquer la situation des agents durant le confinement.

C'est en juillet et dans le cadre du programme Tech.gouv que la DINUM a commencé à dénicher et labelliser des solutions technologiques, qui seraient mises à disposition des différents ministères, peu importe la situation logistique de l'agent. Avec l'objectif de se doter d'un portefeuille de 50 à 80 services d'ici fin 2022.

L'État veut propulser ses solutions auprès de ses agents

De quoi sera composé ce sac à dos numérique, par exemple ? D'abord, l'important est d'y inclure un service de visioconférence. La base du télétravail collaboratif. La plateforme utilisée par l'État pendant le confinement, Webconf, a très vite été sollicitée. Capable d'héberger jusqu'à cent visioconférences en simultané, elle n'est accessible qu'aux agents publics, et doit encore grandir.

Le second service, lui, opère des fonctionnalités de messagerie instantanée, toujours uniquement accessible aux agents de l'État. Bien aidé par la crise, Tchap, lancé l'année dernière, a atteint la barre des 160 000 utilisateurs à la fin de ce mois d'août. Le service est désormais utilisé par des personnels de l'Assurance-Maladie, de l'APHP ou de la métropole du Grand Lyon.

Enfin, l'État, qui veut mettre un point d'honneur à ne pas migrer vers la suite de Microsoft, Office 365, a développé deux espaces numériques hébergés dans le Cloud, à l'initiative de PME françaises, pour proposer différents outils bureautiques.

Télétravail : des bénéfices environnementaux rognés par la visioconférence

www.actu-environnement.com 30 septembre 2020

En cette période de crise sanitaire du coronavirus, le Gouvernement recommande de continuer à privilégier le télétravail, lorsque cela est possible. L'Agence de la transition écologique (Ademe) a étudié, en juillet dernier, l'impact du travail en ligne à domicile qui a été plébiscité par les salariés pendant le confinement. Dans une nouvelle étude publiée le 22 septembre, l'Ademe prévient toutefois des « effets rebond » qui pénalisent les bénéfices environnementaux de cette pratique. L'agence a mené une enquête terrain auprès de 26 organisations françaises comptant 350 000 salariés. Ces entreprises ont été interrogées sur leur politique en matière de télétravail actuelle et future, permettant de caractériser les éventuels effets rebond. Ainsi, l'absence de trajets quotidiens pour aller au bureau est le principal avantage des télétravailleurs. Un jour de télétravail permet en effet de réduire de 69 % le volume des déplacements du jour. L'Ademe estime que la réduction des trajets domicile-travail génère un bénéfice environnemental moyen de 271 kilogrammes équivalent carbone (kg eqCO_2) annuels, par jour de télétravail hebdomadaire.

Pour les entreprises, l'agence ajoute aussi des bénéfices, en intégrant les réductions des surfaces immobilières qu'il induit, quand il est couplé « *au flex office* ». C'est-à-dire lorsque les collaborateurs d'une entreprise ne disposent plus de poste de travail attitré. La balance environnementale globale du télétravail augmente de 52 % par jour de télétravail hebdomadaire, si le télétravailleur est en flex office. Cela représente une baisse des émissions carbone de 234 kg eqCO_2/an pour chaque jour de télétravail hebdomadaire supplémentaire. Le flex office génère donc un effet rebond positif qui englobe la réduction de l'emprise foncière mais aussi la baisse des consommations énergétiques associées au sein de l'entreprise. Le télétravail réduit également les consommations de « bureaux » (papier, encre, fournitures, gobelets, décoration, vidéoprojecteurs, etc.).

La visioconférence parmi les effets rebond défavorables

En revanche, l'Ademe identifie quatre effets rebond directs et « *défavorables* » qui réduisent en moyenne de 31 % les bénéfices environnementaux du télétravail : les déplacements supplémentaires, la relocalisation du domicile, l'usage de la visioconférence et les consommations énergétiques du domicile. Ainsi, la consommation d'énergie et la sollicitation des serveurs nécessaires aux services de visioconférence génèrent, en moyenne, des émissions de l'ordre de 2,6 kg eqCO_2/an, pour un jour de télétravail hebdomadaire. À noter : une minute de visioconférence émet 1g de CO_2, souligne l'Ademe. La consommation d'énergie au domicile augmenterait aussi de 20,7 kg eqCO_2/an pour un jour de télétravail hebdomadaire.

L'Ademe pointe aussi les changements d'utilisation du véhicule pour des trajets personnels. Par exemple, les parents amenaient les enfants à l'école lors du même trajet en voiture que pour aller au bureau et continuent de le faire en télétravail. La proximité avec le lieu de vie suscite aussi de nouveaux déplacements quotidiens des télétravailleurs (micro-shopping, transport d'un proche, etc.). Ces effets rebond généreraient ainsi une hausse des émissions de 67,7 kg eqCO_2/an, pour un jour de télétravail hebdomadaire. Les télétravailleurs pourraient en outre s'éloigner davantage du lieu de travail, en changeant de région qui pourrait être moins bien desservie. Ce qui entraînerait une augmentation de la distance parcourue en voiture.
L'Ademe conclut que les bénéfices environnementaux sont *« significatifs et justifient l'encouragement du développement du télétravail»*. Néanmoins, l'agence prévoit de poursuivre son évaluation des effets rebond à plus long terme.

Le télétravail généralisé est source de fracture numérique et de nouvelles pratiques managériales

www.weka.fr 17 septembre 2020

L'agenda social national du deuxième semestre 2020 est connu depuis le 9 septembre dernier et il est particulièrement chargé. Au programme des discussions sera notamment à nouveau abordée la pratique du télétravail. Les enseignements doivent être tirés de la généralisation du télétravail suite à la crise sanitaire et au confinement.

Les conditions d'accompagnement et de cadrage du télétravail doivent être affinées, notamment en termes de formation managériale à distance et de fracture numérique.

Le déploiement massif du télétravail a accentué les inégalités d'accès au numérique

La généralisation du télétravail durant le confinement a accentué les inégalités d'accès au numérique des salariés. L'« illectronisme » (difficulté, voire incapacité, à utiliser les outils numériques en raison d'un manque de connaissance) touche déjà 16,5 % de la population française. Et avec le déploiement du télétravail en une période record dans le secteur public à cause de la crise sanitaire, des agents quels que soient leurs niveaux de responsabilité ont été perdus en route, faute d'avoir su leur apporter le haut débit ou de les équiper d'ordinateurs.

Cette exclusion numérique, qui date de bien avant l'épidémie de Covid-19, s'est constituée au fil des années, au fur et à mesure que les services en ligne se sont imposés dans la vie quotidienne. Mais le confinement l'a mise cruellement en lumière. La lutte contre l'illectronisme devient donc une priorité pour les employeurs publics. La fracture numérique s'est de plus greffée sur la fracture sociale des salariés.

Des milliers de foyers de salariés ont vécu une double peine : le confinement et l'isolement. Il a manqué parfois d'un plan d'accompagnement à distance des salariés qui se sont retrouvés dans cette situation, toutefois cette démarche pouvait difficilement être mise en place dans le contexte sanitaire rencontré.

L'absence des compétences numériques de base ou de connexion à internet, par manque de matériel ou de connaissances, doit désormais être accompagnée par l'intermédiaire de plans de formation annuels. Les difficultés pour utiliser certains logiciels, pour rechercher des informations sur internet, pour effectuer des manipulations informatiques sont encore trop prégnantes.

La crise sanitaire fait naître de nouvelles pratiques managériales

Les administrations ont un souhait : accélérer le retour physique des salariés dans les locaux, mais crise sanitaire oblige, avec des conditions particulières, dont le port obligatoire du masque dans les espaces clos et partagés depuis le 1er septembre 2020, l'ensemble des effectifs est cependant en mode mixte télétravail/présentiel. Le télétravail perdure de façon sûre mais cette fois en mode hybride.

Il faut cependant éviter de nouvelles fractures sociales entre ceux qui pourraient télétravailler à 100 % et les autres. L'évolution du travail dans la période post Covid doit ainsi tendre vers plus d'autonomie des salariés, d'avantage de collaborations entre les équipes et de transparence. Mais ce changement n'est pas simple à gérer compte tenu de la culture managériale française dans laquelle les responsables hiérarchiques ont l'habitude d'avoir leurs équipes « sous la main ».

Désormais le rôle des managers s'est complexifié. Les attentes à leur égard sont nombreuses, avec pour base de ce nouveau management un trio autonomie, confiance et responsabilité. Les managers doivent donc être encore plus clairs sur leur vision et leurs priorités. Et il est impératif qu'ils veillent à entretenir le lien social au sein de leur équipe et qu'ils aient conscience des risques psychosociaux.

Pourtant, passer de la théorie aux pratiques nouvelles de management ne se fera pas tout seul. Il y aura des coûts notamment en matière de formation et il faudra laisser du temps aux administrations pour qu'elles s'adaptent.

Avec le télétravail vient la hausse des cyberattaques

www.ledevoir.com – 4 février 2021

Devant la hausse des cyberattaques et des tentatives d'hameçonnage en raison du télétravail, les entreprises informatiques n'ont d'autres choix que de resserrer leurs mesures de sécurité. Une situation qui profite à des start-up qui y voient une occasion de faire des affaires.

« Les cyberattaques fonctionnent un peu à la façon de l'électricité. Elles vont se produire là où il y a le moins de résistance », illustre Lukas Lhotsky, président de FX Innovation, une compagnie montréalaise qui accompagne des entreprises dans le déploiement d'infrastructures informatiques.

Depuis le début de la pandémie, le nombre de cyberattaques a considérablement augmenté. Il aurait crû de 151 % au cours des six premiers mois de 2020 comparativement à la même période l'année précédente, selon une étude du Centre des opérations de sécurité de la firme américaine d'analyses Neustar. Non seulement ces actes malveillants étaient plus nombreux, mais leur durée était également plus longue.

Il faut dire que l'augmentation de la pratique du télétravail a multiplié les risques : utilisation d'appareils personnels et augmentation des transferts d'informations sensibles d'un lieu à un autre. « Évidemment, le travail à distance n'est pas l'unique raison, mais ça a accentué une tendance de fond qui était déjà observable depuis plusieurs années », soutient Lukas Lhotsky.

Outre la multiplication des lieux, « il y a des organisations qui se sont retrouvées dans une situation financière précaire », observe de son côté Marcel Labelle, directeur général de Cybereco, un organisme qui s'intéresse à la cyberrésilience et qui regroupe de nombreuses entreprises et universités. « Et si leurs dirigeants n'étaient pas en mesure d'évaluer convenablement les risques, inévitablement, ces entreprises s'exposent. »

Suivre la trace des données

L'accroissement du nombre de cyberattaques n'étonne en rien Jean Le Bouthillier, p.-d.g.-fondateur de Qohash, une start-up de Québec spécialisée en cybersécurité. L'année 2020 marque un point d'inflexion, estime-t-il. « Il y a eu une transition forcée vers le travail à distance qui s'ajoute à une accélération de la transformation numérique qui était déjà en cours avant la crise. On assiste actuellement à une sorte de rattrapage. »

De plus, le travail à distance a, selon lui, permis de constater l'ampleur de la dépendance à l'égard d'une ressource : la donnée. « La donnée est intéressante parce que, plus on la maîtrise, plus on peut devenir efficace. Par contre, plus on l'utilise, plus on en devient dépendant. Et c'est là où la question de la sécurité devient importante. »

Qohash a développé une technologie qui s'appuie en partie sur l'intelligence artificielle. Celle-ci permet de cibler les informations sensibles et d'en assurer la traçabilité. « On est

capable de savoir sur quel poste de travail se trouve une information en particulier. À partir de là, il est possible d'évaluer un employé en termes de risques. » Quels sont ceux qui détiennent la plus grande quantité de données sensibles ? Quels sont ceux dont les comportements sont les plus à risque ?

Le contexte actuel aura facilité l'obtention de huit millions de dollars canadiens lors de la plus récente ronde de financement de la start-up en janvier. D'autant plus que Qohash déploie sa solution dans des secteurs ciblés régulièrement par les cyberattaques : les institutions financières et les compagnies d'assurances.

Une récente étude de la firme Varonis relate l'importance du problème dans l'industrie financière en contexte de télétravail : un employé aurait accès à « 13 % du nombre total des fichiers » d'une société. Ceux-ci peuvent « visualiser, copier, déplacer, modifier et supprimer des données » sensibles.

Le risque gagne en importance en fonction de la taille de l'institution : « Le nombre de fichiers exposés double à mesure que la taille de l'entreprise augmente ». Aux États-Unis, les plus grandes institutions financières auraient en moyenne plus de 20 millions de dossiers accessibles aux employés, selon Varonis.

Plus que jamais, la maîtrise et la protection des données s'imposent à la fois comme le levier d'une organisation et comme son principal talon d'Achille, estime M. Le Bouthillier : « La donnée, ça va être le plus grand créateur et destructeur d'entreprises au cours des prochaines décennies. »

Prévention

Outre les solutions informatiques, il y a la prévention et la planification. Deux aspects non négligeables pour Lukas Lhotsky de FX Innovation : « On le dit souvent, mais il n'y a pas que le système qui sert de porte d'entrée. Très souvent, le problème se trouve devant l'écran ; le facteur humain joue pour beaucoup », rappelle-t-il.

C'est le cas lors de tentatives d'hameçonnage. Leur nombre a considérablement augmenté depuis le début de la pandémie. Cet automne, la firme Atlas VPN relatait une hausse de 19,91 % du nombre de sites Web servant à l'hameçonnage, tel que recensé par Google. Leur nombre dépasserait aujourd'hui deux millions.

À cela s'ajoute la mise en place d'une stratégie pour réagir promptement en cas de pépin. Lukas Lhotsky cite la mise en place d'un plan de reprise d'activités (*Disaster Recovery Plan*) qui permet de reconstituer un système informatique s'il est attaqué. « Personne n'a envie d'être le maillon faible à l'origine d'actes malveillants », dit-il.

Recommandations de sécurité informatique pour le télétravail en situation de crise

www.cybermalveillance.gouv.fr 23 mars 2020

La situation de crise et de confinement liée à l'épidémie du CORONAVIRUS – COVID-19 engendre une intensification du recours au télétravail. Pour beaucoup d'employeurs et de collaborateurs, cette situation inédite et qui va s'inscrire dans la durée, n'avait pas été anticipée. Une mise en œuvre non-maîtrisée du télétravail peut augmenter considérablement les risques de sécurité pour les entreprises ou organisations qui y recourent. Elle peut même mettre en danger leur activité face à une cybercriminalité qui redouble d'efforts pour profiter de cette nouvelle opportunité.
En complément des mesures générales de vigilance cybersécurité publiées sur la crise du CORONAVIRUS – COVID-19, cet article décrit les conseils de Cybermalveillance.gouv.fr tant pour les collaborateurs que pour les employeurs afin de limiter les risques de sécurité informatique liés au télétravail.

État de la situation

La crise sanitaire mondiale du CORONAVIRUS – COVID-19 a nécessité la mise en place de mesures de confinement et de stricte limitation des déplacements aux seuls motifs indispensables. Face à cette situation exceptionnelle et inédite, les entreprises, associations, administrations ou collectivités qui en avaient la possibilité ont dû mettre en place le télétravail pour préserver au moins les activités essentielles que ce mode de fonctionnement peut permettre.

Certaines de ces organisations étaient déjà préparées au télétravail, mais pas pour y faire face de manière aussi massive et en s'inscrivant autant dans la durée.

Pour beaucoup d'autres organisations, la mise en place du télétravail a dû se faire dans l'urgence, voire elles ont dû l'initier « à distance » avec des collaborateurs confinés et sans réelle maîtrise des mesures de sécurité à mettre en place pour protéger de manière satisfaisante le système d'information de l'organisation.

Dans certains cas, et faute d'avoir pu déployer les moyens nécessaires, le télétravail s'opère même depuis les équipements personnels des collaborateurs, dont le niveau de sécurité ne peut pas être évalué et encore moins garanti.

Parallèlement, on peut observer dans cette crise du CORONAVIRUS – COVID-19 une intensification des activités de cybercriminels qui, comme dans toute situation exceptionnelle, cherchent à profiter de l'aubaine et des vulnérabilités induites.

Cette situation engendre une augmentation des risques de cybermalveillance pour les organisations qu'il est indispensable de juguler au mieux sous peine de dommages considérables.

Conseils généraux en situation de crise

Restez zen ! Dans toute situation de crise, il est indispensable de conserver son calme et de ne pas céder à la panique au risque de fausser son jugement et de prendre des décisions ou mesures inadaptées, potentiellement inefficaces, voire dangereuses pour l'organisation.

Prenez le temps de la réflexion ! La nécessaire réactivité dans ce type de situation ne doit pas signifier pour autant une précipitation excessive et inconsidérée. Évaluez au mieux les conséquences possibles de vos actions avant de les mettre en œuvre, en ayant conscience des risques induits.

Ne sacrifiez pas votre sécurité à l'efficacité ! Rechercher l'efficacité à tout prix peut engendrer de problèmes de sécurité importants. Ne cédez pas à la facilité. Ayez conscience que la préservation, voire le renforcement, de votre sécurité, sont indispensables dans les situations difficiles.

Principaux risques et cybermenaces liés au télétravail

Avec l'intensification du télétravail, les cybercriminels vont chercher à mettre à profit la possible désorganisation et confusion des entreprises et organisations, ainsi que la dématérialisation des procédures qui en résulte, pour intensifier leurs attaques. Les principales cyberattaques que l'ont peut envisager sont :

– **L'hameçonnage (*phishing*)** : Messages (*email*, SMS, chat…) visant à dérober des informations confidentielles (mots de passe, informations personnelles ou bancaires) en usurpant l'identité d'un tiers de confiance. Conséquences possibles : piratage de comptes professionnels de messagerie ou d'accès aux systèmes d'information de l'organisation, intrusion sur le réseau de l'entreprise, rançongiciels (ransomware), fraude aux faux ordres de virement… .

– **Les rançongiciels (*ransomware*)** : Attaque qui consiste à chiffrer ou empêcher l'accès aux données de l'entreprise et à généralement réclamer une rançon pour les libérer. Ce type d'attaque s'accompagne de plus en plus souvent d'un vol de données et d'une destruction préalables des sauvegardes. Ces attaques sont généralement rendues possibles par une intrusion sur le réseau de l'entreprise, soit par ses accès à distance, soit par la compromission de l'équipement d'un collaborateur. Conséquence : arrêt de l'activité de l'entreprise, perte de données… .

– **Le vol de données :** Attaque qui consiste à s'introduire sur le réseau de l'entreprise, ou sur ses hébergement externes (cloud), pour lui dérober des données afin de la faire « chanter », ou de les revendre, ou encore de les diffuser pour lui nuire. Comme pour les rançongiciels (cf. supra), ces attaques sont généralement possibles par une intrusion dans le réseau ou sur les systèmes hébergées de l'entreprise via ses accès à distance ou bien encore par la compromission du poste d'un collaborateur. Conséquences : atteinte à l'activité et à l'image de l'entreprise ou de l'organisation.

– **Les faux ordres de virement (FOVI/BEC) :** Escroquerie réalisée, parfois suite au piratage d'un compte de messagerie, par message et même téléphone, en usurpant l'identité d'un dirigeant ou d'un de ses mandataires, d'un fournisseur ou d'un prestataire, voire d'un collaborateur, pour demander un virement exceptionnel et confidentiel, ou un changement des

coordonnées de règlement (RIB) d'une facture ou d'un salaire. Conséquence : perte financière pour l'entreprise ou l'organisation.

« Bien connaître les risques permet de mieux détecter les attaques et de comprendre l'intérêt des mesures de sécurité à appliquer. »

10 recommandations de sécurité pour les télétravailleurs

Vous êtes confinés et devez avoir recours au télétravail pour maintenir votre activité. Vous ne disposez parfois pas d'équipement professionnel pour télétravailler et devez le faire avec vos moyens informatiques personnels (ordinateur, tablette, téléphone, comptes de messagerie…). Afin de préserver au mieux la sécurité de votre entreprise, appliquez les 10 recommandations suivantes :

1. **Si vous disposez d'équipements professionnels, séparez vos usages** : Séparez bien vos usages professionnels et personnels au risque de les confondre et de générer des fautes de sécurité qui pourraient être préjudiciables à votre entreprise. L'activité professionnelle doit se faire sur vos moyens professionnels et seulement sur vos moyens professionnels et l'activité personnelle doit se faire seulement sur vos moyens personnels. .

2. **Appliquez strictement les consignes de sécurité de votre entreprise** : Ces mesures de sécurité visent à protéger votre entreprise, donc votre activité. Si vous rencontrez des difficultés à appliquer les mesures prescrites, remontez l'information et demandez conseil à votre entreprise, mais ne les contournez pas de votre propre chef, car vous n'êtes probablement pas en mesure d'apprécier l'étendue des risques que vous pourriez prendre et faire prendre à votre entreprise

3. **Ne faites pas en télétravail ce que vous ne feriez pas au bureau :** A fortiori sur vos équipements professionnels si vous en disposez. Ayez une utilisation responsable et vigilante de vos équipements et accès professionnels. Si vous utilisez vos moyens personnels en télétravail, ayez conscience que vos activités personnelles peuvent faire prendre un risque aussi à votre entreprise, redoublez donc d'attention et de prudence.

4. **Appliquez les mises à jour de sécurité sur tous vos équipements connectés (PC, tablettes, téléphones…)** : Et ce dès qu'elles vous sont proposées afin de corriger les failles de sécurité qui pourraient être utilisées par des pirates pour s'y introduire et les utiliser pour attaquer le réseau de votre entreprise au travers de vos accès. .

5. **Vérifiez que vous utilisez bien un antivirus et scannez vos équipements** : Vérifiez que tous vos équipements connectés (PC, téléphones, tablettes…) sont bien protégés par un antivirus, qu'il est bien à jour, et effectuez une analyse complète (scan) de vos matériels. Si un matériel ne peut avoir d'antivirus, évitez le plus possible de l'utiliser pour accéder au réseau de votre entreprise.

6. **Renforcez la sécurité de vos mots de passe** : Utilisez des mots de passe suffisamment longs, complexes et différents sur tous les équipement et services auxquels vous accédez, qu'ils soient personnels ou professionnels. La majorité des attaques est due à des mots de passe trop simples ou réutilisés. Au moindre doute ou même en prévention, changez-les et activez la double authentification chaque fois que cela est possible. .

7. **Sécurisez votre connexion WiFi** : Le télétravail s'opère en général principalement sur votre connexion WiFi personnelle. Il est donc primordial de bien la sécuriser pour éviter toute

intrusion sur votre réseau qui pourrait être utilisée pour attaquer votre entreprise. Utilisez un mot de passe suffisamment long et complexe (voir plus haut) et assurez vous que vous utilisez bien le chiffrement de votre connexion en WPA2. Pensez également à mettre à jour régulièrement votre « box Internet » en la redémarrant ou depuis son interface d'administration.

8. **Sauvegardez régulièrement votre travail** : La sauvegarde est le seul moyen permettant de retrouver ses données en cas de cyberattaques, mais également en cas de panne ou de perte de son équipement. Si vous en avez la possibilité, sauvegardez régulièrement votre travail sur le réseau de l'entreprise ou les moyens qu'elle met à disposition à cet effet, mais aussi sur un support externe à votre équipement (clé ou disque USB) que vous débranchez une fois la sauvegarde effectuée.

9. **Méfiez-vous des messages inattendus** : Que ce soit par messagerie (*email*, SMS, chat...) en cas de message inattendu ou alarmiste, demandez toujours confirmation à l'émetteur par un autre moyen. Il peut s'agir d'une attaque par hameçonnage (*phishing*) visant à vous dérober des informations confidentielles (mots de passe), de l'envoi d'un virus par pièce-jointe ou d'un lien qui vous attirerait sur un site piégé, ou encore d'une tentative d'arnaque aux faux ordres de virement (voir menaces supra).

10. **N'installez vos applications que dans un cadre « officiel » et évitez les sites suspects** : Sur vos équipements professionnels, n'installez de nouvelles applications qu'après l'accord de votre support informatique. Sur vos équipements personnels utilisés en télétravail, n'installez des applications que depuis les sites ou magasins officiels des éditeurs (exemple : Apple App Store,Google Play Store) pour limiter les risques d'installation d'une application piégée pour pirater votre équipement. De même, évitez les sites Internet suspects ou frauduleux (téléchargement, vidéo, streaming illégaux) qui pourraient également piéger vos équipements.

12 recommandations de sécurité liées au télétravail pour les employeurs

Pour faire face à la crise et au confinement imposé par l'épidémie du CORONAVIRUS – COVID-19 les employeurs, entreprises, associations, administrations, collectivités se sont vues devoir mettre en place ou développer dans l'urgence le télétravail pour maintenir, au moins a minima, leurs activités essentielles. L'ouverture vers l'extérieur du système d'information de l'entreprise peut engendrer des risques sérieux de sécurité qui pourraient mettre à mal l'entreprise, voire engager sa survie en cas de cyberattaque. Voici 12 recommandations à mettre en œuvre pour limiter au mieux les risques :

1. **Définissez et mettez en œuvre une politique d'équipement des télétravailleurs** : Privilégiez autant que possible pour le télétravail l'utilisation de moyens mis à disposition, sécurisés et maîtrisés par l'entreprise. Lorsque ce n'est pas possible, donnez des directives d'utilisation et de sécurisation claires aux employés en ayant conscience que leurs équipements personnels ne pourront jamais avoir un niveau de sécurité vérifiable (voire sont peut être déjà compromis par leur usage personnel).

2. **Maîtrisez vos accès extérieurs** : Limitez l'ouverture de vos accès extérieurs ou distants (RDP) aux seules personnes et services indispensables, et filtrer strictement ces accès sur votre pare-feu. Cloisonnez les systèmes pour lesquels un accès à distance n'est pas nécessaire pour les préserver, surtout s'ils revêtent un caractère sensible pour l'activité de l'entreprise.

3. **Sécurisez vos accès extérieurs** : Systématisez les connexions sécurisées à vos infrastructures par l'emploi d'un « VPN » (*Virtual Private Network* ou « réseau privé virtuel » en français). Outre le chiffrement de vos connexions extérieures, ces dispositifs permettent également de renforcer la sécurité de vos accès distants en les limitant aux seuls équipements authentifiés. La mise en place sur ces connexions VPN d'une double authentification sera également à privilégier pour se prémunir de toute usurpation.

4. **Renforcez votre politique de gestion des mots de passe** : Qu'il s'agisse des mots de passe des utilisateurs en télétravail, mais aussi de ceux en charge du support informatique, les mots de passe doivent être suffisamment longs, complexes et uniques sur chaque équipement ou service utilisé. La majorité des attaques est due à des mots de passe trop simples ou réutilisés. Au moindre doute ou même en prévention, changez-les et activez la double authentification chaque fois que cela est possible. .

5. **Ayez une politique stricte de déploiement des mises à jour de sécurité** : Et ce, dès qu'elles sont disponibles et sur tous les équipements accessibles de votre système d'information (postes nomades, de bureau, tablettes, smartphones, serveurs, équipements réseaux ou de sécurité...) car les cybercriminels mettent peu de temps à exploiter les failles lorsqu'ils en ont connaissance. Un défaut de mise à jour d'un équipement est souvent la cause d'une intrusion dans le réseau des entreprises. .

6. **Durcissez la sauvegarde de vos données et activités** : Les sauvegardes seront parfois le seul moyen pour l'entreprise de recouvrer ses données suite à une cyberattaque. Les sauvegardes doivent être réalisées et testées régulièrement pour s'assurer qu'elles fonctionnent. Des sauvegardes déconnectées sont souvent indispensables pour faire face à une attaque destructrice par rançongiciel (*ransomware*). En outre, il convient également de s'assurer du niveau de sauvegarde de ses hébergements externes (cloud, site Internet d'entreprise, service de messagerie...) pour s'assurer que le service souscrit est bien en adéquation avec les risques encourus par l'entreprise. .

7. **Utilisez des solutions antivirales professionnelles** : Les solutions antivirales professionnelles permettent de protéger les entreprises de la plupart des attaques virales connues, mais également parfois des messages d'hameçonnage (*phishing*), voire de certains rançongiciels (*ransomware*). Utiliser des solutions différentes pour la protection des infrastructures et pour les terminaux peut s'avérer très complémentaire et donc démultiplier l'efficacité de la protection dans un principe de défense en profondeur.

8. **Mettez en place une journalisation de l'activité de tous vos équipements d'infrastructure** : Ayez une journalisation systématique et d'une durée de rétention suffisamment longue de tous les accès et activités de vos équipements d'infrastructure (serveurs, pare-feu, proxy...), voire des postes de travail. Cette journalisation sera souvent le seul moyen de pouvoir comprendre comment a pu se produire une cyberattaque et donc de pouvoir y remédier, ainsi que d'évaluer l'étendue de l'attaque.

9. **Supervisez l'activité de vos accès externes et systèmes sensibles** : Cette supervision doit vous permettre de pouvoir détecter toute activité anormale qui pourrait être le signe d'une cyberattaque, tels une connexion suspecte d'un utilisateur inconnu, ou d'un utilisateur connu en dehors de ses horaires habituels, ou encore un volume inhabituel de téléchargement d'informations...

10. **Sensibilisez et apportez un soutien réactif à vos collaborateurs en télétravail** : Donnez aux télétravailleurs des consignes claires sur ce qu'ils peuvent faire ou ne pas faire et sensibilisez

les aux risques de sécurité liés au télétravail. Cela doit se faire avec pédagogie pour vous assurer de leur adhésion et donc de l'efficacité des consignes. Les utilisateurs sont souvent le premier rempart pour éviter, voire détecter les cyberattaques. Utilisez au besoin nos supports et notre kit de sensibilisation ou encore les recommandations aux télétravailleurs décrites supra. Ces utilisateurs coupés de leur entreprise ont également besoin d'un soutien de qualité et réactif pour éviter toute dérive.

11. **Préparez-vous à affronter une cyberattaque** : L'actualité démontre qu'aucune organisation, quelle que soit sa taille, n'est à l'abri d'une cyberattaque. Il faut donc admettre que cela n'arrive pas qu'aux autres. La question n'est donc plus de savoir si on va être victime d'une cyberattaque, mais quand on le sera. Il faut donc s'y préparer. L'évaluation des scénarios d'attaques possibles (cf. menaces supra) permet d'anticiper les mesures à prendre pour s'en protéger et de définir également la conduite à tenir pour réagir quand elle surviendra : plans de crise et de communication, contractualisation avec des prestataires spécialisés pour recourir à leur assistance...

12. **Dirigeants : impliquez-vous et montrez l'exemple !** La sécurité est toujours une contrainte qu'il faut accepter à la mesure des enjeux qui peuvent s'avérer vitaux pour les entreprises. L'implication et l'adhésion des dirigeants aux mesures de sécurité est indispensable, tout comme leur comportement qui doit se vouloir exemplaire afin de s'assurer de l'adhésion des collaborateurs.

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

Dernière mise à jour des données de ce texte : 01 janvier 2021

NOR : RDFF1519812D

JORF n°0036 du 12 février 2016

Version en vigueur au 07 mai 2020

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

Modifié par Décret n°2020-524 du 5 mai 2020 - art. 1

Le télétravail désigne toute forme d'organisation du travail dans laquelle les fonctions qui auraient pu être exercées par un agent dans les locaux où il est affecté sont réalisées hors de ces locaux en utilisant les technologies de l'information et de la communication.

Le télétravail peut être organisé au domicile de l'agent, dans un autre lieu privé ou dans tout lieu à usage professionnel.

Un agent peut bénéficier au titre d'une même autorisation de ces différentes possibilités.

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.

NOTA :
Conformément à l'article 9 du décret n° 2020-524 du 5 mai 2020, les dispositions issues dudit décret s'appliquent aux demandes initiales ainsi qu'aux demandes de renouvellement présentées à compter de sa date d'entrée en vigueur.

Article 2-1

Création Décret n°2020-524 du 5 mai 2020 - art. 2

L'autorisation de télétravail est délivrée pour un recours régulier ou ponctuel au télétravail. Elle peut prévoir l'attribution de jours de télétravail fixes au cours de la semaine ou du mois ainsi que l'attribution d'un volume de jours flottants de télétravail par semaine, par mois ou par an dont l'agent peut demander l'utilisation à l'autorité responsable de la gestion de ses congés.

Un agent peut, au titre d'une même autorisation, mettre en œuvre ces différentes modalités de télétravail.

NOTA :
Conformément à l'article 9 du décret n° 2020-524 du 5 mai 2020, les dispositions issues dudit décret s'appliquent aux demandes initiales ainsi qu'aux demandes de renouvellement présentées à compter de sa date d'entrée en vigueur.

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°2020-524 du 5 mai 2020 - art. 3

Il peut être dérogé aux conditions fixées à l'article 3 :

1° Pour une durée de six mois maximum, à la demande des agents dont l'état de santé, le handicap ou l'état de grossesse le justifient et après avis du service de médecine préventive ou du médecin du travail ; cette dérogation est renouvelable, après avis du service de médecine préventive ou du médecin du travail ;

2° Lorsqu'une autorisation temporaire de télétravail a été demandée et accordée en raison d'une situation exceptionnelle perturbant l'accès au service ou le travail sur site.

NOTA :
Conformément à l'article 9 du décret n° 2020-524 du 5 mai 2020, les dispositions issues dudit décret s'appliquent aux demandes initiales ainsi qu'aux demandes de renouvellement présentées à compter de sa date d'entrée en vigueur.

Article 5

Modifié par Décret n°2020-524 du 5 mai 2020 - art. 4

L'exercice des fonctions en télétravail est accordé sur demande écrite de l'agent. Celle-ci précise les modalités d'organisation souhaitées. Lorsque le télétravail est organisé au domicile de l'agent ou dans un autre lieu privé, une attestation de conformité des installations aux spécifications techniques, établie conformément aux dispositions prises en application du 9° du I de l'article 7, est jointe à la demande.

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 et l'intérêt du service. Lorsque l'autorité investie du pouvoir de nomination est le Centre national de gestion, cette appréciation est assurée :

1° Par le chef d'établissement pour les directeurs adjoints et les directeurs des soins ;

2° Par le directeur général de l'agence régionale de santé pour les chefs des établissements mentionnés aux 1°, 3° et 5° de l'article 2 de la loi du 9 janvier 1986 susvisée ;

3° Par le préfet du département pour les établissements mentionnés aux 4° et 6° du même

article 2.

Une réponse écrite est donnée à la demande de télétravail dans un délai d'un mois maximum à compter de la date de sa réception ou de la date limite de dépôt lorsqu'une campagne de recensement des demandes est organisée.

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.

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 d'autorisation de télétravail ainsi que l'interruption du télétravail à l'initiative de l'administration doivent être motivés et précédés d'un entretien.

NOTA :
Conformément à l'article 9 du décret n° 2020-524 du 5 mai 2020, les dispositions issues dudit décret s'appliquent aux demandes initiales ainsi qu'aux demandes de renouvellement présentées à compter de sa date d'entrée en vigueur.

Article 6

Modifié par Décret n°2020-524 du 5 mai 2020 - art. 5

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. L'employeur n'est pas tenu de prendre en charge le coût de la location d'un espace destiné au télétravail.

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 ou, à défaut, selon les cas, l'une des autorités mentionnées aux troisième, quatrième et cinquième alinéas de l'article 5, met en œuvre sur le lieu de télétravail de l'agent les aménagements de poste nécessaires, sous réserve que les charges consécutives à la mise en œuvre de ces mesures ne soient pas disproportionnées, notamment compte tenu des aides qui peuvent compenser, en tout ou partie, les dépenses engagées à ce titre par l'employeur.

Lorsqu'un agent demande l'utilisation des jours flottants de télétravail ou l'autorisation temporaire de télétravail mentionnée au 2° de l'article 4, l'administration peut autoriser l'utilisation de l'équipement informatique personnel de l'agent.

NOTA :
Conformément à l'article 9 du décret n° 2020-524 du 5 mai 2020, les dispositions issues dudit décret s'appliquent aux demandes initiales ainsi qu'aux demandes de renouvellement présentées à compter de sa date d'entrée en vigueur.

Article 7

Modifié par Décret n°2020-524 du 5 mai 2020 - art. 6

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° Les conditions dans lesquelles l'attestation mentionnée à l'article 5 est établie.

Lorsque l'autorité investie du pouvoir de nomination est le Centre national de gestion, la décision fixant les modalités et règles mentionnées au présent I est prise :

1° Par le chef d'établissement pour les directeurs adjoints et les directeurs des soins ;

2° Par le directeur général de l'agence régionale de santé pour les chefs des établissements mentionnés aux 1°, 3° et 5° de l'article 2 de la loi du 9 janvier 1986 susvisée ;

3° Par le préfet du département pour les établissements mentionnés aux 4° et 6° du même article 2.

La décision n'est pas soumise à l'avis du comité consultatif national.

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 le comité consultatif national en application du présent article.

NOTA :
Conformément à l'article 9 du décret n° 2020-524 du 5 mai 2020, les dispositions issues dudit décret s'appliquent aux demandes initiales ainsi qu'aux demandes de renouvellement présentées à compter de sa date d'entrée en vigueur.