FEDIL

The Voice of Luxembourg's Industry

LES IMPLICATIONS SÉCURITÉ DE LA CRISE SANITAIRE DE LA COVID-19 POUR LE SECTEUR INDUSTRIEL

TABLE DES MATIÈRES

PRÉFACE

La **FEDIL, The Voice of the Luxembourg's Industry**, en collaboration avec le **Ministère de l'Économie** (Direction du commerce électronique et de la sécurité de l'information) a mis en place un **Forum sur la Cybersécurité** dédié à l'industrie manufacturière (IND) suivant les principes d'un « **Information Sharing and Analysis Center** » (ISAC). La mission de l'IND-ISAC est de promouvoir la coopération en matière de cybersécurité au sein du secteur de l'industrie manufacturière au Luxembourg et dans la Grande Région au profit de l'attractivité de l'écosystème.

Comme mentionné dans les orientations politiques de la Commission Européenne 2019-2024, « *nous devons passer du besoin de savoir au besoin de partager* »[1] . La mission est réalisée grâce (1) au partage d'informations et de connaissances entre les représentants de confiance des organisations membres, et (2) à la diffusion d'informations sur les risques propres à l'industrie manufacturière, pertinentes pour le public.

L'objectif principal de l'IND-ISAC est de créer une taxonomie, ce langage commun nécessaire pour favoriser les synergies et se doter d'une compréhension commune des risques au sein d'une entreprise, d'un groupe et d'un écosystème en valorisant :

- l'importance d'une gouvernance informée, c'est-à-dire une gouvernance de la cybersécurité au niveau sectoriel basée sur autant d'informations factuelles que possible et constituant un avantage pour les responsables sécurité / RSSI,
- l'importance de la gestion des risques et surtout de l'utilisation d'autant d'informations objectives et factuelles que possible, et
- l'importance d'établir la communication entre la sécurité technique et organisationnelle en impliquant la Direction des entreprises.

L'IND-ISAC est composé d'entreprises de plusieurs types d'industries, représentées par des personnes en charge de la sécurité de l'information au sein de leur entité.

Le présent document est la première publication, fruit du travail de l'IND-ISAC et est axé sur la crise du COVID-19.

L'IND-ISAC va poursuivre ses travaux en permettant aux entreprises de partager des informations, leurs expériences, connaissances et les bonnes pratiques entre pairs dans un climat de confiance. Il vise à identifier les scénarios de risques, les vulnérabilités et les menaces spécifiques au secteur de l'industrie et fournit aux entreprises un accompagnement concret dans la conduite d'une analyse de gestion des risques.

Si vous souhaitez rejoindre l'IND-ISAC et devenir un membre actif, nous vous invitons à contacter notre équipe.

FEDIL

1 https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf

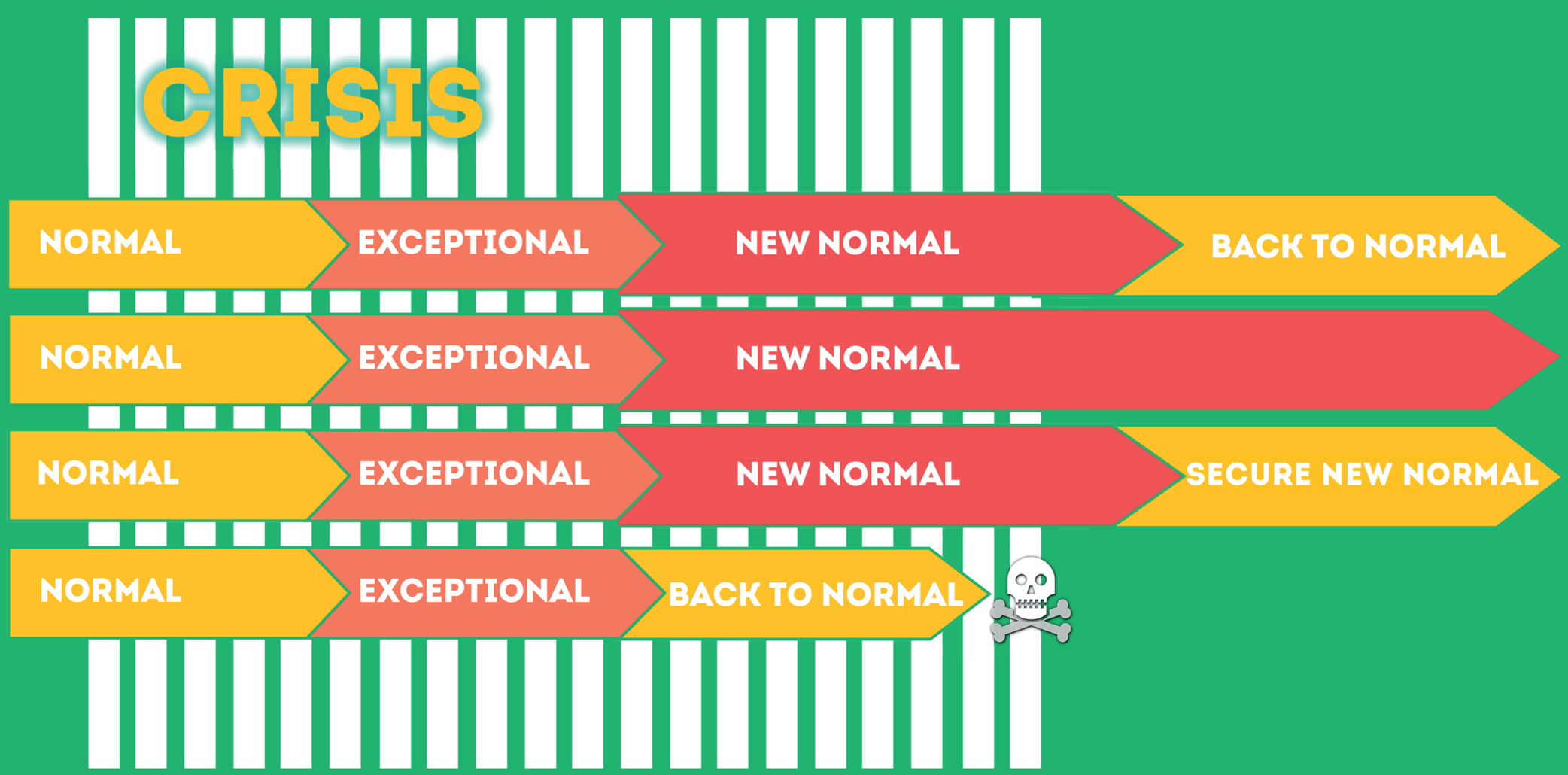
INTRODUCTION

Comme de nombreux autres secteurs, les secteurs industriel et manufacturier ont été durement touchés par la crise sanitaire et économique engendrée par la pandémie COVID-19. Cependant, la crise a également permis à ces derniers de déceler les faiblesses dans les plans de continuité d'activité et de gestion de crise, représentant ainsi un test en conditions réelles pour la gestion des risques. Il est donc important de mettre à profit les observations faites pour améliorer les performances lors des crises ultérieures (ou des vagues ultérieures de la crise actuelle).

Peu de temps après le déclenchement de la crise, la plupart des organisations sont passées d'un fonctionnement normal à un état exceptionnel, au cours duquel la production a été soit fortement réduite, soit temporairement arrêtée. Cette situation inattendue s'est accompagnée de problèmes imprévus, qui ont exigé le déploiement de solutions rapides et parfois non conventionnelles. Certaines organisations ont réussi à sortir de cet état en quelques jours, d'autres ont eu besoin de semaines - mais dans toutes les entreprises, a pu être observé l'installation d'un état de « nouvelle normalité ».

Dans cet état de « nouvelle normalité », la sécurité est parfois, souvent affaiblie, soit parce que les décisions ont été prises à la hâte, soit parce que les conditions antérieures (telles qu'un environnement sûr) ne sont plus réunies. Dès lors, la crise du COVID-19 doit être considérée comme une opportunité unique d'introduire de nouveaux concepts de sécurité (notamment liés au télétravail) et de les tester dans des conditions réelles - non seulement pendant la durée de la crise, mais également après le retour au bureau depuis un certain temps.

Pour le secteur industriel, les étapes de l'activité principale sont les matériaux, la production et la vente de biens manufacturés, c'est pourquoi les aspects de sécurité les plus importants sont liés à la réduction de la production et à la baisse de ventes. Il s'est avéré pendant la crise que ces deux aspects peuvent être impactés soit directement (par exemple, par les mesures prises par le gouvernement telles que la fermeture des frontières), soit indirectement par des interdépendances - qu'il s'agisse de clients, de partenaires ou d'investisseurs.



CONTENU DE CE DOCUMENT

Ce document aborde les changements dans le paysage des risques qui ont pu être détectés pendant ou causés par la crise de la COVID-19. En particulier, il traite des sujets suivants:

- les risques importants qui ont été négligés avant la crise;
- les nouveaux risques qui sont apparus pendant la crise;
- la prise en compte de la revue de l'évaluation des risques (changement de probabilité et/ou impact des scénarios de risques existants);
- les vulnérabilités créées lors du passage à la « nouvelle normalité »;
- l'attention portée à la sécurité pour le « retour à la normale »;
- les opportunités pour améliorer la sécurité sur le long terme.

NOUVELLES PERSPECTIVES DE ET POUR L'INDUSTRIE

1/ CHAÎNE LOGISTIQUE EN AVAL

PRINCIPALES CONSTATATIONS

La chaîne logistique est considérée comme un des actifs les plus importants de l'industrie manufacturière, car elle a un impact direct sur la production et donc sur l'activité principale de l'entreprise. Par conséquent, les entreprises avaient évalué les risques liés à l'achat de matières premières, avant même le début de la crise. En effet, on a constaté que les entreprises ont disposé de stocks suffisants et ont pu faire appel à des fournisseurs de remplacement lorsque la crise a frappé.

Jusqu'à ce jour, les risques liés à la partie en aval de la chaîne logistique avaient été négligés. Cependant, il est à noter que la crise n'a pas seulement impacté les fournisseurs mais également les clients, provoquant ainsi une forte baisse de la demande des biens produits. En peu de temps, les entrepôts se sont remplis et la production a dû être ralentie, voire arrêtée complètement, même si la crise n'a pas eu d'impact direct sur le fabricant au départ. La nécessité de réduire la production a engendré des coûts fixes élevés par rapport aux revenus comparativement faibles, menaçant l'existence même de l'entreprise.

ACTIONS CLÉS

A. EXPOSITION À DE NOUVEAUX RISQUES (LIÉS À LA CRISE)

- Inclure le risque « arrêt de la production en raison d'un manque de demande » dans l'évaluation des risques, en tenant compte de toutes les interdépendances au sein de la chaîne d'approvisionnement en aval.

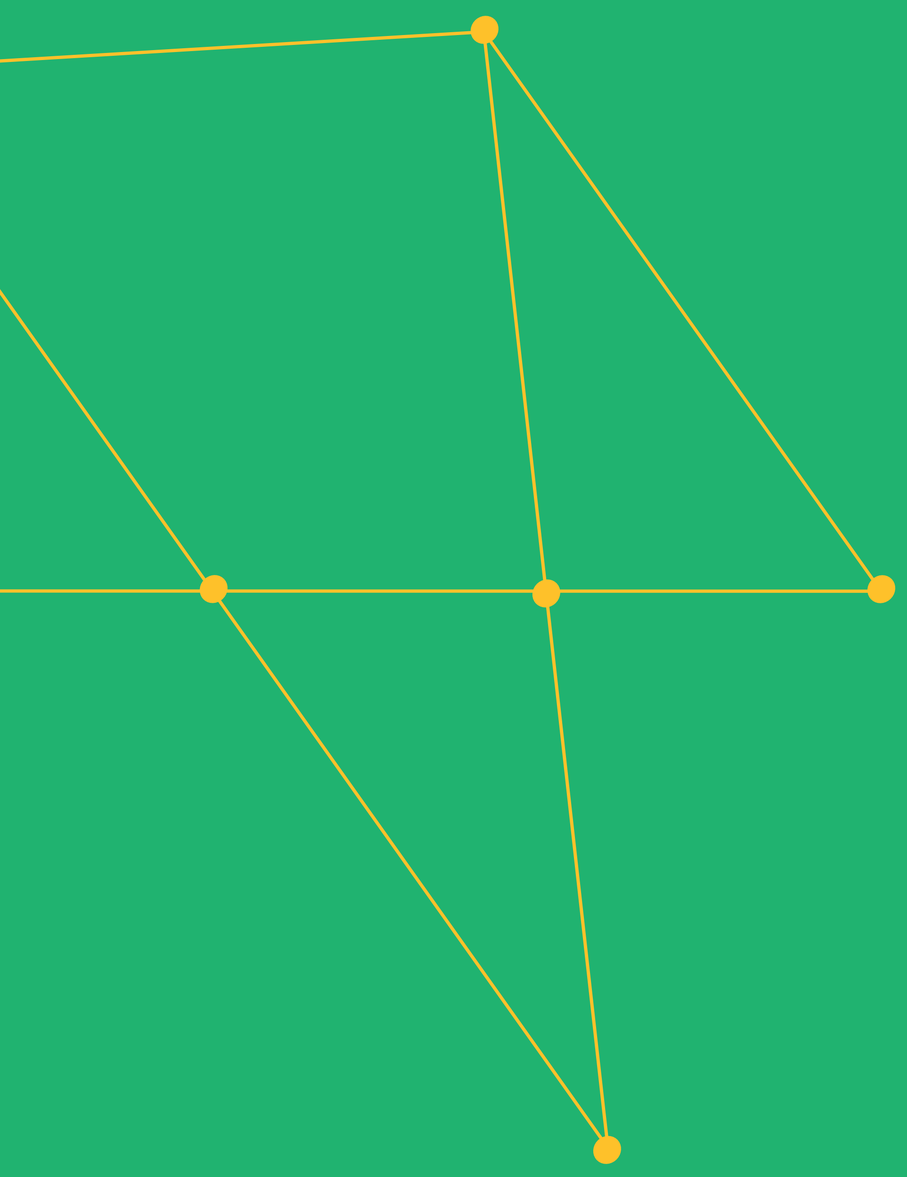
2/ RESTRICTIONS LOCALES VS GLOBALES

PRINCIPALES CONSTATATIONS

Lorsque la pandémie a frappé l'Europe et s'est étendue au monde entier, elle existait déjà depuis environ deux mois en Extrême-Orient. Par conséquent, la phase de reprise a pu commencer plus tôt dans ces régions également, permettant aux concurrents de prendre l'avantage sur les entreprises dans des régions encore ou nouvellement confinées.

Des observations similaires ont également été faites sur une portée de moindre ampleur quand les gouvernements européens n'ont pas coordonné la mise en place des restrictions et leur levée de manière opportune, créant ainsi des inégalités au sein du marché unique européen.

Il faut également relever une particularité propre aux pays comme le Luxembourg ayant plusieurs frontières avec des pays voisins; la législation fiscale pour les frontaliers, qui établit un seuil de jours de télétravail par an depuis l'étranger pour les salariés qui varie d'un pays à l'autre.



ACTIONS CLÉS

A. EXPOSITION À DE NOUVEAUX RISQUES (LIÉS À LA CRISE)

- Inclure le risque « perte de clients en raison de restrictions gouvernementales uniquement locales ou non synchronisées entre les pays ».

3/ GESTION DE CRISE

PRINCIPALES CONSTATATIONS

De manière générale, la relance des activités a pris un certain temps (jusqu'à plusieurs semaines), et ce, malgré l'existence de plans de reprise d'activité. Cela a été dû à plusieurs facteurs.

- En raison du confinement, la plupart des membres du personnel a été renvoyée chez elle pour travailler à distance. Par conséquent, le personnel clé désigné par les plans de reprise d'activité pour relancer les activités n'était pas disponible sur site. Néanmoins, la présence physique a souvent été nécessaire, soit parce que l'accès à distance était interdit pour des raisons de sécurité, soit parce que les processus n'étaient pas numérisés (ce qui est souvent le cas dans le secteur industriel pour la production de biens).
- De plus, le confinement n'a pas été levé d'un seul coup, dès lors des restrictions (telles que la distanciation sociale, le port de masques, la réduction des effectifs,...) ont été de rigueur de sorte que toutes les entreprises n'ont pas réactivé l'ensemble de leur effectif dans leurs locaux dès la fin du confinement. Néanmoins, il s'est avéré que souvent, le personnel qui devait être réactivé en premier et celui qui pouvait rester hors site n'était pas clairement défini.

À titre d'exemple, au Luxembourg, plus de 50% du personnel du secteur de la santé est constitué de frontaliers. Le gouvernement considérant la fermeture des frontières comme l'un des risques majeurs pour ce secteur, il a été proposé aux personnels de santé de loger dans des hôtels au Luxembourg. Même si le pourcentage de frontaliers n'est pas aussi élevé dans le secteur industriel, le même risque existe.

Un autre sujet important à aborder est la réactivité en cas de crise. En effet, une réaction rapide vise généralement une réduction importante de l'impact. Il est requis pour une entreprise de maîtriser / connaître sa capacité à réduire le délai de réaction à une crise pour préserver ses actifs.

ACTIONS CLÉS

A. CONSIDÉRER LA REVUE DE L'ÉVALUATION DES RISQUES

- La marge d'erreur pour l'estimation correcte des risques liés à une pandémie de la part des grouvernements est importante. Dans le cas d'une éventuelle crise, estimer soi-même les risques et collecter les informations pour être prêt avant qu'une crise n'éclate.

B. AMÉLIORER LES MESURES DE SÉCURITÉ EXISTANTES

- Concevoir des plans de continuité d'activité de manière à ce que des processus métier puissent être gérés à distance.
- Concevoir des plans de reprise d'activité de manière à ce qu'ils puissent être exécutés à distance.
- Définir des priorités qui permettent de déterminer dans quel ordre le personnel est réactivé.
- Prendre en compte les capacités de gestion de crise des gouvernements ainsi la prédisposition de la population à suivre les recommandations du gouvernement.
- Vérifier si les procédures de gestion de crise traitent également des crises de longue durée.
- Améliorer les capacités de détection et de traitement des premiers signaux d'une crise latente

C. CONSIDÉRER LES MESURES DE SÉCURITÉ COMPLÉMENTAIRES

- Fournir un logement aux personnes-clés si les frontières sont fermées ou risquent de l'être.
- Mettre en place des outils et des solutions numériques qui permettraient de digitaliser les fonctions répétitives.
- Soumettre la situation de gestion de crise à des tests de résistance au stress.

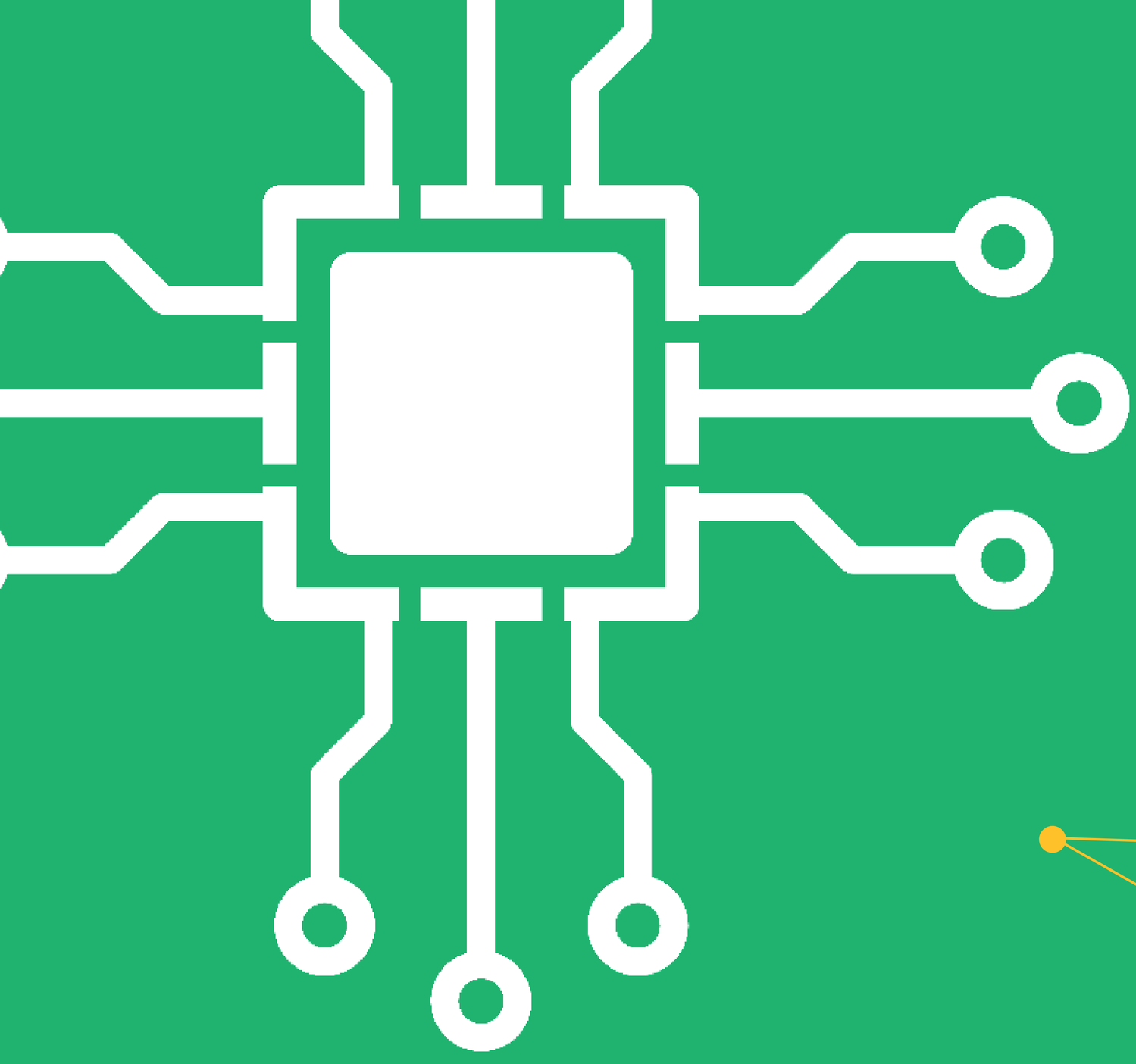
4/EXPOSITION DES INFRASTRUCTURES INTERNES À L'EXTÉRIEUR

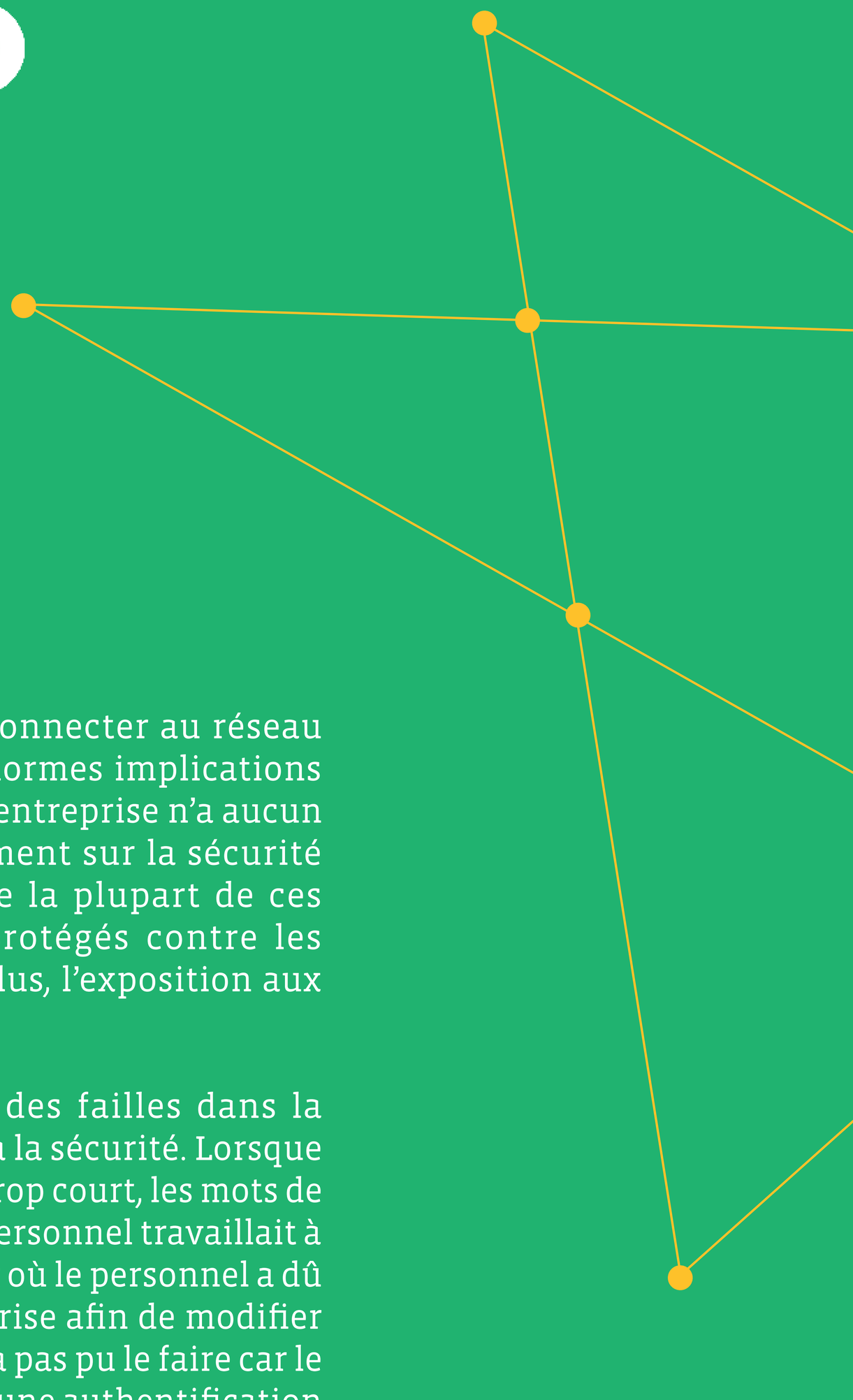
PRINCIPALES CONSTATATIONS

Le personnel travaillant à domicile a eu besoin d'accéder aux systèmes d'information ou aux systèmes de contrôle, qui n'étaient souvent accessibles qu'à partir du réseau de l'entreprise et non disponibles dans le cloud. Alors que dans des circonstances normales, une telle approche est plus sûre en termes de confidentialité, le personnel n'a dès lors pas pu travailler à domicile pendant le début de la crise.

Certaines entreprises ont exposé des services critiques (y compris des systèmes de contrôle industriels) sur Internet lors de la prise de mesure d'urgence. Celles-ci ont, en effet, jugé la disponibilité des services plus importante que l'intégrité (ou parce qu'elles n'étaient pas conscientes des implications en matière de sécurité). Cependant, dans l'industrie, ces systèmes sont souvent propriétaires, obsolètes ou issus d'acquisitions et donc souvent non sécurisés par nature (contenant des vulnérabilités, des normes de sécurité insuffisantes, des mots de passe par défaut, etc.). Par conséquent, de nombreux systèmes critiques sont désormais exposés même à des attaques non ciblées, créant ainsi une énorme faille de sécurité.

Une autre manière de procéder est la mise en place de réseaux privés virtuels (VPN). Toutefois, on a constaté que les solutions VPN n'étaient souvent pas en place et, lorsqu'elles l'étaient, les appareils personnels n'étaient pas configurés pour s'y connecter. En effet, non seulement un client logiciel doit être installé et configuré, mais des jetons d'authentification forte (qui sont souvent des périphériques physiques) doivent également être distribués.





De plus, permettre au personnel de se connecter au réseau interne avec ses propres appareils a d'énormes implications en matière de sécurité. Étant donné que l'entreprise n'a aucun contrôle sur ces appareils, plus précisément sur la sécurité de ceux-ci, on a constaté là encore que la plupart de ces appareils ne sont pas correctement protégés contre les logiciels malveillants et le piratage. De plus, l'exposition aux menaces est inconnue.

La crise a également mis en évidence des failles dans la conception de certaines procédures liées à la sécurité. Lorsque le délai d'expiration du mot de passe a été trop court, les mots de passe ont expiré pendant la période où le personnel travaillait à distance. Cela a conduit à un cercle vicieux où le personnel a dû se connecter à l'infrastructure de l'entreprise afin de modifier ou réinitialiser son mot de passe, mais il n'a pas pu le faire car le mot de passe a expiré. Lorsque, de plus, aucune authentification forte n'avait été mise en place, des solutions de contournement provisoires ont dû être trouvées qui ont exposé les interfaces internes au public sans niveau de sécurité supplémentaire.

ACTIONS CLÉS

A. CONSIDÉRER LA REVUE DE L'ÉVALUATION DES RISQUES

- Exposition aux menaces accrue en raison des points d'entrée pour l'accès à distance qui ont été mis en place à la hâte. Une fois cette faille connue, les criminels peuvent également chercher à l'exploiter, ce qui augmente encore davantage le paysage des menaces.

B. CONSIDÉRER LES MESURES DE SÉCURITÉ COMPLÉMENTAIRES

- Prévoir de travailler à distance en dehors des périodes de crise en mettant en place un accès à distance sécurisé.
- Déployer systématiquement une authentification forte (pour tous les systèmes critiques et tout le personnel).
- Considérer l'utilisation des solutions cloud modernes avec une authentification forte.

5/ TÉLÉTRAVAIL

PRINCIPALES CONSTATATIONS

Pour les entreprises ayant la possibilité de travailler à distance déjà instaurée, la crise a rapidement montré ses limites.

- Premièrement, il n'y a pas eu assez de matériel disponible (qu'il s'agisse d'ordinateurs portables, de téléphones ou de jetons de sécurité) pour équiper l'ensemble du personnel.
- Deuxièmement, l'infrastructure ou le réseau lui-même ne possédait pas la capacité de gérer un grand nombre de connexions simultanées.
- Troisièmement, toutes les procédures n'étaient pas entièrement numérisées, de sorte qu'elles n'ont pas pu être déroulées à distance correctement.
- Quatrièmement, comme la crise a frappé l'ensemble de l'économie, l'achat de jetons d'authentification forte a été largement retardé en raison de la demande accrue (de même que pour les masques et les désinfectants).

Dans certains cas, en particulier, pour les groupes internationaux, tous les travailleurs ne disposaient pas d'une connexion Internet fiable et des points d'accès 4G ont du être fournis par l'entreprise.

Par ailleurs, le télétravail a créé de nouveaux problèmes de sécurité. D'une part, chaque personne qui se connecte à distance représente un point d'entrée vers les systèmes internes et augmente ainsi la surface d'attaque. Malheureusement, il est très difficile de protéger ces périphériques de point de terminaison, sans parler des réseaux de terminaison. D'autre part, comme toutes les communications internes se sont faites alors par e-mail, le phishing et d'autres attaques d'ingénierie sociale sont devenus beaucoup plus simples et plus efficaces.

Les plateformes de visioconférence ont été largement utilisées. Il s'est avéré que toutes n'étaient pas suffisamment sécurisées (par exemple, manque de cryptage) et donc inappropriées pour les réunions internes. De nombreux cas d'attentats à la conférence (participation non sollicitée) ont été signalés au début de la crise.

En général, les entreprises n'ont pas rencontré beaucoup de problèmes informatiques chez les utilisateurs finaux, mais ont mis en place un support informatique permanent pour palier la situation si nécessaire. La plupart du support a pu être fourni à distance via VPN.

Lorsque les employés ont travaillé à distance, les mesures de sécurité normales (antivirus, SIEM, serveurs de correctifs et de sauvegarde) n'ont pas été nécessairement disponibles, en particulier lorsque les employés ne se connectaient pas au VPN. Des solutions alternatives ont donc été nécessaires, comme rendre des services internes accessibles à partir de l'Internet public. Les employés ont été encouragés à utiliser le stockage cloud pour enregistrer leurs fichiers - mais il a été très difficile de s'assurer qu'ils utilisaient réellement le stockage cloud et non leur système de fichiers local (qui n'est pas sauvegardé).

ACTIONS CLÉS

A. CONSIDÉRER LA REVUE DE L'ÉVALUATION DES RISQUES

- Le risque accru de phishing et d'ingénierie sociale.
- Les appareils personnels (non surveillés) sont connectés aux réseaux internes.
- Les données sensibles peuvent éventuellement sortir du périmètre de l'entreprise.
- La communication entre les membres de l'entreprise se fait principalement sur Internet.
- Le risque accru de perte de données dû au fait que les sauvegardes ne sont pas effectuées à distance.

B. EXPOSITION À DE NOUVEAUX RISQUES (LIÉS À LA CRISE)

- Considérer la situation où les lignes de télécommunications et l'infrastructure informatique seront saturées en raison de l'accumulation de connexions (considérer le stockage du fichier journalier des connexions pour préparer un incident).

C. AMÉLIORER LES MESURES DE SÉCURITÉ EXISTANTES

- Renforcer la sensibilisation aux questions de sécurité et l'adapter à la nouvelle situation (travail à distance).
- Revoir les procédures complexes pour les rendre résistantes aux crises.
- Soumettre les infrastructures d'accès à distance à des tests de résistance (le reste de la crise étant une bonne opportunité). Envisager d'acquérir des solutions VDI (infrastructure de bureau virtuel).

D. CONSIDÉRER LES MESURES DE SÉCURITÉ COMPLÉMENTAIRES

- Digitaliser les processus en mettant en place des plateformes cloud et de signatures électroniques sécurisées.
- S’assurer que tout le personnel peut travailler à distance en cas de besoin.
- S’assurer que suffisamment de jetons d’authentification de rechange sont disponibles.
- Résoudre le problème de sécurité des terminaux (fournir du matériel d’entreprise aux utilisateurs travaillant à domicile pour éviter les problèmes de confidentialité et être en mesure de renforcer la sécurité).
- Interdire explicitement aux employés d’utiliser leur boîte de messagerie privée à des fins professionnelles.
- Les entreprises devraient investir dans une plateforme open source hébergée dans leurs locaux ou auprès d’un fournisseur de services d’une entreprise de confiance. Le chiffrement de ces flux de conférence doit être standard, ce qui n’est pas le cas pour la plupart d’entre eux pour le moment.

6 / PAYSAGE DES MENACES - CYBERMENACES

PRINCIPALES CONSTATATIONS

Au début de la crise, il est devenu évident que les cybercriminels ont rapidement réagi au fait que la plupart des entreprises, préparées ou non, ont commencé à travailler à distance. Les arnaques et les cas de phishing en particulier, mais aussi les ransomwares, ont rapidement augmenté. Dans certains cas, des attaques DDoS à petite échelle ont été observées sur l'infrastructure de communication.

Le télétravail a également eu un impact direct sur le paysage des menaces. Avant le confinement, les menaces devaient être stoppées sur site. Cela implique qu'à l'intérieur des locaux, tout le trafic était prévisible et bien connu, et que tout écart était suspect. Lorsque le personnel a commencé à travailler à domicile, les mécanismes de détection ont dû également couvrir les appareils et les réseaux domestiques, et ont donc confrontés à beaucoup plus de bruit qu'auparavant. Cela a augmenté le nombre d'alertes et a rendu les attaques beaucoup plus difficiles à détecter qu'auparavant. Cependant, la sécurité renforcée des terminaux a permis également de détecter les attaques plus tôt.

Des formations de sensibilisation à la sécurité ont été dispensées afin d'aborder le risque accru d'attaques (de phishing). Pour organiser la formation, des plateformes d'apprentissage en ligne ont été utilisées.

ACTIONS CLÉS

A. CONSIDÉRER LA REVUE DE L'ÉVALUATION DES RISQUES

- Dans une situation imprévue, comme dans une situation dans laquelle leur santé est en jeu, les employés sont avides de mises à jour et d'informations régulières. Dans cette situation, il est facile pour un criminel d'inciter les employés à ouvrir des pièces jointes.
- Les portes d'accès à distance sont devenues des points de défaillance uniques, qui doivent être protégés contre la perte de disponibilité.
- Les décisions prises par le gouvernement peuvent avoir un impact sur la disponibilité du personnel (congé pour raisons familiales,...).
- Les tensions géopolitiques.

B. AMÉLIORER LES MESURES DE SÉCURITÉ EXISTANTES

- Les personnes clés doivent rester disponibles même si elles ont le droit aux congés (par exemple, congé pour raisons familiales). Ces personnes clés doivent être très engagées et fidèles à l'entreprise et être enclin à rester disponibles. Prévoir la possibilité de prise en charge de leurs enfants avec le personnel qualifié sur place.
- Renforcer la formation de sensibilisation à la sécurité, en mettant l'accent sur l'ingénierie sociale.

C. CONSIDÉRER LES MESURES DE SÉCURITÉ COMPLÉMENTAIRES

- Fournir en permanence aux employés des informations sur la situation, les rendre attentifs aux escroqueries en cours.
- Prévoir les techniques ou l'infrastructure d'atténuation des attaques DDoS.
- Être capable de gérer un cyber-incident en temps de crise, c'est-à-dire même lorsque les ressources ne seront pas rapidement disponibles sur place.

La FEDIL vous rappelle que la check-list Cybersécurité concernant les dispositifs, les e-mails, l'accès au cloud et au réseau ainsi que les visioconférences, établie en collaboration avec SECURITYMADEIN.LU est disponible sur le site de la FEDIL: Cyberscurity Checklist

Si vous souhaitez rejoindre l'IND-ISAC, merci de contacter:

Céline Tarraube
Adviser Digital & Innovation
celine.tarraube@fedil.lu
(+352) 43 53 66 610