LIVRE BLANC

Coronavirus et Cybersécurité

Eviter une crise dans la crise

version du 25/03/2020

INFORTIVE

infortive.com

Maitrise des Crises

maitrisedescrises.com

Ce document a été réalisé le 24 mars 2020 et ses recommandations sont évolutives. Nous vous invitons à collaborer aux mises à jour que nous publions sur :

www.infortive.com/coronavirus/

Les DSI d'Infortive et maitrisedescrises.com ont joint leurs efforts pour réunir ces recommandations et ne pas rajouter une crise cyber à la crise sanitaire en cours.

Maitrisedescrises.com, service d'analyse et recommandations, intervenant majeur sur l'accompagnement des entreprises en matière de risque systémique, et la **Communauté des DSI de transition Infortive** (entraînés aux situations d'urgence) vous proposent un livre blanc des bonnes pratiques qui doivent se mettre en œuvre immédiatement.

SOMMAIRE

Les DSI de transition Infortive et Maitrisedescrises.com vous livrent leurs recommandations en cybersécurité pour éviter une crise dans la crise :

Cybersécurité : éviter une crise dans la crise

La cybersécurité est souvent le parent pauvre des budgets informatiques. Les entreprises sont en majorité peu préparées. Dans le contexte actuel ajouter une crise au-dessus de la crise est un risque à éviter.

Covid-19, le confinement va se poursuivre

Plus de deux milliards de personnes sont actuellement confinées, les collaborateurs sont en inactivité, en situation de travail à distance ou bien sur site, mais dans des conditions inhabituelles. Le risque lié à la continuité d'activité des entreprises est désormais transféré à la DSI et repose beaucoup sur la robustesse et la résilience du Système d'Information.

Le confinement va être prolongé et va confronter au télétravail une plus large population aux fonctions moins critiques et en général moins autonome.

Les directions informatiques qui ont adapté les procédures de télétravail dans l'urgence doivent reprendre la main sur la sécurité.

Le basculement brutal en télétravail a créé un risque

Dans l'urgence, les entreprises ont pu ouvrir des accès pour permettre à des PC personnels d'accéder au SI (BYOD) et certains postes de travail vont rester longtemps hors de leurs infrastructures. Ces postes devront donc être impérativement mis à jour tout au long de la crise.

Le collaborateur, isolé à son domicile, ne pourra échanger aussi efficacement avec ses collègues sur l'opportunité d'alerter la cellule cybersécurité.

Dans tous les cas une cellule de riposte doit être armée afin de réagir très rapidement, quitte à couper les accès, systèmes, serveurs et postes de travail de façon à sécuriser l'essentiel.

Recommandations de sécurisation pour les postes de travail des utilisateurs distants

Rediffuser les recommandations de sécurité de base vers les utilisateurs.

Redoubler de vigilance concernant le phishing et entraîner les utilisateurs à l'identifier

- → Vérifier que les liens contenus dans les mails sont authentiques (survoler le lien pour le lire),
- → Vérifier l'adresse mail de l'émetteur et celui de la réponse,
- → Ne pas ouvrir les mails de personnes que vous ne connaissez pas.

Remonter toute anomalie vers le Service Desk. Il n'y a aucune mauvaise question ou alerte en cybersécurité

Utiliser systématiquement le VPN fourni par l'entreprise,

- → VPN entreprise : accès aux applications dans le datacenter de l'entreprise,
- → VPN personnel : à ne pas utiliser car sert en général à faire du téléchargement depuis un autre pays.

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,
- → Pas d'usage professionnel sur matériel personnel sauf bureaux virtuels (ex : Citrix…) ou suite en ligne comme Office365, Google Suite...

Ne jamais donner son mot de passe au téléphone, appeler la cellule support au moindre doute

Respecter les procédures face aux tentatives de fraude en cours

- → Augmentation avérée des tentatives de fraudes aux faux ordres de virements (pas de changement de compte bancaire sans vérification lourde),
- → Fraude au service support,
- → Changement de compte fournisseur, etc…

Prévenir ses clients, ce qui peut aussi être une opportunité de renouer des contacts.

Recommandations à la DSI selon la typologie de postes

Activer l'authentification multi-facteur immédiatement

Désactiver immédiatement tous les comptes des personnels qui ne font plus partie de l'entreprise

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 ou sur BYOD

- Profiter de cette possibilité 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.

Recommandations générales pour la DSI

- Support : prendre en charge les problématiques informatiques personnelles pour les connexions à distance (box opérateurs, wifi domestique...),
- Inventorier les documentations des différentes boxes pour aider les utilisateurs
- Sécuriser autant que possible les connexions Microsoft RDP. Pour sécuriser voir : https://www.deltasight.fr/securiser-serveur-rdp-port-3389/.

Recommandations de sécurisation des infrastructures existantes

Serveurs, mise à jour, sauvegarde, débit sur le collaboratif (visio…) etc.

Dans le contexte COVID-19, la meilleure stratégie est de sécuriser l'existant avec sagesse plutôt que de déployer des nouveautés en urgence

Cyber attaques

- Redoubler de vigilance car c'est un moment privilégié pour les attaques (c'est un moment rêvé pour les pirates).
- Vérifier en temps réel l'absence d'attaques en cours :
  - Sur les serveurs,
  - 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 :
  - Ex : 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 Operation 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.

Réseau et API

- 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.
- 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.

Compétences critiques

- Veiller à la redondance des compétences critiques pour effectuer les manœuvres sur l'infrastructure (ingénieurs réseaux, sécurité télécom, architecture système, experts applicatifs) en mettant en place des roulements sur les compétences (en conservant des personnes disposant de privilèges élevés), accès à la documentation...

Les auteurs

Vincent BALOUET, ancien consultant puis chargé de mission du Cigref, de la fédération des assurances, du MEDEF, fut appelé successivement par ces derniers de 1992 à 1999 puis missionné à Bercy afin d'assurer le succès de la mobilisation nationale du secteur lors du passage informatique à l'an 2000. Il intervient sur de nombreux grands risques systémiques pour l'économie en France et à l'étranger et a créé Maitrisedescrises.com, service d'analyses et recommandations, disponible sur abonnement illimité.

Plus d'informations sur
www.maitrisedescrises.com

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 (et produites en 48h) 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

CONTACTS

Pierre Fauquenot
pfauquenot@infortive.com
+33 (0)6 07 41 49 99

Vincent Balouet
vincent.balouet@maitrisedescrises.com
+33 (0)6 81 85 99 87

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