Sujet élaboré par une cellule pédagogique nationale

CONCOURS EXTERNE, INTERNE ET DE 3ème VOIE DE TECHNICIEN TERRITORIAL PRINCIPAL DE 2ème CLASSE

SESSION 2020
REPORTÉE À 2021

ÉPREUVE DE RAPPORT AVEC PROPOSITIONS OPÉRATIONNELLES

ÉPREUVE D'ADMISSIBILITÉ :

Rédaction d'un rapport technique portant sur la spécialité au titre de laquelle le candidat concourt. Ce rapport est assorti de propositions opérationnelles.

Durée : 3 heures
Coefficient : 1

SPÉCIALITÉ : INGÉNIERIE, INFORMATIQUE ET SYSTÈMES D'INFORMATION

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 28 pages.

Il appartient au candidat de vérifier que le document comprend le nombre de pages indiqué.

S'il est incomplet, en avertir le surveillant.

Vous êtes technicien territorial principal de 2ème classe au sein de la direction des systèmes d'information (D.S.I.) de la commune de Techniville (80 000 habitants).

La Directrice générale des services (D.G.S.), à la demande du Maire de la commune, envisage la mise en place du télétravail pour une partie du personnel communal. Dans ce cadre, elle interroge la direction des systèmes d'information sur les mesures à mettre en place pour offrir aux futurs télétravailleurs les moyens informatiques nécessaires tout en assurant la sécurité du système d'information de la collectivité.

Dans un premier temps, votre supérieur hiérarchique, le directeur des systèmes d'information, vous demande de rédiger à son attention, exclusivement à l'aide des documents joints, un rapport technique sur le télétravail et la sécurité informatique.

10 points

Dans un deuxième temps, il vous demande d'établir un ensemble de propositions opérationnelles permettant la mise en place du télétravail de manière sécurisée pour les agents comme pour les ressources informatiques de la commune.

Pour traiter cette seconde partie, vous mobiliserez également vos connaissances

10 points

Liste des documents :

Document 1 : « 8 bonnes pratiques pour bien installer le télétravail en entreprise » - Naéva Measso - *hubone.fr* – 24 octobre 2016 - 2 pages.

Document 2 : « Le travail nomade exige de repenser en profondeur la sécurisation des données des entreprises » - Alexandre Grellier - *lesechos.fr* - 9 janvier 2019 - 2 pages.

Document 3 : « Ce que le Cloud apporte aux travailleurs nomades » - Colin Steele - *lemagit.fr* - avril 2019 - 2 pages.

Document 4 : « Guide ANSSI - Recommandations sur le nomadisme numérique » (Extrait) - *ANSSI* - octobre 2018 - 6 pages.

Document 5 : « Télétravail et RGPD : comment éviter la faille de sécurité ? » - Me Pierre-Randolph Dufau - *itforbusiness.fr* - février 2019 - 1 page.

Document 6 : « Le télétravail dans les trois versants de la fonction publique - Bilan du déploiement » (Extrait) - *Ministère de l'action et des comptes publics* - décembre 2018 - 4 pages.

Document 7 : « BYOD : quelles sont les bonnes pratiques ? » - *cnil.fr* - février 2019 - 2 pages.

Document 8 : « 3 risques de sécurité IT à gérer pour protéger les ressources des télétravailleurs sans impacter leur productivité » - William Culbert - *beyondtrust.com* - avril 2019 - 2 pages.

Document 9 : « Zero Trust, la clé d'une transformation numérique réussie » Xavier Daspre - *journaldunet.com* - mai 2018 - 2 pages.

Document 10 : « Télétravail et travail mobile : comment réduire le risque de fuite de données ? » - Jan Van Vliet - *L'Usine nouvelle* - novembre 2018 - 2 pages.

DOCUMENT 1

« 8 bonnes pratiques pour bien installer le télétravail en entreprise »

Naéva Measso - *hubone.fr* - 24 octobre 2016

Bien que 83% des Français soient favorables au travail à distance*, très peu d'entreprises ont mis en place un réel système de télétravail, car il n'est pas facile de savoir par où commencer ni quels outils privilégier… Et pourtant, 72% des managers y seraient favorables, mais à condition de bien l'encadrer. Voici les 8 bonnes pratiques qui permettent d'installer le télétravail de manière efficace dans les structures.**

Plusieurs solutions technologiques existent déjà et certaines sont indispensables pour le bon fonctionnement du télétravail en entreprise. Tandis que d'autres permettent d'en faciliter la pratique et amènent du confort aux collaborateurs pour une meilleure réussite dans cette nouvelle organisation de travail.

1) Mettre en place un VPN

Un télétravail fonctionnel passe forcément par la mise en place d'un VPN (Virtual Private Network, Réseau Privé Virtuel) qui donne l'accès au réseau local d'une entreprise à distance via une connexion Internet sécurisée.

2) Donner l'accès à un Webmail

Un **Webmail** est aussi nécessaire car il permet d'avoir un accès distant au serveur de messagerie d'entreprise, sans requérir la configuration d'un client de messagerie dit lourd tel qu'Outlook par exemple.

3) Développer une messagerie instantanée

Pour faciliter les échanges, qui peuvent paraître difficiles lorsque tous les collaborateurs ne se trouvent pas au même endroit, les entreprises peuvent développer un Chat/Messagerie instantanée d'entreprise qui fournit, un moyen de communication instantanée entre deux ou plusieurs collaborateurs (discussion privée) mais aussi de connaître la disponibilité du correspondant recherché. Moins formel que le mail, cet outil est à la fois un moyen de contact rapide et immédiat, ou différé si l'un des collaborateurs n'est pas disponible à l'instant T.

4) Mettre à disposition des outils de communications asynchrones

Utiliser des Outils de communications asynchrones (forums, wikis, blogs, etc), offre la liberté aux collaborateurs de communiquer quand ils le souhaitent, sur des sujets concernant plusieurs personnes à la fois (discussion ouverte), sans que celles-ci ne soient connectées simultanément mais qui auront la possibilité de consulter l'information quand elles seront disponibles.

5) Profiter du softphone

Mettre à disposition des collaborateurs un Softphone, logiciel de téléphonie où les appels sont gérés depuis l'ordinateur, permet aux collaborateurs de téléphoner comme s'ils le faisaient depuis leur poste fixe d'entreprise : avec le même numéro unique, en ayant accès à l'annuaire d'entreprise et en utilisant simplement un micro et un casque.

6) S'appuyer sur le travail collaboratif

S'appuyer sur une plateforme de travail collaboratif (workflow, agenda partagé, gestion électronique de document, etc) apporte plus de confort aux collaborateurs. Cette solution leur offre un partage instantané, un accès direct aux modifications en cours, un échange facilité et donc une meilleure harmonisation entre les différents interlocuteurs d'une même équipe, d'un même projet, etc.

7) Migrer des logiciels en mode SaaS

Migrer les logiciels d'entreprise vers un mode SaaS, contribue à la mobilité des collaborateurs puisqu'ils y accèdent via Internet et depuis n'importe quel endroit et n'importe quel device/support.

8) Créer des réunions virtuelles avec la webconférence

Enfin, se servir d'un outil de Webconférence ou de visioconférence est très courant pour créer une salle de réunion virtuelle où les collaborateurs peuvent se retrouver visuellement, communiquer mais aussi partager des données en temps réel comme s'ils étaient assis autour de la même table.

De manière générale ces outils d'information et de communication sont accessibles à partir d'une simple connexion internet et permettent de travailler à distance, sans qu'il n'y ait d'impact sur la qualité du travail réalisé. Toutes ces solutions sont à la portée des entreprises pour mettre en place le télétravail, qui permet une certaine autonomie et liberté pour les salariés, mais aussi un gain financier pour les dirigeants. En effet, ils voient leurs coûts de transports, de location d'espace de travail ou encore d'entretien se réduire. Qu'attendez-vous pour passer au télétravail ?

*Baromètre de l'innovation de mars 2015, réalisé par Odoxa pour le Syntec Numérique en partenariat avec L'Usine Digitale
**Chiffre étude Regus 2014.

DOCUMENT 2

« Le travail nomade exige de repenser en profondeur la sécurisation des données des entreprises »

Alexandre Grellier - *lesechos.fr* - 9 Janvier 2019

Les nouveaux modes de travail exposent les données

Un quart des salariés français ont aujourd'hui recours au télétravail et 42 % des cadres disent le pratiquer de façon informelle (enquête IFOP, novembre 2017). Les Français et leurs employeurs accordent de plus en plus d'importance pour ce mode de travail qui augmenterait la productivité grâce au "mieux-être" au travail (moins de temps de transport, moins de stress, management plus flexible, confiance réaffirmée, etc.). Avec les ordonnances réformant le Code du travail, le dispositif a d'ailleurs été assoupli afin de permettre au plus grand nombre d'en bénéficier.

À l'ère du salarié nomade, marquée par une mobilité plus importante, le risque en matière de fuites de données confidentielles s'est fortement accru. Les données sont plus accessibles, peuvent être plus facilement vues par des tiers lors des déplacements en train par exemple, sans parler de la perte ou du vol d'un ordinateur ou d'une clé USB, etc.

L'enjeu pour les directions informatiques des entreprises est ainsi de sécuriser au maximum leurs données confidentielles.

Une stratégie de sécurité à mettre en place et à faire connaître à tous les collaborateurs

Mis en place depuis plus de 6 mois maintenant, le Règlement Général sur la Protection des Données a largement incité les entreprises à davantage s'assurer de la protection de leurs applications et de leurs données, sous peine de se voir exposées à des amendes. Toutefois, les erreurs humaines sont bel et bien le premier risque de mise en péril des systèmes d'accès aux données.

Et il convient de souligner qu'une prise de conscience est désormais nécessaire de la part des dirigeants et du haut management. En effet, moins d'une entreprise française sur cinq a mis en œuvre des mesures de protection (baromètre IPSOS – octobre 2018). Pour autant, 84 % des entreprises françaises déclarent avoir été victimes d'attaques (rapport annuel Cisco Sécurité 2018).

Avec un binôme faisant le lien entre télétravail et stratégies de sécurité, les services informatiques et les directions des ressources humaines sont naturellement impliqués pour mettre en œuvre un cadre de référence. La priorité revient aux solutions qui permettent de crypter les données et de les rendre inaccessibles par des tiers, notamment en cas de perte ou de vol, aux utilitaires de cryptage ou de masquage, ou encore aux datarooms électroniques.

Une fois ces processus mis en place, il conviendra de s'assurer de leur partage auprès de l'ensemble des collaborateurs et surtout de leur adhésion et de leur formation en matière de protection des données.

Privilégier les solutions en mode cloud

Allié à la bonne utilisation de la part des collaborateurs en entreprise et au respect du cadre fixé, le Cloud présente aujourd'hui les meilleures garanties pour un réseau ouvert et accessible en matière de besoins de nomadisme des postes de travail et de protection des données. Le Cloud propose des performances plus intéressantes en matière de sécurisation de la data que les terminaux physiques. Les fournisseurs mettent à disposition des infrastructures ultra-poussées, testées et éprouvées, ainsi que des moyens humains dont de nombreuses entreprises – et notamment les PME et ETI, ne peuvent pas disposer. Les solutions qu'ils proposent permettent une gestion des permissions des utilisateurs en temps réel permettant d'agir immédiatement en cas de fuite.

D’autres outils existent comme l’accessibilité horaire et géographique des documents marqués par filigrane pour éviter toutes copies d’écrans frauduleuses, un double contrôle par code et SMS, ou encore un mot de passe qui ne peut plus s’enregistrer automatiquement.

De plus en plus, les responsables de sécurité envisagent des solutions de virtualisation du poste de travail (environnements étanches) ou encore de cryptage des données avec la technologie Blockchain.

Lors de la sélection d'un fournisseur, les entreprises doivent s'assurer qu'elles choisissent des éditeurs de solutions cloud qui peuvent indiquer à leurs clients où se trouvent les données qu'ils traitent et stockent. Il existe de nombreuses raisons de privilégier des fournisseurs de Cloud européens. Aujourd’hui, par exemple, en faisant le choix de fournisseurs basés aux États-Unis (même s’ils disposent de datacenters en Europe), toute donnée pourra être transférée outre-Atlantique puisque ces prestataires adhèrent, à la différence de leurs homologues européens, à l'US Privacy Shield, aux BCR ou encore aux Model Clauses. En outre, le Cloud Act, mis en place depuis 2018, vise à faciliter l'accès par les autorités américaines aux données stockées à l'étranger par des entreprises américaines dans le cadre de procédures judiciaires.

Dernier point important : pour renforcer l'efficacité des mesures de sécurité mises en place par le fournisseur choisi, il est indispensable d'exécuter une stratégie cloud fiable, intégrant des autorisations et des paramètres appropriés pour tous les utilisateurs. En effet, d'après Gartner : "jusqu'en 2022, au moins 95 % des défaillances de la sécurité du cloud seront provoquées par des erreurs des clients".

Utiliser intelligemment l’intelligence artificielle

L’intelligence artificielle progresse sur tous les fronts avec aujourd’hui un besoin majeur en compétences. Si elle ne peut pas être l’unique solution en matière de sécurisation des données, elle offre une très grande efficacité d’analyse, en raison de sa forte réactivité. Par exemple, avec des solutions qui intègrent le deep machine learning, les responsables de sécurité peuvent être désormais automatiquement prévenus de comportements inhabituels ou suspects pour agir en conséquence. Nombreux sont les éditeurs à travailler sur le sujet.

DOCUMENT 3

« Ce que le Cloud apporte aux travailleurs nomades »

Colin Steele - *lemagit.fr* - avril 2019

Synchronisation et partage de fichiers d'entreprise

Les services d'EFSS ont émergé du marché grand public. Les utilisateurs se sont tournés vers le cloud public pour trouver un endroit où stocker des fichiers, y accéder à partir de plusieurs appareils et les partager sans avoir à traiter avec des pièces jointes encombrantes. Au fur et à mesure que de plus en plus de gens apportaient leurs terminaux mobiles au travail, ils ont commencé à stocker des données d'entreprise dans ces services sans aucune surveillance.

Les EFSS visent à fournir le même niveau de fonctionnalités conviviales ainsi que des fonctions d'administration et de sécurisation. La plupart de ses services offrent une application mobile et une interface Web grâce auxquelles les utilisateurs peuvent télécharger des fichiers, les partager avec d'autres et les ouvrir avec des applications bureautiques compatibles, telles que Microsoft Word.

Cette approche ouvre l'accès aux données de l'entreprise à une plus grande variété d'appareils. Bien sûr, plus d'accès signifie plus de préoccupations en matière de sécurité. Les services de partage et de synchronisation d'entreprise permettent aux services informatiques de contrôler les droits de partage des utilisateurs et de suivre l'accès à des fichiers spécifiques. Et certains fournisseurs offrent une version sur site ou en cloud privé pour plus de tranquillité d'esprit.

Backend mobile en mode service

Les EFSS sont pertinents pour l'accès à des fichiers. Mais lorsqu'une application mobile a besoin d'accéder régulièrement à de grandes quantités de données d'entreprise, il peut être préférable de recourir à un service de backend mobile (MBaaS) pour intégrer cet accès directement dans une application.

Traditionnellement, il est complexe de développer une application mobile native qui se connecte à un système de backend. Cela nécessite un important travail de développement manuel, et tout changement au niveau du backend peut conduire à d'importantes adaptations. Et les développeurs doivent faire face à ces problèmes pour chaque système auquel une application doit accéder.

Le MBaaS vise à simplifier le processus. Il déporte l'infrastructure backend et présente une interface unique et unifiée dans le cloud. Les développeurs connectent ensuite leurs applications au MBaaS à l'aide d'API et de kits de développement logiciel ; le service gère les connexions aux composants de l'infrastructure souhaitée.

Virtualisation des postes de travail et des applications

La virtualisation et la mobilité ont une relation complexe. D'une part, l'exécution de postes de travail et d'applications Windows dans un centre de calcul et leur présentation sur des terminaux mobiles constitue un moyen relativement simple d'apporter des logiciels patrimoniaux sur des terminaux modernes.

Mais Windows est conçu pour un clavier et une souris… avec un écran tactile, l'expérience utilisateur n'est généralement pas exactement satisfaisante. Et il convient de ne pas oublier le coût et la complexité souvent associés au VDI.

Mais là encore, le nuage est apparu comme une alternative viable. Le VDI en mode Cloud, ou DaaS, permet aux entreprises de profiter des avantages d'une infrastructure de postes de travail

virtuels, tandis qu'un tiers gère l'infrastructure sous-jacente. De même, les applications en mode service permettent aux utilisateurs d'accéder à des applications virtuelles individuelles via le cloud.

L'avenir du cloud mobile

Il n'y a pas une seule bonne façon d'utiliser le cloud pour répondre aux besoins des collaborateurs mobiles. De nombreuses entreprises s'appuient sur une combinaison d'EFSS, d'applications mobiles natives, de postes de travail virtualisés et d'applications en mode service, et plus encore.

Pour s'adapter à cette diversité, les spécialistes l'informatique des utilisateurs finaux offrent désormais des suites d'espaces de travail – des ensembles de technologies qui offrent aux collaborateurs un point d’accès unique à toutes leurs applications et données, à partir de n'importe quel appareil.

DOCUMENT 4

« Guide ANSSI - Recommandations sur le nomadisme numérique » (Extrait)
ANSSI - octobre 2018

2.3 Risques

Le lieu de connexion du travailleur nomade peut présenter des niveaux de sécurité variables selon l'environnement.

Cela dépend non seulement de la protection physique et logique du lieu (contrôle d'accès par badge, surveillance), mais également du fait que les locaux sont partagés ou non entre plusieurs entités. Un des cas les plus sensibles est celui où l'utilisateur travaille depuis un espace complètement ouvert au public (cafétéria, bibliothèque, etc.).

De même, le domicile à partir duquel un utilisateur fait du télétravail est à considérer comme un lieu non maîtrisé, car il est très difficile d'évaluer de façon pérenne l'environnement du point de vue de la sécurité.

Ainsi, la principale caractéristique du nomadisme est le degré d'exposition de l'information, en raison de la localisation de l'utilisateur dans des lieux n'ayant pas les moyens de protection physique habituellement mis en œuvre dans les locaux de l'entité. C'est le cas par exemple :

- lorsque l'on travaille à l'hôtel pendant un déplacement professionnel ;
- pendant le trajet domicile-travail, dans les transports en commun ;
- lorsque l'on travaille dans des salles d'attentes ou tout autre lieu public ;
- lorsque l'on se connecte depuis un espace de *co-working*.

Dans tous ces lieux de travail non maîtrisés par l'entité, les risques suivants sont exacerbés :

- la perte ou vol de matériel ;
- la compromission du matériel, par exemple pendant une absence temporaire de l'utilisateur ;
- la compromission des informations contenues dans le matériel volé, perdu ou emprunté ;
- l'accès illégitime au SI de l'entité (et donc la compromission de celui-ci) ;
- l'interception voire altération des informations (perte de confidentialité et/ou d'intégrité).

Ainsi, il est considéré que le lieu de travail d'un utilisateur nomade peut difficilement apporter des garanties de sécurité suffisantes par rapport au besoin de protection des informations auxquelles l'utilisateur a accès lors de son activité professionnelle nomade.

Objectif

L'objectif d'un SI nomadisme est de réussir à tendre vers un niveau de sécurité le plus proche possible de celui du SI interne de l'entité, en répondant aux risques d'exposition plus forts listés ci-dessus.

Des mesures spécifiques au nomadisme et au télétravail doivent être définies dans la PSSI de l'entité concernée.

R1

Intégrer le nomadisme dans la PSSI de l'entité

L'entité doit mettre à jour sa PSSI, c'est-à-dire redéfinir les objectifs de sécurité à atteindre, les acteurs concernés ainsi que les moyens mis en œuvre pour accomplir la cible de sécurité de son SI nomadisme.

Une fois les différents risques liés au nomadisme évoqués, le chapitre suivant aborde les différents éléments qui composent la chaîne de connexion nomade, et les mesures de sécurité permettant de réduire ou de couvrir ces risques.

3
Architecture

3.1 Architecture globale

La figure 3.1 présente de façon macroscopique les éléments qui composent un SI nomadisme :

- l'utilisateur nomade ;
- l'équipement d'accès (ou poste de travail) ;
- le canal d'interconnexion ;
- la passerelle d'interconnexion ;
- les ressources accessibles par les équipements nomades dans le SI interne de l'entité.

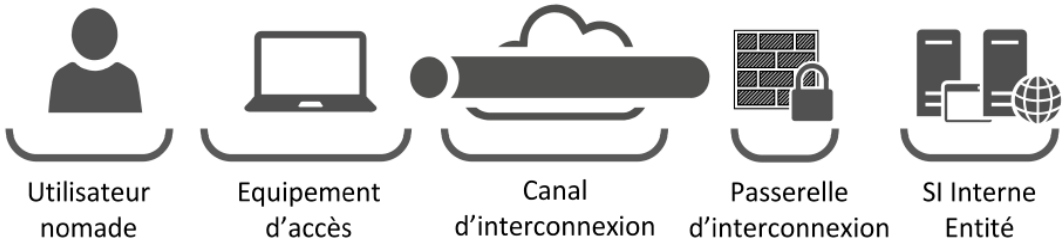


FIGURE 3.1 – Architecture globale du SI nomadisme

Dans une démarche de défense en profondeur, chaque élément doit mettre en œuvre des mécanismes de protection afin de réduire les risques d'attaques potentielles. Les sections suivantes présentent les mesures spécifiques à chaque élément, puis le chapitre suivant présente les mesures générales qui s'appliquent à l'ensemble.

3.2 Utilisateur nomade

3.2.1 Inventaire

Certaines catégories d'utilisateurs, ou bien certaines applications, du fait de leur sensibilité, doivent être exclues du périmètre du nomadisme.

R2

Réaliser l'inventaire des activités des utilisateurs compatibles avec le nomadisme

Il est important d'identifier quels sont les métiers qui sont éligibles au nomadisme et au télétravail. Le travail en dehors des locaux de l'entité peut être interdit par exemple pour les raisons suivantes :

- parce que le niveau de sensibilité des données ou de l'activité est trop élevé ;
- pour des contraintes réglementaires ;
- parce qu'il existe des restrictions liées au métier (utilisation de matériel spécifique par exemple).

Il est important de bien tenir à jour la liste des utilisateurs nomades, comme cela doit être fait pour la gestion en général des utilisateurs de l'entité. Il faut surveiller le statut des utilisateurs nomades, et notamment s'assurer que dans le cas d'un changement de fonction, ils n'exercent pas ensuite une activité incompatible avec le nomadisme numérique.

De même, il est possible de catégoriser les utilisateurs nomades en fonction du niveau de risque auquel ils sont exposés, et d'appliquer des règles spécifiques selon cette catégorisation (accès restreint, etc.). Par exemple, cela peut tenir compte de la localisation géographique de l'utilisateur nomade, lors de ses déplacements professionnels.

R3

Maîtriser la gestion des utilisateurs nomades

Il faut documenter et mettre en place des procédures pour gérer correctement les changements dans le groupe d'utilisateurs nomades. Il faut définir au minimum des procédures pour les arrivées, les mutations et les départs des utilisateurs. Celles-ci doivent être formalisées, validées et appliquées strictement. Elles concernent notamment :

- la gestion et la révocation des comptes et des droits d'accès au SI nomadisme ;
- le changement de catégorie de l'utilisateur nomade ;
- la gestion des équipements mobiles nomades.

3.2.2 Sensibilisation

Le comportement de l'utilisateur nomade est susceptible de provoquer des situations à risques, favorisant, par exemple :

- le vol ou la compromission de matériel et d'informations ;

- des indiscrétions et fuites d'informations.

Il est donc indispensable de mettre en place des campagnes de sensibilisation spécifiques pour tous les futurs utilisateurs nomades, afin que ceux-ci soient bien conscients des risques liés à ce mode de travail particulier.

R4

Sensibiliser et former les utilisateurs nomades

Les utilisateurs doivent suivre des formations à la sécurité numérique. Ils doivent maîtriser parfaitement les outils, connaître les risques et les comportements à adopter en fonction de leur lieu de travail et des circonstances. La charte informatique de l'entité doit également intégrer les règles d'usage liées au nomadisme.

3.2.3 Lien avec l'équipement d'accès

Dans un contexte d'utilisation nomade, il est fréquent que les équipements d'accès soient partagés entre plusieurs utilisateurs, si ces équipements ne sont utilisés que de façon ponctuelle par exemple. Cependant, chaque utilisateur nomade doit être identifié et authentifié lorsqu'il se connecte au SI de l'entité.

Le partage d'un poste de travail rend la tâche de supervision plus compliquée pour les administrateurs, et pose également un problème de confidentialité entre les utilisateurs qui partagent le poste, pour les données présentes localement sur celui-ci. Ainsi, il est fortement déconseillé de mettre en place des postes ou des comptes partagés pour la pratique du nomadisme.

R5

Dédier l'équipement d'accès à un utilisateur nomade identifié

Chaque équipement doit être lié à un utilisateur nomade. L'utilisateur doit être identifié et référencé dans le système de gestion d'équipements de l'entité.

Cependant si l'utilisation de postes partagés est nécessaire au bon fonctionnement de l'entité, alors il est important de mener une analyse de risques, et de prendre des mesures compensatoires, pour éviter principalement qu'un utilisateur ne puisse accéder aux données d'un autre utilisateur en partageant le même poste.

L'annexe B présente quelques-unes de ces mesures.

R5 -

Sécuriser la mise en place de postes nomades partagés

Si le partage des équipements d'accès nomades est une fonctionnalité retenue, il est important de mettre en œuvre des mesures de sécurité complémentaires pour s'assurer d'un cloisonnement entre les utilisateurs partageant le même poste de travail nomade.

3.3 Équipement d'accès

3.3.1 Maîtrise du poste

L'équipement d'accès de l'utilisateur nomade peut être entre autres :

- un poste de travail portable ;
- un mobile multifonction (ou *smartphone*) ;
- une tablette.

Toutes les recommandations suivantes s'appliquent pour tout type de matériel fourni à l'utilisateur, et quel que soit le système d'exploitation présent sur cet équipement d'accès.

Il est important de bien considérer que la connexion depuis l'extérieur au SI de l'entité ne se fait pas forcément depuis le même équipement que l'on utilise quand on travaille en interne dans les locaux de l'entité. Un utilisateur réalisant ses tâches sur un poste bureautique fixe à l'intérieur de l'entité peut utiliser une tablette lorsqu'il se déplace à l'extérieur, chez des clients par exemple.

Il est nécessaire de maîtriser complètement l'ensemble des équipements sur lesquels les utilisateurs nomades se connectent.

L'utilisation d'équipements personnels par l'utilisateur (AVEC [3] en français ou *BYOD* [4] en anglais) pour se connecter au SI de l'entité est donc à proscrire. Cela est justifié entre autres pour les raisons suivantes :

- l'impossibilité de garantir le niveau de sécurité de l'équipement personnel ;
- la multiplication des environnements utilisateur, qui rend la gestion du cycle de vie des applications difficile (navigateurs Web, interfaces homme-machine, etc.) ;
- la complexité de l'investigation en cas d'incidents.

Certains équipements permettent de mettre en œuvre un système de conteneur sécurisé et cloisonné, destiné à l'usage professionnel. À titre d'exemple, *Samsung Knox*, *Blackberry Dynamics*, ou bien les conteneurs configurables dans les solutions de *MDM* [5] tels *AirWatch* ou *MobileIron* proposent cette fonction de sécurité sur les appareils mobiles.

Cependant, même si le conteneur professionnel dispose de fonctions de cloisonnement logique ou physique, et de chiffrement du conteneur, son utilisation reste partagée avec un système d'exploitation qui n'est pas protégé.

Si l'entité fait le choix d'utiliser ce système, elle doit donc impérativement maîtriser l'ensemble de l'équipement, c'est-à-dire le conteneur dédié à l'usage professionnel, mais également la partie du système qui n'est pas protégée. En particulier, il est important que l'utilisateur ne puisse pas être en mesure d'installer n'importe quelle application présente dans les magasins (ou *store*) publics

3. Apportez votre équipement personnel de communication.
4. *Bring your own device.*
5. *Mobile device management.*

sur les systèmes protégé et non protégé. Des restrictions d'usage doivent donc être mises en place, avec un outil de MDM par exemple.

De manière non exhaustive, il est possible de citer les mesures de restrictions suivantes :

- mettre en place un *store* privé d'entreprise et interdire l'installation manuelle d'applications ;
- désactiver les services qui ne sont pas nécessaires d'un point de vue métier et qui sont potentiellement sources de menaces, comme la géolocalisation, le Bluetooth, le *NFC*[6], etc. ;
- filtrer la navigation sur Internet.

R6

Maîtriser l'équipement d'accès de l'utilisateur nomade

Seuls les équipements d'accès gérés et configurés par les équipes informatiques de l'entité, ou un prestataire mandaté, doivent pouvoir être utilisés par les utilisateurs nomades. L'utilisation d'équipements personnels est à proscrire.

De même, l'usage d'équipements professionnels fournis par l'entité pour des besoins personnels est à proscrire, ou bien a minima à encadrer strictement. Dans tous les cas, il faut toujours considérer l'usage d'un équipement professionnel pour des besoins personnels comme dangereux et source de compromission, et ceci est d'autant plus important dans le cadre du nomadisme, du fait du degré d'exposition des équipements.

3.3.2 Protection physique

Dans le cadre du nomadisme, un attaquant est susceptible de faire acte d'indiscrétion sur l'écran de l'équipement, de piéger ou de voler du matériel appartenant à l'entité.

Particulièrement dans les environnements publics (transports en commun, cafétérias, etc.), il est hautement probable que l'affichage de l'équipement d'accès soit visible par l'entourage proche de l'utilisateur nomade.

Il est donc nécessaire de protéger physiquement l'équipement d'accès lorsque le contexte d'utilisation l'exige.

R7

Mettre en œuvre des moyens de protection physique de l'équipement d'accès nomade

L'entité doit mettre à disposition les moyens suivants pour protéger les équipements d'accès :

- un filtre écran de confidentialité (pour les postes de travail, mais aussi pour les tablettes ou mobiles multifonction) ;
- des scellés pour identifier une éventuelle compromission matérielle ;
- des verrous de ports USB et RJ45 si nécessaire ;
- éventuellement un câble antivol.

6. *Near Field Communication*.

DOCUMENT 5

« Télétravail et RGPD : comment éviter la faille de sécurité ? »

Me Pierre-Randolph Dufau - *itforbusiness.fr* - février 2019

Les faits : L'ordonnance dite « Macron », entrée en vigueur le 22 septembre 2017, a assoupli les conditions permettant de recourir au télétravail. Pour que ce mode d'organisation ne devienne pas le maillon faible de la protection des données à caractère personnel en entreprise, il convient de s'assurer que les conditions de sa mise en oeuvre respectent les dispositions du RGPD, notamment en matière de sécurité des données.

Eu égard à ses nombreux avantages, les entreprises ont de plus en plus recours au télétravail. Toutefois, le maniement des données professionnelles par les salariés par le biais d'un accès à distance aux outils et systèmes informatiques de l'entreprise n'est pas sans risque en termes d'atteinte à leur sécurité.

Il est donc nécessaire, à la lumière des dispositions du RGPD, de prévoir des mesures spécifiques et adaptées tant à l'activité de l'entreprise qu'à l'organisation du travail de ses salariés. Ainsi, à première vue et de façon évidente, afin de se prémunir du vol ou de la tentative de connexion malintentionnée, l'accès à la session informatique du salarié se doit d'être protégé par un mot de passe complexe et le renouvellement des identifiants en cas d'erreur répétée. Outre l'accès physique, le risque d'intrusion aux systèmes d'informations est également bien souvent imperceptible, par le biais de piratage, virus ou malwares, contre lesquels un certain nombre de mesures simples comme l'activation de pare-feu ou le cryptage d'une partie des données échangées entre les salariés et ses interlocuteurs s'avèrent là aussi efficaces.

Mais la stratégie de sécurité ne se limite pas à des mesures techniques. Le RGPD impose en effet désormais la formalisation de processus internes rigoureux destinés tant à prévenir les failles de sécurité qu'à les traiter efficacement en cas de violation et ainsi sensibiliser les salariés susceptibles, par méconnaissance des risques, de mettre en péril la sécurité des données. La Cnil préconise à ce titre d'édicter des règles de bonne conduite, au sein de la charte informatique de l'entreprise par exemple, notamment relatives à l'impérieuse nécessité pour le salarié de révéler toute faille de sécurité intervenue dans le cadre du télétravail, ou invitant à la prudence lors du téléchargement de nouveaux logiciels ou la connexion à de nouveaux supports mobiles, comme le chargement d'un téléphone étranger sur son ordinateur.

Pour s'assurer du caractère effectif et contraignant de ces dispositions organisationnelles internes, il est conseillé de contractualiser un certain nombre de pratiques, mais également de prévoir des sanctions tant disciplinaires que pénales à l'encontre des salariés qui, bien que correctement formés à l'importance des enjeux sécuritaires, viendraient à compromettre la sécurité de certaines données. De son côté, l'entreprise doit s'assurer, en cas d'incident, de pouvoir identifier rapidement les données qui ont été exposées et les risques sur la vie privée des personnes concernées. En cas de risque élevé, il est impératif de notifier à la CNIL et aux personnes concernées la violation intervenue, dans les 72 heures après sa découverte.

Ce qu'il faut retenir :

Le télétravail peut s'avérer dommageable pour l'entreprise en matière de protection des données personnelles en l'absence de mesures de sécurité adaptées. Au-delà des mesures techniques élémentaires visant à éviter l'interception de données ou toute intrusion malveillante, l'entreprise doit s'assurer de la parfaite sensibilisation de ses salariés à ces questions et avoir formalisé à ce titre un processus organisationnel adéquat.

DOCUMENT 6

« Le télétravail dans les trois versants de la fonction publique - Bilan du déploiement » (Extrait)

Ministère de l'action et des comptes publics - décembre 2018

Le télétravail dans les trois versants de la fonction publique

La loi n° 2012-347 du 12 mars 2012 ainsi que le décret n° 2016-151 du 11 février 2016 encadrent la possibilité, pour les agents publics civils et les magistrats, d'exercer leurs fonctions en télétravail.
En mars 2018, on comptait 4,65 % d'agents en télétravail pour l'administration territoriale de l'État et en moyenne 3,5 % pour l'administration centrale.
Au-delà des chiffres, le bilan réalisé par la DGAFP met en évidence les actions menées par les services les plus engagés dans le déploiement du télétravail.
En identifiant les obstacles rencontrés et les conditions de réussite, il met en lumière les impacts du télétravail sur les organisations de travail et souligne les facteurs clés du déploiement de cette modalité de travail à distance.

2.3.5 Les conditions matérielles d'exercice du télétravail

L'article 2 du décret prévoit que 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.

Quand le lieu d'exercice est le domicile de l'agent, ce qui est le cas à 95 %, celui-ci doit répondre à plusieurs exigences :

- conformité de l'installation électrique du poste de travail : certificat de conformité ou attestation sur l'honneur ;
- attestation de conformité du domicile à l'exercice du télétravail : couverture du risque incendie, connexion internet haut débit adapté aux besoins professionnels de l'agent, conditions d'ergonomie suffisantes ;
- enfin l'agent doit pouvoir rejoindre son lieu d'affectation (à ses frais) en cas de nécessité de service y compris si le lieu de télétravail est éloigné du lieu d'affectation.

Les règles de gestion varient fortement selon les administrations : certaines administrations demandent des certificats de conformité aux installations électriques, d'autres se contentent d'attestations sur l'honneur. Certaines administrations autorisent le télétravail après avoir vérifié (par photos) l'espace dédié de l'agent au télétravail, d'autres n'exigent qu'une attestation sur l'honneur.

Certains ministères, dans leur note de gestion, fournissent des conseils ergonomiques d'installation du poste de travail :

(extrait de l'instruction du 11 août 2016 du ministère de l'Agriculture sur les modalités pratiques de mise en œuvre du télétravail).

Les actes déclinant les règles de gestion ont précisé différemment les dispositions de l'article 2 du décret.

En général, il est précisé qu'au-delà du domicile de l'agent, le télétravail peut s'exercer dans tout bâtiment de l'État, d'un établissement public, d'une collectivité territoriale ou d'un organisme privé dédié mis à disposition à cet effet et dès lors qu'il est situé à proximité du domicile de l'agent.

Mais certains arrêtés ministériels ont exclu toute possibilité pour l'agent d'exercer dans un autre lieu que le domicile ou l'autorisent de façon exceptionnelle. C'est ainsi le cas de l'arrêté ministériel pour les services du Conseil d'État et des juridictions financières : « *le télétravail s'exerce au domicile principal de l'agent dont l'adresse est précisée dans la décision individuelle d'autorisation des fonctions en télétravail* » ainsi que de l'arrêté ministériel du Ministère des Affaires étrangères : « *sauf exception dûment motivée et autorisée, le télétravail est effectué au domicile de l'agent* ».

L'arrêté ministériel pour les agents d'administration centrale des services du Premier Ministre autorise le télétravail dans un télécentre public agréé ce qui exclut de fait les espaces privés de coworking.

Concernant les exigences en matière de conditions matérielles d'exercice, certaines des structures rencontrées ne demandent pas d'attestations, considérant que les pratiques de télétravail à distance ne peuvent pas, par nature, être identiques aux conditions de travail en présentiel et qu'il est illusoire de transposer le bureau à domicile (que ce soit en matière de temps de travail ou d'espace de travail).

Les actes de déclinaison exigent seulement que les locaux dédiés au télétravail soient couverts par une assurance habitation permettant l'exercice du télétravail.

Des questions d'agents télétravailleurs ont été transmises à la DGAFP concernant les pratiques de certaines compagnies d'assurances qui imposent un surcoût lorsqu'il s'agit de mentionner l'exercice du télétravail dans l'assurance multirisque habitation. Ce point doit être expertisé.

2.3.6 La prise en compte des coûts

Dans les négociations des chartes locales pour définir les modalités de mise en œuvre du télétravail, les organisations syndicales ont régulièrement demandé à ce que les coûts supplémentaires liés à la conformité

2 Bilan de la mission

du domicile soient pris en compte par l'administration (coûts d'assurance, de mobilier, de chauffage et d'électricité).

Quasiment aucun employeur n'est allé au-delà de ce que prévoit le décret : « *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* ».

2.3.7 Télétravail et immobilier

La plupart des administrations mette à disposition des agents télétravailleurs un équipement informatique mobile à double usage, mobile et bureau sur une station fixe permettant de s'y rattacher. Aucune administration n'est allée jusqu'ici à remettre en cause la personnalisation des bureaux avec un réaménagement des espaces permettant de répondre à différents usages au travail comme l'ont fait un certain nombre d'entreprises privées.

Une expérimentation du schéma directeur régional immobilier (SDIR) en Occitanie sur l'impact du télétravail sur l'organisation immobilière de l'État montre que le télétravail :

- remet en cause le modèle du bureau traditionnel qui, avec un taux d'occupation moyen de moins de 45 % peut apparaître comme une aberration financière et écologique ;
- contraint à repenser l'organisation du travail mais aussi le lieu de travail qui ne peut plus se résumer à un tout bureau individuel et qui prend des formes variées avec des usages multiples.

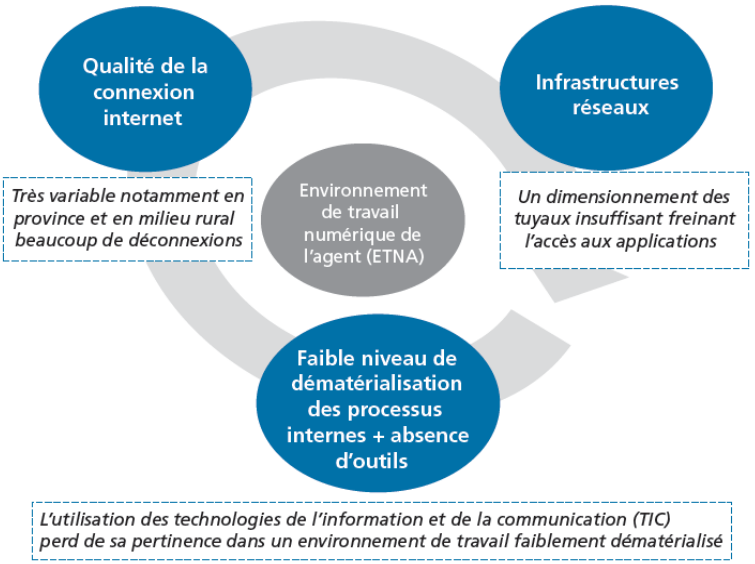
L'innovation déployée en Occitanie transforme le bureau en un « hub de rencontres et d'échanges intensifs » avec le domicile ou des espaces dédiés privés pour se concentrer et éviter les déplacements, des tiers lieux de travail qui ont pour ambition d'offrir un nouveau lien social avec son éco système professionnel et un lieu de passage idéal en situation de mobilité.

2.3.8 Les équipements informatiques

C'est un élément déterminant pour la mise en œuvre du télétravail. La majorité des structures équipe les agents d'ordinateurs portables munis de clés pour assurer l'accès aux applications métiers et parfois de téléphone portable uniquement vocal, le reste étant à la charge de l'agent (abonnement internet, électricité,…).

En moyenne, le coût d'équipement est de 1 000 euros, pris en charge par l'employeur, à l'exception de l'abonnement internet. C'est dans ce domaine que les agents rencontrent le plus de difficultés.

De façon schématique, trois types de difficultés sont à prendre en considération :



C'est donc l'environnement numérique de travail de l'agent qu'il faut reconsidérer lors du déploiement des dispositifs de télétravail. Il conviendrait d'associer plus étroitement les directions des systèmes d'information dès la phase avant-projet car on a là des pré-requis indispensables.

2.3.9 La sécurité des données

Lors de la mise en place du télétravail, la sécurité des données constitue un enjeu majeur pour les administrations qui traitent des données sensibles et confidentielles. Cet enjeu est encore plus sensible avec l'entrée vigueur le 25 mai 2018 du règlement général de protection des données (RGPD) et les risques potentiellement encourus par les administrations qui ne s'y conformeraient pas. Il appartient ainsi à la direction des systèmes d'information de veiller à ce que le réseau utilisé par l'agent en télétravail soit sécurisé (via le VPN par exemple).

Les chartes collectives ou protocole d'accord prévoient également une information complète de l'agent sur les différents points liés à la sécurité des données comme par exemple la confidentialité des informations traitées dans le cadre de ses activités, la protection des données de son administration ou encore les risques potentiels d'intrusion au domicile de l'agent.

La note de gestion du 28 novembre 2016 relative aux conditions de mise en œuvre du télétravail au ministère de l'environnement, de l'énergie et de la mer, du logement et de l'habitat durable rappelle les incompatibilités définies dans l'arrêté du 21 juillet 2016 :

- *« en ce qui concerne les données à caractère sensible, il s'agit de données numériques qui font l'objet de restrictions d'utilisation ou d'accès en dehors des locaux de l'administration ou qui nécessitent des conditions de manipulation incompatibles avec un travail externalisé ;*
- *les activités comportant l'accomplissement de travaux nécessitant l'utilisation de logiciels ou applications font l'objet de restrictions d'utilisation à distance.*

Pour exercer leur mission en télétravail, les agents concernés disposent des moyens matériels et logiciels alloués par le ministère et accèdent aux systèmes d'information "métiers" via une connexion sécurisée au réseau du ministère (accès dit "VPN"). Par défaut, toutes les applications sécurisées par le portail d'authentification sont accessibles aux télétravailleurs dans les mêmes conditions que sur leur lieu de travail. Toutefois, l'environnement dans lequel se trouve le télétravailleur peut ne pas présenter les mêmes garanties de confidentialité que celles mises en place sur le lieu de travail pour assurer l'instruction et la gestion des dossiers à caractère sensible (dossiers de personnel, par exemple). Dans ce cas, l'utilisation à distance de certaines applications "métiers" pourrait être proscrite ».

Néanmoins, compte tenu des difficultés d'accès à certaines applications métiers et/ou au poste de travail à distance, certaines pratiques de contournement évoquées par les agents risquent de mettre à mal le dispositif de sécurité à distance prévue par les directions des systèmes d'information.

Il s'agit par exemple d'enregistrement de dossiers sur une clé USB, de la transmission de ces dossiers par courriel, de l'utilisation de poste personnel, ou encore du transport à domicile des dossiers papier avec des données à caractère personnel.

L'impact du RGPD sur le télétravail

Avec le RGPD, il s'agit de faire face aux abus d'utilisation des données personnelles des ressortissants européens. Cela interroge le mode de collecte des données personnelles, le type de traitement effectué notamment par les agents télétravailleurs et les procédures techniques et organisationnelles mises en place par la direction des systèmes d'information (DSI) pour sécuriser les données.

Le télétravail (à domicile ou nomade), de par les stratégies de contournement qu'il induit du fait de difficultés informatiques rencontrées par les agents télétravailleurs, est-il de nature à fragiliser les systèmes de sécurité compte tenu des contraintes qui pèsent dorénavant sur toutes les structures collectant et traitant des données personnelles ?

.../...

DOCUMENT 7

« BYOD : quelles sont les bonnes pratiques ? »

Cnil.fr - février 2019

Avec le développement du BYOD, la frontière entre vie professionnelle et personnelle s'efface. La CNIL rappelle les bonnes pratiques permettant de concilier sécurité des données de l'entreprise et protection de la vie privée du salarié connecté.

Qu'est-ce que le « *Bring Your Own Device* » (BYOD) ?

L'acronyme « BYOD » est l'abréviation de l'expression anglaise « *Bring Your Own Device* » (en français : « Apportez Votre Equipement personnel de Communication » ou AVEC), qui désigne l'usage d'équipements informatiques personnels dans un contexte professionnel.

Il peut s'agir par exemple d'un salarié qui, pour se connecter au réseau de l'entreprise, utilise un ordinateur, une tablette ou son *smartphone* personnel.

Les outils personnels ne peuvent être utilisés qu'à titre subsidiaire dans un cadre professionnel

Le droit du travail impose à l'employeur de fournir à ses employés les moyens nécessaires à l'exécution de leurs tâches professionnelles.

L'utilisation d'outils informatiques personnels à des fins professionnelles ne permet pas de s'affranchir de cette obligation.

Quelles mesures prévoir pour la sécurité des données ?

L'employeur est responsable de la sécurité des données personnelles de son entreprise, y compris lorsqu'elles sont stockées sur des terminaux dont il n'a pas la maîtrise physique ou juridique, mais dont il a autorisé l'utilisation pour accéder aux ressources informatiques de l'entreprise.

Les risques contre lesquels il est indispensable de se prémunir vont de l'atteinte ponctuelle à la disponibilité, l'intégrité et la confidentialité des données, à la compromission générale du système d'information de l'entreprise (intrusion, virus, chevaux de Troie, *etc*.).

Comment réduire ces risques ?

1. identifier les risques, en tenant compte des spécificités du contexte (quels équipements, quelles applications, quelles données ?), et les estimer en termes de gravité et de vraisemblance.
2. déterminer les mesures à mettre en œuvre et les formaliser dans une politique de sécurité.

Par exemple :

- cloisonner les parties de l'outil personnel ayant vocation à être utilisées dans un cadre professionnel (création d'une « bulle de sécurité ») ;
- contrôler l'accès distant par un dispositif d'authentification robuste de l'utilisateur (si possible à l'aide d'un certificat électronique, d'une carte à puce, *etc*.) ;
- mettre en place des mesures de chiffrement des flux d'informations (VPN, HTTPS, *etc*.) ;
- prévoir une procédure en cas de panne/perte du terminal personnel (information de l'administrateur réseau, mise à disposition d'un équipement alternatif professionnel, effacement à distance des données professionnelles stockées sur le terminal personnel) ;
- exiger le respect de mesures de sécurité élémentaires telles que le verrouillage du terminal avec un mot de passe conforme aux bonnes pratiques et l'utilisation d'un antivirus à jour ;

- sensibiliser les utilisateurs aux risques, formaliser les responsabilités de chacun et préciser les précautions à prendre dans une charte ayant valeur contraignante ;
- subordonner l'utilisation des équipements personnels à une autorisation préalable de l'administrateur réseau et/ou de l'employeur.

Quelles garanties pour la vie privée ?

La sécurité du système d'information de l'entreprise doit être conciliée avec le respect de la vie privée des employés qui utilisent des équipements personnels dans le cadre de leur activité professionnelle. Par exemple, il n'est pas possible de prévoir des mesures de sécurité ayant pour objet ou effet d'entraver l'utilisation d'un *smartphone* dans un cadre privé, au motif que cet équipement peut être utilisé pour accéder aux ressources de l'entreprise (interdire la navigation sur internet, le téléchargement d'applications mobiles).

De telles restrictions pourraient difficilement être considérées comme justifiées par la nature de la tâche à accomplir et proportionnées au but recherché.

De la même manière, l'employeur ne peut accéder à des éléments relevant de la vie privée stockés dans l'espace personnel de l'équipement (liste des sites internet consultés, photos, films, agenda, annuaire).

Si l'employeur peut prévoir un effacement à distance de la partie du terminal personnel spécifiquement dédiée à l'accès distant aux ressources de l'entreprise, il ne peut en revanche s'arroger le droit d'effacer à distance l'ensemble des données présentes sur le terminal de l'employé.

Quelles formalités ?

Le BYOD n'est pas un « traitement de données à caractère personnel ». C'est un moyen technique particulier, sur lequel reposent des traitements. De ce fait, recourir au BYOD ne change pas les obligations auxquelles les traitements métiers sont soumis (inscription au registre et, le cas échéant, demande d'avis, demande d'autorisation, analyse d'impact relative à la protection des données, *etc*.).

DOCUMENT 8

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

William Culbert - *beyondtrust.com* - avril 2019

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.

DOCUMENT 9

« Zero Trust, la clé d'une transformation numérique réussie »

Xavier Daspre - *journaldunet.com* - mai 2018

La notion de "Zero Trust", modèle de sécurité dont le principe est de "vérifier et ne jamais faire confiance", permet aux entreprises de protéger leurs activités et d'accélérer leur développement.

La transformation numérique a des répercussions non négligeables sur l'exposition des entreprises aux attaques, mais aussi sur leurs architectures réseau et de sécurité. 70% des entreprises ont enregistré un incident de sécurité ayant eu des répercussions sur leurs activités au cours de l'année passée.

Selon un article de CBS Money, les usages des salariés ont changé et la surface d'exposition aux attaques dans l'entreprise s'est étendue. Les utilisateurs/terminaux et les applications/données sortent progressivement du périmètre de l'entreprise et de sa sphère de contrôle, ainsi plus de 67 % des salariés utilisent leurs terminaux personnels au travail. Ces changements des usages créent, sous l'impulsion de la transformation numérique, de nouveaux processus métier qui étendent, de ce fait, la surface d'exposition aux risques. La politique qui consiste à faire confiance tout en vérifiant n'est plus envisageable, avec l'apparition de menaces avancées qui s'infiltrent dans le périmètre de l'entreprise. Les périmètres classiques sont complexes, porteurs de risques et ne conviennent plus aux modèles économiques actuels. Il s'agit donc de repenser la structure même de l'entreprise par l'évolution de ses réseaux et le renforcement de sa sécurité.

Le périmètre classique de l'entreprise, un véritable frein à la transformation numérique

Le périmètre classique de l'entreprise dont fait partie la fameuse "zone démilitarisée" ou "DMZ", se compose souvent d'un assortiment de composants matériels et logiciels auxquels s'ajoutent de nombreux fournisseurs pour les accès, les systèmes de gestion d'identité (IAM), la diffusion, les performances et d'autres services. Pour des questions de redondance et de haute disponibilité, ce périmètre doit être reproduit afin de couvrir l'ensemble des zones et des centres de données. Si on multiplie ces déploiements par le nombre de sites de l'entreprise et la quantité de fournisseurs qui peuvent intervenir, on perçoit aisément le problème de complexité posé par ce type de périmètre. En effet, le périmètre classique ne répond pas aux deux principes inhérents au modèle "Zero Trust", qui sont à la fois de tout vérifier, n'accorder aucune confiance aux utilisateurs du réseau et également de limiter la diffusion des applications et des données aux seuls terminaux/utilisateurs authentifiés et autorisés au sein de l'entreprise.

Des risques humains et technologiques

Les entreprises qui ne prennent pas pleinement conscience de l'élargissement de leur périmètre s'exposent à la fois à des risques technologiques et humains.Technologiques car les terminaux présents sur le réseau de l'entreprise sont toujours plus nombreux et diversifiés alors que le périmètre réseau s'efface. Selon le cabinet d'études Gartner, le nombre de terminaux IoT installés devrait dépasser 20,4 milliards à l'horizon 2020. Les pirates du net développent toujours plus de nouveaux types d'attaques (credential stuffing, malwares, etc.) à mesure que s'étend le périmètre des entreprises. En effet, imaginons un malware qui se répande dans l'ensemble du réseau de l'entreprise et infecte à la fois l'équipement réseau, les smartphones et autres objets connectés. Les dommages sur les assets de la société seraient considérables. Humains, car le manque d'éducation à la cybersécurité des employés et la mobilité grandissante de ceux-ci sont des freins à la confiance à leur accorder au sein de l'entreprise. En effet, un terminal personnel utilisé dans l'espace de travail est amené à être utilisé à la fois dans les transports en communs, les espaces de loisirs (cinéma, restaurants,.) mais aussi lors de possibles sessions de télétravail dans des lieux partagés comme les cafés ou espaces de coworking par exemple.

Faire évoluer son réseau en mettant en place un périmètre cloud,

afin d'assurer à la fois la sécurité et la performance du réseau. Les DSI ont alors la responsabilité d'accompagner la transformation numérique de leur entreprise d'un modèle "Zero Trust". Il est nécessaire de repenser le périmètre de l'entreprise et de passer à un périmètre cloud, articulé à Internet en tant que réseau principal. Faire évoluer le réseau en passant par le cloud permet aux entreprises de réussir leur transformation, valoriser leur activité et stimuler l'innovation. Elles gagnent également en agilité et en simplicité au niveau de la sécurité et de l'infrastructure informatique. Basculer dans le cloud permet également aux responsables d'appliquer un modèle de sécurité dont le principe central est de « vérifier et ne jamais faire confiance » (autrement dit, « zero trust »). Ils y gagneront à la fois une gestion des accès, la sécurisation des applications et une performance optimisée.

Toutefois repenser le périmètre de l'entreprise pour aller vers le cloud n'est pas suffisant. Il faut également faire évoluer les paramètres de sécurité de l'entreprise en cessant toute distinction entre « l'interne » et « l'externe » en partant du principe que tout est extérieur à l'entreprise, comme c'est le cas sur le web. Il faut donc que les DSI s'assurent d'avoir une visibilité complète des activités du réseaux afin de pouvoir déterminer ce qui est "normal" ou non.

Concrètement, il faut entreprendre des mesures en terme d'accès direct aux applications avec le contrôle systématique des utilisateurs par exemple, mais également en terme de protection systématique des applications contre les attaques volontaires ou involontaires (terminal compromis) émanant des utilisateurs en déployant des vérifications systématiques avec une journalisation complète et des analyses des comportement. Enfin, il ne faut pas négliger les paramètres de diffusion d'application et performances afin de proposer une expérience réseau optimale en réduisant la latence grâce à la diffusion des applications dans le cloud.

Afin de réussir leur transformation numérique et gagner en flexibilité et productivité, les entreprises ne peuvent ignorer plus longtemps les nouvelles habitudes de travail et risques qui en découlent. Les périmètres des entreprises doivent s'adapter à cette nouvelle ère. Que ce soit d'un point de vue de l'usage, de la sécurité ou de l'efficacité du réseau de l'entreprise, le modèle Zero Trust permet d'accompagner sereinement cette évolution.

DOCUMENT 10

« Télétravail et travail mobile : comment réduire le risque de fuite de données ? »

Jan Van Vliet - *L'Usine nouvelle* - novembre 2018

Les équipements qu'utilisent les employés pour travailler à distance contiennent souvent des données importantes de l'entreprise : des e-mails confidentiels, des informations personnelles ou des données sensibles (voire financières). La disparition de ces appareils augmente le risque d'accès non autorisé et d'une fuite ou perte conséquente de données, observe Jan van Vliet, vice-président et directeur général EMEA de la société Digital Guardian.

Le mois dernier, le parlement britannique a révélé qu'au cours de l'année 2017, les voyageurs se rendant sur leur lieu de travail ont perdu plus de 26 000 appareils électroniques sur le réseau de transport londonien. Pour beaucoup, il est devenu courant de travailler en déplacement, mais les risques que cela implique en matière de sécurité sont souvent négligés.

Dans le cadre du Régime Général de Protection des Données (RGPD), la perte d'un appareil mobile professionnel contenant des données personnelles constitue une défaillance, passible d'amendes allant jusqu'à 20 millions de dollars ou 4 % du chiffre d'affaires annuel mondial. De toute évidence, les conséquences de la perte d'un ordinateur portable ou d'un téléphone par un employé n'ont jamais été aussi lourdes.

Malheureusement, il est impossible d'empêcher les employés de perdre leurs appareils mobiles à 100 %. La tentation est forte de limiter le travail sur mobile pour minimiser le risque de perte de données ou d'amende, mais cela risque d'impacter la productivité et la satisfaction des employés. La plupart des employés attendent une certaine souplesse dans leur travail, et la journée de travail de 9 h à 17 h se raréfie. Il est donc crucial que les organisations mettent en place des politiques et prennent des mesures de sécurité pour les télétravailleurs et les travailleurs mobiles, dans l'optique de réduire le risque de perte de données.

1. Mise au point d'une politique concernant le travail mobile

Les employés doivent recevoir une information claire sur les procédures et les meilleures pratiques de leur organisation en matière de télétravail et de travail mobile. La politique de sécurité et de sensibilisation doit couvrir plusieurs points essentiels, notamment :

- Les applications et actifs auxquels l'accès est autorisé à partir des appareils mobiles
- Les contrôles de sécurité minimum pour ces appareils
- Les composants fournis par l'entreprise, comme les certificats SSL pour l'authentification des appareils
- Les droits de l'entreprise à altérer l'appareil, par exemple en effaçant à distance les appareils perdus ou volés. Cela comprend la responsabilité de l'entreprise par rapport aux données personnelles d'un employé, si un appareil devait être effacé par mesure de précaution. Cela comprend aussi la responsabilité de l'employé par rapport à la fuite de données sensibles de l'entreprise en raison de sa négligence ou d'une mauvaise utilisation.
- La responsabilité de sauvegarder régulièrement les données de l'entreprise et de les stocker de façon appropriée

2. Chiffrement

Beaucoup des mesures de sécurité de l'entreprise n'ont aucune emprise sur les données utilisées dans le cadre du BYOD, car ces données sortent de leur zone de contrôle. Les organisations doivent donc relever l'enjeu majeur du chiffrement des données sensibles au repos et en transit. Ce chiffrement a pour but de protéger la confidentialité des données numériques lors de leur stockage sur des systèmes informatiques et lors de leur transmission sur Internet ou sur d'autres réseaux

informatiques. Les solutions de protection des données peuvent permettre de chiffrer les appareils, les e-mails et les données elles-mêmes. Dans de nombreux cas, ces fonctionnalités de chiffrement sont complétées par des outils de contrôle pour les appareils, les e-mails et les données.

Une messagerie sécurisée et chiffrée est la seule réponse conforme aux réglementations pour le personnel en télétravail, le BYOD et l'externalisation des projets. Les solutions haut de gamme de prévention de la perte de données permettent aux employés de poursuivre leur travail et leurs échanges par e-mail pendant que le logiciel et les outils marquent, classent et chiffrent les données sensibles contenues dans les e-mails et pièces jointes de façon proactive.

3. DLP (Prévention de la perte de données)

Le télétravail et le travail mobile ont pratiquement rendu le périmètre réseau classique obsolète. Il n'est plus possible de construire un mur autour de l'informatique de votre organisation et de présumer que vos données sont en sécurité. Les organisations doivent reporter leur attention de la sécurisation du périmètre vers celle des données, où qu'elles se trouvent. La DLP est en ensemble d'outils et de processus utilisés pour empêcher la perte de données, leur mauvaise utilisation ou l'accès à ces données par des utilisateurs non autorisés. Un logiciel de DLP classe les données critiques dans diverses catégories : métier, confidentielles et régulées, puis identifie les transgressions aux politiques définies par les organisations ou à un ensemble de politiques prédéfinies, généralement régi par la conformité à une réglementation, par exemple le RGPD. Une fois ces transgressions repérées, la DLP applique une remédiation composée d'alertes, de chiffrement (comme indiqué ci-dessus), et d'autres actions protectrices pour empêcher les utilisateurs finaux de partager accidentellement ou par malveillance des données pouvant entraîner un risque pour l'organisation.

Les outils de DLP surveillent et contrôlent également les activités des terminaux, filtrent les flux de données sur les réseaux professionnels et surveillent les données dans le cloud pour protéger les données au repos, en mouvement, et en cours d'utilisation. Ces solutions mettent en évidence les tentatives de déplacement des données qui ne respectent pas les politiques de sécurité ou de confidentialité, et les bloquent. Cela peut empêcher des travailleurs mobiles d'obtenir des données jugées trop sensibles.

4. Formation

Des sessions de formation régulières peuvent aider les employés à comprendre les risques et les conséquences potentielles de la perte d'un appareil mobile, et renforcer leur prudence. Ces sessions de formation doivent souligner l'importance de signaler rapidement la perte ou le vol des appareils.

Globalement, le travail mobile est un aspect essentiel de la culture d'entreprise aujourd'hui. Bien que les organisations ne soient pas en mesure d'empêcher les employés de perdre leurs appareils, elles peuvent certainement réduire les probabilités de fuite de données ou de manquement de conformité qui peuvent s'ensuivre. Grâce à la formation et la sensibilisation des employés, à des politiques définies et à des technologies de sécurité axées sur les données permettant de protéger les données à la source, les organisations peuvent réduire considérablement le facteur de risque associé à la perte d'appareils.