TRAIN FOR TRADE

NATIONS UNIES
CNUCED

Cours spécial :
Développer la résilience des ports face aux pandémies

Manuel du participant

Section 3 – Préparation technologique

Renforcer les connaissances
et les compétences par des approches innovantes
pour un développement économique durable

Compte des Nations Unies pour le Développement
Département des affaires économiques et sociales

Irish Aid
Government of Ireland
Rialtas na hÉireann

learn.unctad.org

Table des matieres

Photo: Tom Fisk / Pexel

3. PRÉPARATION TECHNOLOGIQUE

Les ressources technologiques (applications, processus, systèmes d'information et de communication) sont généralement conçues pour être utilisées dans des circonstances et des conditions normales. Exemples de décisions de conception qui sont généralement prises dans des circonstances normales :

- Les principaux systèmes d'information de l'entreprise ne sont rendus accessibles qu'au niveau local (depuis le bureau via le réseau local d'entreprise, LAN) pour des raisons de confidentialité et de sécurité.
- Bien que de nombreux progrès aient été réalisés et continuent d'être réalisés dans la numérisation et la suppression du papier à la recherche d'une plus grande efficacité et du respect de l'environnement, de nombreux processus ne sont pas encore numérisés. Dans des circonstances normales, la numérisation de ces processus papier est considérée comme importante, mais pas urgente.
- Dans la plupart des cas, il n'est pas jugé nécessaire de mettre en place des outils collaboratifs, de visioconférence et de télétravail en raison de la présence sur site de la main-d'œuvre portuaire.
- Le mode de travail sur site signifie que généralement les ressources informatiques (IT) mises à disposition des utilisateurs sont des appareils fixes (postes de travail) en raison de leur faible ratio coût/performance.
- Les lignes de communication (internes, externes et internet) sont dimensionnées et sécurisées en tenant compte des flux d'informations (et des bandes passantes) qui sont nécessaires lorsque la plupart des employés travaillent sur site.

Toutes ces décisions de conception peuvent ne plus être valides dans une situation de pandémie et peuvent devoir être reconsidérées, repensées et leur hiérarchie redéfinie. C'est cet aspect qui sera abordé dans cette section ainsi que ce qui est nécessaire pour préparer les ressources technologiques à affronter une situation de pandémie.

Les objectifs de cette section seront de :

- identifier des solutions technologiques appropriées pour des modes de travail alternatifs
- planifier la dématérialisation ;
- identifier et mettre en place des outils de communication numérique efficaces.

3.1 Technologie, capacité et sécurité du télétravail

Les ressources technologiques ont été conçues dans des circonstances normales, le personnel de l'organisation effectuant habituellement ses tâches en personne à partir du poste de travail mis à sa disposition qui comprend les dispositifs technologiques nécessaires (ordinateur personnel ou tablette, imprimante, etc.). Dans une situation de pandémie, où les personnes peuvent devoir rester isolées chez elles, les organisations doivent s'assurer que les ressources nécessaires sont disponibles à distance et ont une capacité suffisante.

En situation de confinement, il est nécessaire de vérifier et d'adapter les moyens technologiques pour que :

- le personnel dispose des ressources nécessaires pour accéder à distance aux systèmes informatiques de l'entreprise.

Il faut s'assurer que tout le personnel qui travaille à distance dispose des moyens nécessaires et suffisants pour le faire. Les exigences minimales doivent être un PC et une connexion Internet disponible à l'endroit à partir duquel ils vont travailler (par exemple leur domicile).

Dans un premier temps, il convient d'établir une liste du personnel qui serait en télétravail et à partir de quel endroit le travail se ferait :

√ Le service informatique du port identifie les employés qui disposent actuellement d'un ordinateur portable qui leur permettrait de travailler à distance.

√ Chaque salarié doit indiquer s'il dispose de son propre équipement (PC) et d'une connexion internet haut débit WIFI ou 4G/5G à l'endroit où se situerait son poste de travail distant.

Politique d'ordinateur unique

Il est recommandé que le port fournisse des PC pour s'assurer qu'ils sont équipés des mécanismes et mesures de sécurité de l'entreprise (par exemple, antivirus, politique de mise à jour des correctifs de sécurité et nécessaires pour une connexion sécurisée aux systèmes d'information). Il est donc conseillé d'acquérir les appareils nécessaires pour équiper les employés qui n'en disposent pas et d'envisager la mise en œuvre de la politique « d'ordinateur unique » dans l'organisation. À ce jour, la plupart des organisations ont fourni aux employés un ordinateur de travail (PC) à leur poste de travail habituel, en le complétant par un ordinateur portable (PC) uniquement pour ceux qui devaient être mobiles en raison des exigences de leur travail.

En situation de pandémie, l'exigence de mobilité est étendue à l'ensemble (ou à la majorité) de la main-d'œuvre portuaire. Il n'est plus nécessaire (sauf dans de très rares cas) pour un utilisateur d'avoir deux ordinateurs. C'est le sens de la politique de l'ordinateur unique : l'organisation met à disposition de chaque utilisateur uniquement un ordinateur portable. Le rapport coût/performance est toujours meilleur pour les PC de bureau que pour les portables, mais l'écart se réduit. Le besoin de mobilité en cas de pandémie, une plus grande sécurité des équipements de l'entreprise et une réduction des coûts matériels et logiciels par rapport à la maintenance de deux ordinateurs, font que la politique de l'ordinateur unique est un élément à envisager et à mettre en œuvre dans l'organisation.

Si les employés disposent d'un ordinateur portable personnel plutôt que d'un ordinateur portable d'entreprise pour effectuer des tâches de télétravail, l'équipement devra répondre à certaines exigences minimales :

√ dernières mises à jour du système d'exploitation et de sécurité installées ;

√ antivirus à jour installé.

En plus du matériel (PC), chaque utilisateur doit disposer d'une connexion WIFI Internet haut débit. Sinon, des connexions ad-hoc 4G/5G devront être acquises, l'organisation doit également vérifier si l'employé dispose d'un téléphone mobile d'entreprise/personnel avec un forfait données qui permet de partager les données avec un ordinateur et de les utiliser comme une connexion 4G/5G.

En plus du PC et de la connexion internet, il est important de s'assurer que les utilisateurs disposent du matériel nécessaire pour pouvoir télétravailler. Par exemple, pour les

organisations qui appliquent un système de signature électronique dans leurs processus de gestion et disposent d'un certificat numérique sur une carte cryptographique, il peut être nécessaire de fournir un lecteur de carte cryptographique pour les employés qui sont en télétravail.

En résumé de cette section : il est important de s'assurer que tout le personnel qui va travailler à distance dispose à la fois des ressources minimales (PC et connexion internet haut débit) et des ressources complémentaires pour accéder et interagir avec les systèmes informatiques commerciaux de l'organisation. La première étape devrait être de dresser une liste et de s'assurer que tout le monde est correctement équipé.

- Les systèmes informatiques de l'entreprise sont accessibles à partir de l'extérieur de l'organisation

Une deuxième étape consiste à s'assurer que les applications et les services informatiques nécessaires à l'exécution des fonctions des employés qui vont télétravailler sont accessibles depuis l'extérieur et que l'expérience utilisateur est acceptable. Le temps de réponse des systèmes et des applications doit être adéquat afin que les employés ne soient pas pénalisés par l'accès à distance.

Il est donc nécessaire de fournir les moyens de rendre les systèmes d'entreprise accessibles et utilisables de l'extérieur de l'organisation. À cet égard; il convient de prendre en compte les points suivants :

a) Solution d'entreprise d'accès à distance

Une solution d'accès à distance permet d'établir ce qu'on appelle un VPN (Réseau privé virtuel) entre les appareils distants et le réseau de l'organisation. Il crée une extension sécurisée (en établissant un tunnel IPSec ou SSL) du réseau local (LAN) de l'organisation sur un réseau public et, par défaut, sur un réseau non sécurisé comme Internet. De nombreux fabricants proposent ce type de solution. En cas d'indisponibilité, les deux alternatives (solution locale ou nuage) doivent être évaluées pour voir laquelle est la mieux adaptée aux besoins de l'organisation.

Solution d'accès à distance au nuage

Si l'organisation n'a pas encore installé de solution d'accès à distance, elle peut envisager une solution basée sur le nuage, qui permet un déploiement rapide et sécurisé, même si la capacité nuage disponible au sein de l'organisation est limitée. Ce type de solution, proposé par de nombreux fabricants sur une base de facturation à l'utilisation, permet un accès temporaire à l'organisation depuis n'importe quel endroit avec les mesures de sécurité nécessaires pour le type d'informations traitées. Elle repose sur la transmission de la couche de présentation des systèmes de l'entreprise à n'importe quel ordinateur

distant dans la mesure où l'authentification appropriée a été effectuée. Dans ce cas, il est complètement isolé de la plate-forme d'accès au réseau de l'entreprise, pour éviter de mettre les systèmes de l'entreprise en danger en raison des vulnérabilités des clients.

L'architecture nécessaire pour fournir ce type d'accès repose principalement sur l'infrastructure utilisée par le nuage. L'utilisateur a uniquement besoin d'accéder à une page Web pour s'authentifier et accéder aux services de l'entreprise. La seule partie de l'architecture qui relève de la responsabilité de chaque organisation est le déploiement d'une petite machine virtuelle, le « Connecteur », qui établit une communication sécurisée entre le nuage et les services de l'entreprise.

Quel que soit le type de solution d'accès distant choisie (locale ou nuage), une fois mise en place, un test de contrainte doit être réalisé en surveillant les connexions simultanées et en analysant le comportement du système. Un test contrôlé avec l'aide des utilisateurs serait la méthode de test la plus fiable et la plus idéale. Si cela n'est pas possible, le service informatique doit simuler un test de charge.

b) Accessibilité aux applications et aux systèmes de l'organisation

Les applications Web et les systèmes qui fonctionnent avec des protocoles d'accès Internet standard (par exemple http, https) ainsi que des interfaces utilisateur allégées (par exemple html, JavaScript) doivent être accessibles immédiatement après l'établissement de la connexion VPN.

Les applications et les systèmes impliquant des interfaces utilisateur lourdes ou des protocoles non standard peuvent ne pas offrir l'expérience utilisateur requise. Elles peuvent ne pas offrir des temps de réponse acceptables ou peuvent même ne pas fonctionner. Il convient de tester l'accès à distance à ce type particulier d'application. Si l'accessibilité n'est pas efficace via VPN, une solution de type VDI (Virtual Desktop Infrastructure) doit être envisagée.

Si l'utilisateur dispose déjà d'un ordinateur (PC) sur son lieu de travail, une solution rapide qui ne nécessite pas la mise en place d'un VDI est pour l'utilisateur de se connecter à distance en ouvrant d'abord une connexion VPN puis une connexion RDP (Protocole de bureau à distance) (Remote Desktop Protocol) avec l'ordinateur de bureau. Microsoft Windows possède une application/fonctionnalité appelée « Connexion de Bureau à distance » (Remote Desktop Connection) qui permet d'établir une connexion entre les ordinateurs Windows. C'est une solution simple et rapide recommandée lorsque l'utilisateur distant va se connecter à un ordinateur d'entreprise physique situé dans les bureaux de l'organisation. Dans ce cas, certaines conditions doivent être prises en compte, telles que :

- selon la configuration choisie, il peut être nécessaire de s'assurer que certains équipements informatiques situés dans les locaux du port (par exemple serveurs, PC) restent opérationnels (« allumés ») afin que l'accès à distance soit possible.
- Activer la fonctionnalité WOL (Wake On Lan) (Réveil par le réseau local) afin qu'en cas de besoin (après un arrêt involontaire ou une panne de courant), ils puissent être allumés à distance par le service informatique.
- L'ordinateur distant est un ordinateur d'entreprise durci qui dispose d'une solution de sécurité pour le point de terminaison.
- La politique d'accès VPN devrait limiter les utilisateurs distants à établir uniquement une connexion RDP avec leur propre équipement de bureau.

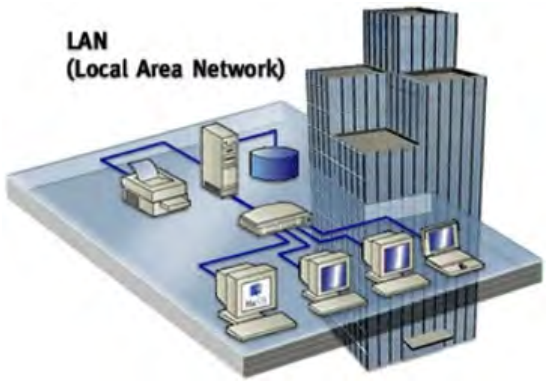
Il est déconseillé d'installer une solution ou une application d'entreprise sur des équipements personnels ou non professionnels. Au lieu de cela, cet équipement doit uniquement être utilisé en tant que client pour établir une connexion RDP distante à l'équipement physique d'entreprise parfaitement durci de l'utilisateur ou à un bureau virtuel (si on a déployé une infrastructure de bureau virtuel).

Lorsqu'il est nécessaire d'installer des applications d'entreprise sur des équipements n'appartenant pas à l'entreprise, il est recommandé de mettre en place une solution de type NAC (Network Access Control) (Commande d'accès de réseau) qui permet de contrôler les appareils, garantissant qu'ils sont conformes aux mesures de sécurité de l'organisation avant d'établir la connexion à distance.

Pour résumer cette section : chaque ordinateur distant doit avoir un mode d'accès client ou VPN, et ceux qui auront besoin d'accéder au bureau distant (l'ordinateur de bureau physique ou un ordinateur de bureau virtuel) doivent disposer d'un client RDP.

Il est également très important de préparer un bref manuel d'utilisation, détaillant comment installer, se connecter et se déconnecter à la fois du VPN et du Bureau à distance, le cas échéant. Les organisations ont souvent tendance à se concentrer sur les moyens technologiques et à oublier les utilisateurs qui vont les utiliser. Il est donc important de fournir aux utilisateurs des instructions claires et simples.

- Les lignes de communication ont la bande passante nécessaire et suffisante pour prendre en charge le travail à distance



Les lignes de communication, en particulier la bande passante de la connexion Internet, sont conçues en fonction des besoins de l'organisation dans une situation normale. En situation normale, la connexion entre les systèmes informatiques de l'entreprise et les utilisateurs s'établit principalement via le LAN. La capacité de la ligne d'accès Internet est conçue pour que des ressources externes à l'organisation (par exemple, les services de nuage, la communication avec des tiers et l'accès aux services Internet) puissent y accéder.

En situation de pandémie, le scénario est inversé. Les utilisateurs distants utilisent leur propre connexion Internet haut débit WIFI ou 4G/5G pour accéder à des ressources extérieures à l'organisation (par exemple, les services en nuage, la communication avec des tiers et l'accès aux services Internet) et consomment la bande passante d'une ligne d'accès Internet d'entreprise lorsqu'ils accèdent aux systèmes d'information internes de l'organisation.

Il est donc nécessaire de s'assurer que la ligne de communication vers Internet est suffisante pour prendre en charge le travail à distance.

Comme mentionné ci-dessus, l'accès à distance aux systèmes et aux applications doit être agile et doit offrir pour l'utilisateur une expérience aussi proche que possible de celle offerte dans une situation normale. Même si des protocoles d'accès légers sont toujours utilisés après l'établissement de la connexion VPN (par exemple http ou https pour l'accès aux applications Web et RDP pour le reste des systèmes et applications), il

est nécessaire de vérifier que la ligne de connexion Internet de l'organisation est capable de prendre en charge le trafic entrant qu'implique le télétravail. Afin d'atteindre cet objectif, il est recommandé d'effectuer un test contrôlé en surveillant la bande passante et en prenant des mesures après l'ouverture de plusieurs connexions RDP et VPN avec les applications Web de l'organisation. Une fois ces mesures effectuées et après avoir estimé le nombre de connexions RDP et VPN simultanées, il est possible de réaliser un calcul approximatif de la bande passante nécessaire.

Il est tout aussi important d'offrir des instructions claires et simples aux membres de l'organisation afin d'éviter que la ligne vers l'Internet de l'entreprise ne se détériore, en précisant que :

- la connexion VPN ne doit être utilisée que pour accéder aux services internes de l'organisation, aux applications Web d'entreprise et à une connexion de bureau à distance.
- Aucune connexion VPN ne doit être établie pour accéder aux services du nuage, pour communiquer avec des tiers ou accéder aux services Internet.

Tout au long de cette section, nous avons souligné qu'il est important de fournir des instructions claires et simples sur la façon de procéder pour les employés qui télétravaillent. Il est recommandé d'accompagner ces instructions d'une petite formation/webinaire ad hoc. L'enregistrement d'une vidéo de formation et son téléchargement sur l'intranet de l'organisation est une option.

3.2 Outils de productivité en télétravail

Dans une situation normale devant la proximité naturelle des employés et la possibilité de se déplacer d'un endroit à un autre ou dans une autre ville, si nécessaire, les organisations ont eu tendance à tenir pour acquis que les réunions d'affaires se tiennent en présentiel.

Et lors de l'établissement de relations d'affaires (à la fois internes et externes), peu d'organisations ont vu le besoin de mettre en œuvre des solutions de télétravail (par exemple, visioconférence, chat, travail dans le nuage, réseaux sociaux d'entreprise, etc.) car, dans l'hypothèse d'une présence du site, le retour sur investissement (ROI) peut être faible.

Dans une situation de pandémie, les outils qui permettent aux collègues d'interagir à distance sont nécessaires car ils éliminent la barrière de la distance. Ces outils doivent être simples d'utilisation et doivent offrir une expérience utilisateur qui imite au plus près le contact personnel.

De nombreux outils disponibles sur le marché peuvent aider au télétravail. Il existe des outils spécialisés dans la visioconférence et d'autres qui disposent de cette fonctionnalité mais qui intègrent également d'autres fonctions telles que le chat individuel, le chat d'entreprise, le travail en groupe, le partage de documents et l'intégration d'applications. Ces derniers sont appelés **plateformes collaboratives**.

Afin de pouvoir faire face à une situation de télétravail, il est conseillé de mettre en place une solution collaborative. Selon la manière dont la solution choisie a développé ses capacités de visioconférence et les besoins de l'organisation en la matière, il peut être nécessaire de la compléter par un outil de visioconférence spécialisé.

Dans tous les cas, les outils de productivité et de visioconférence (si nécessaire) mis en œuvre doivent être multi-supports. Ils doivent fonctionner indépendamment de l'appareil dont dispose le télétravailleur (par exemple, smartphone, tablette, ordinateur portable ou ordinateur de bureau).

Google Workspace et Microsoft 365 sont des exemples de plateformes collaboratives et Zoom, Microsoft Teams et Cisco Webex sont des exemples d'outils spécialisés pour la visioconférence.

Les **principales fonctionnalités de base** qui doivent être fournies aux télétravailleurs et qui sont généralement proposées par ces outils sont les suivantes :

- **Courriel** : L'adresse électronique est l'outil par excellence de la communication numérique à distance. Les organisations disposent généralement déjà d'un système ou d'un service de messagerie, mais elles doivent s'assurer que ce service a été déployé dans tous les départements et que chaque employé dispose d'un compte de messagerie.
- **Visioconférence** : Un outil de visioconférence remplace les réunions en face à face et doit permettre une interaction agile et efficace entre les participants aux réunions en proposant des fonctionnalités de base telles que le partage d'écran et la modération de réunion. Il est important de garder à l'esprit que les personnes de l'organisation elle-même et de l'extérieur doivent pouvoir assister aux réunions tenues par vidéoconférence. L'organisation doit donc sélectionner un outil permettant aux participants de rejoindre et de participer aux réunions virtuelles indépendamment du matériel et des logiciels installés sur leur appareil.
- **Appels audio** : La plupart des plateformes permettent, via le même outil de visioconférence, d'émettre des appels audio vers d'autres utilisateurs de la plateforme au moyen du la VoIP (voix sur protocole internet). Les appels vers des tiers (hors plateforme) et qui nécessitent une connexion au système téléphonique ont généralement un coût supplémentaire et peuvent nécessiter une passerelle d'intégration avec le système téléphonique de l'entreprise.
- **Messagerie instantanée** : Cette fonction permet aux utilisateurs d'envoyer un message contextuel (« pop-up ») à une personne spécifique, à un groupe de personnes ou même à l'ensemble de l'organisation.
- **Chat/canaux** : Cette fonction permet aux utilisateurs d'établir des fils de conversation spécifiques qui peuvent éviter les courriels inutiles et, dans certains cas, ingérables.
- **Partage de documents** : Cette fonction permet aux utilisateurs de stocker, de partager des documents et d'y accéder. Certains systèmes collaboratifs ont une capacité de co-création qui permet aux utilisateurs de travailler sur le même fichier en même temps avec une synchronisation automatique et instantanée des modifications, permettant également de suivre l'historique des versions.
- **Espaces de travail virtuels en groupe** : Cette fonction permet aux utilisateurs d'organiser les télétravailleurs par équipes de travail, projets, départements, etc. de sorte qu'il est plus facile d'interagir avec un groupe de personnes prédéfinies (par exemple, partage de documentation, chat, envoi d'un message instantané, tenue d'une vidéo ou audioconférence)

Les organisations doivent chercher à mettre en œuvre une solution qui offre ces sept fonctionnalités pour faciliter le télétravail. Certaines plateformes collaboratives peuvent offrir des fonctions supplémentaires qui peuvent compléter les fonctions de base pour atteindre une plus grande efficacité et agilité dans le travail collaboratif.

Outre la mise en œuvre de ces outils logiciels, il est important de ne pas négliger les outils matériels nécessaires à l'exécution de la solution choisie.

Il est fortement recommandé de fournir des appareils mobiles tels que des smartphones ou des tablettes au personnel de gestion car il a été prouvé que la principale interface utilisateur utilisée à ce niveau est celle des appareils mobiles. Cela ajoutera de l'agilité et de l'immédiateté aux communications.

Formation et groupe de soutien en ligne

Enfin, la planification de la formation et de la préparation des télétravailleurs à l'utilisation des outils nécessaires au télétravail, et la mise en place d'un groupe de soutien en ligne pour répondre aux demandes ou aux éventuels incidents sont tout aussi importants que la sélection et le déploiement des outils.

En fonction du temps disponible pour mettre en œuvre le changement de modèle de travail (du modèle présentiel au modèle à distance), différentes **alternatives pour former les télétravailleurs** seront possible, notamment :

- Cours de formation standard ;
- Session de formation condensée ;
- Formation spécifique sur les sujets les plus pertinents et
- Publication des instructions techniques nécessaires à une mise en œuvre urgente.

Les utilisateurs étant appelés à changer d'environnement de travail et d'outils, le nombre de requêtes et d'incidents liés au télétravail sera, au début, presque certainement élevé. Il est donc recommandé de mettre en place un **groupe de soutien en ligne** pour les employés en télétravail.

- Dans la mesure du possible, le groupe de soutien en ligne doit être un groupe dédié et spécialisé pour ce type d'incident, indépendant du groupe traitant des incidents habituels avec les systèmes de l'organisation. Ce dernier doit suivre le parcours habituel défini par l'organisation.
- Il devrait y avoir deux canaux distincts : **1) pour les incidents** et **2) pour les questions non urgentes** telles que les doutes ou les interrogations. Cela permet au groupe de soutien de hiérarchiser les problèmes qui empêchent les employés de commencer ou de poursuivre le télétravail par rapport aux doutes ou à des questions moins urgents sur la façon d'utiliser les outils nouvellement mis en œuvre.
- Si nécessaire, des outils permettant l'accès à distance et le contrôle de l'ordinateur des télétravailleurs par l'équipe d'assistance doivent être disponibles.
- Il doit également y avoir des solutions disponibles en cas de problème qui ne peut pas être résolu à distance. Ainsi, en cas de problème matériel avec l'ordinateur portable d'un télétravailleur, un ordinateur de remplacement peut être envoyé via un service de messagerie et l'ordinateur qui pose problème être récupéré pour être réparé.

Pour résumer cette partie, afin de faciliter le télétravail, il est nécessaire de doter le personnel d'équipements informatiques de mobilité ainsi que d'outils logiciels collaboratifs. Il est également important de former tous les télétravailleurs à l'utilisation de ces ressources.

3.3 Dématérialiser

Les flux d'informations dans un environnement portuaire sont généralement très complexes et impliquent un grand nombre d'agents. Chaque mouvement de conteneur nécessite de multiples communications entre les membres de la communauté portuaire, créant ainsi un réseau complexe d'informations. C'est pourquoi un système ou une plate-forme électronique neutre et ouvert est nécessaire pour permettre un échange d'informations intelligent et sécurisé entre les agents publics et privés. C'est dans cette optique que les **Port Community Systems (PCS)** ont été créés.

Les PCS visent à optimiser, gérer et automatiser les processus portuaires et logistiques de manière efficace grâce à une transmission de données unique et à une connexion aux chaînes de transport et de logistique, afin d'atteindre :

- Une plus grande efficacité dans les transactions ;
- L'optimisation des ressources ;
- L'automatisation des processus ;
- Des économies de coûts;
- Une réduction des erreurs ;
- Un gain de temps et
- Un meilleur service à la clientèle.

En plus du PCS, les agents ou organisations qui ont choisi de numériser leurs processus s'engagent en faveur d'une culture dématérialisée. Les raisons pour la transition vers des médias numériques et pour encourager une réduction de l'utilisation du papier sont multiples. Certains des avantages d'une culture dématérialisée :

√ **Sûreté, sécurité et fiabilité.** Le stockage au format numérique nous permet de contrôler toutes les informations et de savoir qui accède aux documents et à quel moment.

√ **Plus grande productivité.** La gestion électronique des documents accélère les processus de consultation et de gestion de l'information.

√ **Optimisation des ressources.** Le stockage numérique élimine les coûts du processus traditionnel dérivé, par exemple, de l'impression, de l'envoi d'articles par la poste et de la destruction du papier.

√ **Amélioration de l'environnement.**

√ **Signature électronique.** Nous pouvons signer des documents électroniquement à partir de n'importe quel endroit et appareil mobile, réduisant ainsi le temps nécessaire pour conclure des accords, des négociations, etc.

Heureusement, les plateformes PCS permettent la numérisation des principaux processus de la chaîne logistique. La première étape consiste à déterminer s'il existe déjà une culture dématérialisée entièrement mise en œuvre. En période de pandémie, lorsque le personnel travaille à distance, les processus encore gérés sur papier représentent un handicap. Des efforts doivent être déployés pour les numériser.

Il est donc nécessaire d'identifier les processus qui ne sont pas encore numérisés et de les traiter au cas par cas. Selon le temps disponible pour s'occuper de leur numérisation, celle-ci peut se faire avec un degré d'automatisation plus ou moins important.

Des outils gratuits peuvent vous aider à vous débarrasser des processus au format papier. Les étapes d'un processus simple avec peu d'automatisation pourraient être les suivantes :

1. **Création** : Utiliser le traitement de texte (par exemple Microsoft Word ou Google Docs) de la plateforme collaborative pour numériser/convertir au format PDF standard (Portable Document Format) tout document généré dans l'organisation.
2. **Signature** : Si le document nécessite une signature, le détenteur de la signature électronique de l'entreprise ou l'application Adobe Acrobat Reader DC peuvent être utilisés.
3. **Diffusion** : Utiliser les outils de gestion de messagerie (ex. Microsoft Outlook ou Google Gmail) ou les outils de partage de documents (ex. Microsoft OneDrive/ SharePoint ou Google Drive) disponibles sur la plateforme collaborative.

Ces outils et ces étapes doivent faire partie de la phase de communication et de formation mentionnée dans la section précédente.

En résumé, les processus qui sont encore pris en charge au format papier doivent être identifiés pour aider à concentrer les efforts de numérisation. Il est recommandé d'aborder progressivement la transition vers la dématérialisation. Initialement, l'optimisation de l'automatisation ne doit pas être une priorité en raison du temps que cela implique. Cela pourra être abordé à un stade ultérieur.

3.4 Sécurité informatique et résilience

Dans une situation normale, les ressources informatiques de l'entreprise sont connectées et accessibles via le réseau local de l'organisation. La plupart des applications, bases de données, équipements (PC), etc. sont interconnectés via un réseau fiable et sécurisé. Dans cette situation, l'un des piliers les plus importants de la sécurité informatique est la sécurité du périmètre, c'est-à-dire qu'un périmètre de sécurité est établi autour du réseau de l'organisation. La pratique habituelle consiste à protéger le périmètre du réseau local avec des dispositifs de type pare-feu, permettant un accès sécurisé à partir des ordinateurs du réseau aux ressources extérieures et empêchant les ordinateurs extérieurs d'accéder aux ressources et systèmes internes de l'entreprise.

Cependant, en situation de télétravail, les équipements des télétravailleurs (par exemple les PC) doivent quitter le périmètre sécurisé établi en situation normale et, pour les besoins du système de sécurité du périmètre de l'organisation, ils seront traités comme tout autre équipement connecté à internet, c'est-à-dire comme un équipement peu fiable.

Lorsque les employés travaillent à distance, il est plus difficile de contrôler et d'arrêter les menaces. Dans cette situation, de nouveaux risques (cyber-risques) apparaissent et doivent être évalués, traités et atténués dans la mesure du possible.

Vous trouverez ci-dessous les recommandations et les mesures que nous devons prendre en compte afin de parvenir à un environnement informatique aussi sécurisé que possible et, reconnaissant qu'il n'est pas possible de garantir une sécurité absolue, d'avoir des mesures de reprise rapide en cas d'attaques délibérées. Les actions répertoriées sont les suivantes :

Recommandations générales

Il est recommandé, à titre de mesures générales de protection de :

- √ Installer les dernières mises à jour du système d'exploitation ;
- √ Mettre en place un protocole d'authentification puissant et un Active Directory de l'organisation. Dans le cas de services en nuage ou d'accès VPN, il est recommandé de ne pas avoir uniquement un accès par mot de passe mais d'avoir un système d'authentification à deux facteurs (2FA) ;
- √ Protéger le BIOS (Basic Input/Output System) avec un mot de passe fiable ;
- √ Disposer de solutions de sécurité spécifiques dans les postes de travail : compléter l'antivirus traditionnel et indispensable (EPP - Endpoint Protection Platform) par une solution de type EDR (EndPoint Detection and Response) ;
- √ Mettre en place une politique d'administration centralisée des équipements de travail dans laquelle les utilisateurs n'ont pas d'identifiants d'administrateur ;
- √ Protéger les informations. La plupart des ordinateurs portables professionnels disposent d'une puce TPM (Trusted Platform Module) grâce à laquelle les données du disque dur peuvent être cryptées, protégeant les informations même en cas d'accès physique au disque ;
- √ Disposer d'une liste à jour des personnes, adresses IP, téléphones, adresses électroniques du personnel qui accède aux systèmes à distance ;
- √ Examiner les enregistrements et auditer les connexions à distance ;
- √ Restreindre le montage d'unités d'organisation mappées sur des ordinateurs distants non sécurisés.

Diagnostiquer les nouvelles menaces

Le télétravail comporte plusieurs risques qui doivent être pris en compte en amont afin de mettre en place les solutions les plus sûres.

Le début d'une crise telle qu'une pandémie s'accompagne d'un besoin d'information. Les gens ont besoin de savoir quoi faire en cas de contagion, quelles mesures de protection doivent être prises, comment la pandémie évolue, quelles dispositions sont prises pour un vaccin, etc. Ce fait est exploité par les cybercriminels.

Ainsi, on a enregistré plus de 20 000 domaines utilisant des termes liés à la COVID-19, plus de 50 % des enregistrements ont été effectués en mars 2020 (alors que le confinement était total dans certaines parties du monde), nombre d'entre eux servaient clairement des objectifs malveillants. Des solutions de prévention et technologiques sont nécessaires pour affronter ces nouvelles menaces.

Prévenir

Les adresses électroniques sont un point d'entrée pour les attaques par hameçonnage (phishing). En période de pandémie, les courriels avec des objets de message et des adresses qui semblent être des sources officielles et fiables abordant le problème de la pandémie abondent. Cependant, derrière ces messages se cachent des fichiers ou des liens très dangereux.

Il est important de bien informer les employés de l'existence de ce danger, car ils peuvent ignorer cette réalité.

Former

L'organisation doit expliquer à ses employés comment protéger leur équipement informatique et leurs connexions lorsqu'ils travaillent à distance, et doit vérifier que des techniques de cryptage d'équipement appropriées et des systèmes d'authentification sécurisés sont utilisés. De plus, les employés doivent être formés sur la façon de gérer une menace conformément au protocole de l'organisation pour faire face aux cyberattaques. À cet égard, il est recommandé de réaliser une simulation de campagne de hameçonnage qui aidera les employés à comprendre le problème de manière palpable et à les former à des situations réelles.

Plan d'urgence

Les organisations les mieux préparées disposent d'un plan d'urgence qui leur permet d'anticiper les difficultés qui peuvent survenir. Au contraire, ceux qui ont été surpris par la situation sans plan d'action et ont même été contraints d'improviser un système de télétravail faute de planification, ont vu leurs systèmes saturés par l'augmentation du

trafic d'accès à distance et ont dû fournir aux équipements distants des mesures de sécurité dans une course contre la montre.

Aucune organisation ne veut arrêter son activité. Pour l'éviter, un **Plan d'urgence** doit être conçu et mis à la disposition des travailleurs concernés. Ce plan doit être testé périodiquement pour confirmer sa validité et son efficacité et être mis à jour si nécessaire. Avoir un plan d'urgence non testé ou obsolète est inutile.

Cyber-résilience

Aujourd'hui, pour développer et maintenir leur activité, les organisations dépendent de la technologie. À l'ère de la transformation numérique, une faille de sécurité peut paralyser les entreprises et les processus de production, entraînant des pertes économiques et d'autres conséquences qui compromettent la continuité de l'organisation.

La cyber-résilience est la capacité d'une organisation à anticiper, résister, récupérer et évoluer pour améliorer ses capacités face aux conditions défavorables, au stress ou aux attaques contre les cyber-ressources dont elle a besoin pour fonctionner.

On dit d'une organisation qu'elle est cyber-résiliente si elle est consciente que la sécurité absolue n'existe pas et suppose donc que certaines attaques ne seront pas stoppées. Partant de cette hypothèse, elle dispose d'un plan d'action qui lui permet de reprendre l'activité de l'organisation dans les plus brefs délais si une telle attaque se produit.

L'organisation qui a mis en place des plans d'urgence, de continuité et de crise sera en mesure de surmonter une cyber-attaque en moins de temps et à un moindre coût économique. La planification et la prévention sont les meilleurs moyens pour assurer une protection adéquate contre les cyberattaques et pour devenir une organisation cyber-résiliente.

Mesurer la cyber-résilience

Dans quelle mesure mon organisation est-elle cyber-résiliente ? Quel est son niveau de cyber-résilience ? La cyber-résilience ne peut être améliorée que si elle peut être mesurée.

Il existe des méthodes qui permettent de mesurer le degré de cyber-résilience d'une organisation. Le cadre de référence des indicateurs de cyber-résilience proposé par MITRE[1] est l'un des plus répandus. Ce cadre s'appuie sur les quatre objectifs qu'une organisation cyber-résiliente doit atteindre : anticiper, résister, restaurer et évoluer :

- √ **Anticiper** : maintenir un état de préparation éclairé afin de prévenir les compromissions de la mission/des fonctions commerciales dues aux attaques de l'adversaire.
- √ **Résister** : maintenir les fonctions essentielles du métier de la mission/du métier malgré l'exécution réussie d'une attaque par un adversaire.

1 MITRE (2012), Cadre d'ingénierie de la cyber-résilience.
https://www.mitre.org/publications/technical-papers/cyber-resiliency-engineering-framework

- √ **Restaurer** : restaurer les fonctions essentielles de la mission/du métier dans toute la mesure du possible après l'exécution réussie d'une attaque.
- √ **Évoluer** : modifier les missions/fonctions commerciales et/ou les cyber-capacités de soutien, afin de minimiser les impacts négatifs des attaques réelles ou prévues.

Afin d'atteindre ces quatre objectifs et d'être finalement considérée comme une organisation cyber-résiliente, les éléments suivants doivent être pris en compte :

- √ **Anticiper**
  - Politique de cybersécurité : avoir une politique qui définit les exigences en matière de cyber-résilience, traite les risques de cybersécurité, attribue les responsabilités et est communiquée dans l'ensemble de l'organisation.
  - Gestion des risques : identifier, analyser et atténuer les risques pour les actifs de l'organisation, qui pourraient affecter négativement le fonctionnement et la prestation des services.
  - Formation à la cybersécurité : promouvoir le développement des connaissances et des compétences des individus à l'appui de leurs rôles, pour atteindre et maintenir une cyber-résilience et une protection opérationnelles.
- √ **Résister**
  - Gestion des vulnérabilités : identifier, analyser et gérer les vulnérabilités des actifs qui soutiennent les services essentiels.
  - Surveillance continue : rassembler, compiler et diffuser des informations sur le comportement et les activités des systèmes et des personnes pour soutenir le processus continu d'identification et d'analyse des risques pour les actifs et les services essentiels de l'organisation qui peuvent affecter négativement leur fonctionnement et leur prestation.
- √ **Restaurer**
  - Gestion des incidents : établir des processus pour identifier et analyser les événements, détecter les incidents et déterminer et mettre en œuvre une réponse organisationnelle appropriée.
  - Gestion de la continuité des services : déterminer comment l'organisation effectue la planification des activités pour assurer la continuité des services essentiels en cas d'incident ou de catastrophe. Une attention particulière est accordée à l'objectif de restauration, pour lequel il existe un système de sauvegarde et de restauration (sauvegarde ou récupération de site) qui garantit qu'il existe des copies de toutes les informations de l'organisation.
- √ **Évoluer**
  - Gestion de la configuration et des changements : établir des processus pour maintenir l›intégrité de tous les actifs (technologie, informations et installations) nécessaires pour fournir les services essentiels.
  - Communication : établir des processus pour assurer la communication entre les responsables du fonctionnement des services essentiels, tant internes qu›externes à l›organisation.

Pour résumer cette section, en situation de pandémie, de nouveaux risques (cyber-risques) apparaissent et doivent être évalués, traités et atténués. À cet égard, il existe une série de recommandations pour obtenir l'environnement informatique le plus sûr possible.

Consciente qu'il existe des risques et des menaces qui ne peuvent être atténués, l'organisation doit être en mesure d'évaluer son état de cyber-résilience afin de progresser vers les objectifs qui n'ont pas encore été atteints et de permettre d'atteindre le degré de cyber-résilience nécessaire et acceptable.

Le cadre du MITRE est un bon référentiel pour mesurer l'état et améliorer le degré de cyber-résilience d'une organisation. Il s'appuie sur quatre objectifs (anticiper, résister, restaurer et évoluer), qui à leur tour incluent une série de domaines fonctionnels sur lesquels une organisation doit travailler.