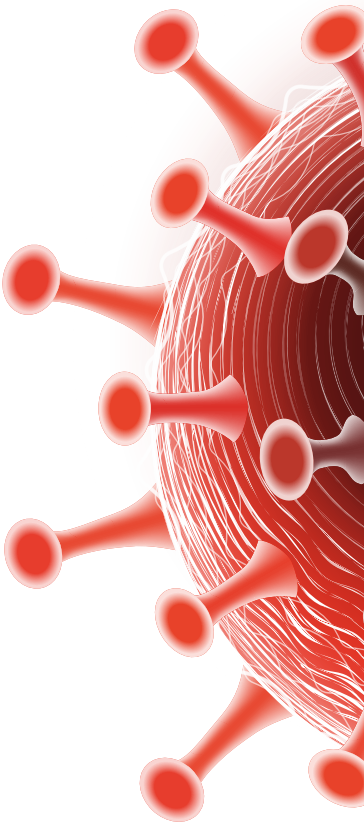
DATAPROTECT
Security is our commitment

TELETRAVAIL SECURISE

CYBERDEFENSE CONTRE LE COVID-19



Livre Blanc

REMERCIEMENT

Fruit d'un travail d'équipe, ce livre blanc est né de la plume de 16 participants ayant pris l'initiative de collaborer et de mettre en œuvre leurs expertises, compétences ainsi que leurs acquis pour réaliser ce travail exhaustif autour de la cybersécurité du télétravail.

Notre vive gratitude et nos remerciements les plus sincères vont à l'ensemble des membres de notre équipe ayant contribué à la réalisation de cet ouvrage. Nous les remercions pour leur attention constante, leurs innombrables efforts ainsi que leur regard bienveillant tout au long de la réalisation de ce livre blanc.

L'équipe DATAPROTECT espère que ces écrits vous seront d'une grande utilité durant cette période de confinement et de télétravail, et ce , en vous apportant un éclairage suffisant et une vision 360° par rapport à la cybersécurité liée au télétravail.

En souhaitant vous donner entière satisfaction, nous vous remercions chers lecteurs de l'intérêt que vous manifestez à nos réalisations.

PARTICIPANTS

Ali El Azzouzi
Badr-eddin Dardour
Chaimaa Boulahia
Chaimaa Hader
Chouaib Ghadfi
Damlan Nassampere
Hamza Waraki
Hicham ABBAD
Imad Ej-jamai
Jean-Guy Rens
Khalid Mahtate
Mohammed Hadrami
Moussa Koita
Rabii Amzerin
Redouane Benatik
Tchabli DJARK

Télétravail Sécurisé

Cyberdéfense contre

LE COVID-19

TABLE DES MATIERES

TABLE DES MATIERES

TABLE DES ILLUSTRATIONS

TABLE DES TABLEAUX

TABLE DES ABRÉVIATIONS

AES	Advanced Encryption Standard
BYOD	Bring Your Own Device
CSOC	Cybersecurity Operations Center
DMZ	Demilitarized Zone
DPL	Data Loss Prevention
EDR	Endpoint Detection and Response
EMM	Enterprise Mobility Management
GPO	Group Policy Object
IAM	Identity and Access Management
IoC	Indicator of Compromise
IPS	Intrusion Prevention System
MDM	Mobile Device Management
MFA	Multi-Factor Authentication
PAM	Privileged Access Management
PAS	Privileged Access Security
PCA	Plan de continuité d'activité
PKI	Public Key Infrastructure
SaaS	Software as a Service
SIEM	Security Information and Event Management
SPOC	Single Point Of Failure
SSL	Secure Socket Layer
TMO	Telework Managing Officer
UEM	Unified Endpoint Management
VDI	Virtual Desktop Infrastructure
VM	Virtual Machine
VPN	Virtual Private Network
WAF	Web Application Firewall

AVANT-PROPOS

Par **Ali El Azzouzi**,
Directeur Général, Dataprotect

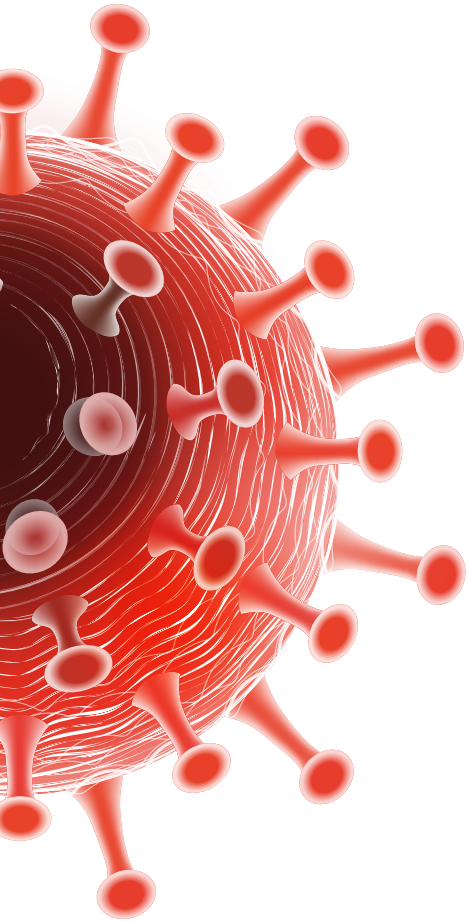
A l'occasion de la pandémie du coronavirus COVID-19, le recours au télétravail a explosé à l'échelle mondiale. Il s'agit pour les entreprises et les agences gouvernementales de préserver leurs activités. À cette fin, les télétravailleurs ont à leur disposition des outils de travail coopératif et de stockage permettant d'accéder à distance aux données opérationnelles, des logiciels de vidéoconférences ainsi qu'une multitude de plateformes de communications et de gestion.

Mais le passage au télétravail exige que les organisations repensent nombre de leurs processus d'affaires et que les employés adaptent leurs méthodes de travail. Ainsi, une mise en œuvre non-maîtrisée du télétravail peut tourner à l'anarchie et porter préjudice à l'organisation. En outre, une transition non planifiée d'un environnement de bureau sécurisé à un travail à distance peut engendrer des risques cruciaux en matière de cybersécurité.

En effet, le télétravail multiplie de façon instantanée les accès externes et mobiles aux systèmes d'information de l'organisation, ce qui accroît d'autant le périmètre informatique et les vulnérabilités. Par voie de conséquence, les cybercriminels profitent de la situation pour accroître leur rythme de menaces et d'attaques. Qui plus est, la crise du COVID-19 crée un sentiment de panique parmi la population, y compris dans les lieux de travail. C'est une aubaine pour les personnes malintentionnées et opportunistes qui profitent de la peur causée pour induire les victimes en erreur et leur extorquer des informations sensibles et confidentielles.

De ce fait, il est important pour toute organisation ayant recours à cette forme alternative de travail d'être prévoyante et de prendre les dispositions nécessaires afin de déployer des solutions adaptées pour maintenir intact le niveau de sécurité.

Pour vous aider à en savoir plus au sujet de la sécurisation du travail à distance, dans ce Livre blanc, nous avons abordé l'approche économique et juridique du contexte, traité les stratégies à adopter en termes de cybersécurité, évoqué les bonnes pratiques à mettre en place ainsi que les recommandations relatives à la sensibilisation.
Nous espérons que ce Livre blanc vous permettra d'apporter une attention diligente et un regard panoramique sur ce sujet. Voulu comme guide, ce Livre blanc sera utile dans l'amélioration de votre stratégie télétravail et ainsi vous apportera un éclairage nouveau, pragmatique et aussi exhaustif que possible en cette période de changements rapides.



1 CONTEXTE DU LIVRE BLANC SUR LE TÉLÉTRAVAIL

1. CONTEXTE DU LIVRE BLANC SUR LE TELETRAVAIL

1.1 - Situation pandémique

La crise du coronavirus COVID-19 n'est pas un cas isolé. Cette pandémie a été précédée par la grippe H1N1, le virus Ebola, le Syndrome respiratoire aigu sévère (SRAS) et le Syndrome respiratoire du Moyen-Orient (SRMO). Au cours des 20 dernières années, les virus et les maladies à propagation rapide sont de plus en plus courants et leur nombre augmente crescendo. Dès 2015, dans une conférence intitulée « La prochaine épidémie ? Nous ne sommes pas prêts », Bill Gates déclarait : « Si quelque chose tue plus de 10 millions de gens dans les prochaines décennies, ça sera probablement un virus hautement contagieux plutôt qu'une guerre.[1]»

Parti d'Asie, le COVID-19 s'est étendu progressivement à tous les continents. Lentement, la pandémie fait son chemin aux quatre coins du monde, y compris l'Afrique. Face à cette progression, le continent africain a rapidement pris des décisions fortes afin d'adopter des mesures draconiennes pour tenter de ralentir la pandémie: frontières fermées, liaisons aériennes et maritimes suspendues, ainsi que confinement à domicile des citoyens. Même si bien des outils existent pour lutter contre cette pandémie, peu de pays dans le monde s'y étaient préparés – contrairement à une poignée de pays asiatiques. En outre, la région Afrique reste particulièrement vulnérable en raison de la faiblesse de ses systèmes d'accès aux soins, marqués par des barrières financières et géographiques.

Aujourd'hui, en Afrique comme partout ailleurs, cette crise suscite une vive inquiétude, tant au niveau sanitaire et sociétal, qu'entrepreneurial et économique. L'ampleur de la propagation du virus n'a épargné aucun secteur de la vie quotidienne : transports, banques, commerces, écoles, entreprises… Tous les acteurs économiques et sociaux subissent des retombées négatives et craignent pour leur avenir.

Ainsi, cette situation du COVID-19, ne dépend pas uniquement des États et des décisions publiques, mais d'une discipline individuelle et collective s'attachant au moindre geste quotidien. En outre, nous avons tous une part de responsabilité et pouvons changer le cours de la situation. En respectant les restrictions imposées, en adoptant les bonnes solutions, en apportant chacun nos compétences et notre humanité, nous pouvons passer l'écueil et mettre fin à cette crise sanitaire.

1.2 - Situation économique

"COVID-19, ou le virus qui grippe l'économie mondiale."

La crise en cours, est exceptionnelle à plus d'un titre, elle diffère de tout ce que nous avons connu dans le passé. Combinant catastrophe sanitaire planétaire, effondrement financier et économique ainsi que de fortes tensions diplomatiques, le coronavirus est non seulement imprévisible, mais il n'a également aucune limite. Cette crise mondiale est unique car pour la première fois les gouvernements mettent tous leurs pouvoirs pour stopper la machine économique. Alors que le rôle traditionnel de l'État est de favoriser le développement économique et, le cas échéant, de favoriser la relance, cette fois-ci, il agit comme un frein.

Bien sûr, cette intervention inédite de l'État a pour but de lutter contre la propagation du coronavirus. Il s'agit de minimiser les interactions interindividuelles, ce que l'on appelle en jargon de crise : la distanciation sociale. On ferme les écoles et les lieux de travail pour ralentir au maximum la propagation du coronavirus dans la société. Il n'en reste pas moins que pour les citoyens, le choc est réel.

L'Afrique n'échappe pas à ce mouvement. Or, il s'agit d'un continent fragile qui amorce seulement son émergence économique. Le filet social qui existe dans les pays industrialisés de longue date y est notoirement absent. Licencier des employés qui n'ont aucun autre moyen de subsistance n'est pas une option. Voilà pourquoi, plus que partout ailleurs dans le monde, il est impératif de maintenir l'activité de l'organisation.

Le télétravail apparaît comme le moyen clé pour satisfaire aux exigences de la distanciation sociale tout en préservant l'outil économique. Les dirigeants doivent faire preuve d'imagination pour adapter le télétravail à l'environnement africain où la relation humaine à base de parole et de face-à-face, est si importante. Mais n'est-ce pas le propre du génie africain de réussir à s'approprier des technologies importées pour les réinventer et les faire prospérer ? Ce que l'Afrique a fait pour le paiement mobile, elle peut le refaire pour le télétravail.

Après le COVID-19, rien ne sera plus comme avant. Le télétravail qui fait irruption dans nos organisations à ce propos est appelé à redéfinir la gouvernance. Toute crise

1 Bill Gates, "The next outbreak? We're not ready", TED (Technology, Entertainment and Design) conference, The Sapling Foundation, mars 2015. - https://www.ted.com/talks/bill_gates_the_next_outbreak_we_re_not_ready

1. CONTEXTE DU LIVRE BLANC SUR LE TELETRAVAIL

est une renaissance. Le télétravail n'est pas qu'une réponse à une crise. Certains pays l'ont érigé comme moyen principal de gestion des organisations privées et publiques avec plus de 70% des employés travaillant à distance (Inde, Indonésie).

« Dans toute crise, apparaissent des leaders qui savent ce qu'ils ont à faire. »

1.3 - Qu'est-ce que le télétravail ?

1.3.1 - Historique

La notion de télétravail est apparue dans les années 1950 aux États-Unis avec les travaux de Norbert Wiener sur la cybernétique. À partir des années 1970, le télétravail est mieux connu grâce aux nouvelles perspectives ouvertes par la « télématique » et les « autoroutes de l'information ».

Depuis, le télétravail se développe partout, mais de façon variable. Les États-Unis, le Royaume Uni et l'Australie affichent des taux de télétravailleurs supérieurs à 25% de la population active alors que tombe à 10% en France et en Allemagne, sachant que ces taux sont donnés à titre indicatif, compte tenu des différences de définitions et de méthodes statistiques entre États.

Les politiques d'appui au développement du télétravail varient en fonction des objectifs fixés par les pouvoirs publics et les secteurs économiques[2].

1.3.2 - Essai de définition

Le télétravail se définit par la possibilité pour un employé, un contractant ou autres types de partenaires, d'utiliser les ressources informatiques privées de l'organisation, sans être présent physiquement au sein de ses locaux.

Traditionnellement, les organisations ont développé des stratégies de sécurité autour d'un environnement fermé et contrôlé. En ce temps de crise, de plus en plus d'organisations ont opté pour le travail à distance ou télétravail. Cette atomisation des activités a pratiquement rendu obsolète le périmètre réseau classique et exposé les organisations à de nouveaux risques.

Le télétravailleur va manipuler des données de l'organisation, sous ses différents niveaux de confidentialité : lire ou envoyer un courriel, accéder aux applications métiers de l'organisation, rédiger ou revoir des documents (confidentiels, internes, publics), animer ou participer à des réunions, etc.

Voilà pourquoi, toute stratégie de télétravail doit comprendre en son cœur même un volet sécuritaire. Adopter le télétravail consiste à modifier nombre de composantes critiques de l'écosystème entrepreneurial, y compris la cybersécurité.

Ce changement donc, à la fois architectural et comportemental, doit être mené d'une manière planifiée, contractuelle et sécurisée.

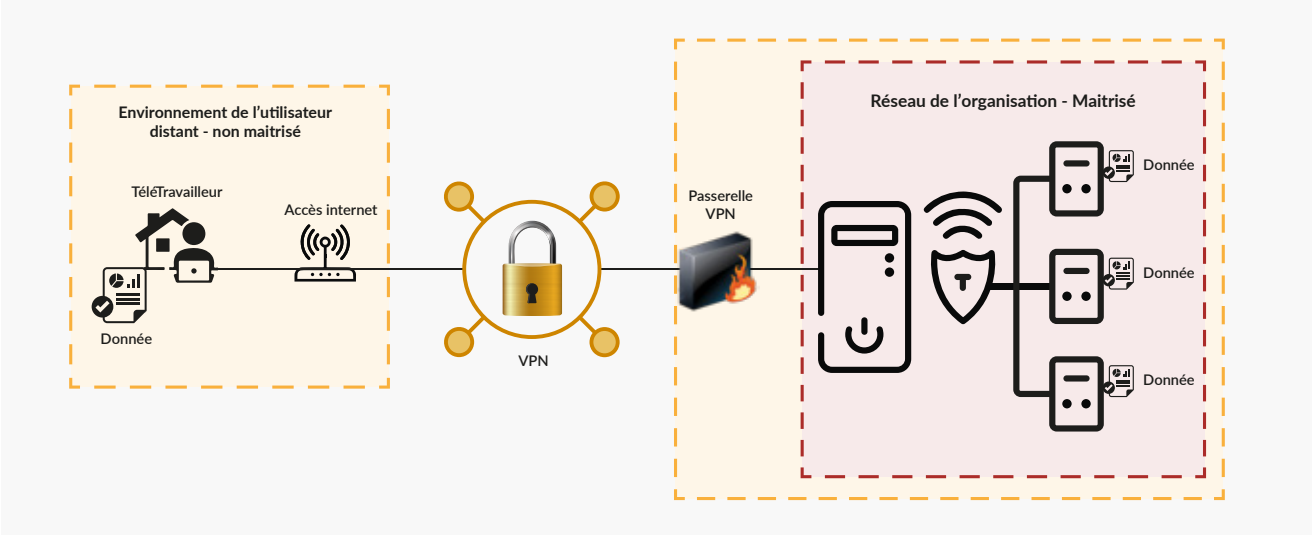


FIGURE 1 : ENVIRONNEMENT THÉORIQUE DU TÉLÉTRAVAIL

2 « Le télétravail dans le monde : Un phénomène récent et une grande diversité de situations », site spécialisé du Commissariat général à l'égalité des territoires (CGET) du gouvernement français : www.teletravailler.fr

La pierre angulaire de la sécurité de ce dispositif est l'employé devenu télétravailleur. La manière avec laquelle il va adopter ce nouveau mode de fonctionnement, va définir le taux de réussite de la stratégie de sécurité du télétravail, choisie par l'organisation. La sensibilisation des employés aux enjeux de sécurité liés au télétravail deviendra donc l'une des priorités à considérer par l'organisation.

1.4 – Lois et juridictions

1.4.1 - Quel cadre légal autour le télétravail

Dans plusieurs pays où le recours au télétravail est répandu, le législateur a défini le cadre légal de la pratique. Aux États-Unis, la Loi du 9 décembre 2010 sur l'amélioration du télétravail (Telework Enhancement Act) a été adoptée pour fournir de la flexibilité dans la gestion de la main-d'œuvre du gouvernement fédéral et, à ce titre, sert de modèle pour les entreprises privées. La loi considère qu'un programme de télétravail bien mis en œuvre est un outil précieux pour atteindre les objectifs de la mission de l'organisation concernée tout en améliorant la productivité de ses employés. Cette loi comporte, entre autres, les dispositions suivantes :

- Tout programme de télétravail doit être conditionnel à un accord écrit entre l'employé et le gestionnaire ;
- Chaque organisation doit intégrer le télétravail dans son plan de continuité des opérations ;
- Chaque organisation doit désigner un directeur général du télétravail ;
- Tout programme de télétravail doit prévoir que les employés et les gestionnaires suivent une formation interactive sur le télétravail…

En France, la réforme du code du travail par les ordonnances du 22 septembre 2017, vise à instaurer un modèle de « flexisécurité » en prévoyant plusieurs dispositions qui facilitent le recours au télétravail. Parmi celles-ci :

- La définition formelle du télétravail ;
- Le droit de l'employé à un retour au mode de travail dit « normal » ;
- L'égalité des droits du « télétravailleur » et du travailleur dit « normal » ;
- La reconnaissance de l'accident de travail en télétravail ;
- Les conditions de passage en télétravail.

Les politiques d'appui au développement du télétravail varient en fonction des objectifs fixés par les pouvoirs publics et les secteurs économiques. Toutefois, partout, ces politiques visent des objectifs d'amélioration de la productivité, de réduction des temps de transport, de la qualité de vie des salariés, en recourant à des méthodes distinctes :

- Les Pays-Bas ont mis en place des recommandations concernant le développement du télétravail dans la fonction publique uniquement ;
- En Allemagne, l'action passe par l'octroi d'aides et l'accompagnement par des actions de communication ;
- Au Royaume-Uni, des guides et des recommandations dédiés au développement et à la mise en place du télétravail ont été développés.

En revanche, dans la majorité des pays africains, nous notons l'absence d'une définition juridique du télétravail et l'absence d'un cadre juridique dédié à la réglementation de la relation entre l'employé et son Responsable de Gestion du Télétravail (Telework Managing Officer ou TMO). Dans la pratique, cette carence décourage les organisations d'adopter ce mode de gouvernance. Elles réservent le télétravail à un groupe restreint de cadres. Exceptionnellement, quelques employés non-cadres sont invités à faire du télétravail en cas de crise. Au contraire, la pandémie du COVID-19 impose un recours massif au télétravail. Du fait de la nature contagieuse de la pandémie, c'est l'ensemble des employés qui est concerné.

En Afrique où la législation n'encadre pas la pratique, il faut se fier à des avis juridiques basés sur la jurisprudence ainsi qu'aux exemples de législations étrangères. Selon les experts consultés, le télétravail est une nouvelle forme d'organisation du travail permettant à un salarié l'exercice d'une manière régulière et volontaire de ses fonctions dans un autre lieu que les locaux de son employeur, grâce aux nouvelles technologies de l'information et de la communication. Ils précisent qu'il ne s'agit pas d'un aménagement du temps de travail, mais d'une modalité d'organisation du travail et que le « mode » télétravail peut être mis en place par un simple accord mutuel entre employeur et salarié.

1. CONTEXTE DU LIVRE BLANC SUR LE TELETRAVAIL

Toutefois, le contrat de télétravail ou l'avenant au contrat initial qui acte le passage au travail à distance est fortement conseillé car c'est à la fois l'occasion pour l'organisation de planifier cette activité et une manière de sensibiliser l'employé à ses responsabilités. On a vu qu'aux États-Unis, un contrat de télétravail est obligatoire dans l'administration fédérale. Un contrat de télétravail type doit mentionner le nom du Responsable de Gestion du Télétravail, le mode de contrôle du temps de travail ou de régulation de la charge de travail ainsi que les plages horaires durant lesquelles l'employeur peut contacter le télétravailleur.

Les juristes affirment également que le télétravailleur est un salarié de l'organisation au même titre que les autres salariés exerçant dans les locaux de l'employeur et qu'il bénéficie donc des mêmes droits que ces derniers, aucune distinction ne pouvant être faite.

Le facteur confiance entre l'employeur et l'employé constitue toutefois, un élément indispensable pour aboutir aux résultats escomptés du télétravail. Voilà pourquoi des communications constantes et bien encadrées sont indispensables. Il s'agit de maintenir l'esprit d'équipe parmi les employés, de fournir une rétroaction continue aux activités des employés et de leur fournir de l'assistance chaque fois que nécessaire. Bref, des communications intensives sont primordiales pour le succès du passage massif au télétravail, comme c'est le cas avec la pandémie de COVID-19 en cours.

1.4.2 - Quid de la vie privée des télétravailleurs ?

A priori, l'employeur est civilement responsable de ses salariés et peut voir sa responsabilité engagée en cas d'activité illégale de ses employés sur Internet. Il est donc recommandé de mettre en place un dispositif de contrôle de l'activité du salarié, à la condition toutefois que le moyen de surveillance en question :

- Soit pertinent et proportionné à l'objectif poursuivi ;
- Et ne soit installé qu'après information du télétravailleur et consultation des délégués du personnel s'il y a lieu.

Tout dispositif de cybersurveillance des salariés doit être déclaré à l'autorité compétente.

1.4.3. Quid de la protection du patrimoine informationnel de l'organisation ?

Il incombe à l'employeur de prendre les mesures qui s'imposent pour assurer la protection des données utilisées et traitées par le télétravailleur à des fins professionnelles. En France, par exemple, l'accord national interprofessionnel du 19 juillet 2005 prévoit dans son article 5 que l'employeur doit informer le télétravailleur:

- Des dispositions légales et des règles propres à l'organisation relatives à la protection des données et à leur confidentialité ;
- De toute restriction à l'usage des équipements ou outils informatiques comme Internet et, en particulier, de l'interdiction de rassembler et de diffuser des matériels illicites via l'Internet ;
- Des sanctions en cas de non-respect des règles applicables.

Étant d'abord un salarié et bénéficiant des garanties prévues pour l'ensemble des salariés travaillant dans les locaux de l'organisation, le télétravailleur est également soumis aux obligations de protéger les données de celle-ci. L'employeur a le devoir de concilier la protection du patrimoine informationnel de l'organisation avec le respect de la vie privée du salarié.

1.5 – Stratégie du télétravail

Pour l'organisation, le télétravail représente un gain réel de productivité. Pour le télétravailleur, cela représente une diminution du stress lié aux déplacements, la possibilité de travailler de façon plus concentrée dans un environnement serein ainsi qu'une flexibilité des heures de travail. Le premier impact de cette forme de gestion est la modification des modes traditionnels d'organisation de la gestion des ressources humaines, notamment des moyens de contrôle des télétravailleurs et de définition des tâches. Les cadres doivent alors s'initier à la gestion par résultats ou par objectifs, au lieu de la gestion « à vue ».

D'un autre côté, si le télétravailleur n'a plus une obligation de présence et de contraintes horaires, il a une obligation de résultat. Tout d'abord, il doit posséder les qualités nécessaires au télétravailleur, c'est-à-dire une certaine autodiscipline, une habileté à agir de façon proactive et à résoudre des problèmes par lui-même, à faire une distinction claire entre le temps consacré aux activités professionnelles et le temps consacré à la vie privée et familiale. Si ces conditions sont réunies, l'organisation doit assurer au télétravailleur les moyens pour mener à bien sa mission.

1. CONTEXTE DU LIVRE BLANC SUR LE TELETRAVAIL

Comment faire ?

Le télétravail n'est pas une activité parmi d'autres. C'est une stratégie structurante qui doit faire l'objet d'une préparation rigoureuse[3]. Et avant de passer à l'implantation du télétravail, il est préférable de s'enquérir des attentes, des opinions et des appréhensions des télétravailleurs potentiels ainsi que des collègues et cadres qui demeureront sur le site et interagiront avec les télétravailleurs. Les nouvelles méthodes de supervision à distance, l'accessibilité des télétravailleurs aux réunions et les moyens pour combattre l'isolement des télétravailleurs sont des sujets à aborder. Des moyens ingénieux existent. Certaines entreprises, par exemple, organisent une « pause-café virtuelle » quotidienne pour supporter les télétravailleurs.

PHASE 1

Constitution d'une équipe de gestion du projet de télétravail

- Nomination d'un Responsable de Gestion du Télétravail et d'une équipe de projet multidisciplinaire. L'équipe détermine les objectifs stratégiques et l'étendue du projet (nombre d'employés concernés, choix technologiques, propriété des appareils de télétravail, etc.). Des indicateurs de réussite des différents aspects du projet sont mis au point.
- Rédaction d'une charte ou d'une politique sur le télétravail qui précise les droits et les devoirs des parties concernées, les conditions d'une utilisation raisonnée et éthique des technologies de l'information et de la communication mises à la disposition du travailleur par son employeur
- Ajout d'une annexe au contrat de travail portant sur les aspects juridiques et fiscaux du télétravail.

PHASE 2

Rédaction du Plan de télétravail

- Une fois constituée, l'équipe va élaborer un plan de transition en tenant compte des quatre facteurs de succès du télétravail : caractéristiques des fonctions ou des postes de travail, caractéristiques personnelles des télétravailleurs, caractéristiques de l'organisation (sa mission), caractéristiques des familles des télétravailleurs. L'équipe doit également déterminer la stratégie et les objectifs du projet de télétravail (par exemple, un projet spécial, ou des aspects à améliorer dans l'organisation ou encore un projet pilote avant le déploiement d'une stratégie de télétravail).
- Intégration du télétravail dans les processus de gestion et formation des gestionnaires responsables des télétravailleurs et de la mobilité.
- Définition d'activités ayant un rendement concret et mesurable. Gestion par objectifs.
- Détermination des besoins en matériel, logiciels et connexions (sécurité comprise) en fonction du type de télétravail, des possibilités et des limites de l'infrastructure actuelle ainsi que des coûts qui y sont liés.

PHASE 3

Lancement du programme de télétravail

Trois éléments constituent l'armature de l'accompagnement du programme de télétravail :

- Sensibilisation et formation au télétravail des cadres et du personnel.
- Mise au point d'instruments pour le soutien du projet de télétravail. Par exemple, création d'une « boite à outils » sur le télétravail qui comprendra des conseils sur l'ergonomie du bureau et les mesures de sécurité, astuces concernant la gestion du temps, la communication électronique ainsi que l'équilibre entre les tâches professionnelles et les activités personnelles.
- Communication auprès du personnel.
  - Préparation d'un texte d'introduction, de pages web, de brochures, de sessions d'information et de formations à l'intention de l'ensemble du personnel (les cadres, les télétravailleurs et leurs responsables, de même que les non-télétravailleurs) pour l'informer, le sensibiliser et, le cas échéant, affiner des compétences spécifiques.
  - Organisation d'une réunion de démarrage pour présenter aux futurs télétravailleurs et à leurs supérieurs les étapes du projet et les moyens qui seront mis en œuvre pour faciliter les communications et soutenir les activités. Offre d'une assistance en ligne ou téléphonique aux télétravailleurs et à leurs superviseurs.

PHASE 4

Rétroaction

Un comité d'étude indépendant par rapport au Responsable de Gestion du Télétravail évalue les résultats du programme en fonction des indicateurs de réussite et soumet son rapport au président-directeur général (PDG). Le cas échéant, des correctifs sont apportés au programme.

3 Michel Walrave, « Comment introduire le télétravail? », Université d'Anvers, janvier 2010.

1.6 – Description de l'environnement physique

Quand un employé fait du télétravail, il peut utiliser deux types d'appareils : les ordinateurs personnels (ordinateurs de bureau, ordinateurs portables) et les dispositifs mobiles (smartphones, tablettes). Chacun de ces appareils peut être la propriété de l'organisation ou celle du télétravailleur – dans ce cas on parle alors de BYOD, abréviation de l'anglais « bring your own device ». Les organisations limitent souvent les types de dispositifs pouvant être utilisés pour l'accès à distance. Par exemple, de nombreuses organisations ont tendance à n'autoriser l'utilisation que de leurs propres ordinateurs personnels et appareils mobiles.

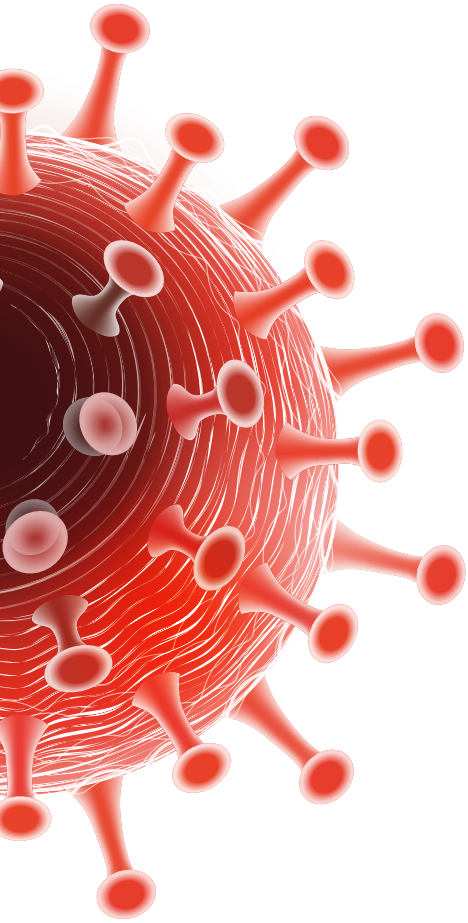
D'autres organisations ont plusieurs niveaux d'accès, par exemple en autorisant les ordinateurs dont elles sont propriétaires à accéder à l'ensemble des SI, tandis que les ordinateurs BYOD ne peuvent accéder qu'à un nombre plus limité de ressources ; enfin, les appareils mobiles BYOD sont limités à une ou deux ressources, comme le courriel. Cela permet à une organisation de limiter le risque qu'elle encourt en permettant aux appareils les plus contrôlés d'avoir le plus d'accès et aux appareils les moins contrôlés d'avoir un accès minimal.

Or, la grande majorité des télétravailleurs utilisent des appareils BYOD. Selon une étude menée en 2013, 71 % des employés interrogés utiliseraient à titre professionnel des appareils non mis à disposition par leur organisation. Bien sûr, dans la majeure partie des cas, il s'agit d'un recours épisodique au télétravail et non d'un recours massif et continu pendant une longue période comme c'est le cas aujourd'hui.

Quoiqu'il en soit, il est fortement recommandé que l'organisation vérifie automatiquement l'hygiène sécuritaire de chaque appareil qui tente d'utiliser l'accès à distance afin de s'assurer qu'il est conforme aux exigences institutionnelles. Ces contrôles consistent par exemple à vérifier que le système d'exploitation d'un ordinateur personnel soit entièrement mis à jour, qu'il dispose d'un logiciel antivirus à jour et qu'un pare-feu est activé ; dans le cas des smartphone, il faut examiner si l'appareil a été piraté ou son code brisé.

En effet, lorsqu'un dispositif de télétravail utilise l'accès à distance, il devient une extension logique du réseau privé de l'organisation. Par conséquent, si le dispositif de télétravail n'est pas correctement sécurisé, il présente un risque supplémentaire non seulement pour les informations auxquelles le télétravailleur accède, mais aussi pour tous les autres systèmes de l'organisation. Chaque dispositif de télétravail doit être soigneusement protégé et sa sécurité doit être maintenue en mode continu[4].

4 Murugiah Souppaya et Karen Scarfone, "User's Guide to Telework and Bring Your Own Device (BYOD) Security", Department of Commerce, Washington, juillet 2016, 34 pages.



2 PLAN DE CONTINUITÉ D'ACTIVITÉ

2. PLAN DE CONTINUITE D'ACTIVITE

2.1 - Contexte marocain

Toute organisation qui entend planifier la continuité de ses activités en temps de crise devra impérativement prévoir une coordination avec les pouvoirs publics. À cet égard, il convient de prendre en considération la stratégie globale de gestion des risques adoptée par le royaume du Maroc. Cette stratégie repose sur la veille et la surveillance permanente des risques, ainsi que la mise en place des mesures de prévention et des dispositifs d'alerte et de secours. Elle est supportée par un arsenal juridique adapté au contexte national et international du pays.

D'une façon générale, la réponse à une crise se fait par la création d'une cellule de crise spécifique afin de mettre en œuvre les mesures nécessaires pour limiter les dégâts et gérer la situation. Cette cellule comprend toute les parties prenantes concernées, à savoir la protection civile, les sapeurs-pompiers, le croissant rouge, le ministère de la santé, etc.

Notons qu'en 2014, le Maroc a participé au Forum de Haut Niveau sur les politiques de gestions des risques de l'OCDE qui vise à une meilleure gouvernance de la gestion des risques dans les pays membres. À son issue, un projet biparti entre le Maroc et l'OCDE a été mis en place afin d 'établir une meilleure politique de gestion des risques majeurs au Maroc[5].

2.2 - Importance de la préparation en amont

L'apparition de virus grippaux pandémiques reste une préoccupation majeure. Comme nous l'avons vu plus haut, le COVID-19 n'est pas la première pandémie à frapper l'humanité. Immanquablement, d'autres pandémies surviendront et rien n'indique que la prochaine aura le caractère relativement modéré de celle d'aujourd'hui.

La pandémie COVID-19, de par sa contemporanéité, entraîne la paralysie forcée des organisations et des chaînes d'approvisionnement avec des conséquences tant sur le plan humanitaire que socio-économique. Ce genre de perturbation n'est pas propre à une crise sanitaire. D'autres catastrophes peuvent frapper nos sociétés qui auront des conséquences similaires : guerre, terrorisme, tremblement de terre, tsunami, inondation, catastrophe nucléaire ou chimique, etc.

Voilà pourquoi, il est d'autant plus urgent pour toute organisation de se doter d'un Plan de continuité d'activité (PCA) permettant de se préparer à une catastrophe, qu'il s'agisse de la crise sanitaire du COVID-19 ou de tout autre scénario de rupture de l'activité socio-économique.

Ce que nous devons retenir, c'est que la négation du risque n'est pas une forme acceptable de gestion du risque. Plutôt que de se contenter d'espérer que le pire ne survienne jamais, mieux vaut s'y préparer en établissant un PCA. Or, un tel plan de continuité ne s'improvise pas.

Le PCA est un exercice d'anticipation qui consiste pour l'organisation à prévoir les moyens pour protéger ses employés, faire face à la baisse d'effectifs, poursuivre ses activités essentielles et assurer un retour rapide à la normale face à une crise dont l'ampleur, la cinétique et le caractère inattendu dépasse ses capacités habituelles. Le premier geste à poser dans le cadre de la préparation du PCA est la constitution d'une cellule de préparation aux urgences composée d'un responsable de la prise en charge pour chacune des unités d'affaires.

Cette cellule devra bénéficier du support actif de la haute direction pour avoir la crédibilité et les moyens nécessaires. Son premier mandat consistera à départager les activités essentielles de l'organisation. Pour chaque activité essentielle, il faudra déterminer les niveaux de service à préserver ainsi que les ressources et procédures à déployer, en tenant compte des ressources critiques qui peuvent avoir été perdues, jusqu'à la reprise de la situation normale. Il en résultera un document qui décrira de façon détaillée le rôle de chacun, y compris les clients et les fournisseurs.

Nul besoin d'être une grande entreprise pour planifier la continuité de ses activités. Il existe des méthodologies éprouvées qui sont bien adaptées à la réalité des PME.

5 Houssem Barkaoui, Alain Guinet, Tao Wang, Nadine Meskens, « Les plans de gestion de crises dans les pays francophones », 8ème conférence francophone en Gestion et Ingénierie des Systèmes Hospitaliers, GISEH, juillet 2016, Casablanca, Maroc. 2016.

2.3 - Gestion de la crise

L'incertitude est le propre de toutes les crises. S'il est possible de la réduire, on ne peut jamais l'éliminer totalement. Cette incertitude est particulièrement forte dans les crises sanitaires qui ont tendance à se prolonger dans le temps sans que l'on puisse jamais prévoir la fin, ni l'évolution du degré d'intensité. Lors d'une pandémie, il faut donc accepter une forte part d'inconnu et apprendre à gérer la crise dans un contexte très incertain.
Dans le cadre d'une crise sanitaire, le plan de continuité « pandémie », rédigé sans connaître le scénario qui se concrétisera, doit donc être flexible et s'efforcer d'avoir une valeur générique. Le tableau qui suit indique la chronologie de la gestion d'une crise type.

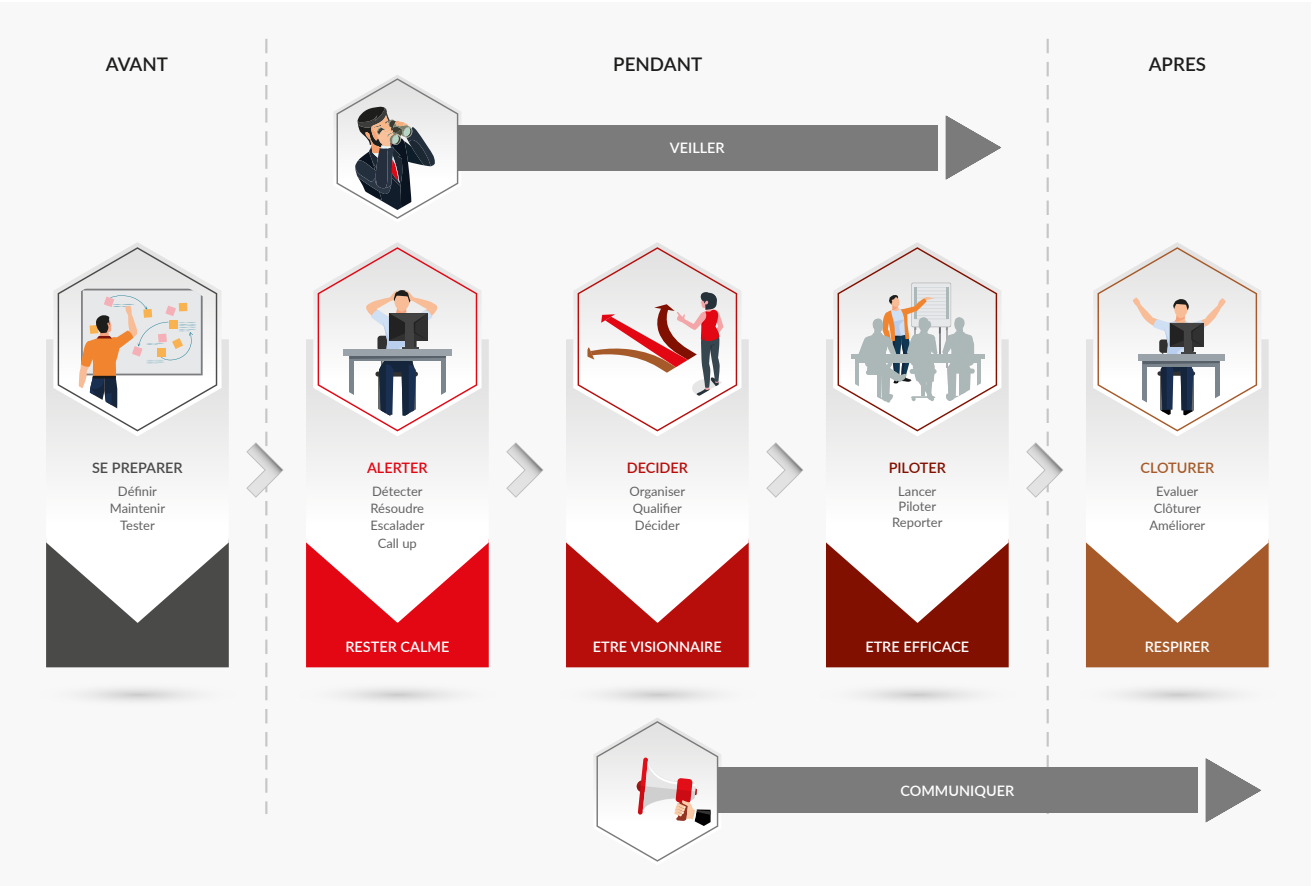


FIGURE 2 : CHRONOLOGIE DE LA GESTION D'UNE CRISE TYPE

Une cellule de préparation aux urgences doit donc être instaurée en amont de la crise, dans le cadre du PCA. Cette cellule a pour mandat, lors d'une crise sanitaire, d'éclairer les orientations et prendre les décisions nécessaires eu égard :

- Au pilotage de la situation de crise ;
- À l'adaptation en mode continu du PCA ;
- Au maintien des prestations essentielles ;
- À la protection des employés et, le cas échéant, des clients et des fournisseurs ;
- À la satisfaction des obligations légales et règlementaires ;
- À la préservation de l'image et de la réputation de l'organisation.

Cette cellule analyse la situation régulièrement dans les différentes étapes de la crise sanitaire et prend les décisions nécessaires à la poursuite des activités de l'organisation.

2. PLAN DE CONTINUITE D'ACTIVITE

2.4 - Stratégies de continuité

Le PCA doit contenir plusieurs stratégies de continuité en lien avec chacune des conséquences potentielles de la crise. Ces stratégies devront être conçues de façon à garantir la non-régression des mesures de sécurité définies par l'organisation pour protéger les données. Au contraire, le PCA devra veiller à leur renforcement. Les stratégies identifiées dans la figure suivante sont présentées à titre indicatif.

Mise en place de mesures sanitaires renforcées
Nettoyage des locaux plus fréquents, distribution de masques, consignes sanitaires aux collaborateurs,...

Restriction des accès aux sites
Selon l'ampleur de la crise, restriction des accès uniquement aux collaborateurs internes, puis uniquement aux contributeurs d>activités critiques devant exercer sur site

Recours au plan de succession
Pour le remplacement de collaborateurs indisponibles (malades, congés, garde des enfants,...)

Priorisation des activités
Focalisation des collaborateurs sur les activités critiques, priorisation des clients actifs et des contrats en cours

Gel des prestations de services non critiques
Arrêt des prestations externes non indispensables pour le bon fonctionnement de l'entreprise

Recours au télétravail
Pour éviter la propagation du virus et la contamination des effectifs

Adaptation des horaires de travail
Pour pallier aux perturbations dans les transports publics et permettre aux collaborateurs de prendre soin de proches malades

FIGURE 3 : QUELQUES EXEMPLES DE STRATÉGIES DE CONTINUITÉ

2.5. Communication et coordination continue

Chaque crise entraîne son lot de rumeurs qui l'aggravent. Face aux informations erronées ou aux rumeurs qui peuvent circuler, les informations correctrices doivent être apportées immédiatement par l'organisation sans hésiter à recourir à des moyens de communications en-dehors des structures classiques. Si la fausse information provient d'un canal inhabituel, il faudra systématiquement répondre sur ce même canal.

2.5.1 - Les principes à suivre

Chaque mesure du plan de continuité « pandémie » doit s'accompagner d'un effort de communication exceptionnel. À cette fin, il est recommandé de prévoir la mise en place d'une « SWAT Team » ou d'une « War Room » pour gérer les opérations, les communications à l'interne comme à l'externe.

Pour chaque mesure organisationnelle décidée, un volet « communication » doit être défini conjointement. Les points énumérés ci-dessous ont pour but d'aider à construire ce volet. L'objectif consiste à maintenir un dialogue permanent avec les partenaires.

a - Être à l'écoute :
• Connaître, en temps réel, l'information sanitaire et de ses conséquences afin de réajuster les modes de travail et le plan de communication.
• Détecter les rumeurs infondées, directement ou indirectement dirigées sur l'organisation et expliquer pourquoi elles sont fausses dans le contexte de son activité.
b - Communiquer avec les partenaires :
• S'appuyer sur les porte-paroles pour maintenir une communication efficace avec les partenaires.
• Inciter chaque employé à devenir acteur et responsable face au risque et à favoriser la solidarité (aide aux personnes vulnérables, etc.).
c - Délivrer de l'information et les messages importants :
• Répondre sans délai aux attentes et questions des employés, de la clientèle et des partenaires.
• Fournir de l'information crédible sur la situation et les mesures prises.

2.5.2 - Un impératif de crise : les relations avec les autorités publiques.

La relation avec les autorités compétentes est importante en amont car elle permet d'établir des procédures de contact qui spécifient quand et comment recourir à ces autorités en cas crise. N'oublions pas qu'une crise sanitaire comme celle du COVID-19 n'exclut pas que se produise une urgence étrangère à la crise qui pourrait affecter considérablement les capacités et moyens d'action de chaque organisation. Cela peut être le cas d'une cyberattaque, d'une inondation ou dégâts d'eau, d'un incendie, etc.

Pour ce faire l'organisation doit idéalement disposer d'un service interne ou avoir recours à des prestations de veille, afin d'être capable d'analyser la situation, de pouvoir anticiper l'évolution des événements et déclencher à temps les procédures d'alerte interne ainsi que de faciliter la coordination de la gestion de crise.

Plus que jamais, il faudra alors être en contact étroit avec les autorités chargées de la sécurité des biens et des personnes (police ou gendarmerie), de la cybersécurité (agences gouvernementales de veille de réponse aux incidents, CERT, etc.) et la santé publique (Ministère de la Santé).

2.6 - Préparation du retour à la normale

La cellule de crise devra être maintenue jusqu'à la sortie de crise. C'est à elle qu'il incombe de piloter le retour en fonctionnement « normal » sous la conduite de la haute direction et en coordination avec les pouvoirs publics. Ainsi, le retour des employés aux sites habituels de travail ne peut être décidé qu'après autorisation des autorités sanitaires.

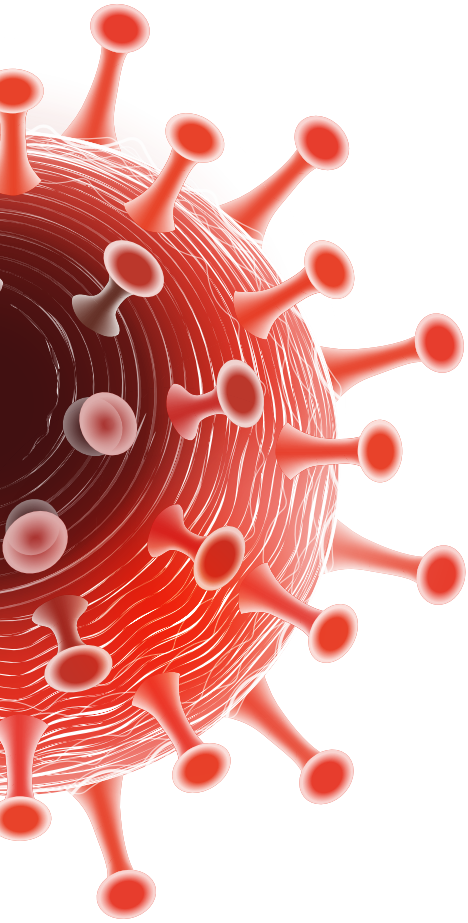
Cependant, il ne faut pas croire que la situation « normalisée » correspondra exactement à l'état avant la crise. En effet, il y a eu atteinte aux capacités opérationnelles de l'organisation – d'où le déclenchement du PCA. Plus déterminant encore : il y a eu crise nationale et internationale majeure.

Si certaines organisations pourront reprendre leurs activités traditionnelles, d'autres devront modifier en profondeur leur raison d'être. Dans un cas comme dans l'autre, il est recommandé de prévoir la possibilité d'un fonctionnement plus ou moins pérenne en mode télétravail afin de conserver une grande souplesse d'adaptation.

Il convient de rassembler dès que possible les éléments qui permettront de faire un bilan de l'événement, un retour d'expérience pour engager des plans d'actions.

Le Club de la Continuité d'Activité (CCA) définit deux types de retour d'expérience : l'un à chaud, pour ne pas perdre d'informations, et l'autre à froid, pour prendre des décisions avec un recul suffisant. Le premier type de retour d'expérience s'appuie sur l'analyse des informations recueillies tout au long du déroulement de la crise. À cet effet, il faut prévoir dans le PCA un responsable chargé de la tenue d'un « journal de bord » quotidien. Le deuxième type de retour d'expérience est réalisé à la fin du retour à une situation jugée normale, il conduit à la rédaction d'un bilan en vue de déterminer l'impact sur les opérations, d'examiner la qualité de gestion de la crise, pour l'améliorer et envisager les changements permanents à apporter à la gouvernance de l'organisation[6].

6 « Lexique structuré de la continuité d'activité », Club de la Continuité d'Activité, vol. 3, Levallois-Perret, France, décembre 2012.



3 PRINCIPES DE BASE DU PROGRAMME DE TÉLÉTRAVAIL

3. PRINCIPES DE BASE DU PROGRAMME DE TELETRAVAIL

Ce Livre blanc considère le télétravail comme devant constituer le cœur de la stratégie de continuité à adopter par l'organisation en temps de crise de pandémie.

3.1 - Scénarios pour l'accès distant

Afin d'assurer un accès distant hautement sécurisé des employés aux ressources IT internes de l'organisation, nous avons jugé utile de présenter quatre types de scénarios. Chacun d'entre eux, apporte une approche différente, pointue et ciblée. Les scénarios sont indépendants les uns des autres mais peuvent être déployés simultanément pour se compléter, souvent pour des populations d'utilisateurs différents.

Les scénarios ont été classés en fonction de deux critères :

- **Complexité de mise en œuvre**. Dans un contexte de mise en place « urgente » du télétravail, la rapidité, et facilité pour la mise en œuvre, ainsi que la dépendance de composants externes sont les maîtres mots de la mise en œuvre. Il s'agit pour les décideurs du premier facteur évalué pour le choix des scénarios.
- **Robustesse.** Certains scénarios présentent une assurance sécurité maximum car ils intègrent par design un ensemble de contrôles sécurité. D'autres se contentent d'interdire l'accès à certains services internes. Ils sont limités à des technologies SI spécifiques et sont donc considérés moins robustes.

Le tableau ci-dessous synthétise l'évaluation des différents scénarios.

TABLEAU 1 : QUATRES SCÉNARIOS DE GESTION DE L'ACCÈS DISTANT

Scénarios	Complexité	Robustesse
Scénario 1 : Publication directe des services sur Internet	X	X
Scénario 2 : Accès aux services internes à travers des portails spécialisés	XXX	XX
Scénario 3 : Accès à travers un VPN	XX	XXXX
Scénario 4 : Accès à travers un poste de travail virtuel (VDI)	XXXX	XXXXX

Scénario 1 : publication directe des services sur Internet

Dans ce scénario, les services adoptés par les employés sont directement publiés sur Internet, leur utilisation nécessite uniquement la connaissance du couple identifiant/mot de passe.

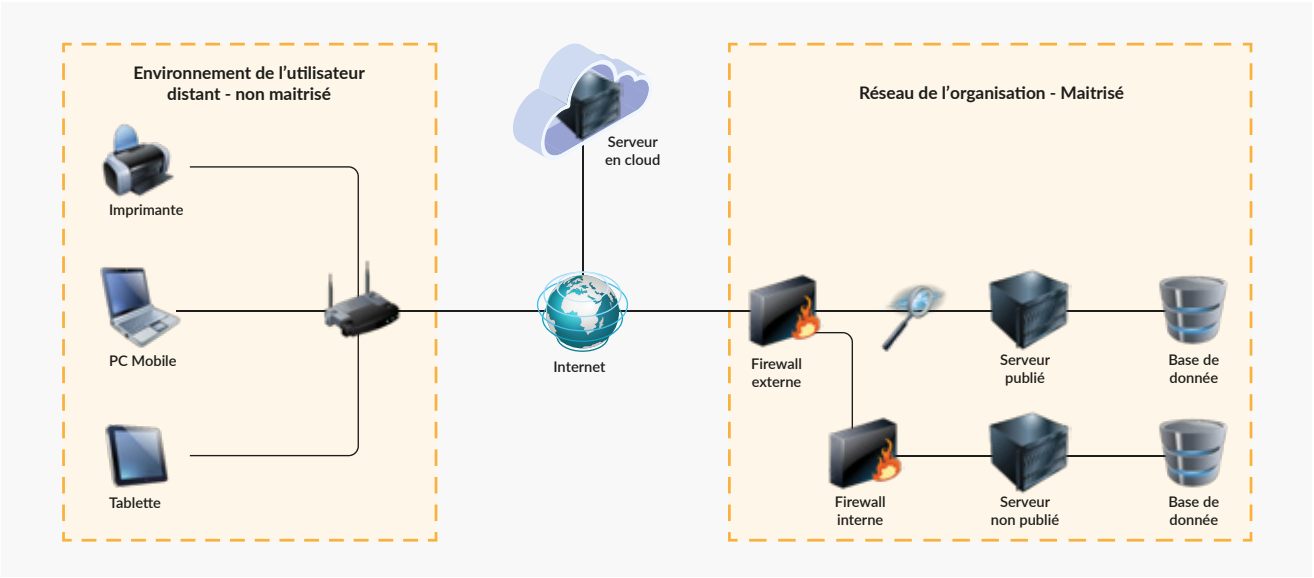


FIGURE 4 : ACCÈS DIRECT AUX SERVICES SUR INTERNET

Parmi les usages les plus fréquents nous pouvons citer :

- La messagerie électronique sous format Webmail ou à travers des clients lourds (Outlook)
- Les services de partage de contenu, ou de fichier ou d'intranet tel SharePoint, ou les portails d'achats pour les fournisseurs externes.
- Les services de téléphonie ou de vidéoconférence
- Dans ce scénario, les services peuvent être publiés sur le réseau de l'organisation, ou sur un environnement cloud dédié (dit private cloud).

Avantages du scénario :

Il s'agit du scénario le plus rapidement installable dans toute la gamme des plateformes compatibles. Il ne nécessite pour les organisations qu'un investissement minimal pour l'acquisition et la mise en place de nouvelles solutions techniques.

Le scénario reste aussi très simple pour les utilisateurs finaux, puisque les plateformes sont accessibles dès l'établissement des paramètres d'accès (URL, compte). Dans la plupart des cas, il ne nécessitera pas de configuration spéciale sur leurs postes de travail.

Inconvénients du scénario :

Toutes les applications ne sont pas compatibles avec ce scénario. En effet, celui-ci est conçu en fonction des applications accessibles par web, ou utilisant des protocoles pensés initialement pour Internet (services de messagerie, téléphonie IP, etc.).

En outre, les services mis en ligne sont directement accessibles sur Internet et le contrôle d'accès applicatif a généralement lieu après l'authentification. Ceci implique plusieurs risques :

- Toute vulnérabilité d'une composante du service mis en ligne (vulnérabilité serveur web, vulnérabilité serveur applicatif, vulnérabilité OpenSSL tel HeartBleed) pourra être exploitée par les cybercriminels pour compromettre le service et l'infrastructure qui l'héberge, pour récupérer des données d'authentification ou encore pour accéder à des données stockées sur la plateforme.
- Les cybers criminels maintiennent des listes des différents services accessibles sur Internet avec différents détails sur les composantes (des services professionnels tel Shodan.io facilitent même cette activité) et seront en mesure d'exploiter les nouvelles vulnérabilités, très souvent avant l'intervention des équipes sécurité.

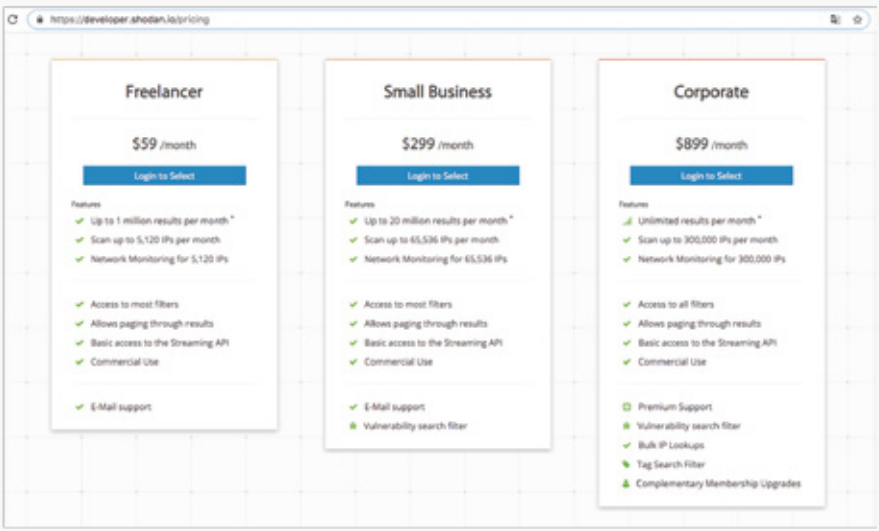


FIGURE 5 : LES FORMULES D'ABONNEMENT À LA PLATEFORME SHODAN.IO

3. PRINCIPES DE BASE DU PROGRAMME DE TELETRAVAIL

• En l'absence de mécanismes de gestion spécifique, il sera possible pour des cybercriminels déterminés, d'identifier les utilisateurs et d'essayer de récupérer par la force informatique brute les mots de passe utilisés pour l'authentification. Ces mots de passe en plus de donner des accès non autorisés aux services, pourraient être exploités pour attaquer d'autres services de l'organisation, ou pour lancer des attaques vers d'autres entités (hameçonnage de partenaires ou clients dans le cas de compromission du courriel par exemple).
• Ces services directement publiés sont naturellement plus exposés aux attaques de type DDOS qui vont saturer la capacité de traitement des services et les rendre indisponibles.
• Le poste de l'utilisateur n'est pas protégé et reste vulnérable aux différentes menaces sur son réseau wi-fi ou sur Internet.

Contrôles de sécurité à prévoir :

• La plateforme doit être conçue nativement pour résister aux attaques continues des cybercriminels. La plateforme doit respecter la charte de développement sécurisé créée par des experts indépendants préalablement à sa mise en ligne. Cette charte inclut le durcissement des différentes composantes et la révision du code chaque fois qu'un nouveau développement est ajouté.
• Après la mise en ligne, un examen de sécurité régulier doit être mené de façon à valider la robustesse de la plateforme face aux nouvelles techniques d'attaques.
• Dans la mesure de ce qui est possible sur le plan technologique, des composantes spécialisées doivent être installées en coupure de sorte à intercepter le trafic, l'analyser et bloquer les tentatives d'attaques (Firewalls, IPS, WAF, etc.).
• Une supervision continue de toutes les activités (malveillantes et légitimes) doit être effectuée sur les plateformes mises en ligne, avec des mécanismes de réponses bien rodés et réactifs de façon à bloquer tout attaquant potentiel.

Scénario 2 : Accès aux applications internes à travers des portails spécialisés

Dans ce scénario, les services utilisés par les employés sont mis en ligne sur un portail d'accès spécialisé, qui est lui-même directement disponible sur Internet.
Parfois les solutions VPN (voir scénario 3 dans la section suivante) intègrent cette fonctionnalité (sous l'appellation portail VPN SSL).

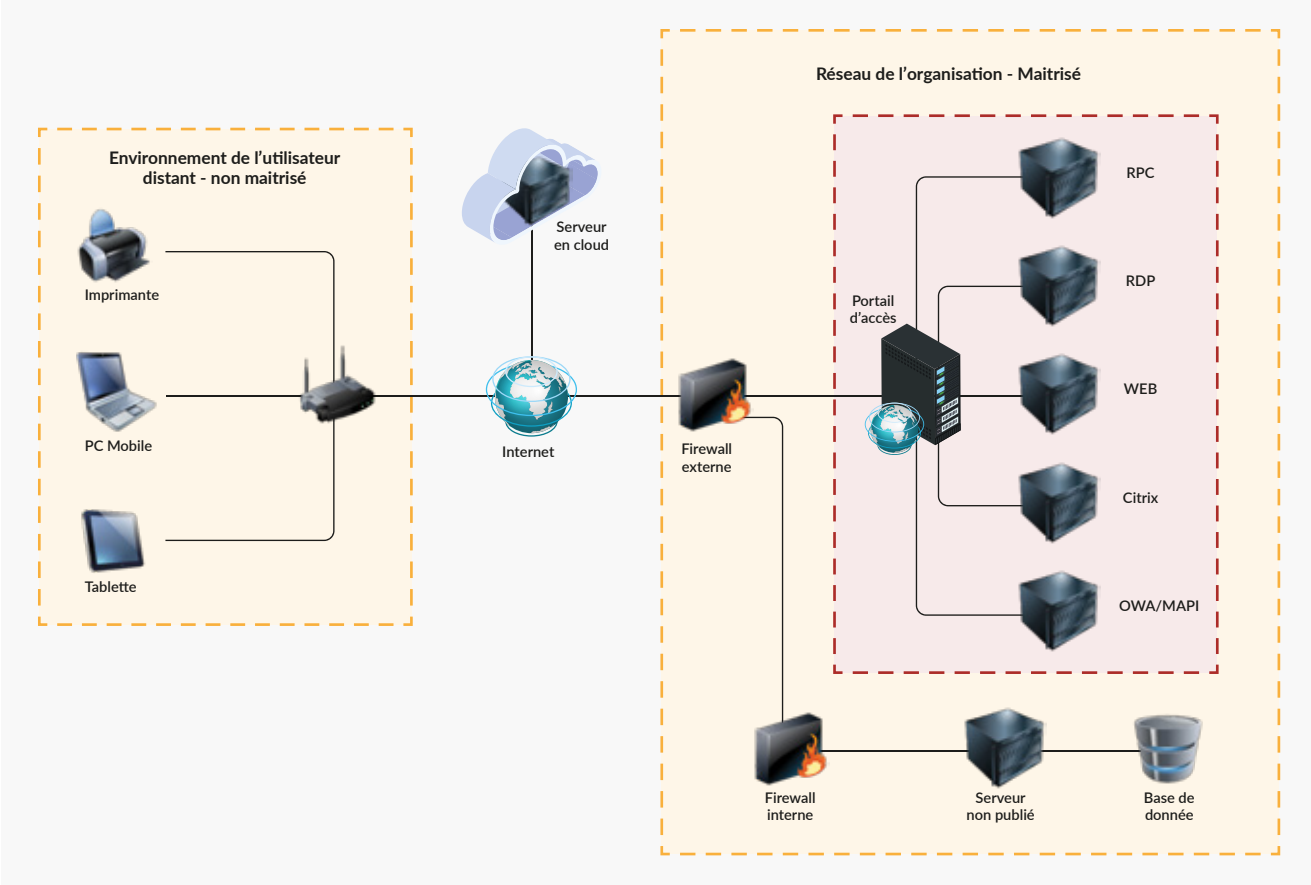


FIGURE 6 : ACCÈS AUX SERVICES AU MOYEN D'UN PORTAIL

Avantages du scénario :

• L'accès pour l'utilisateur final reste tout aussi simple que dans le scénario 1, car il n'y a pas de prérequis supplémentaire de son côté.
• Le portail de mise en ligne des applications est généralement un progiciel spécialisé conçu pour être continuellement disponible sur Internet et souvent indépendamment certifié comme sécurisé. Les services internes, quant à eux, ne sont techniquement plus exposés sur Internet. Également, il y a une rupture protocolaire des flux entre les services internes et les flux émanant d'Internet.
• Le portail permet généralement de centraliser, fédérer et sécuriser l'authentification pour les utilisateurs. Il est alors interfacé avec solution d'authentification forte, ce qui permet d'étendre ce contrôle pour toutes les applications, mêmes celles qui ne le soutiennent pas nativement.
• Le portail permet aussi de durcir le canal utilisé à travers l'adoption des derniers mécanismes de sécurisation (TLS1.3, Next Gen Encryption SP800-131A) indépendamment des limitations des services internes.
• Certaines plateformes intègrent aussi des mécanismes de traçabilité plus ou moins détaillés, permettant d'identifier plus facilement les tentatives d'utilisation frauduleuse des services par les cybercriminels.

Inconvénients du scénario :

• Toutes les applications internes ne sont pas compatibles avec ce scénario. Comme dans le cas du scénario 1, celui-ci est conçu pour les applications accessibles par web ou utilisant des protocoles initialement conçus pour Internet (services de messagerie, téléphonie IP, etc.).
• Une fois mis en ligne, le portail de publication devient un SPOF (Single Point Of Failure) et une cible de choix (High Value Target) pour les cybercriminels. À ce titre, le portail devra faire l'objet d'un suivi maximal en termes de sécurité et de réactivité pour le déploiement des correctifs.
• Dans ce scénario également, le poste de l'utilisateur n'est pas protégé et reste vulnérable aux différentes menaces sur son réseau wi-fi ou Internet. Un cybercriminel pourrait contrôler ce poste et récupérer les paramètres d'accès légitimes pour les réutiliser dans d'autres attaques malveillantes.

Contrôles de sécurité à prévoir :

• Une fois déployée, la solution du portail doit être reconnue comme sécurisée (certifications, références solides) et devra être paramétrée selon les meilleurs pratiques en termes de durcissement sécurité.
• Un examen exhaustif de sécurité devra être réalisé préalablement à la mise en ligne, puis régulièrement (au minimum chaque trimestre ou après chaque publication majeure) pour s'assurer de la robustesse de la plateforme face aux nouvelles techniques d'attaques.
• Le portail devrait être interfacé avec une solution d'authentification forte permettant de garantir l'identification des utilisateurs sur la base de mécanismes impossibles à briser (ce que je sais, ce que j'ai et/ou ce que je suis). Plus de détails dans la section 3.6 - Authentification à plusieurs facteurs.
• Si ce n'est pas déjà intégré et activé dans le portail, des solutions de coupe-feu devront être prévues pour protéger tous les sites et services web en ligne. Comme dans le scénario 1, une supervision continue de toutes les activités (malveillantes et légitimes) doit être effectuée sur les plateformes mises en ligne, avec des mécanismes de réponses bien rodés et réactifs de façon à bloquer tout attaquant potentiel.

Scénario 3 : Accès à travers un VPN

Dans ce scénario, une passerelle VPN est utilisée au niveau central pour contrôler les accès vers les services publiés. Un VPN est un « tunnel » sécurisé qui relie l'appareil du télétravailleur au réseau de l'organisation. Une fois le tunnel établi, le télétravailleur peut accéder à de nombreuses ressources informatiques de l'organisation (applications, serveurs de fichiers et imprimantes). L'utilisation d'un VPN nécessite l'installation et la configuration d'un logiciel client sur chaque dispositif de télétravail. Diverses applications, telles qu'un traitement de texte pour la visualisation et la modification de documents, peuvent également devoir être installées.

En raison des besoins d'installation et de configuration des logiciels, l'accès via un VPN est généralement réservé à des ordinateurs fournis et contrôlés par l'organisation. Toutefois, certaines organisations autorisent les télétravailleurs à installer des clients VPN sur leurs propres ordinateurs et appareils mobiles. Dans ce cas, le logiciel client est le plus souvent préconfiguré par l'organisation et fourni aux télétravailleurs. Il est aussi possible de permettre aux télétravailleurs d'acquérir leurs propres clients VPN.

3. PRINCIPES DE BASE DU PROGRAMME DE TELETRAVAIL

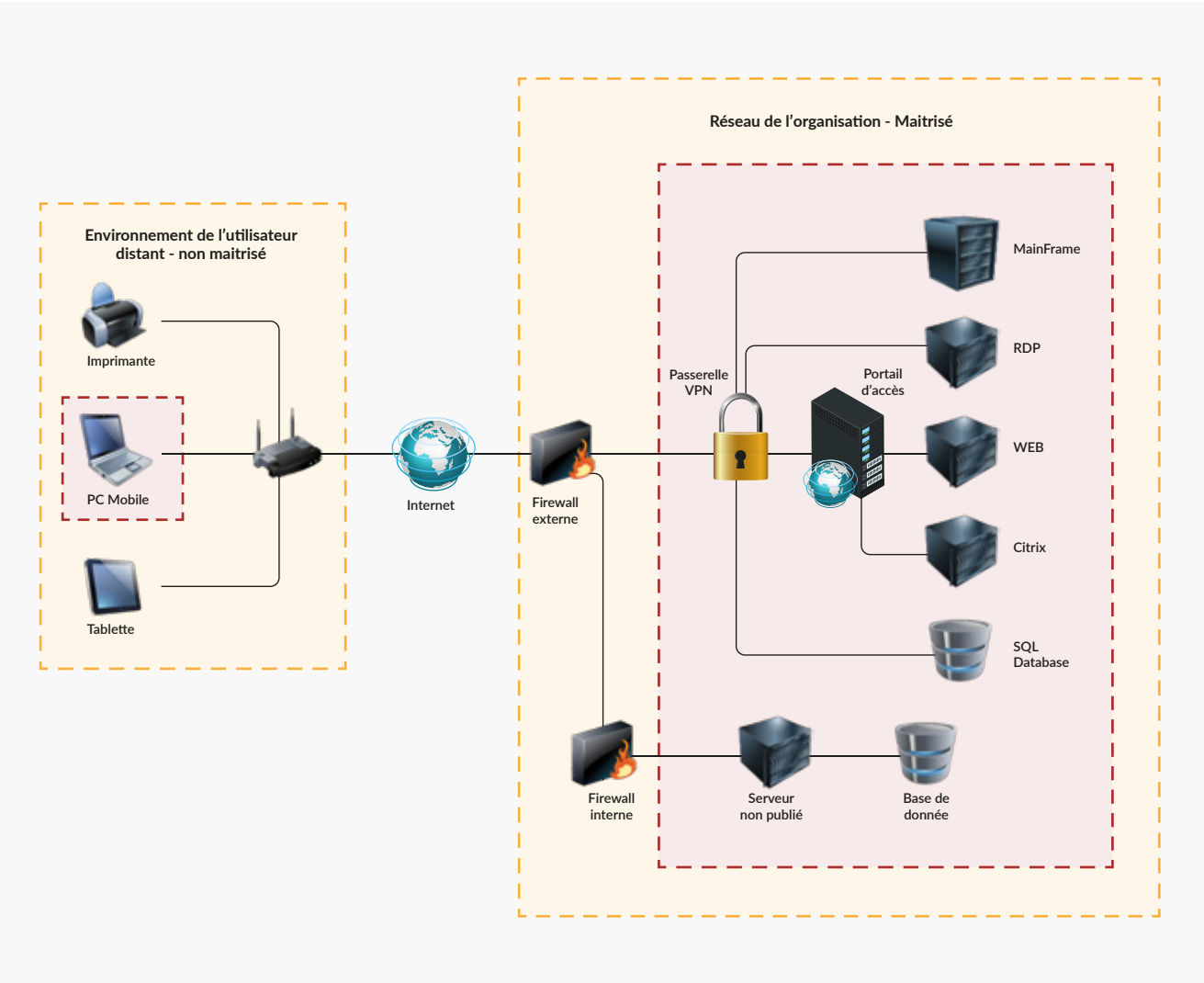


FIGURE 7 : ACCÈS AUX SERVICES AU MOYEN D'UN VPN

À la différence des scénarios 1 et 2, une fois le VPN établi, l'utilisateur final disposera d'un accès IP quasi similaire à celui dont il dispose depuis le réseau de l'organisation. Les seules limites seront la performance réseau et, bien sûr, les autorisations attribuées.

Il n'est pas exclu de mettre au point un environnement où l'utilisateur après connexion au VPN, soit autorisé à accéder uniquement au portail (scénario 2) pour avoir accès aux services internes (pour plus de détails sur le VPN, voir la section 3.5 - VPN et accès distant).

Avantages du scénario :

• La passerelle VPN est généralement un composant spécialisé conçu pour être continuellement exposé sur Internet et souvent indépendamment certifié comme sécurisé.
• Pour donner un accès complet au réseau de l'organisation, la passerelle VPN encapsule et sécurise le trafic depuis le réseau de l'organisation jusqu'au poste de l'utilisateur. Les administrateurs n'autorisent que le trafic nécessaire selon le profil des utilisateurs. Ces possibilités d'extension du réseau de l'organisation font que le service VPN était classiquement utilisé pour les accès d'administration informatique ou de la haute direction, avant que son utilisation soit de plus étendue vers des accès métiers plus diversifiés.
• Le concentrateur VPN peut aussi sécuriser les accès à travers l'interfaçage avec une solution d'authentification forte.
• Le logiciel installé sur le poste du client peut être configuré pour isoler le poste de travail (désactivation de la fonction de split-tunneling), de sorte que l'ordinateur soit uniquement connecté au réseau de l'organisation, et qu'il ne permette pas à des cybercriminels de se connecter par rebond au réseau de l'organisation depuis le poste compromis de l'utilisateur.
• Certains logiciels de VPN permettent aussi de vérifier la conformité du poste de travail (antivirus actif et à jour, correctifs de sécurité installés, privilèges utilisateurs restreints, poste appartenant à l'organisation, etc.) préalablement à sa connexion au réseau et peuvent déclencher les actions de correction de manière automatisée.
• L'accès VPN permet d'utiliser des services qui utilisent le protocole IP, c'est-à-dire la grande majorité des flux qu'on retrouve dans un environnement standard, ce qui en fait une solution compatible avec les différents services internes.

Inconvénients du scénario :

• Comme dans le scénario 2, la plateforme VPN devient un SPOF (Single Point Of Failure) et une cible de choix (High Value Target) pour les cybercriminels. Elle devra donc faire l'objet d'un suivi permanent en termes de sécurité et de réactivité pour le déploiement des correctifs.
• La compromission de la plateforme VPN ou des erreurs dans sa configuration pourrait avoir un impact plus important sur la sécurité de l'organisation, en raison de l'étendue des accès permis par la solution.
• Ce scénario nécessite l'installation d'un logiciel (client VPN) sur les postes utilisés pour l'accès. Si ce procédé est relativement simple sur les tablettes et téléphones mobiles, il demeure plus complexe sur les postes de travail fixes car ils nécessitent des privilèges élevés, et peuvent souffrir d'incompatibilité notamment sur des postes de travail non maitrisés.

Contrôles de sécurité à prévoir :

• Identique au scénario 2.

3. PRINCIPES DE BASE DU PROGRAMME DE TELETRAVAIL

Scénario 4 : Accès à travers une infrastructure de bureau virtuel (VDI)

Dans ce scénario, tous les accès distants se font vers une infrastructure de bureau virtuel (virtual desktop infrastructure – VDI) contenant l'environnement de l'utilisateur. Ce poste hébergé et exécuté depuis le centre de données de l'organisation regroupe les applications, documents et autres données adoptés par l'utilisateur.

Généralement cet environnement virtuel est utilisé pour tout accès aux services métiers aussi bien depuis le réseau de l'organisation que depuis l'extérieur du réseau. Il s'agit d'un environnement indépendant du poste utilisé qui permet donc naturellement le télétravail dès lors que ce poste virtuel est accessible à distance (portail ou VPN). Les mesures de sécurité sont appliquées sur l'infrastructure de bureau virtuel et non plus sur le poste utilisé pour l'accès.

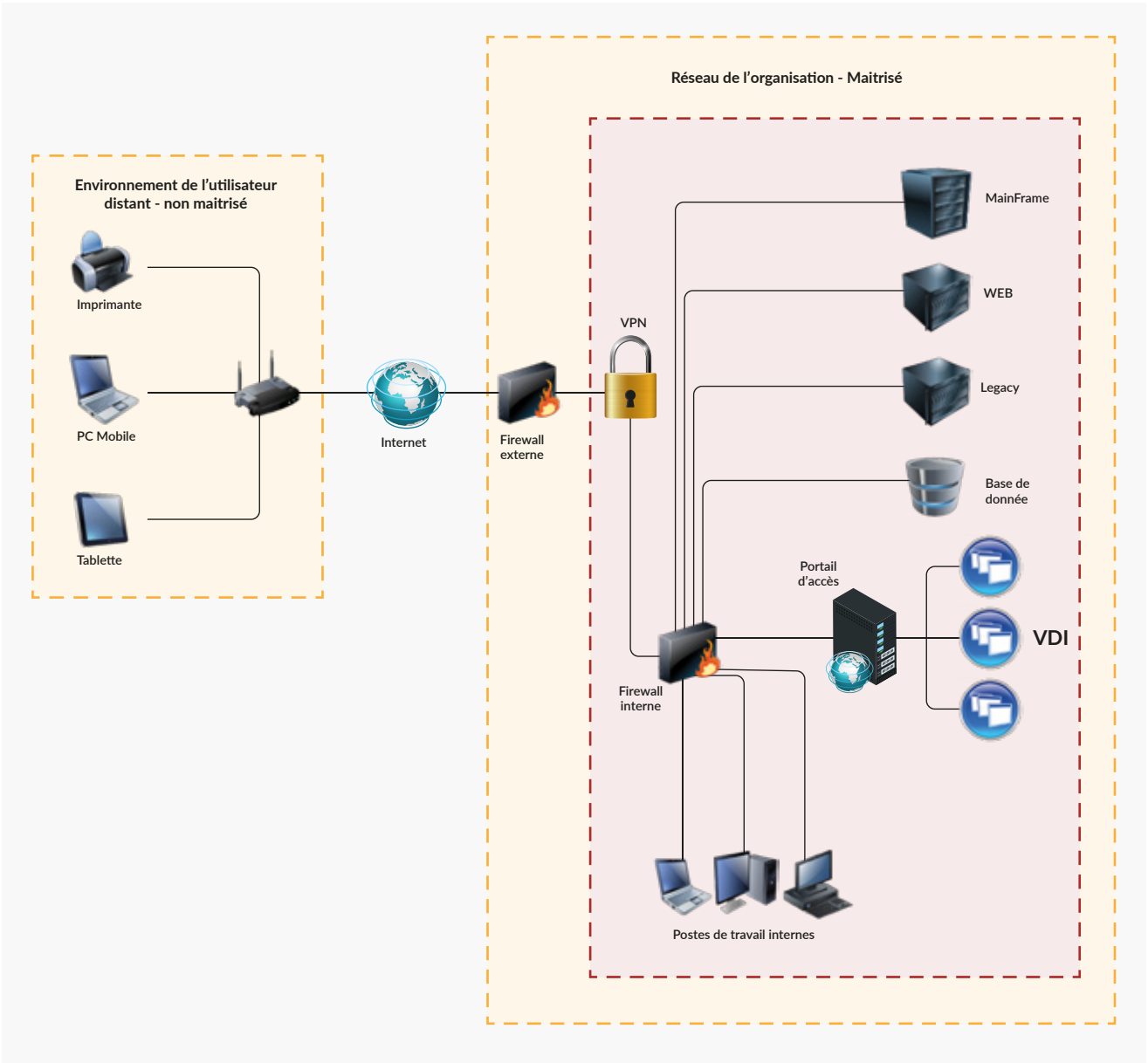


FIGURE 8 : ACCÈS AUX SERVICES AU MOYEN D'UNE INFRASTRUCTURE DE BUREAU VIRTUEL

Avantages du scénario :

• Ce mode permet une couverture maximale en termes d'accès distant aux services de l'organisation, puisque les services accessibles à l'externe sont équivalents à ceux accessibles depuis l'interne.
• Ce scénario permet aussi d'assurer, de mieux contrôler les données de l'organisation qui peuvent être confinées aux postes virtuels dans ses centres de données et de ne plus se soucier de les sécuriser sur les postes de travail utilisés pour l'accès.
• Les efforts de sécurité seront orientés vers l'infrastructure de bureau virtuel qui est entièrement maîtrisée et exclusivement dédiée aux activités professionnelles. Les postes de travail peuvent alors être utilisés pour les accès Internet ou autres, sans avoir d'impact significatif sur la sécurité de l'organisation.
• Les utilisateurs retrouvent toujours le même environnement, indépendamment de l'équipement utilisé pour l'accès (ordinateur fixe, portable, Windows ou Mac, voire aussi tablette et téléphone).
• Il est aussi possible de profiter de la centralisation des accès pour mettre en place des outils de traçabilité et de supervision de la productivité.

Inconvénients du scénario :

• Ce scénario nécessite un investissement initial significatif pour la mise en place de l'infrastructure de virtualisation des postes de travail.
• Il sera aussi nécessaire de mettre en place un accès VPN ou un portail d'accès (scénarios 2 ou 3) pour permettre l'accès aux postes de travail virtuels depuis Internet.
• Comme dans les scénarios 2 et 3, la plateforme VPN devient un SPOF (Single Point Of Failure) et une cible de choix (High Value Target) pour les cybercriminels. Elle devra donc faire l'objet d'un suivi permanent en termes de sécurité et de réactivité pour le déploiement des correctifs.

Contrôles de sécurité à prévoir :

• Les images des postes de travail virtuel devraient faire l'objet d'un durcissement maximal et être strictement cloisonnées d'Internet. Ils devraient par ailleurs faire l'objet d'examens de sécurité exhaustifs et réguliers.
• L'accès distant aux postes virtuels doit être effectué à travers un portail ou un une plateforme VPN (respectivement scénarios 2 et 3) avec une authentification forte.
• Il est préconisé que les utilisateurs effectuent une authentification double pour l'ouverture de session sur les postes de travail.

3. PRINCIPES DE BASE DU PROGRAMME DE TELETRAVAIL

3.2 - Outils de télétravail

Le télétravail nécessite une communication fluide et efficace. Les boites de courriel encombrées de messages étant contre-productives, il est préférable d'utiliser des outils de communication spécialement conçus pour le « coworking ».

Cette section présente un ensemble d'outils pratiques issus des retours d'expérience de projets pilotes conduits en entreprise permettant de faciliter le télétravail.

3.2.1 - Plateformes de télétravail coopératif

Bonne nouvelle, la plupart des technologies qui permettent le travail à distance, comme le service de vidéoconférence Hangouts Meet et la messagerie Slack, sont désormais abouties et fiables. La mauvaise nouvelle, c'est que leur mode d'emploi est encore à inventer . Voilà pourquoi, la planification du télétravail et la formation des employés sont deux préalables indispensables. Bien conçue, la transition au télétravail peut non seulement aider à traverser une crise comme celle que nous connaissons, mais revigorer l'ensemble du processus de gestion. Ci-après une « check-list » de critères indispensables à avoir dans les outils de travail choisis:

- Communications unifiées.
- Intégration des applications professionnelles.
- Personnalisation et évolutivité pour les équipes.
- Facilité de recherche des fichiers, des contenus et des personnes.
- Enregistrement des conférences et archivage en accès partagé.
- Simplicité d'utilisation pour les employés ainsi que le service informatique de l'organisation.
- Sécurité de bout en bout (chiffrement des échanges, etc.).

Pour vous aider à faire le choix le plus adapté à vos besoins, nous avons effectué une sélection parmi les outils les plus utilisés. Cette liste n'a pas la prétention d'être un classement des meilleures plateformes de télétravail, ni celle d'être exhaustive, il s'agit tout au plus d'une liste indicative pour faciliter le travail des praticiens.

Microsoft Teams : Ce réseau social est intégré dans Office 365 et n'induit donc aucuns frais supplémentaires pour les utilisateurs de la suite. Cette intégration dispose d'une foule de caractéristiques facilitant la coopération, parmi elles:

- Une conversation incluant du texte, du son, des vidéos et la possibilité de partager des fichiers et les écrans;
- Une conversation privée, idéale pour le développement d'une idée, puis possibilité de partage avec l'ensemble de l'organisation;
- Stockage de tous les fichiers et documents au même endroit ;
- Intégration de vos applications favorites: Trello, GitHub, Planificateurs, etc.
- Liaison avec SharePoint.
- Enregistrement des réunions et des conférences ;
- Intégration des fonctionnalités de communication et de téléphonie de Skype Entreprise, etc.

En mars 2020, Microsoft Teams comptait 44 millions d'utilisateurs. Microsoft propose une déclinaison gratuite de Microsoft Teams pour les PME, limitée à 300 utilisateurs, avec à la clé une capacité de stockage incluse de 2 Go par utilisateur et 10 Go de stockage partagé. La version payante commence à partir de 4,20$ US/mois et par utilisateur.

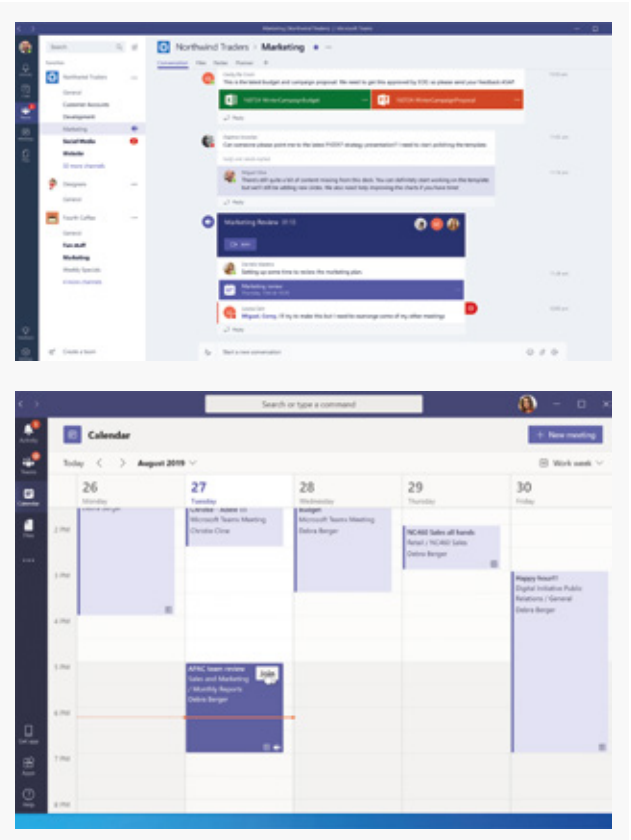


FIGURE 9 : INTERFACE DE L'OUTIL MICROSOFT TEAMS

7 Tim Bradshaw, "Travail à distance : les bonnes pratiques", Courrier international, 13 mars 2020.

G Suite : La G Suite (ancien Google Apps for Work) est un logiciel multifonctionnel de collaboration fourni sur le cloud. C'est la version de Google Drive pour les entreprises, qui comprend des logiciels de productivité populaires comme Google Docs, Sheets et Slides, un espace de stockage des documents (30 Go par utilisateur en version de base) ainsi qu'une application de vidéoconférence. La G Suite permet aux équipes d'accéder aux données, calendriers, planifications de projets etc. en utilisant simplement une connexion Internet et un navigateur. Des fonctions de partage et de synchronisation en temps réel fluidifient le travail en équipe. Google affirme que la plateforme avait cinq millions d'utilisateurs payants à la fin de 2019[8] . La plateforme est offerte à partir de 6$ US/mois et par utilisateur.

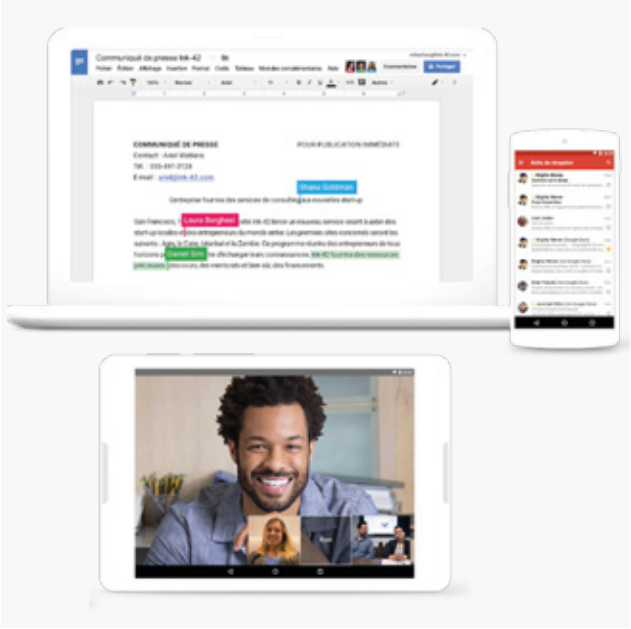


FIGURE 10 : INTERFACE DE L'OUTIL G SUITE

Slack : Ce logiciel de travail collaboratif est destiné à créer un réseau de travail à l'échelle de l'organisation. L'application se propose de rendre collectifs les messages et de les classer sous forme de chaînes comme sur un réseau social ou sur une discussion WhatsApp. Le but du logiciel est de rompre l'isolement des messages et de permettre la création de groupes de travail.

Avec Slack, par exemple, vous créez des rubriques pour transférer documents et fichiers audio ou vidéo aux membres de votre équipe. Vous échangez via une messagerie instantanée et faites évoluer votre projet en temps réel, chacune de vos actions étant instantanément mise à jour et visible de tous les participants. Slack fluidifie nettement les échanges à distance, contrairement au courriel, dont le mode de fonctionnement ne permet pas d'être efficace face à un gros volume d'échanges[9].

Slack comporte 12 millions d'utilisateurs actifs. Avec une belle interface et la possibilité de partager des données, vous pourrez essayer gratuitement et de manière illimitée l'application avec l'intégration de logiciels classiques du pack Office 365, ou même des applications développées par Google. Pour un service plus complet, vous pouvez souscrire à des formules Standard, Plus ou Entreprise Grid à partir de 8$ US/mois.

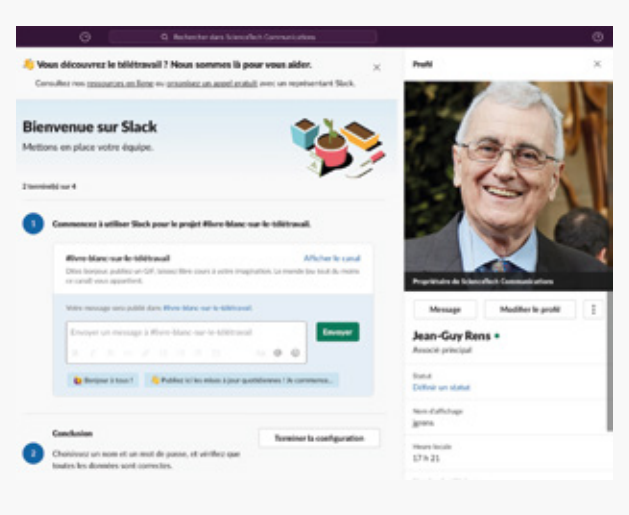


FIGURE 11 : INTERFACE DE L'OUTIL SLACK

8 Google affirme parfois que la G Suite compte deux milliards d'utilisateurs, mais les observateurs estiment qu'il s'agit principalement des utilisateurs du service de courriel Gmail.

9 Christelle Ibach, « Coronavirus et télétravail : les meilleures applications du manager », Cadre & Dirigeant Magazine, 17 mars 2020. https://www.cadre-dirigeant-magazine.com/manager/teletravail-meilleures-applications-manager/

3. PRINCIPES DE BASE DU PROGRAMME DE TELETRAVAIL

DingTalk : La plateforme DingTalk du géant chinois Alibaba possède un grand nombre de fonctionnalités identiques à celles de Slack, notamment les communications de groupe, les appels vocaux et vidéo et le partage de fichiers. Toutefois, DingTalk comprend également une série de fonctions de surveillance que l'application américaine ne possède pas. La fonction de message DingTalk permet aux responsables d'envoyer un « ping » à des employés spécifiques, non seulement dans l'application, mais aussi par le biais d'appels téléphoniques et de messages texte automatisés.

La fonction d'horloge d'entrée/sortie de l'application envoie des rappels aux utilisateurs sur le nombre de minutes qui leur restent avant de commencer le télétravail. DingTalk enregistre également l'heure à laquelle les employés commencent à travailler en enregistrant l'heure à laquelle ils se connectent au wi-fi du bureau et celle à laquelle ils se déconnectent, par exemple pour aller déjeuner. Si cette fonction permet également aux travailleurs de suivre et d'être payés pour les heures supplémentaires, elle permet également aux organisations de mesurer les retards à la minute près, et de savoir si un travailleur fait ce qu'il a dit qu'il ferait lorsqu'il n'est pas au bureau.

DingTalk adopte une approche à structure légère qui permet à des fournisseurs tiers d'offrir des services sur sa plate-forme. L'application exécute les fonctions de base à l'interne – la messagerie en étant une – mais elle ne veut pas tout faire elle-même. La cybersécurité, la réservation de voyages d'affaires et l'achat de papeterie de bureau, à titre d'exemple, sont offerts par des entreprises spécialisées, transformant DingTalk en écosystème très diversifié.

Le résultat de ce mélange de souplesse de de précision chirurgicale dans le contrôle des ressources humaines est que DingTalk est la première plateforme de télétravail au monde avec déjà 200 millions d'utilisateurs à la fin de 2019 – depuis la crise du coronavirus, le nombre d'utilisateurs a explosé. L'application est entièrement gratuite, mais n'existe qu'en version anglaise.

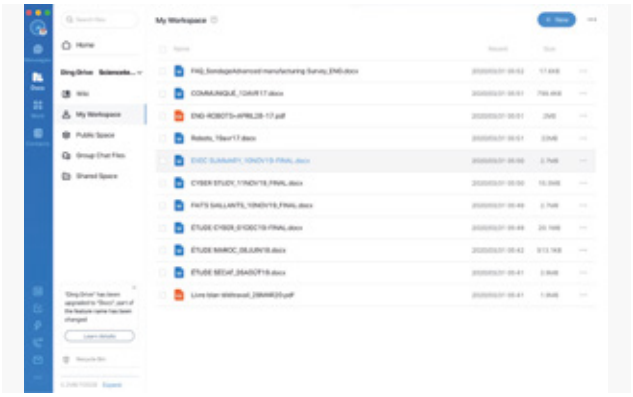


FIGURE 12 : INTERFACE DE L'OUTIL DINGTALK

Cisco Webex Teams : Anciennement connu sous le nom de Cisco Spark, la plateforme de Cisco fournit un environnement virtuel intégré pour la messagerie individuelle, le chat et le partage de contenu, ainsi que pour les réunions audio, vidéo et web. Au nombre de ses fonctionnalités se trouvent :

- Envoi de messages et partage ds fichiers en toute sécurité et sans limite.
- Voir les fichiers instantanément sans téléchargement pour accéder rapidement aux informations importantes.
- Travailler en toute confiance avec un cryptage de bout en bout du contenu afin que seuls les destinataires visés puissent lire les messages et les fichiers partagés.
- Commencer les réunions en face à face avec partage d'écran pour accélérer la prise de décision.
- Examiner l'historique des messages et des fichiers afin que chacun puisse toujours être à jour, quel que soit son fuseau horaire ou son lieu de résidence.

La plateforme Cisco Webex Team compte 130 millions d'utilisateurs actifs. La version personnelle est gratuite, tandis que la version d'affaires commence à 17,95$ US/mois par utilisateur dans la version PME.

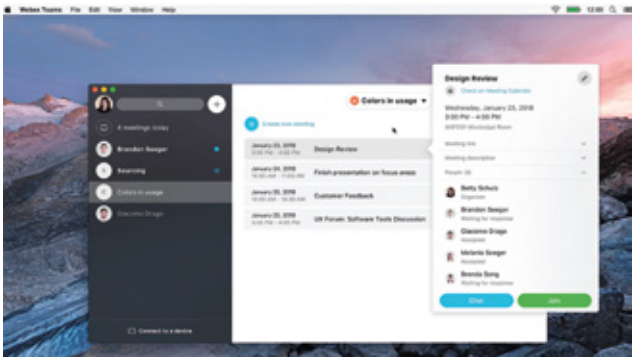


FIGURE 13 : CISCO WEBEX TEAMS

3.2.2 - Outils de vidéoconférence

Le système de vidéoconférence **Hangout Meet** par Google est disponible gratuitement en raison de la pandémie de coronavirus. Si vous utilisez G-Suite ou G-Suite for Education, vous pourrez également bénéficier gratuitement des fonctionnalités avancées de vidéoconférence de Hangouts Meet jusqu'au 1er juillet 2020, avec la possibilité d'organiser des meetings jusqu'à 250 participants et enregistrer les vidéoconférences.

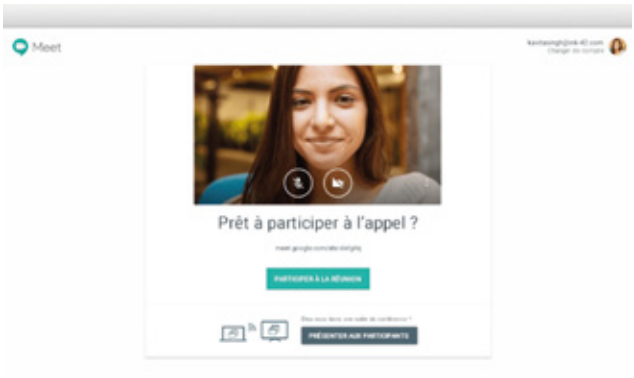


FIGURE 14 : INTERFACE DE L'OUTIL HANGOUT MEET

La solution **Skype** de vidéoconférence de Microsoft : La version grand public de Skype est idéale pour les travailleurs indépendants ou les sociétés jusqu'à 20 personnes et elle s'interface parfaitement dans un groupe utilisant Skype Entreprise. Dans cette version professionnelle, on peut créer des réunions jusqu'à 250 employés, inviter des équipes à l'aide de liens personnalisés, partager un écran ou un fichier. Il est également possible d'envoyer des messages instantanés lors d'une réunion pour proposer des nouvelles idées, télécharger des présentations PowerPoint, des annotations, etc.

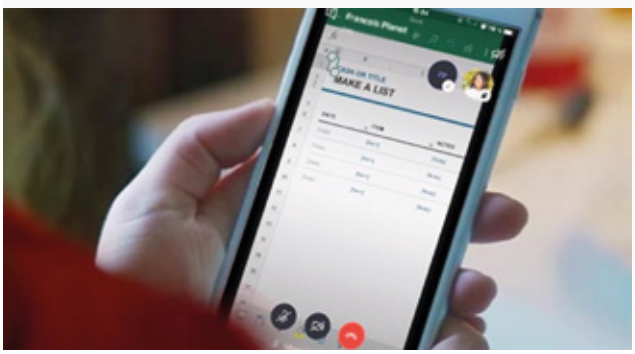


FIGURE 15 : INTERFACE DE L'OUTIL SKYPE

GoToMeeting permet d'organiser des conférences web en toute sécurité. Il propose un essai gratuit avec jusqu'à 250 participants pour 14 jours. Ci-dessous quelques fonctionnalités :

- Vidéo HD, Partage d'écran
- Ligne de téléconférence
- Nombre illimité de réunions
- Réunions de durée illimitée
- Business Messaging
- Espace de réunion personnel
- Chiffrement Secure Socket Layer (SSL)
- Chiffrement AES sur 256 bits
- Centres de données certifiés SOC2 et Conformité HIPAA
- Enregistrement mobile dans le cloud

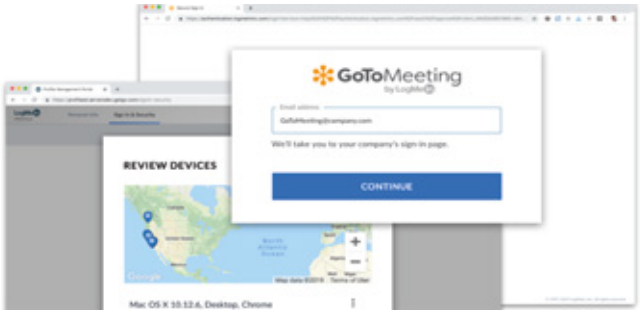


FIGURE 16 : INTERFACE DE L'OUTIL GOTOMEETING

3.2.3 - Outils de partage et de stockage des documents

Les services de stockage cloud (Google Drive, Dropbox, Miscrosoft OneDrive, Apple iCloud, etc.) demeurent une bonne alternative pour avoir accès en temps réel à tous les documents partagés. L'espace de stockage fourni dépendra du forfait et de la version que vous choisirez (gratuite ou payante).

3. PRINCIPES DE BASE DU PROGRAMME DE TELETRAVAIL

3.2.4 - Outils de coordination

Les outils de coordination comme Trello, Asana, Droptask ou encore Azendoo sont des bons outils pour définir les missions à effectuer pendant une journée de travail à distance. Ils permettent de suivre l'avancée des projets, d'assigner des tâches à des employés. Certains d'entre eux sont gratuits et possèdent de nombreuses fonctionnalités.

3.2.5 - Les outils de support et de prise en main à distance

Cisco Webex Support est une plateforme conviviale pour assurer l'assistance technique à distance. Elle propose plusieurs fonctionnalités permettant de :

- Réduire le nombre de déplacements en offrant un service de téléassistance rapide ;
- Accélérer le diagnostic et la résolution des problèmes technique en travaillant directement sur les ordinateurs des utilisateurs ;
- Échanger directement avec les utilisateurs via le « chat » instantané afin de faciliter la compréhension des demandes et des problèmes ;
- Contrôler le bureau à distance ;
- Enregistrer les sessions afin de garder les traces des échanges ;
- Transférer les fichiers depuis le poste de l'utilisateur (logs, message d'erreur, etc.) ;
- Sécuriser les échanges par des technologies de chiffrement telles que SSL et AES.

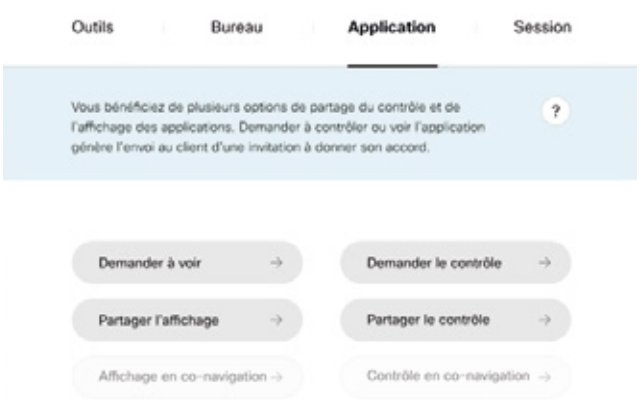


FIGURE 17 : INTERFACE DE L'OUTIL CISCO WEBEX SUPPORT

Microsoft Teams : Outre les fonctionnalités de télétravail classique, Microsoft Teams permet la prise de contrôle sur les postes de travail pour réaliser des actions de télémaintenance. Si vous voulez qu'un autre participant modifie un fichier, vous aide à présenter ou à montrer quelque chose, vous pouvez lui donner le contrôle. Les deux parties pilotent alors ensemble le contrôle, mais l'utilisateur initial peut reprendre la maîtrise à tout moment.

FIGURE 18 : INTERFACE DE L'OUTIL MICROSOFT TEAMS

3.3 - Spécial COVID-19

Par mesure de solidarité à l'occasion de la crise du corona-virus, plusieurs éditeurs d'applications offrent des solutions temporaires pour faciliter le télétravail.

3.3.1- Offre spéciale de Cisco

L'offre Cisco pour assurer une connectivité sécurisée des organisations durant cette pandémie consiste à proposer :

• Accès VPN des licences AnyConnect PLUS/APEX gratuites de 90 jours pour les clients disposant des boîtiers ASA ou Cisco FTD.

• Pour les nouveaux clients, la proposition de l'ASAv30 sur cloud privé ou public avec une remise de 75% incluant les 750 licences AnyConnect gratuitement.

• La solution d'authentification Mulifacteur DUO avec une licence d'évaluation étendue de 30 jours supportant toutes les fonctionnalités.

• L'extension de la licence d'évaluation d'Umbrella jusqu'à 90 jours afin de sécuriser la navigation Internet des utilisateurs nomades.

3.3.2 - Offre spéciale de Fortinet

L'entreprise de cybersécurité Fortinet accompagne ses clients lors de la transition vers le télétravail sans l'ajout d'un coût supplémentaire :

• La plate-forme de pare-feu d'entreprise Fortigate inclut les fonctionnalités et les outils nécessaires pour assurer une connectivité sécurisée pour les employés.

• Fortinet offre une version gratuite pour l'accès distant : FortiCLient VPN.

• Une plateforme gratuite de E-Learning qui fournit les informations de base sur la cybersécurité.téléphonie de Skype Entreprise, etc.

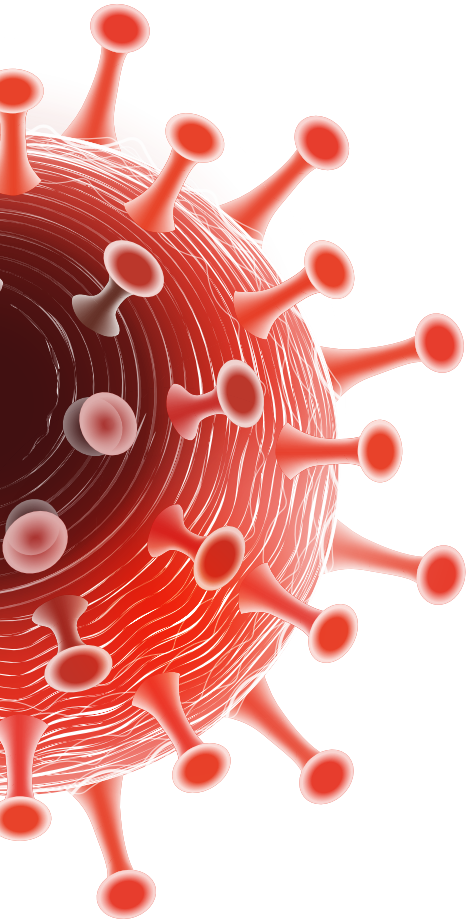
3.3.3 - Offre spéciale de Palo Alto Networks

Afin d'assurer la continuité des activités aux organisations en leur assurant le même niveau de sécurité au télétravail que dans leurs locaux, Palo Alto Networks offre :

•Une souscription gratuite et rapide aux services de Global Protect pour les clients disposant d'un pare-feu de nouvelle génération (physique ou virtuel).

• Une extension du nombre des utilisateurs supportés par la plateforme Prisma Access pour une durée de 90 jours.

• Les clients intéressés par la solution Prisma Access reçoivent un soutien professionnel pour le déploiement rapide de la solution gratuitement pendant 90 jours.



4 STRATÉGIE DE SÉCURITÉ POUR LE TÉLÉTRAVAIL

4. STRATÉGIE DE SÉCURITÉ POUR LE TÉLÉTRAVAIL

4.1- Introduction

Ce chapitre aborde les attaques sur le télétravail et illustre les stratégies sectorielles destinées à rendre cette activité sécuritaire.

4.2- Attaques sur un système de télétravail

D'un point de vue technique, les attaques ciblant un système d'information de télétravail peuvent se classer en sept grandes catégories :

1• Écoutes passives : Ces attaques peuvent aller de l'espionnage visuel à la mise en écoute du réseau, en passant par l'analyse des signaux compromettant (TEMPEST).

2• Attaques ayant essentiellement un impact sur la confidentialité. Les données écoutées sont compromises.

3• Dénis de service : Ces attaques auront essentiellement un impact sur la disponibilité des SI.

4• Intrusions (accès non autorisé avec prise de contrôle à distance) : Ces attaques peuvent avoir plusieurs types d'impacts :

- Impact sur la confidentialité : À la suite d'une intrusion réussie, les données accessibles à partir de la cible de l'attaque peuvent être compromises.
- Impact sur la disponibilité : À la suite d'une intrusion réussie, un déni de service peut être effectué par l'attaquant.
- Impact sur l'intégrité : Les données et services accessibles à partir de la cible d'une attaque réussie peuvent être modifiées par l'attaquant
- Impact sur la preuve : les journaux de preuves peuvent être effacés par l'attaquant suite à une attaque réussie. Les traces peuvent être également altérées par injection de fausses entrées ou attribution d'actions au mauvais acteur.

5• Les vols de données (confidentialité) ou la modification des données (intégrité) lors de leur stockage sur le support de travail (smartphone, ordinateur fixe ou portable, tablette).

6• Les attaques contre les moyens de détection et de traçabilité.

7•Les attaques causées par une mauvaise configuration technique (au niveau de l'infrastructure VPN, au niveau du poste de travail, au niveau des serveurs applicatifs).

Il faut aussi tenir compte des défaillances d'ordre organisationnel qui donnent la possibilité aux attaquants de cibler un système de télétravail. Nous les avons regroupées comme suit :

• Manipulation des utilisateurs (en particulier ceux ayant des accès à privilèges) au moyen de manœuvres d'ingénierie sociale. Les employés non sensibilisés aux bonnes pratiques de sécurité sont particulièrement à risque.

• Absence d'inventaire des équipements du télétravail, surtout quand ils appartiennent aux employés et non à l'organisation (appareils non déclarés ou changement d'appareils sans notification).

• Absence de classification des actifs essentiels de l'organisation.

• Absence de cartographie des risques, laissant ainsi un flou sur la gestion des priorités des projets d'investissement en sécurité.

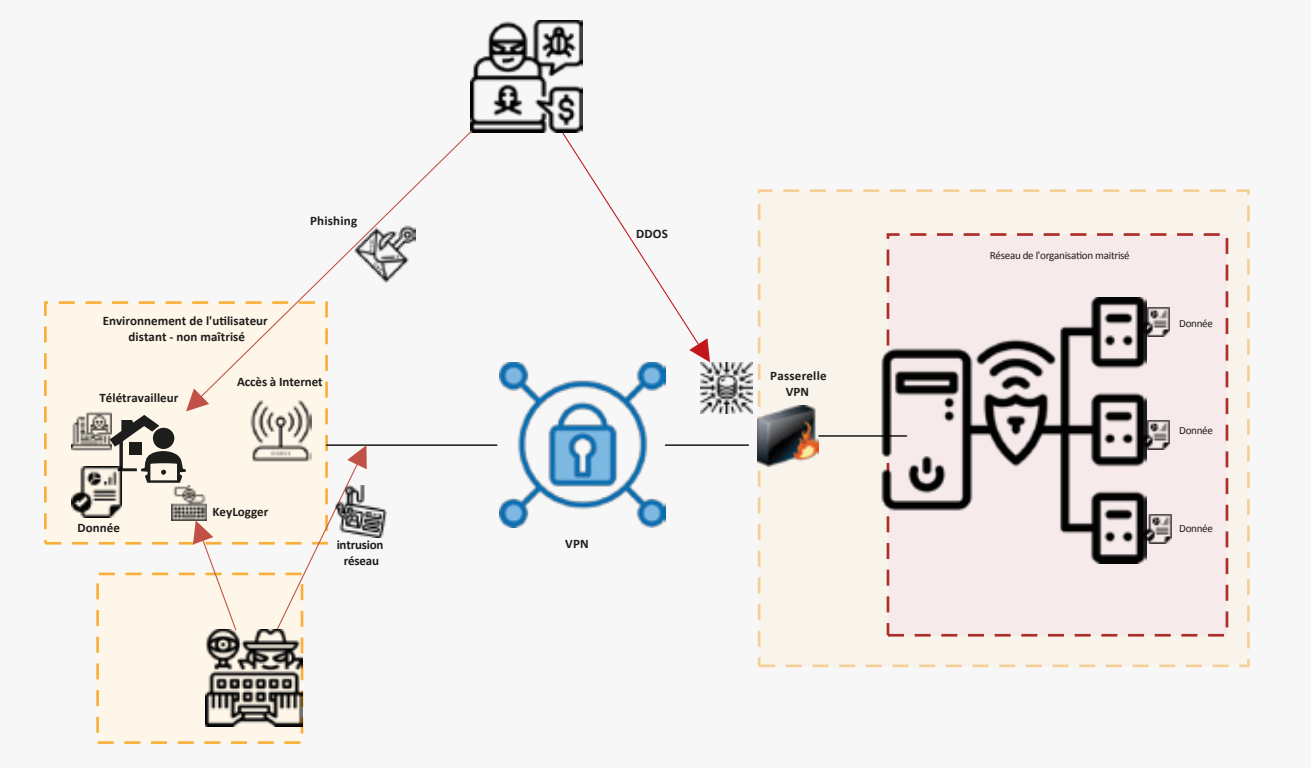


FIGURE 19 : CARTOGRAPHIE DES RISQUES DANS UN ENVIRONNEMENT DE TÉLÉTRAVAIL

4.3 - Classification des données et analyse des risques

Avant de mettre en place un projet de télétravail, l'organisation doit identifier clairement les risques qu'elle encourt. Voilà pourquoi, elle doit classer ses données et ressources selon leur degré de criticité. Si la mission d'un employé implique un accès permanent à des informations critiques (par exemple le core banking dans le métier bancaire), celle-ci doit faire l'objet de mesures techniques renforcées et d'une supervision continue.

Il convient en premier lieu d'identifier les informations les plus sensibles afin de mettre en place des mécanismes de sécurité renforcés – dans un contexte de pandémie, quand tous les employés fonctionnant en mode télétravail, il est impossible d'en interdire l'accès à distance.

Une information accessible en télétravail, doit être protégée en fonction de son importance pour l'institution. Pour juger de son importance, on cherche à évaluer sa sensibilité, en fonction de l'impact qui résulterait d'une atteinte aux critères « Disponibilité, Confidentialité, Intégrité et Traçabilité ».

Une attention particulière doit être accordée aux données manipulées ou stockées en local sur la machine du télétravailleur.

Au final, les mesures de protection à mettre en place pour cette information sont déterminées à partir de, et selon, le résultat de l'analyse de risques.

Le scénario des risques est élaboré à travers la démarche suivante :

- Identifier des actifs supports pouvant être impactés par les menaces,
- Identifier pour chaque couple menace/actif les vulnérabilités pouvant être exploitées par les criminels,
- Identifier le ou les critère(s) de sécurité impactés(s) : Disponibilité, Intégrité, Confidentialité, Traçabilité.

Nous arrivons ainsi à une grille de classification qui permet d'organiser les informations sensibles selon plusieurs niveaux faciles à comprendre :

- Informations publiques ;
- Informations internes ;
- Informations internes et confidentielles ;
- Informations internes et secrètes.

4. STRATÉGIE DE SÉCURITÉ POUR LE TÉLÉTRAVAIL

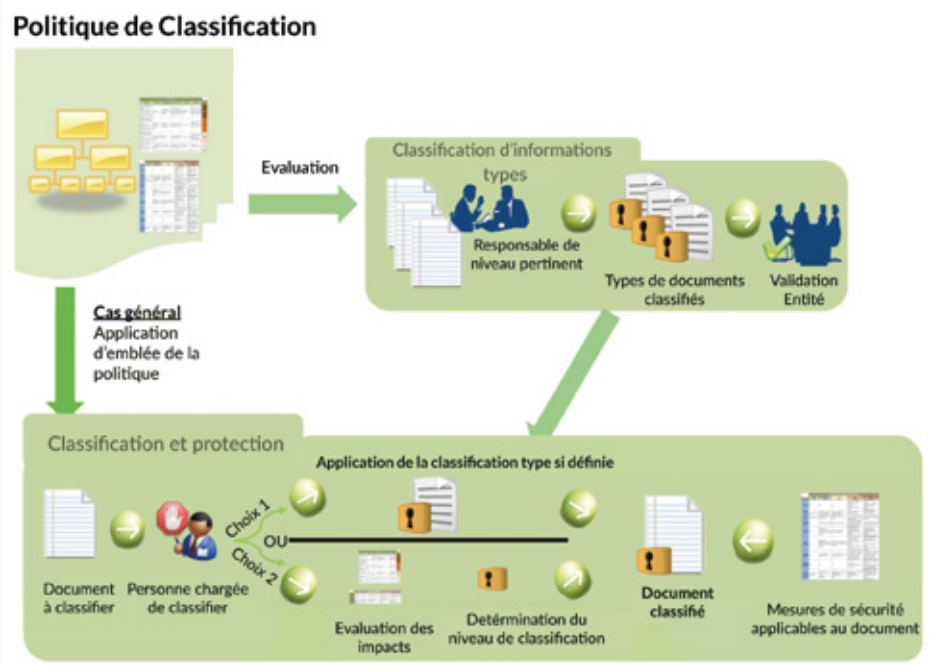


FIGURE 20 : STRATÉGIE DE CLASSIFICATION DE L'INFORMATION

Au-delà des impératifs de sécurité et de protection, la gestion des informations sensibles repose sur une culture interne. Cette culture n'est pas celle du secret mais plutôt du juste niveau de communication des informations sensibles. À cette fin, l'organisation doit mettre en place des outils de communications qui favorisent la bonne appropriation et la bonne diffusion en interne de cette culture.

4.4 - Sécurisation des canaux d'accès

Pour accéder à distance aux ressources de l'organisation, l'employé doit utiliser le média non sécurisé qu'est Internet. Cette contrainte expose le poste de travail et les données qu'il contient aux attaques de cybercriminels. Toutes les communications transitent sans aucune garantie par défaut sur leur confidentialité, intégrité et non répudiation. Pour palier cette vulnérabilité majeure, il est obligatoire de sécuriser les flux et les canaux de communication au moyen d'un VPN.

Pour les principes du VPN, voir la section 3.2 – Scénarios pour l'accès distant. Pour les principes techniques du VPN, voir la section 5.5 – Accès distant par VPN.

4.5 - Nécessité d'une authentification forte

Le poste de travail du télétravailleur reste exposé au risque de vol ou peut simplement être utilisé sans précaution par une autre personne. Pour éviter toute intrusion sur le système d'information central, il est essentiel d'être en mesure d'identifier avec exactitude le télétravailleur au moment de l'authentification. En plus de l'utilisation d'un identifiant nominatif unique et d'un mot de passe robuste, son authentification doit se faire au moyen d'une authentification basée sur plusieurs facteurs. La section 5.6 – Authentification à plusieurs facteurs présente les différentes catégories de facteurs disponibles et la façon de les déployer.

4.6 - Protection des données

Parmi les risques les plus redoutés pour une institution figure la fuite de ses données. Le respect de certaines règles permettra cependant de limiter ce risque.

4.6.1 - Solutions DLP

Grâce à l'utilisation d'une solution de type DLP (Data Loss Prevention), il est possible de protéger l'organisation contre la fuite de données au moyen d'algorithmes capables de détecter un accès anormal aux données sensibles. Le but est d'interdire aux malfaiteurs d'accéder aux données non autorisées ou aux utilisateurs maladroits de partager les données hors du cercle des personnes autorisées d'accès.

Une solution DLP se distingue d'un produit de contrôle des ports USB sur un point très important : alors que le contrôle des ports interdit uniquement l'utilisation de certains périphériques, une solution DLP va plus loin en contrôlant les données transmises. Elle est à même d'identifier les données sensibles et peut empêcher leur copie, même sur les supports de stockage autorisés.

Dans le domaine des solutions DLP, on distingue essentiellement deux approches techniques : les solutions orientées réseau et les solutions client.

• **Les solutions réseau** sont faciles à mettre en œuvre et couvrent tous les protocoles courants comme HTTP, HTTPS, SMTP, POP3 et IMAP tout en protégeant l'ensemble du réseau de l'organisation. Cependant, elles n'offrent aucune protection pour les supports de stockage amovibles, les captures d'écran ou les processus de copier/coller sur les postes client.

• **Les solutions client** exigent en revanche l'installation d'un agent sur le poste client à contrôler. Les règles mises en œuvre par l'agent sont définies par un administrateur système sur une console de gestion DLP centrale. Comme l'agent fonctionne directement sur le poste client, il peut contrôler toutes les opérations qui y ont lieu. Par rapport aux solutions basées sur le réseau, il est donc possible de mettre en œuvre des mesures de protection plus étendues.

En cas de violation d'une règle, la notification utilisateur peut même être visualisée immédiatement et très clairement via des messages d'avertissement sous forme de fenêtres pop-up. L'agent étant également actif en dehors du réseau de l'organisation, les ordinateurs portables fonctionnant à distance sont aussi protégés[10].

4.6.2 - Chiffrement des données

En cas de vol ou de perte du poste de travail utilisé dans le télétravail, les cybercriminels peuvent facilement récupérer les données stockées sur le disque dur sans même avoir besoin des éléments d'authentification de la machine. Pour faire face à ce risque, il est primordial pour l'organisation de se doter d'une solution de chiffrement des disques des postes de travail.

Quand le télétravail doit être déployé de toute urgence, comme dans le cas d'une crise majeure, il faut au minimum procéder au chiffrement des postes de travail à privilèges (haute direction, administrateurs informatiques, utilisateurs manipulant des données métiers critiques, etc.). Cette mesure est encore plus nécessaire quand il s'agit des postes de travail non maitrisés par l'organisation (BYOD).

La solution optimale consiste à chiffrer l'ensemble du disque ou, à défaut, toutes les partitions pouvant contenir des informations sensibles (partition SYSTEM par exemple pour les postes de travail sous le système d'exploitation Windows).

Une autre possibilité, qui nécessite moins d'espace mémoire et est très facile à mettre en place, consiste à utiliser des conteneurs de fichiers chiffrés. Ce mode de chiffrement permet d'assurer l'accès aux seuls destinataires autorisés et identifiés (soit l'utilisateur du poste de travail lui-même, ou bien les destinataires des fichiers chiffrés avec une clé partagée).

10 *François Prat, « Qu'est-ce que le DLP et comment le mettre en œuvre de façon optimale ? », Journal du Net, 18 mai 2009.*

4. STRATÉGIE DE SÉCURITÉ POUR LE TÉLÉTRAVAIL

4.7 - Sensibilisation des employés

L'extension du périmètre informatique de l'organisation aux postes de télétravail situés dans autant de sites hétérogènes qu'il y a de résidences d'employés, crée un environnement sécuritaire à géométrie variable. Plusieurs dispositifs ou couches de sécurité des données fournies dans les locaux et réseaux informatiques de l'organisation, n'existent plus. De manière générale, le passage au télétravail implique un transfert massif de responsabilité depuis l'environnement soigneusement sécuritaire des locaux de l'organisation, vers une série de sites non maîtrisés où, en outre, résident et circulent nombre de personnes étrangères à l'organisation.

Les pirates informatiques ont vite compris comment mettre à profit les changements apportés par la transition brutale au télétravail et ont adapté leurs techniques d'attaque aux bouleversements suscités par la crise du COVID-19. Le gros de leur effort criminel est dirigé sur l'utilisateur final. L'idée pour eux est de mettre à profit le climat de tension engendré par la situation de crise et la courbe d'apprentissage au télétravail de la majorité des employés peu familiarisés avec ce mode opérationnel. En effet, le nombre de malwares et de courriels de hameçonnage exploitant le contexte pandémique a explosé depuis l'apparition du COVID-19. Les cybercriminels misent sur l'erreur humaine pour s'introduire dans les réseaux de télétravail et dans les SI des organisations afin de commettre leurs forfaits.

La protection des données institutionnelles, voire la survie de l'organisation, dépend de la vigilance de l'utilisateur ainsi que de sa connaissance des risques et des bonnes pratiques cybersécurité. La maturité que l'on exige de l'utilisateur passe par le déploiement d'un programme de sensibilisation bien conçu et déployé en mode continu. Nous partons de l'axiome qui veut qu'un employé bien sensibilisé est un risque à moitié traité.

En période normale, un bon programme de sensibilisation à la cybersécurité repose sur une liste couvrant l'ensemble de la problématique de la sécurité informatique. Un des principaux défis de la sensibilisation consiste alors à capter l'attention des utilisateurs au milieu de la de « fatigue électronique » suscitée par la surabondance de l'information en ligne.

Quand l'organisation entre en mode de crise, elle doit interrompre la campagne de sensibilisation en cours et la remplacer immédiatement par des messages qui collent à l'actualité en temps réel. Le but est double : maintenir le lien entre l'équipe de cybersécurité et le télétravailleur pour qu'il ne sente pas livré à lui-même (éviter la panique) ; passer les messages clés clairement axés sur les risques prioritaires.

Vous éviterez ainsi que vos employés cliquent sur des pièces jointes ou liens malveillants ou remplissent des formulaires douteux avec des données sensibles parce qu'ils ont reçu un courriel alarmant sur l'expansion du COVID-19.

Dans un contexte de télétravail, toutes les actions de sensibilisation recourront exclusivement à des outils de communication à distance. Au cours de la période de transition vers le télétravail, la messagerie demeure le moyen privilégié pour passer des messages urgents en temps réel.

Par la suite, les campagnes de sensibilisation en cybersécurité seront lancées au moyen d'une plateforme accessible en mode SaaS (Software as a Service). Nous préconisons l'utilisation d'une plateforme vidéo interactive comme outil privilégié de sensibilisation. Le contenu est présenté sous forme de dessin animé de trois ou quatre minutes, hautement dynamique et n'hésitant pas à recourir à l'humour chaque fois que possible. Cela permet aux employés de suivre les campagnes de sensibilisation depuis leur lieu de télétravail à partir de n'importe quel terminal connecté à Internet. C'est le cas de la plateforme SensiPRO de DATAPROTECT.

Afin de tester la vigilance de vos employés au télétravail, il convient de lancer des campagnes de simulation de hameçonnage réalistes ancrées dans le thème de la crise en cours. Il s'agit de vérifier qu'ils sont conscients des questions de sécurité, même s'ils sont installés dans la quiétude du foyer familial et loin de l'environnement habituel de travail. Les employés qui échouent au test de simulation doivent alors faire l'objet d'une mini-campagne de sensibilisation additionnelle.

En plus des thèmes de cybersécurité couverts en situation normale de travail, le programme de sensibilisation de crise devra être complété et mis à jour pour englober les points suivants :

- Confidentialité des données professionnelles ;
- Protection physique du matériel de travail à la maison ;
- Sécurité des terminaux mobiles en déplacement ;
- Connexions hors réseaux d'entreprise ;
- Sécurité du réseau domestique (wi-fi) ;
- Hameçonnage et autres formes d'ingénierie sociale de crise utilisés par des cybercriminels opportunistes ;
- Signalement d'incidents et évènements liés à la sécurité des données.

Nous proposons en annexe de ce Livre blanc, des exemples de messages de sensibilisation à transmettre à vos employés en télétravail tout au long de la période de pandémie au COVID-19.

4.8- Surveillance et traçabilité

La situation est d'autant plus favorable aux malfaiteurs que la mobilité des utilisateurs oblige les dirigeants d'organisations à rendre accessibles des services internes qui n'avaient nécessairement pas été conçus en fonction du télétravail. Les organisations doivent s'assurer que toutes les mesures permettant la détection et l'identification des attaques, l'analyse et l'assistance à la réponse aux incidents cybersécurité, sont (1) en place et sont (2) opérationnelles.

La traçabilité des accès a prouvé à plusieurs reprises son efficacité dans la lutte contre la fraude. Elle répond à des objectifs multiples notamment la supervision et la conservation du journal des opérations des utilisateurs en télétravail, ou encore aux obligations de conformité réglementaire telles que PCI DSS, Sarbanes Oxley, Loi 09-08, etc.

Pour y parvenir, nous proposons une démarche par étapes, accessible à tous les acteurs économiques en télétravail, y compris les PME.

ÉTAPE 1: L'écoute systématique des signaux faibles

Souvent, les traces informatiques générées par les systèmes et outils de sécurité, ne sont pas traités à temps. Les équipes informatiques sont concentrées sur la mise à disposition des services ainsi que sur le paramétrage des règles de sécurité. Résultat : elle n'ont pas toujours les moyens de vérifier à flux tendu les évènements de sécurité sur chaque équipement. Ce suivi intermittent ne permet pas de détecter les cyberattaques assez vite pour prévenir l'intrusion.

Toutes les traces générées par les postes de travail et par les SI doivent être transmises à une solution dédiée de centralisation et de corrélation des logs ou SIEM. Une solution SIEM est d'abord un outil de collecte filtrant les différents flux informatiques pour ne conserver que les événements de cybersécurité. C'est aussi un outil de stockage centralisé, une couche de valorisation (corrélation, alerte, reporting) permettant d'exploiter les événements de sécurité. Enfin, c'est une couche de présentation. Bien sûr, ce dispositif nécessite une organisation en place pour assurer la surveillance.

ÉTAPE 2 : Quoi surveiller et comment le faire ?

La supervision consiste à procéder au monitoring, à l'identification et à l'analyse afin de fournir la réponse adaptée aux incidents de cybersécurité. Pour cela, il est nécessaire de définir la structure adéquate permettant de s'assurer du bon traitement et de la qualification des incidents en provenance des accès au réseau. Parmi les formules existantes, c'est l'abonnement à un service Cyber SOC opérant 24/7, qui permet le mieux de répondre à ce besoin.
Un Cyber SOC sert à traiter en temps réel les alertes SIEM et à effectuer des recherches spécifiques pour identifier les comportements suspects :

- Communications sortantes vers Internet.
- Communications VPN depuis des sources non sûres (avec le confinement, toute tentative de connexion VPN depuis une source IP qui ne figure pas sur la liste de celles où résident les employés, fait automatiquement l'objet d'une alerte).
- Flux d'administration hors des solutions de traçabilité des accès à privilèges.
- Authentification anormales (hors horaires de travail, ou avec des comptes privilégiés, etc.).
- Communications suspicieuses avec des adresses IP publiques, notamment celles identifiées comme étant malveillantes par les sources alimentant les bases de connaissance du Cyber SOC (Outils de Threat intelligences, MISP, Honey Pot, analyses de malwares, veille propriétaire, etc.).
- Utilisation d'outil d'administration à distance sur des serveurs internes.
- Recherches des derniers indicateurs de compromission (IoC) pertinents aux contextes des clients.
- Etc.

ÉTAPE 3 : La réponse adaptative aux incidents

Une fois l'attaque détectée, il est nécessaire qu'une bonne gouvernance permette la remontée d'information, la prise de décision et les actions de blocage aptes à éradiquer la menace.

4. STRATÉGIE DE SÉCURITÉ POUR LE TÉLÉTRAVAIL

• Remontée des incidents

Les incidents sécurité peuvent survenir à tout moment. Hors des périodes de crises, les hackers avaient l'habitude de profiter des moments d'absence des employés ou de baisse d'attention des équipes IT et sécurité pour lancer leurs attaques. Dans un contexte où les organisations basculent dans le télétravail, cela incite plus que jamais l'appétit des hackers, qui profitent de l'absence de contrôle et de présence physique.

Afin de faire face à ces menaces, les organisations en situation de crise doivent disposer d'une structure souple et disponible à tout moment pour prendre en charge la remontée des alertes et les traiter sans délais. Pour y parvenir, un interlocuteur privilégié doit être désigné, ainsi qu'une procédure d'escalade incluant les différents acteurs pouvant agir efficacement lorsqu'une attaque survient. À cet égard, le Responsable de Gestion du Télétravail doit jouer un rôle central pour veiller à la fluidité de la gouvernance sécuritaire.

• Blocage des attaques

Lorsque le Cyber SOC ou le service en charge de la surveillance en matière de sécurité détecte une attaque, il est important de réagir quasi instantanément pour la stopper. L'organisation doit disposer d'un outil permettant d'isoler à distance l'ordinateur attaqué et d'évaluer à chaud de l'état de compromission du système d'information via une recherche spécifique. Dans les cas les plus graves, l'ordinateur est mis en quarantaine et les services aux télétravailleurs suspendus. Ses liens avec les autres systèmes sont désactivés le temps de la quarantaine. L'ordinateur est restauré et sa remise en service est conditionnée à la vérification de l'absence de résidus vestigiaux de l'agent compromettant. La remise en service s'accompagne de la délivrance d'une autorisation.

Pour rendre efficace la réponse aux incidents, l'interface peut être automatisée avec les éléments ci-après.

Technologies	Apport dans la réponse aux incidents	Quelques exemples
EDR (Endpoint Detection and Response)	Un EDR fonctionne par le biais d'une surveillance continue du terminal à l'aide d'indicateurs de compromis (IoC). La nature automatisée de l'EDR lui permet de remplir les fonctions suivantes : • Isolement des ordinateurs et serveurs infectés ; •Remontée des logs des ordinateurs au niveau du SIEM à travers la console EDR ; •Protection avancée contre les attaques ciblées et les rançongiciels ; •Capacité de recherche étendue au niveau de tout le parc informatique, pour identifier les signes d'infection similaires ou les IoC.	FireEye EDR Kaspersky KATA
Firewall frontaux et IPS	• Création d'une blacklist (ip/domaine) à laquelle s'ajouteront tous les domaines malveillants identifiés par le CSOC. •Interconnexion de l'IPS et de la base de signature à une solution de Threat intelligence pour l'alimentation continue avec les derniers IoC. •Blocage des IPS malveillants, coupure de la connexion Internet si nécessaire, ou révision des règles de filtrage.	Cisco PaloAlto Fortigate CheckPoint
Autres solutions de sécurité	•Installation des règles de blocage. •Activation des mécanismes (SPF, DKIM, DMARK) au niveau des proxy courriel. •Activation de l'inspection SSL, ainsi que du sandboxing au niveau du proxy web. •Verrouillage systématique des comptes au-delà des heures de travail (LDAP, authentification forte, etc.). •Activation de l'authentification contextuelle (limitation géographique des authentifiants, nombre de sessions, double facteurs, etc.). •Whitelisting/Backlisting applicatif au niveau des postes de travail et serveurs. •Renforcement de la politique antivirale et de la politique d'accès réseaux. •Etc.	

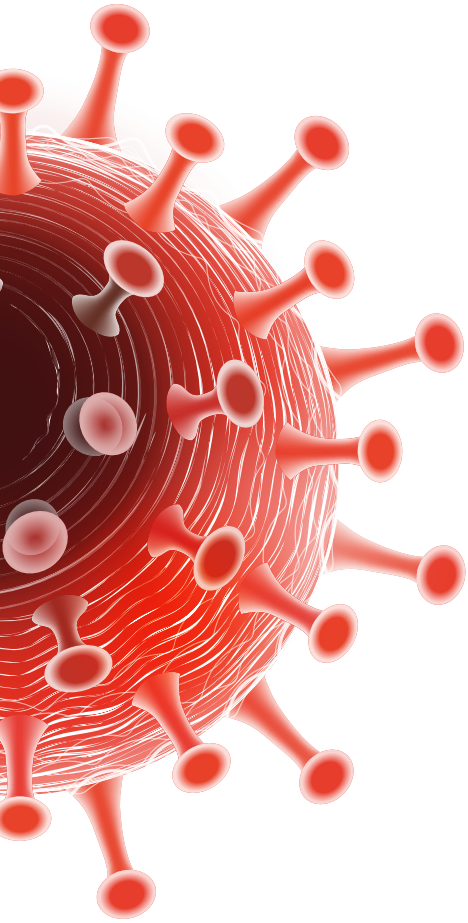
Tableau 2 : Principaux types de réponses aux incidents informatiques

4.9 - Modèle de maturité

Sur la base de l'état de préparation et d'anticipation de l'organisation, ainsi que de la robustesse des moyens en place, nous avons développé le modèle de maturité suivant.

	RÉACTIF (Organisation non préparée à faire face à une situation de crise et à effectuer une transition de télétravail massif et sur une longue période)	STABLE (Organisation dotée de mesures de sécurité périmétrique suffisantes pour activer une ouverture partielle de son SI au télétravail)	PROACTIF (Organisation visionnaire et prédictive dotée de capacités importantes pour faire face à un recours massif au télétravail sur une longue période)
Caractéristiques	• Posture cybersécurité non évaluée préalablement à l'activation du télétravail • Décisions ad hoc • Ressources de télétravail non prévues à l'avance (ordinateurs, connexion dominicale, outil de conférence, licences, etc.) • Données sensibles non suffisamment identifiées • Improvisation des mesures de sécurité • Recours à des solutions/outils gratuits ou non qualifiés • Procédures de sécurité /continuité ad hoc • Nécessité de s'assurer de la qualité des sauvegardes • Sensibilisation « fiévreuse » des utilisateurs	• SI peu enclin à l'ouverture au monde externe (émanant du choix d'évitement des risques par la Direction générale) • Gestion de crise dans le cadre d'un PCA classique • Mesures de sécurité / configurations minimales en place au niveau du réseau • Approche/culture de classification présente • Capacité de prévention/détection des menaces (IPS, IDS, ...) • Technologies de sécurité d'accès distant prévues dans l'infrastructure, souvent activé au cas par cas (tiers, utilisateurs itinérants, ...) • Recours au plan de sensibilisation habituelle • Application des procédures de sécurité prédéfinies • Plans de continuité prévu et intégrant les ressources pour les effectifs minimaux	• Cellule de crise opérationnelle • Plan de continuité « pandémie » générique tiré du Plan mondial de l'OMS de préparation à une pandémie • Ressources planifiées et prévues dans le cadre du PCA classique • Mesures de sécurité efficaces et fiables en place (restrictions d'accès aux données, surveillance des accès, chiffrement, authentification forte, etc.) • Plans de continuité à jour pour faire face à l'imprévisible durant la pandémie • Évaluation du niveau de sécurité des sites de télétravail • Capacité à contrôler continuellement son exposition aux menaces (veille sécurité, analyse des tendances avec les outils de sécurité, etc.) • Continuité de la sécurité clairement intégrée dans le plan de continuité d'activité • Prise en compte des aspects de protection des données personnelles dans le télétravail
Exemples de mesures à mettre en place	• Monter une cellule de crise • Étudier le recours aux outils gratuits de sécurité • Densifier la sensibilisation en ciblant les thématiques en relation avec le champ de prédilection des cybercriminels (hameçonnage, rançongiciel, etc.) • Souscrire à des technologies de télétravail réputées sécurisées • Lancer des scans de vulnérabilités et corriger sans délai les failles découvertes • Lancer une activité de veille sécurité et informationnelle • Faire signer un engagement de sécurité spécifique aux employés	• Activer la cellule de crise et étudier la possibilité de l'élargir à des experts • Activer la politique de sécurité au télétravail • Publier une note interne sur le BYOD • Identifier les données sensibles à protéger • Augmenter la capacité de surveillance des évènements (alertes, sources de logs, etc.) • Densifier la sensibilisation des utilisateurs • Lancer des recettes de sécurité sur les accès de télétravail	• Recours aux solutions d'authentification forte • Recours à des techniques d'accès distant sécurisés • Recours aux bastions de sécurité pour la traçabilité • Recours à des solutions de sensibilisation dématérialisée pour atteindre le grand nombre • Pratiques de tests de vigilance des utilisateurs en exploitant la situation pandémique • Recours à un SOC pour la supervision en temps réel • Tests d'intrusion externes récurrents • Utilisation de postes de travail ou d'environnements maitrisés pour le télétravail

Tableau 3 : Modèle de maturité



5 GUIDE PRATIQUE DES MESURES DE CYBERSÉCURITÉ

5.GUIDE PRATIQUE DES MESURES DE CYBERSÉCURITÉ

Les employés qui travaillent à distance sont le maillon faible de vos efforts la protection de votre organisation contre les cyberattaques. Voilà pourquoi, il est essentiel de les sensibiliser à la cybersécurité. Ci-dessous une série de conseils pratiques à l'intention des télétravailleurs qu'il convient de diffuser de manière aussi large que possible.

5.1- Règles de base à l'intention du personnel en télétravail

.• Ne désactivez pas et ne tentez pas de contourner les outils de sécurité installés par votre employeur sur vos terminaux de travail (antivirus, routines de mise à jour systèmes, outils de chiffrement de données, etc.).

• Éviter le recours au ShadowIT : l'utilisation d'outils autres que ceux mis à disposition par le service informatique exposent les données de l'organisation à des risques de compromission (outil collaboratif, de vidéoconférence, de partage de fichiers volumineux, de scan de documents, de modification des fichiers PDF en ligne, etc.).

• Veiller à bien choisir vos mots de passe et à les garder secrets.

• En cas de besoin d'un outil, les salariés doivent avoir le réflexe de contacter le service informatique au lieu de le télécharger eux-mêmes.

• Appliquer le principe bureau propre et de l'écran vide (ne laissez pas trainer des documents sensibles sans protection à l'intérieur de la maison ou sur le bureau de votre poste de travail et verrouillez systématiquement les sessions).

• Éviter, dans la mesure du possible, l'utilisation de vos équipements personnels pour les accès distants au réseau d'entreprise.

• Dans le cas où des outils de vidéoconférence publics sont utilisés, évitez de partager des documents sensibles à l'écran. Ces outils peuvent potentiellement enregistrer les données partagées ce qui expose les informations sensibles de l'organisation à des risques de compromission.

• Éviter l'utilisation des clés USB personnelles ou, si absolument nécessaire, procédez à une analyse anti-virus avant utilisation.

• Éviter l'utilisation des postes de travail professionnels pour des besoins personnels (visionnement de films en streaming, consultation de réseaux sociaux, etc.)

• Installer les mises à jour de sécurité et surtout pensez à redémarrer chaque jour les postes de travail.

• Éviter de connecter vos terminaux professionnels à des réseaux wi-fi ouverts, que leurs noms vous semblent connus ou pas.

• Renforcer la sécurité de votre réseau domestique à travers quelques actions simples :

  • Changez le mot de passe par défaut de votre équipement d'accès Internet et renforcez celui de votre réseau wi-fi, en optant pour un chiffrement WPA2-PSK, plus fiable

  •Évitez de nommer votre réseau wi-fi en utilisant votre nom.

  •Faites attention aux appareils personnels connectés à votre réseau wi-fi comme les smartphones, les consoles de jeux et même les appareils ménagers. Il est important de vous assurer de leur sécurité.

•Utiliser les sources officielles pour suivre l'épidémie ainsi que pour télécharger l'attestation de déplacement dérogatoire.

•Ne jamais ouvrir un document sur le thème COVID-19 (fichier Zip, PDF, Word, Excel, etc.) et ne jamais activer les macros des documents qui proviennent d'Internet.

•Ne pas installer les applications mobiles sur le thème du COVID-19.

•Faire attention aux SMS qui vous incitent à cliquer sur un lien ou à ouvrir un document sur le thème du COVID-19.

• Faites attention aux courriels d'hameçonnage liés au thème du COVID-19. Apprenez à reconnaître un courriel frauduleux.

• Notifier systématiquement le service informatique en cas d'incident ou d'événement lié à la sécurité des données : un cas de perte/vol d'un poste de travail ou d'infection par un malware par exemple.

• Profiter du confinement pour sensibiliser tous les membres de votre famille aux risques et enjeux de la cybersécurité.

5.2- Protection des terminaux mobiles

5.2.1- Configuration durcie du système d'exploitation

Pour être sûr que les postes mobiles fournis aux utilisateurs nomades respectent vos exigences en termes de sécurité des postes de travail, il est nécessaire de préparer une image-type des systèmes d'exploitation que vous allez installer avec un paramétrage durci. Vous pouvez par exemple utiliser sysprep qui est un outil Microsoft destiné aux administrateurs informatiques afin de créer une image d'installation Windows 10 à partir d'un système déjà installé et configuré.

Si l'utilisateur n'a pas pu être doté d'un poste mobile fourni par l'organisation, il est possible de mettre à sa disposition une image durcie sous format de machine virtuelle (VM), téléchargée depuis le site de l'organisation ou transmise sur clé USB. La VM pourra être exécutée sur le poste avec un outil de virtualisation et sera utilisée pour tous les accès distants.

5.2.2- Installer ou activer une solution antivirale

La majorité des organisations dispose de solutions de protection des terminaux qui imbriquent plusieurs modules de sécurité tels que :

- Anti-malware ;
- Contrôle d'application ;
- Sécurité du navigateur web ;
- Pare-feu local ;
- Chiffrement de disque ;
- Détection et réponse des menaces (EDR).

Ces modules aident à protéger différents types de terminaux, tels que les ordinateurs portables ou de bureaux, les smartphones et les tablettes. Encore faut-il que l'utilisateur mette à jour régulièrement les logiciels critiques. Voilà pourquoi, il est obligatoire de configurer la mise à jour automatique du système d'exploitation avec les correctifs publiés par l'éditeur.

Dans le contexte du télétravail, il est indispensable de doter les postes nomades de ces solutions pour les protéger indépendamment de toute intrusion ou menace aussi bien interne qu'externe au site physique. La solution retenue doit apporter aux télétravailleurs le niveau de protection attendu, qu'ils exercent leurs fonctions depuis leurs domiciles ou tout autre lieu.

Afin d'assurer la protection des postes des utilisateurs nomades, nous distinguons deux types d'environnement :

- **Cloud :** La plateforme de protection des terminaux est fournie en mode SaaS. Il suffit d'installer des agents de protection au niveau des postes qui vont récupérer les politiques de sécurité configurées sur l'instance cloud.
- **On-premise :** La plateforme de protection des terminaux sera installée dans l'infrastructure interne et gérée entièrement par les équipes TI. Il faut mettre en place un composant de la plateforme au niveau de la DMZ publique pour permettre aux postes nomades de récupérer leurs politiques de sécurité.

5.3- Gestion unifiée des terminaux

Les solutions de gestion unifiée des terminaux ou UEM (Unified Endpoint Management) fournissent aux administrateurs une console centralisée depuis laquelle ils peuvent gérer efficacement divers équipements (laptop, smartphone) fournis par l'organisation. Ces solutions sont capables de gérer des parcs de terminaux iOS, Android, Windows 10 et MacOs. Elles couvrent également la gestion des serveurs virtuels, des imprimantes, des montres et autres objets connectés. Tous ces terminaux sont gérés dans l'intégralité de leur cycle de vie, depuis leur provisionnement jusqu'à leur élimination. Les plateformes UEM automatisent le déploiement de logiciels et de correctifs et facilitent la mise en œuvre de politiques de restriction des applications.

5.GUIDE PRATIQUE DES MESURES DE CYBERSÉCURITÉ

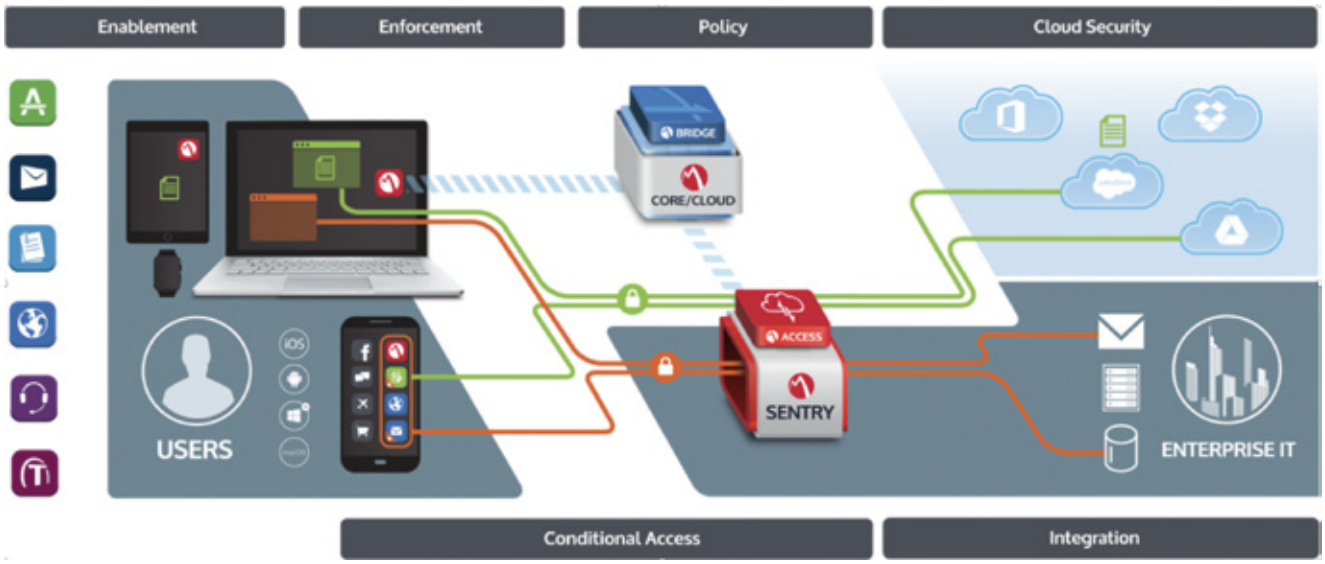


FIGURE 21 : SOLUTION DE GESTION UNIFIÉE DES TERMINAUX OU UEM

Nous utilisons toujours le terme MDM (Mobile Device Management) pour parler de la gestion des terminaux mobiles. Une solution MDM comprend des fonctionnalités telles que l'approvisionnement en appareils, l'inscription, la sécurité et le traçage des déplacements. Elle permet également d'effacer les données en cas de vol ou de perte de l'appareil. En version de base, elle permet d'appliquer les politiques de sécurité, de suivre l'inventaire et d'effectuer une surveillance en temps réel.

Au fil des ans, cependant, les besoins des organisations sont devenus plus complexes : les applications et les contenus nécessitent aussi un accès sécurisé. Pour faire face à ce changement, la solution MDM a évolué vers la gestion de la mobilité des terminaux (EMM) qui incorporait des fonctionnalités plus avancées, telle que la possibilité de gérer les applications et le contenu sur les appareils mobiles ainsi que des politiques spécifiques aux environnements BYOD.

Alors que les directions informatiques ont été amenées à prendre en charge des nouvelles plateformes, comme Windows 10, de nombreux fournisseurs d'EMM ont fait évoluer leurs solutions pour offrir une gestion unifiée des points de terminaison ou UEM. Outre les caractéristiques propres aux solutions MDM/EMM traditionnelles, les plateformes UEM comprennent plusieurs fonctionnalités nouvelles qui permettent la sécurisation des postes nomade. Nous citons les principales :

- Gestion des applications de votre organisation dans un conteneur sécurisé ;
- Gestion des postes des utilisateurs nomades ;
- Actions de réponse à distance en cas de perte et de vol ;
- Prévention contre la fuite de données.

Les plateformes UEM sont disponibles en mode cloud et on-premise.

5.4 - Infrastructure de bureau virtuel

Les postes de travail nomades doivent avoir les mêmes contrôles de sécurité que celles que vous utilisez pour les ordinateurs du SI interne. Cependant, en raison des menaces auxquelles cette catégorie de terminaux est confrontée dans les environnements externes, certains contrôles de sécurité devront être adaptés ou ajoutés pour fonctionner efficacement.

Dans les situations où l'utilisation et le maintien de contrôles de sécurité supplémentaires ne sont pas faisables, d'autres approches peuvent être envisagées, telles que l'utilisation de technologies d'infrastructure de bureau virtuel.

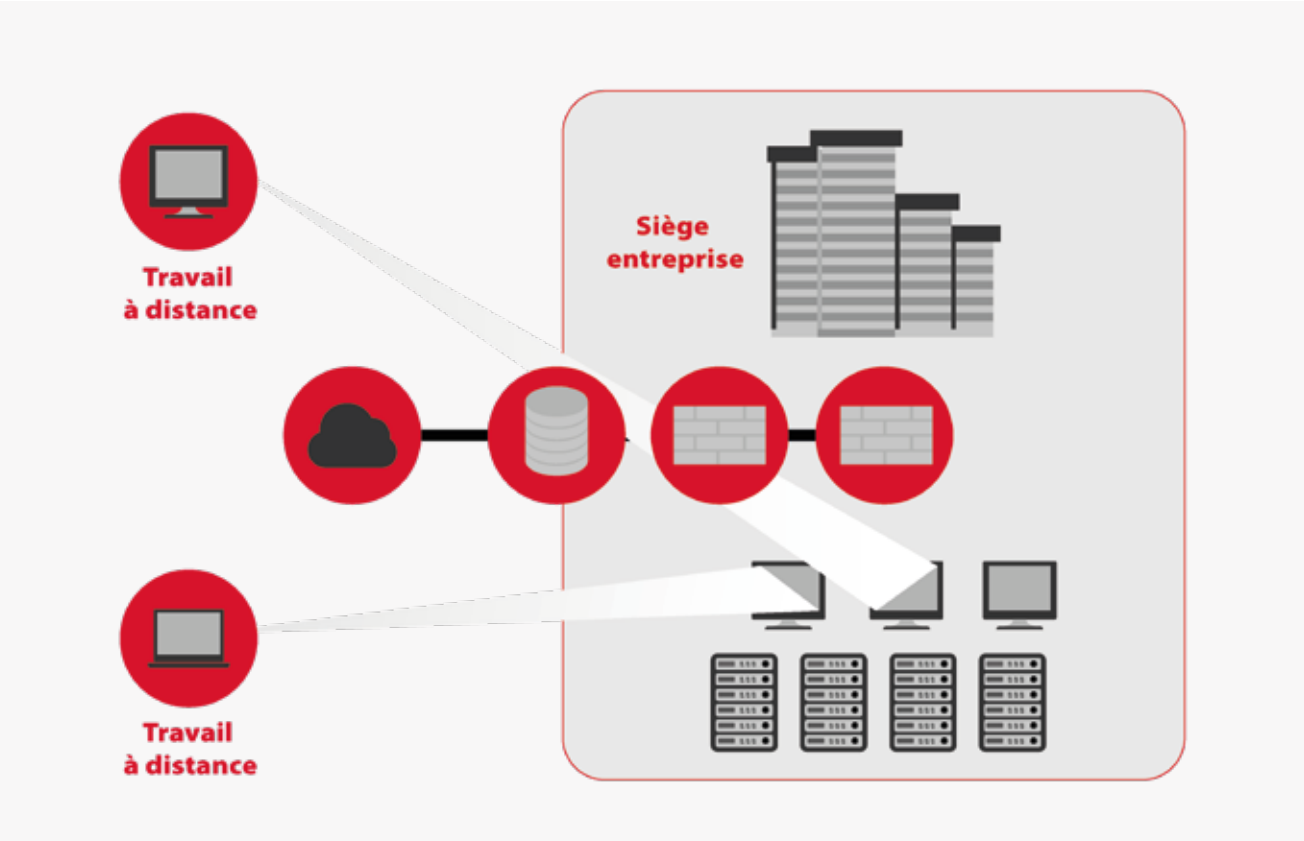


FIGURE 22 : INFRASTRUCTURE DE BUREAU VIRTUEL

Une infrastructure de bureau virtuel (virtual desktop infrastructure ou VDI) consiste à héberger des instances de postes de travail virtuel au niveau d'un centre de données et permet aux utilisateurs d'accéder à leurs environnements de travail à distance via des clients légers. C'est une forme de virtualisation des postes de travail. En effet, les images de chaque poste spécifique s'exécute sur une machine virtuelle (VM) et est placée à la disposition du client final via le réseau. Une fois que le client lance sa session VDI depuis n'importe quel terminal, l'ensemble de son bureau, contenant ses applications et ses documents, s'affiche pour lui permettre d'accomplir son travail.

Une autre forme de VDI existe qui consiste à mettre à la disposition de l'utilisateur final les seules applications auxquelles il a droit. Il peut y accéder de manière sécurisée, via un conteneur qui permet d'isoler l'application du système d'exploitation depuis lequel la session a été lancée.

5.GUIDE PRATIQUE DES MESURES DE CYBERSÉCURITÉ

5.5- Accès distant par VPN

Plusieurs techniques d'accès à distance offrent un canal de communication sécurisé à travers lequel les informations peuvent transiter entre les réseaux, y compris les réseaux publics comme Internet, de façon confidentielle. Ces canaux de communication sécurisés, qu'on appelle tunnels, sont généralement établis via des technologies VPN (voir section 3.2 - Scénarios pour l'accès distant). Grâce à la technologie VPN, un télétravailleur peut établir un accès sécurisé aux SI de son organisation et accomplir les tâches exactement comme depuis un poste de travail interne.

Trois formes d'accès distant par VPN existent et qui permettent d'atteindre cet objectif :

- Portail VPN SSL sans agent : Utilisation d'un portail web pour accéder aux ressources internes du SI de l'organisation.
- Accès VPN SSL client avec agent : Utilisation d'un client VPN installé au niveau du poste mobile pour créer un tunnel sécurisé avec le concentrateur VPN en utilisant le protocole TLS (Transport Layer Security).
- Accès VPN IPSec client : Identique au précédent mais le concentrateur utilise le protocole IPSec (Internet Protocol Security).

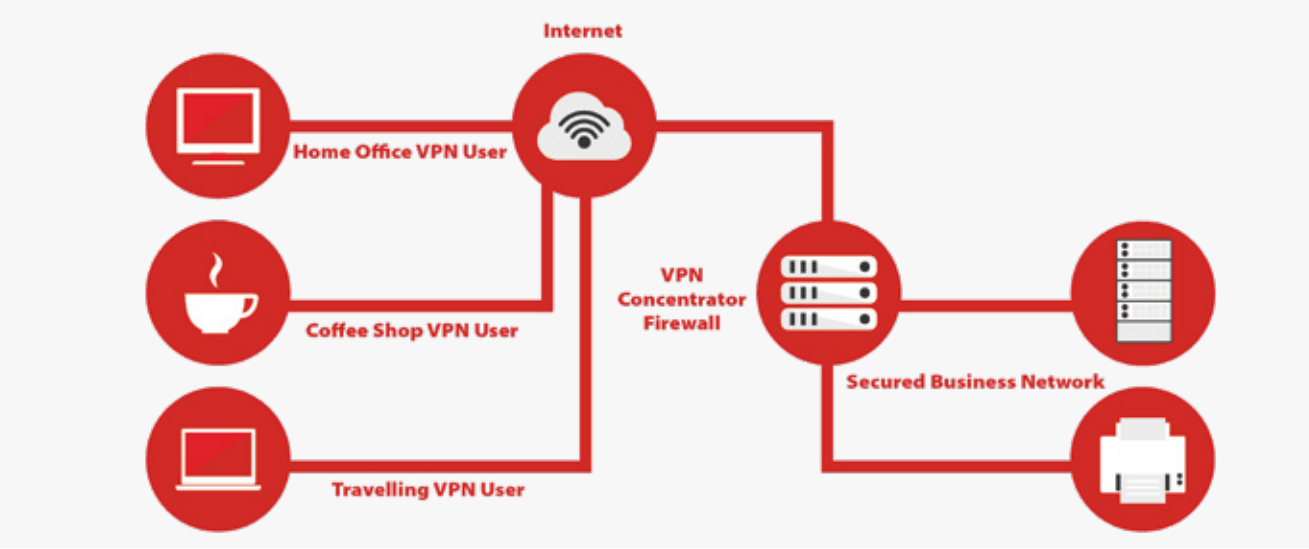


FIGURE 23 : ACCÈS À DISTANCE PAR VPN

Ci-après certaines recommandations que nous vous invitons à appliquer dans votre déploiement d'accès VPN de télétravail :

- Déployer des concentrateurs VPN dédiés à ce rôle. Le déploiement doit se faire en mode clustering pour assurer l'évolutivité de l'architecture.
- Utiliser des suites cryptographiques robustes et restreindre l'usage d'algorithmes faibles et défaillants.
- Installer un certificat VPN SSL sur votre concentrateur VPN signé par votre autorité de certification interne.
- Authentifier les postes de travail avec des certificats numériques. Pour ce faire, il est nécessaire de disposer d'une infrastructure PKI interne.
- Exiger l'authentification à plusieurs facteurs pour l'accès VPN.
- Appliquer le contrôle de conformité aux postes mobiles. La plupart des concentrateurs VPN comportent cette fonctionnalité.
- Rendre obligatoire l'accès VPN pour les postes mobiles des utilisateurs.
- Appliquer des règles de filtrage au moindre privilège pour tous les flux VPN.

Les solutions VPN sont disponibles en mode cloud et on-premise.

5.6- Authentification à plusieurs facteurs

5.6.1 - Principes de l'authentification multi-facteurs

Pour s'assurer de l'identité réelle d'un utilisateur mobile, il convient de mettre en œuvre une authentification forte, c'est-à-dire à plusieurs facteurs (MFA). En effet, les accès mobiles proviennent par définition de lieux non maîtrisés et donnent accès à toute la gamme des applications métiers de l'organisation.

L'authentification MFA est un composant essentiel de la gestion des identités et des accès (IAM). Plutôt que de simplement demander un nom d'utilisateur et un mot de passe, les solutions MFA requièrent d'autres informations d'identification supplémentaires appelés facteurs. Celles-ci peuvent être de trois ordres :

- Ce que vous savez (connaissances) : comme un mot de passe ou un code PIN ;
- Choses que vous avez (possession) : comme un OTP (One-Time Password), une carte à puce, une clé d'authentification qui peut être physique ou virtuelle, un smartphone, etc. ;
- Ce que vous êtes (identité corporelle) : comme les empreintes digitales, l'iris de l'œil, la reconnaissance vocale ou tout autre facteur biométrique.

FIGURE 24 : DIFFÉRENTS FACTEURS D'AUTHENTIFICATION

Certaines solutions MFA prennent aussi en considération le contexte de l'authentification pour appliquer une politique d'accès, comme l'adresse IP depuis laquelle la session d'authentification est effectuée, le lieu, la manière d'accès, l'heure, la cible, etc.

Dans une authentification à deux facteurs, il faut toujours entrer son nom d'utilisateur, suivi d'un premier facteur qui est typiquement un mot de passe (de préférence un mot de passe fort) et d'un deuxième facteur qui se présente sous diverses formes (ce que l'on est ou ce que l'on possède). Le recours à l'authentification MFA pour les utilisateurs nomades est impérative.

FIGURE 25 : UTILISATION D'UNE CLÉ D'AUTHENTIFICATION

5.GUIDE PRATIQUE DES MESURES DE CYBERSÉCURITÉ

5.6.2 - Utilisation de l'authentification multi-facteurs

Dans une chaîne de télétravail, nous avons identifié quatre points sur lesquels il est recommandé de recourir à l'authentification MFA :

- Le poste mobile : Une application peut être installée directement sur le poste de travail pour forcer l'authentification à plusieurs facteurs.
- L'accès VPN : Le concentrateur VPN peut être interfacé avec une solution MFA pour exiger l'authentification forte à l'utilisateur nomade lors de sa tentative d'authentification VPN.
- La solution de traçabilité des accès d'administration : Cela nécessite d'interfacer la solution de traçabilité des accès privilégiés avec une solution MFA.
- Directement sur les applications : Certaines applications comprennent un module d'authentification forte. Si ce n'est pas le cas et si l'application le tolère, on pourra y intégrer une solution MFA.

La majorité des solutions MFA sont basées sur le cloud tout en fournissant des proxys locaux pour l'interfaçage avec les services d'annuaire ou un serveur Radius interne à l'organisation. Parmi les solutions qui acceptent le mode on-premise, nous pouvons noter Safenet Authentication Service (SAS) et RSA Security.

Il convient de signaler que de nombreuses normes internationales exigent des organisations le recours à l'authentification forte pour protéger leurs SI. C'est le cas des normes destinées à protéger les données financières (SOX, PCI-DSS, Bâle 2 et 3, etc.) ou les données personnelles (RGPD, California Consumer Privacy Act, Loi 09-08). La mise en œuvre de l'authentification forte ou multi-facteurs fait alors partie intégrante de leur mise en conformité.

5.6.3- Indépendance des facteurs d'authentification

Prenons le cas des recommandations du Conseil des normes de sécurité PCI pour déployer l'authentification multifacteurs afin de se conformer à la norme PCI DSS (Payment Card Industry Data Security Standard), la norme de sécurité des données applicables à l'industrie des cartes de paiement. Cette norme énumère certaines exigences quant à l'authentification multi-facteurs :

Les facteurs d'authentification doivent être générés de manière indépendante les uns des autres. Ce principe d'indépendance englobe les concepts suivants :

- Une indépendance logique
- Une indépendance physique
- Une indépendance de validation
- Une indépendance de compromission

L'indépendance de compromission est l'élément le plus important : la compromission d'un des facteurs ne doit en aucun cas permettre la compromission d'un autre facteur.

Par exemple, si un couple identifiant/mot de passe est utilisé comme un premier facteur d'authentification pour garantir l'accès au SI de l'organisation et que ce même couple d'identifiant et de mot de passe est exigé pour s'authentifier sur la messagerie sur laquelle un deuxième facteur d'authentification de type OTP est envoyé, ces deux facteurs d'authentification ne sont pas considérés comme indépendants. La compromission (vol ou duplication) du premier facteur va permettre de retrouver le deuxième facteur d'authentification.

5.6.4- Authentification multicanale

L'utilisation de différents canaux pour transporter les données d'authentification est un moyen efficace pour augmenter le niveau de sécurité d'une authentification (un mot de passe saisi sur un formulaire et un OTP généré ou reçu par SMS sur un téléphone mobile, par exemple).

A contrario, si tous les facteurs transitent par le même canal avant d'être soumis au serveur d'authentification, l'efficacité de l'authentification multi-facteurs est considérablement affaiblie dès lors que le composant intermédiaire est compromis.

5.6.5- Protection des facteurs d'authentification

Pour éviter toute utilisation abusive, l'intégrité des mécanismes d'authentification ainsi que la confidentialité des données d'authentification doivent être protégées. Ainsi, la norme PCI DSS définit des exigences bien précises pour garantir la sécurité des facteurs d'authentification :

- Les mots de passe et données du type « ce que vous savez » doivent être robustes et difficiles à deviner.
- Les empreintes biométriques et données du type « ce que vous êtes » doivent être protégées contre les accès non autorisés .
- Les certificats ou données du type « choses que vous avez » ne doivent pas être partageables ou copiables.

5.7 - SIEM

SIEM signifie Security Information and Event Management ou gestion des informations et des événements de sécurité. C'est un outil de collecte en temps réel des évènements de sécurité provenant de multiples sources (serveurs, solutions de sécurité, équipements réseaux…) ainsi que de conservation, de tri et de corrélation. Les logs collectés par le SIEM permettent d'avoir une visibilité étendue de l'ensemble des activités malveillantes visant les infrastructures de l'organisation.

Bien évidemment, il est essentiel que le SIEM adopté soit bien maitrisé par l'équipe assurant la surveillance en mode continu. Le SIEM doit également être doté des règles de corrélation nécessaires à la détection des scénarios d'attaques avancées. Il doit aussi avoir accès aux logs de sources hétérogènes afin de disposer d'une bonne visibilité sur le télétravail (voir tableau ci-dessous).

Sources de Logs	Détails
Firewalls frontaux	• Logs de l'IPS • Logs des règles de filtrage • Logs VPN et accès distants • Logs d'administration
Firewalls dorsaux	• Logs des règles de filtrage • Logs d'administration
Proxy web	• Logs de filtrage web • Logs du serveur de sandboxing • Logs d'administration
Firewall applicatifs	• Logs des serveurs web hébergeant des services publiés • Logs systèmes des plateformes publiées • Logs du firewall applicatif protégeant les services publiés.
Proxy courriel	• Logs de filtrage courriels • Logs du serveur de sandboxing • Logs d'administration
Antivirus / Antimalware	• Logs des tâches d'analyses et de scan • Logs d'administration • Logs de tâches de MAJ et de recherche
Solution de traçabilité des BD	
Solution de gestion des accès à privilèges	• Logs d'accès aux plateformes protégées • Logs de contournement de la procédure d'accès • Logs de modification de configuration et d'administration • Logs systèmes des serveurs hébergeant la solution
Contrôle d'intégrité	• Logs des changements • Logs d'administration de la solution • Logs systèmes des serveurs hébergeant la solution
Serveurs d'authentification forte	• Logs de création de compte • Logs d'authentification et de gestion des accès • Logs de changement des paramètres et d'administration • Logs systèmes des serveurs hébergeant la solution
Serveurs d'authentification forte	• Logs systèmes • Logs applicatifs et bases de données
Équipements réseaux	• Switch, routeurs
Autres	

Tableau 4 : Sources de logs

5.GUIDE PRATIQUE DES MESURES DE CYBERSÉCURITÉ

5.8- Traçabilité des accès privilégiés

Pour assurer une bonne protection des SI de l'organisation dans un environnement de télétravail, il convient d'accorder le plus grand soin à la gestion des accès par les comptes à privilèges détenus par les employés, les partenaires ou les fournisseurs. En effet, les cyber-escrocs sont plus intéressés par les comptes privilégiés que par n'importe quel autre type de compte. C'est pour cette raison qu'ils représentent un défi pour les services informatiques.

Il appartient aux solutions de type Privileged Access Management (PAM) d'assurer en temps réel la sécurité des accès à privilèges. Une solution PAM permet d'exercer un contrôle sur les accès des utilisateurs ayant des autorisations élevées leur permettant d'accéder à des ressources d'entreprise stratégiques. Il peut s'agir d'utilisateurs humains, d'appareils, d'applications et autres types de systèmes informatiques. En définissant le niveau approprié de contrôle pour chaque accès privilégié, la solution PAM permettra à l'organisation de condenser la surface d'attaque, ou tout au moins, d'atténuer les dommages résultant d'attaques externes.

Parmi les fonctionnalités des solutions PAM, relevons :

- Sécurisation des comptes à privilèges ;
- Rotation des mots de passe des comptes à privilèges ;
- Contrôle des sessions des administrateurs et prestataires ;
- Journalisation et enregistrement des sessions d'administration ;
- Sécurisation des flux d'administration en isolant l'utilisateur de la cible.

L'architecture idéale pour les accès d'administration en mode télétravail consiste à mettre en place une des composantes de la solution PAM au niveau de la zone DMZ publique. Chaque flux d'administration provenant de l'extérieur doit passer impérativement par ce composant PAM. Ci-après un exemple d'architecture basée sur le produit Cyberark Core PAS qui pourra être mise en place avec profit.

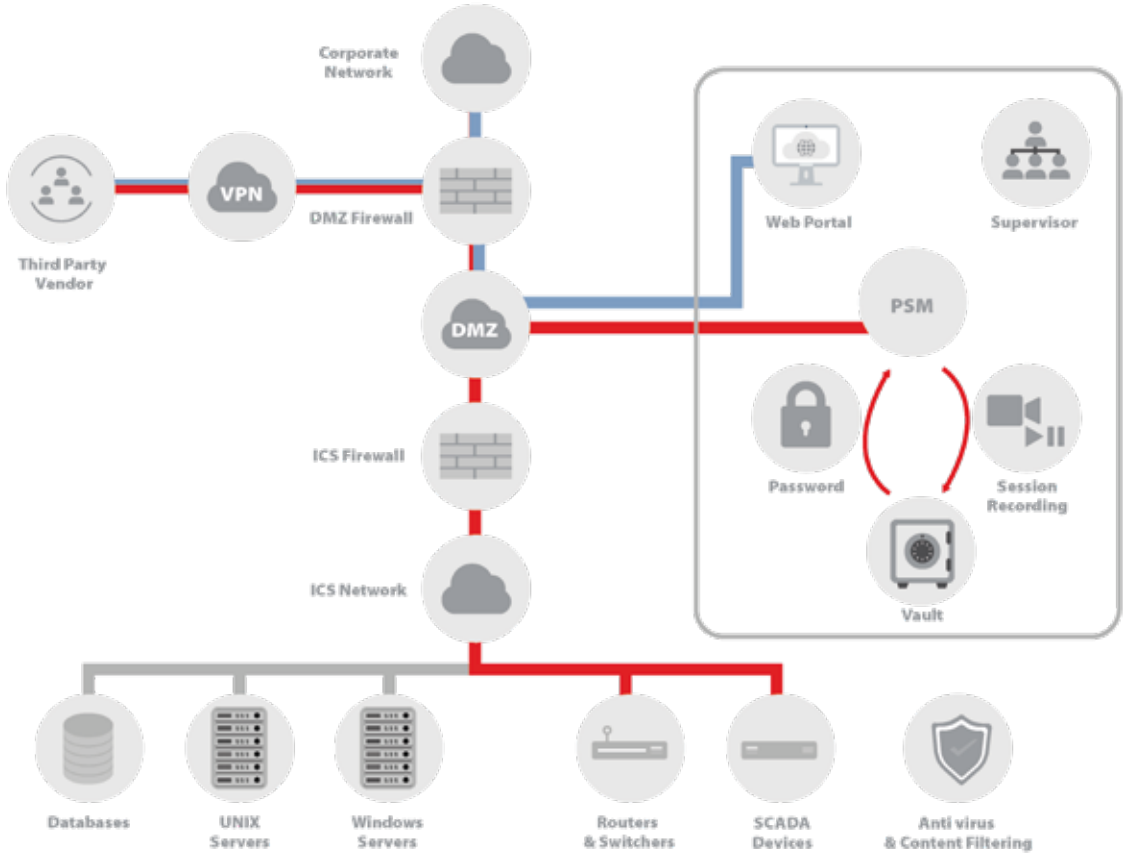
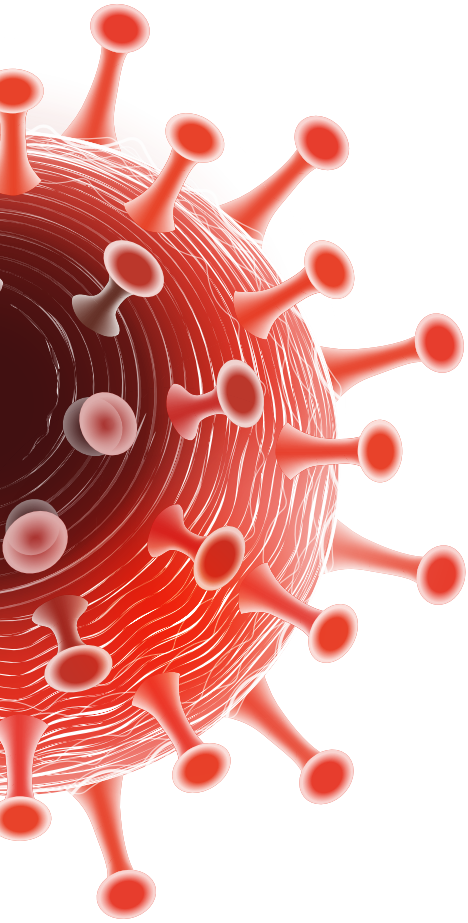


FIGURE 26 : SOLUTION PAM INTÉGRÉE DANS LA ZONE DMZ PUBLIQUE

5.9- Chiffrement des données

Les données d'un poste mobile volé ou perdu qui ne sont pas chiffrées, peuvent facilement être récupérées par des pirates informatiques. Voilà pourquoi, il est recommandé d'utiliser une solution centralisée de chiffrement de disque si vous en disposez pour faciliter la récupération des données en cas d'oubli de mot de passe et de blocage d'accès. Néanmoins, vous pouvez utiliser l'outil BitLocker disponible sous Windows pour faire un chiffrement du poste mobile ou FileVault pour Mac OS.



6 CONCLUSION

6.CONCLUSION

L'expérience de télétravail dans laquelle s'engagent les organisations en 2020 est unique. Toutes les études sur le télétravail effectuées jusqu'à ce jour concordent sur la nécessité de planifier soigneusement le lancement du programme de télétravail, de privilégier le principe du volontariat et d'alterner les périodes de travail à domicile et sur site. Or, le télétravail découvert à l'occasion de la crise du coronavirus COVID-19 est improvisé, imposé et permanent pendant la durée de la pandémie. C'est dire que les conditions de déploiement sont loin d'être idéales.

Pourtant, nous n'avons pas droit à l'échec. Le salut de l'organisation – qu'il s'agisse d'une entreprise privée, de la PME à la multinationale, ou d'une administration publique – est en jeu. Pour tout le monde, l'expérience du télétravail a commencé le vendredi 20 mars à 18h00 avec la proclamation de « l'état d'urgence sanitaire » par les pouvoirs publics. Du jour au lendemain, les organisations ont dû se redéfinir à partir de la dichotomie entre des sites de travail entièrement ou presque vides et des résidences personnelles qu'il a fallu mobiliser.

Il est intéressant de considérer les résultats d'un sondage effectué auprès de la fonction publique canadienne après 15 jours d'urgence sanitaire : plus de 40% des employés font état d'une hausse du sentiment d'isolement et environ 37% disent ressentir une hausse du stress, notamment parce qu'ils trouvent difficile de maintenir les services aux citoyens dans cette situation. Nul doute que ces résultats n'auraient pas été différents dans un autre pays ou dans un autre secteur d'activité.

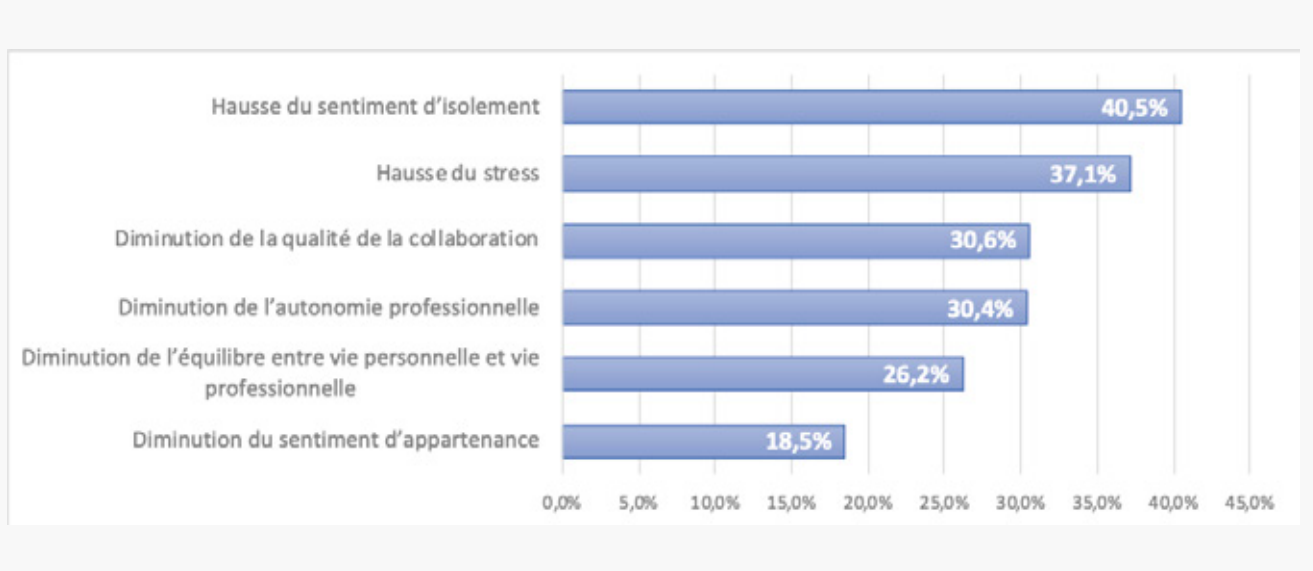


FIGURE 27 : IMPACT DU TÉLÉTRAVAIL SUR LES EMPLOYÉS D'UNE ORGANISATION GOUVERNEMENTALE

1.1- Le facteur humain

La dimension humaine du télétravail doit faire l'objet de toutes les attentions. Le premier geste à poser est la création d'un contrat de télétravail qui constituera la pierre angulaire des relations entre l'employeur et l'employé. Ce geste essentiel a pour objet de diminuer le niveau d'incertitude au sein des télétravailleurs en fixant des objectifs, temps de travail, mécanisme de redditions de compte et d'évaluation du rendement, plages horaires, aménagement de l'espace de travail, confidentialité et protection des données, conservation des documents, utilisation des équipements informatiques, etc.

1.2- L'architecture sécuritaire

Le télétravail exige que les SI de l'organisation soient ouvertes aux accès distants. Pour cela, il convient d'établir des règles strictes à ce sujet et, par l'entremise d'une gestion centralisée, s'assurer que les outils de protection sont mis à jour en permanence. Comme on l'a vu, des solutions sont offertes dans le marché permettant de vérifier un poste de travail à distance avant d'en autoriser la connexion au réseau d'entreprise.

Toutes les données transitant entre le poste du télétravailleur et l'entreprise doivent être chiffrées. La façon la plus simple de le faire est d'utiliser un VPN ou un VDI en tant que connexion réseau unique. En plus de chiffrer toute transmission, le VPN et le VDI peuvent empêcher les liaisons directes entre l'utilisateur et Internet. Pour se relier à Internet, le télétravailleur doit alors passer par le réseau sécurisé de l'organisation, ce qui confère une protection accrue. Bien sûr, les accès VPN ou VDI imposent une contrainte au réseau, mais c'est une hygiène nécessaire – ce qui n'exclut pas le recours à titre provisoire à la publication directe sur Internet ou l'accès par un portail spécialisé.

Une tendance observée au sein des organisations est de privilégier fortement la sécurisation du réseau. On doit se rappeler, cependant, que ce dernier ne constitue qu'un maillon dans la chaîne de sécurité. Il est primordial également d'inculquer aux télétravailleurs certaines habitudes fondamentales. C'est ici que l'exigence technique rejoint la dimension humaine du télétravail.

En résumé, l'expérience de télétravail en cours aujourd'hui a la vocation de redéfinir la nature même de l'organisation.

DATAPROTECT

Security is our commitment

Casablanca Nearshore Park – Shore 4 Boulevard Al Qods , Sidi Maarouf
Contact : contact@dataprotect.ma
Tél : +212 522 218 390