LIVRE BLANC

Cybersécurité en période de crise

version du 25/04/2020

INFORTIVE

infortive.com

SOMMAIRE

Les DSI de transition Infortive vous livrent leurs recommandations pour la cybersécurité en période de crise :

Executive Summary

La crise sanitaire liée au COVID 19 a généré une période de confinement inédite et un recours massif au télétravail qui va devenir courant. Dans ce contexte, les DSI ont dû adapter dans l'urgence le Système d'Information à ces nouvelles contraintes sans pouvoir toujours respecter les règles de l'art en matière de cybersécurité.

Les entreprises ne peuvent pas se permettre d'ajouter une crise de cybersécurité au-dessus de la crise sanitaire.

Les DSI de transition Infortive ont publié dès les premiers jours, des recommandations de cybersécurité face à la crise. Ce support complète les bonnes pratiques déjà diffusées. Il sera utile tant à des DSI que des Directions Générales ou des responsables Métiers qui souhaiteront effectuer une vérification rapide des pratiques actuellement en vigueur dans leur entreprise.

La sécurité absolue n'existe pas et aucune parade n'est jamais définitive.

Ces recommandations abordent les thèmes suivants :

- La gouvernance de crise est fondamentale et repose sur des responsabilités prédéfinies, des outils et procédures de communication qui permettront de tenir un discours sincère et cohérent.
- Une cellule de riposte doit être constituée afin de réagir très rapidement, quitte à couper les accès, systèmes, serveurs et postes de travail pour sécuriser l'essentiel en attente d'un diagnostic plus précis.
- La sécurisation et la redondance des ressources critiques seront également anticipées.
- Les utilisateurs doivent recevoir des instructions claires et pratiques sur les menaces les plus courantes (phishing, tentative d'usurpation …) et l'expérience montre qu'un entraînement des hommes est la meilleure protection.
- Les DSI ont à leur disposition de nombreux dispositifs techniques (VPN, postes de travail virtuels, authentification multi-facteurs …) pour sécuriser les accès et devront renforcer le support aux utilisateurs quitte à prélever des ressources sur des projets devenus moins prioritaires.
- De nombreuses ressources (notamment gouvernementales) existent sur ces sujets et les consulter avant toute crise est indispensable. Des retours d'expériences et des recommandations pertinentes sont disponibles sur des risques devenus malheureusement courants (rançongiciel par exemple).

Bonne lecture et n'hésitez pas à nous faire part de vos remarques et suggestions à contact@infortive.com

Les enjeux de la cybersécurité en période de crise

Objectifs

Rechercher le meilleur équilibre possible entre les besoins de protection et la continuité des activités.

Trouver le meilleur équilibre possible entre les moyens techniques, le niveau de protection souhaité et les investissements nécessaires.

Principes généraux - La sécurité absolue n'existe pas

Adopter une démarche d'amélioration continue basée sur le concept de niveau de maturité qui consiste à évaluer la maturité actuelle (as-is), fixer de nouveaux objectifs (to-be), et définir un plan d'action (programmes/projets et priorités) pour améliorer les pratiques de cybersécurité.

Identifier, catégoriser et concentrer ses efforts sur les opérations, les services, les processus, les données et les systèmes critiques, les plus sensibles.

Surveiller et contrôler les nouveaux types de cyberattaques, exécuter régulièrement les tests opérationnels de sécurité.

Intégrer la dimension humaine (« human firewall ») à l'arsenal technologique (« firewall ») pour développer une participation active, raisonnée et comprise des utilisateurs à la protection des actifs stratégiques de l'entreprise.

Accepter que la sécurité absolue n'existe pas, sortir du marketing de la peur, développer une nouvelle appétence au risque, libérer la créativité des collaborateurs pour innover et anticiper les évolutions rapides des menaces, des marchés, des besoins des clients.

Prendre les dispositions nécessaires pour détecter les tentatives d'accès suspectes, par exemple provenant de sites inhabituels.

Bénéfices attendus

Assurer le niveau de sécurité du SI et la continuité des activités.

Limiter les impacts négatifs d'une cyberattaque.

Gouvernance de crise - Gestion de crise

Cellule de crise

Lors de la mise en place de la cellule de crise :

- Définir son mandat,
- Ses rôles et responsabilités,
- Son fonctionnement (quand lui fait-on appel, la périodicité des réunions…),
- Son reporting au Codir.

Rappeler ou présenter aux membres de la cellule de crise :

- Les enjeux,
- Les types de risques et incidents,
- Les principaux indicateurs à suivre,
- Partager le plan de communication.

S'assurer que les contrats d'assurances couvrent bien les accès en télétravail et sinon procéder à leur révision et mise-à-jour.

Processus de gestion des risques et incidents

Définir et documenter de manière détaillée un processus de gestion des risques (ex : email phishing) et des incidents ; notamment, le processus de gestion des incidents doit montrer un lien avec la gestion des risques.

Former toutes les parties prenantes à son utilité et son utilisation.

Plan de communication

Si ce n'est pas déjà fait, établir un plan de communication :

- Audience,
- Types de messages,
- Niveaux de détail des messages,
- Canaux de distribution,
- Périodicité.

Tenir un discours cohérent et de vérité :

- Dire ce que l'on sait et ce que l'on ne sait pas, de la manière la plus positive possible,
- Reconnaître les responsabilités, les éventuelles erreurs d'appréciation commises,
- Expliquer les solutions, les options possibles pour sortir de la situation,
- Répondre clairement aux questions, avec empathie et d'une manière fiable, ne pas sacrifier la qualité de l'information au besoin de rapidité.

Privilégier une communication rapide, récurrente et directe (SMS), en plus des canaux habituels.

Les communications internes restent fondamentales mais elles doivent être complétées par des communications vers les pouvoirs publics (e.g. ANSSI, ARS) en :

- Les informant de la stratégie interne de sécurité, avant de constater des incidents ou des menaces,
- Entretenant des relations continues avec eux pour, par exemple, être informé d'autres attaques perpétrées contre d'autres entreprises,
- Les informant des attaques, incidents ou menaces survenues dans votre entreprise.

Gestion des compétences critiques

Sécuriser les compétences techniques et veiller à la redondance des compétences critiques et externes (e.g. sous-traitants) pour :

- Effectuer les interventions sur l'infrastructure (ingénieurs réseaux, sécurité télécom, architecture système, experts applicatifs...)
- Mettre en place des roulements sur les compétences (en conservant des personnes disposant de privilèges élevés),
- Organiser l'accès à la bonne information au bon moment.

Réévaluation des projets

S'assurer que les projets en cours intègrent bien la dimension cybersécurité.

Recommandations pour les utilisateurs

Activer l'authentification multi-facteur immédiatement.

Désactiver au plus vite tous les comptes des personnels qui ne font plus partie de l'entreprise.

Avoir un suivi quotidien des connexions et temps de connexion. Toutefois ceci doit être préalablement approuvé par les représentants des salariés à travers un accord.

Protection des données et des documents

Se prémunir contre les risques de vol, ranger et verrouiller les documents et les ordinateurs.

Prendre toutes les dispositions nécessaires pour que les données confidentielles ne soient pas accessibles à des tiers non autorisés.

Ne pas les partager entre PC pro et PC perso, les clés ou disques USB.

Protection des droits d'accès nominatifs/personnels

Ne divulguer à personne (responsable hiérarchique, équipe informatique, autre utilisateur) ses droits d'accès, ses données d'authentification et ses données confidentielles.

Respecter les directives de renouvellement des mots de passe.

Respecter les procédures face aux tentatives de fraude en cours (augmentation avérée des tentatives de fraudes au PDG, pas de changement de compte bancaire sans vérification approfondie, au service support, changement de compte fournisseur, etc…..) et prévenir ses clients, ce qui peut aussi être une opportunité de renouer des contacts.

Ne pas utiliser ou tenter d'utiliser le compte d'un tiers et s'interdire d'accéder ou de tenter d'accéder à des ressources ou des services informatiques sans habilitation explicite au risque d'engager sa responsabilité.

Protection des ressources et des services informatiques

Respecter et protéger les matériels et logiciels mis à sa disposition.

Respecter les mesures de sécurité mises en place par les responsables informatiques, et se conformer à leurs décisions.

Distinguer les usages Pro et Perso : ne pas installer de logiciel.

- Sauf expressément autorisé par l'entreprise, pas d'usage personnel sur le matériel professionnel,
- Si possible éviter l'usage professionnel sur matériel personnel sauf bureaux virtuels (ex : Citrix…) ou suite en ligne comme Office365, Google.

Utiliser systématiquement le VPN fourni par l'entreprise pour accéder aux applications hébergées au sein de l'entreprise.

Signaler sans délai tout dysfonctionnement ou incident de sécurité potentiel dans le cas du processus de gestion des risques et incidents.

Protection vis-à-vis des services Internet

- Etre très vigilant concernant le phishing et entraîner les utilisateurs à l'identifier :
- Vérifiez l'adresse mail émetteur et réponse. Quelques signes évocateurs : fautes d'orthographe, chaînes de lettres et de chiffres incompréhensibles, incohérence entre les noms affichés et l'adresse e-mail (mailto),
- Vérifier que les liens contenus dans le mail sont authentiques,
- Passez votre souris au-dessus des liens et vérifier s'il pointe bien vers l'adresse du site annoncée dans le message,
- Ne pas ouvrir les mails de personnes que vous ne connaissez pas
- Éviter de se connecter à des sites suspects, éviter de télécharger des logiciels.
- Eviter de stocker, de transférer ou partager des données sur des sites externes, mais uniquement en passant par des sites dont la sécurité a été préalablement vérifiée.

Recommandations pour la DSI

Recommandations selon les types de postes

Postes de travail physiques d'entreprises avec VPN :

- S'assurer que la politique de MAJ de l'antivirus, des patchs windows, utilitaires, applications et des mots de passe soit bien appliquée,
- Si pas possible, identifier le plan B (par exemple un retour sur le site pour mettre à jour les postes les plus critiques),
- Intégrer la criticité du poste dans le plan B (paiements, ERP…), adapter le niveau de sécurité pour les postes et fonctions les plus critiques (gouvernance par les risques).

Postes de travail physiques d'entreprises sans VPN :

- Adapter la politique d'administration des postes via l'Active Directory afin de permettre les mises à jour par Internet si le confinement se prolonge.

Postes de travail virtuels (Citrix…) d'entreprises, sur BYOD ou sur Chromebook :

- Profiter de cette possibilité de virtualisation si elle est déployée sur les postes/fonctions les plus critiques.

Postes en BYOD qui accèdent à des applications Internet ou mobiles :

- Activer l'authentification à 2 facteurs partout où c'est possible avec un code sur le téléphone portable (en liaison avec la DRH pour l'utilisation des mobiles personnels sur des fonctions critiques),
- Applications critiques : accès chiffré obligatoire (https, VPN…), si pas possible revenir au bureau pour y accéder,
- Applications non critiques : tolérances possibles.

Service desk et support aux utilisateurs

Renforcer quantitativement et qualitativement le service desk et le support aux utilisateurs pour faire face aux difficultés inhérentes au développement brutal du télétravail.

Mettre en place des actions de sensibilisation continue des utilisateurs (e.g. animation sécurité sur l'intranet, …).

Pour les entreprises multi-sites, mettre en place des correspondants sécurité de proximité au niveau d'un site ou d'un regroupement de sites de manière à soutenir les utilisateurs localement.

Recommandations thématiques

Cyberattaques

Redoubler de vigilance car c'est un moment privilégié pour les attaques.

Vérifier en temps réel l'absence d'attaques en cours sur les serveurs et sur les différentes couches des systèmes (Bios, OS, virtualisation, bases de données, utilitaires, applications...).

Définir en amont et faire appliquer les actions d'urgence en cas d'intrusion e.g. Isolement et coupure en cas de cryptolocker (rançongiciel).

Sauvegarde

Plus que jamais, vérifier et sécuriser les sauvegardes (OS, configurations, équipements de réseaux, sauvegardes de secours impérativement hors ligne permettant de remonter entièrement la configuration. Attention, en cas de crypto virus, les sauvegardes peuvent être corrompues depuis plusieurs mois.

Security Operations Center (SOC)

S'organiser pour gérer les alertes issues des SOC quand ils existent, par niveau de priorité, étudier la mise en place d'astreintes si elles ne sont pas en vigueur.

Infrastructures, Réseau et API

S'il existe plusieurs zones de confiance dans l'organisation, il peut être intéressant d'avoir des solutions de télétravail différentes pour chacune des zones. En fonction des résultats que l'on cherche à obtenir, on peut alors, au niveau des passerelles inter-zones, autoriser ou interdire facilement des accès habituellement autorisés sur un poste « normal ».

Gérer les débits en arbitrant les priorités (téléchargements lourds de nuit, horaires décalés pour les VPN, etc..) en fonction de la criticité des opérations.

Vérifier qu'il y a suffisamment d'accès VPN simultanés.

Accélérer la virtualisation des postes de travail pour éviter le plus possible l'utilisation du matériel personnel. En cette période de crise, éventuellement fournir un poste de travail professionnel aux employés en télétravail.

Vérification et maintien des mises à jour des patchs de sécurité et fonctionnels, de tous les éléments d'infrastructure (Systèmes, Réseaux, Sécurité, …).

Vérifier les vulnérabilités liées aux API : quelles interfaces sont exposées et les sélectionner (toutes ne sont pas candidates en période de crise), ne pas partager toutes les données (fermeture de certains silos), revisiter l'accès à l'environnement humain (collaborateurs, prestataires, clients…) et aux infrastructures tierces.

Vérification des niveaux de maintenance et de support des fournisseurs des infrastructures.

Spécificités pour certains secteurs d'activité

Respecter les règles clés publiées sur esante.gouv.fr (organisation, sensibilisation, gestion des incidents).

Déclarer ses incidents de sécurité via le dispositif de traitement des signalements des incidents de sécurité des systèmes d'information (SSI) du ministère des Solidarités et de la Santé.

Contacter la cellule d'accompagnement des structures de santé ACSS du ministère lorsque votre organisation est confrontée à un incident de cybersécurité provoqué par un rançongiciel.

Liens utiles - Compléments d'informations

https://www.ssi.gouv.fr/administration/bonnes-pratiques/

https://www.cybermalveillance.gouv.fr/cybermenaces/

https://techcommunity.microsoft.com/t5/configuration-manager-blog/managing-patch-tuesday-with-configuration-manager-in-a-remote/ba-p/1269444 : recommandations pour patcher vers internet en mode split-VPN.

Remerciements

Nous tenons à remercier les membres de la communauté Infortive qui ont contribué ainsi que Michel Raimondo (DSI de transition).

La Communauté des DSI de Transition Infortive

Première communauté de DSI de transition en Europe, Infortive réunit des professionnels de la Direction des Systèmes d'Information entraînés par leurs missions de transformation aux situations d'urgence.

Les recommandations publiées dans ce Livre Blanc sont une illustration de leur capacité à intervenir dans l'urgence et en mode collaboratif distant.

Ils mettent leurs compétences aux services des entreprises qui doivent gérer des transformations : fusion d'entreprises, carve-out, externalisation des infrastructures, déploiement d'un projet international, rationalisation des coûts, transformation digitale.

Plus d'informations sur

www.infortive.com

Télécharger aussi le livre blanc sur la Transformation digitale et l'accélération de la DSI