cyber eco

Guide de gestion des incidents

Pour les PME

28 octobre 2021

Sébastien Harbec

À propos de l'auteur

Œuvrant dans le domaine de la cybersécurité depuis 2007 pour diverses industries, je prône une approche collaborative axée sur le développement de la culture de la cybersécurité en entreprise. Cette approche met au cœur de la question les gens, les processus et la technologie en fonction des besoins d'affaires dans un objectif de réduction du risque.

Afin de poursuivre mon développement, je complète un programme de cycle supérieur en cybersécurité de l'Université de Sherbrooke. Dans le cadre du volet « réactif », mon projet de fin d'études m'a amené à m'interroger sur les défis que représente la sécurité pour les petites et moyennes structures organisationnelles. L'idée de donner un coup de main aux PME m'est venue spontanément.

La santé des TI, et particulièrement la sécurité informatique des PME, qu'elles soient québécoises ou mondiales, est un sujet des plus préoccupants. En effet, les petites et moyennes entreprises forment le tissu social et commercial d'un marché en pleine santé. Face à la multiplication des cyberattaques, il devient primordial d'équiper nos PME pour y faire face. Rares sont celles qui sortent indemnes d'une telle épreuve.

Le guide que je propose se veut une aide pratique en cas de cyberattaque. Il apporte des pistes de solution en réaction à un incident. Ce guide ne remplace pas l'avis ou l'appui d'un expert, mais offre un accompagnement de première ligne pour tout gestionnaire ou technicien face à une attaque.

Ce guide offre une introduction à la gestion des cyberattaques sur les modèles du NIST et du SANS. Chaque étape y est détaillée en présentant les meilleures pratiques du secteur. Six cyberattaques typiques sont ensuite exposées pour illustrer différentes méthodes de réaction face à celles-ci, tout en tenant compte des aspects de prévention et de traitement de l'attaque.

Sébastien Harbec, CISSP

La sécurité des PME

Sujets

Gestion des cyberattaques

- Communication
- Investigation
- Endiguement
- Éradication
- Recouvrement
- Leçons apprises
- Conservation de la preuve numérique

Différents types de cyberattaques

- Les phases d’une cyberattaque
- Infiltration réseau
- Fuite de données
- Crypto-rançon
- Hameçonnage
- Compromission de boîte courriel
- Déni de service

Les outils

Lexique

Ressources complémentaires

Références

AVERTISSEMENT

Les avis et conseils contenus dans
le présent guide ne sauraient être
exhaustifs et complets.
Il incombe aux propriétaires
de systèmes d'évaluer et d'assumer
les risques de cybersécurité
qui menacent leurs systèmes
de technologie de l'information (TI).
De plus, il est vivement conseillé
de faire appel à un expert
en sécurité lorsque la situation
ne peut être contrôlée adéquatement.

Référence : cyber.gc.ca

Gestion des cyberattaques

Plusieurs attaques sont opportunistes et ne vous cibleront pas directement. Les attaquants testeront plutôt toutes les portes et ouvriront ou forceront celles qui ne sont pas correctement protégées. Des millions de tests sont faits chaque jour sur Internet. « Selon le Centre pour la cybersécurité canadien, un cyberincident est une tentative non autorisée, réussie ou non, visant à accéder à une ressource système ou à un système informatique ou visant à le modifier, à le détruire, à le supprimer ou à le rendre non disponible. Parmi les exemples, on compte l'hameçonnage, les rançongiciels et les attaques par déni de service distribué (DDos). » Les conseils donnés dans ce document font principalement référence aux principes de gestion de cyberattaques du NIST (National Institute of Standards and Technology) et du SANS (SysAdmin, Audit, Network, Security). Les prochaines fiches détailleront chaque étape illustrée ci-dessous.

Communication

Sonner l'alerte et inviter les bonnes personnes autour de la table

Ajouter des acteurs selon les défis identifiés

Investigation

Enquêter pour identifier la source de l'incident

Poursuivre l'investigation jusqu'à l'identification de la source de l'incident.

Endiguement

Contenir l'incident et retourner vers un état de stabilité

Éradication

Maîtriser l'incident et retourner vers la sécurité

Nettoyer complètement la menace avant le recouvrement

Recouvrement

Procéder à la reprise des opérations et à la remise en fonction des systèmes et du réseau

Leçons apprises

Effectuer un retour sur les points positifs et négatifs; apprendre et partager des informations

Communication

L'aspect de communication lors d'un incident est très important, voire critique. Cela inclut avoir les bons joueurs autour de la table selon le niveau de criticité et le niveau de complexité, mais aussi communiquer l'information correctement à l'intérieur et possiblement à l'extérieur de l'organisation. La communication avec les clients, et possiblement avec les médias et organismes réglementaires, joue un rôle important dans la réputation de l'organisation.

Premiers répondants

Selon l'incident détecté, **les bonnes personnes doivent être rapidement contactées** selon le niveau d'urgence, les compétences requises et les incidences possibles.

Par exemple :

- Un incident majeur pourrait demander de contacter le propriétaire de l'entreprise.
- Un incident particulièrement technique pourrait demander de contacter un expert ou une firme externe.
- Le recours aux forces de l'ordre telles que la police pourrait être nécessaire s'il s'agit d'un crime.
- La personne responsable d'un système ou d'une ligne d'affaires ainsi que l'équipe des communications pourraient aussi être incluses au besoin.

Bonne pratique

Lors d'incidents de tous ordres, le temps est compté. C'est pourquoi **il est conseillé d'établir une liste d'appel en prévision.**

Une liste des employés et des contacts externes en cas d'urgence pour chaque expertise, incluant leur numéro de téléphone et leurs disponibilités, aidera grandement à accélérer l'investigation et la prise de décisions lors de la gestion de l'incident. Ces informations doivent demeurer confidentielles.

La communication externe peut jouer un rôle stratégique pour l'organisation, notamment pour sa réputation. Selon l'importance et la nature de l'incident, il s'agira d'informer les médias ou les clients. La rédaction et le contenu de cette communication seront cruciaux. Il est donc recommandé d'avoir recours à un expert en communications.

Il peut aussi être important d'informer des organismes de réglementation. Par exemple, si une fuite de données inclut des informations de clients européens, même si l'organisation se trouve au Québec, le règlement général sur la protection des données (RGPD) pourrait s'appliquer et la fuite devrait possiblement être communiquée au comité européen de la protection des données et à son délégué à la protection des données (DPD).

La communication interne est un aspect important. De la même façon qu'à l'externe, une stratégie de communication devra être mise en place afin d'établir comment l'information sera diffusée, à qui et à quel moment.

Il n'y a rien de pire que l'incertitude et la panique lors de la gestion d'un incident. **Une communication claire et transparente est souvent plus efficace et montre une confiance envers ses employés.** Sensibiliser ses employés à la confidentialité de ces informations dans la même communication peut aussi être un bon rappel.

Investigation

C'est le moment de rassembler le maximum d'information sur l'incident afin d'analyser les détails et d'identifier la source de l'incident. À chaque découverte, les bons joueurs doivent être impliqués afin d'avoir les expertises requises, que ce soit à l'interne ou en faisant appel à un expert externe. La documentation de chaque étape et action est également importante pour bien s'y retrouver. Le retour à la phase d'investigation peut se faire plusieurs fois, notamment lors de la phase d'endiguement afin de s'assurer de complètement cerner l'incident.

À la découverte de l'incident, il faut tenter de saisir l'ampleur des dégâts, comme des pompiers arrivés sur les lieux d'un incendie.

L'objectif primaire est d'**identifier la source** de l'incident afin de l'endiguer puis de la corriger.

L'objectif secondaire est d'**investiguer les autres systèmes et appareils réseau** pour voir s'ils ont été compromis.

L'incident peut affecter la confidentialité, l'intégrité et/ou la disponibilité des services, des systèmes ou du réseau. Durant l'investigation, il faut se questionner sur ces différentes dimensions.

- Par exemple, les attaques de crypto-rançons incluent souvent l'extraction des données touchant à la fois la confidentialité et la disponibilité.

Votre boîte à outils

L'antivirus permet de détecter l'infection d'un système en utilisant des méthodologies connues et documentées sous forme de signatures. Si une signature concorde avec un comportement malicieux, l'antivirus pourra détecter l'infection. C'est pourquoi les mises à jour sont très importantes, surtout lorsque l'on croit un système infecté.

En cas d'infection, les journaux d'événements pourront aider à identifier la source : Internet, un courriel, une clé USB ou un fichier interne.

- **Attention,** l'antivirus ne détectera pas nécessairement une attaque minutieuse et spécialisée sur un système.

Les journaux d'événements, peu importe le système, pare-feu ou routeur, c'est l'endroit où regarder pour identifier une anomalie. Ils indiquent souvent les détails de connexions réussies et échouées, les erreurs et anomalies détectées ou les changements sur le système.

- Ils aident donc à repérer des tentatives abusives d'authentification, par un haut volume de tentatives refusées, par exemple, ou encore un accès suspicieux à un système, en dehors de la plage horaire habituelle, ou en provenance d'un autre pays n'ayant pas de lien avec votre entreprise.
- **Mais attention, ceux-ci ne sont pas toujours activés.** L'activation et l'archivage des événements sont nécessaires avant que survienne un incident.

Le scan de vulnérabilités permet de voir les faiblesses d'un système. Notamment, cela permet de voir les ports réseau ouverts, l'équivalent des portes ouvertes pour une maison.

- Certains scanneurs peuvent détecter un grand nombre de détails de vulnérabilités et même identifier les plus critiques à corriger.
- Cet outil permet aussi de détecter un changement inhabituel sur un système, surtout si vous connaissez l'état normal du système, aussi nommé l'état de base d'un système. Tout changement non approuvé à partir de l'état de base pourrait être suspect.
- **Attention, cet outil est aussi utilisé par les attaquants qui voudront connaître vos vulnérabilités.** La détection de cet outil sur votre réseau sans son approbation est hautement suspecte. Ainsi, la détection de son utilisation pourrait se faire à partir des journaux d'événements d'un système, d'un routeur ou d'alertes de pare-feu.

Bonne pratique

Testez vos outils avant un incident afin que ceux-ci soient prêts à être utilisés et que vous en ayez l'expertise. Si possible, faites une copie exacte du système avant l'investigation et utilisez cette copie pour investiguer et corriger la situation pour conserver la preuve numérique. N'hésitez pas à consulter un expert au besoin.

Endiguement et Éradication

Cette phase inclut **l'endiguement et l'éradication** des failles de sécurité découvertes lors de l'investigation. Pour limiter les dégâts, il est parfois essentiel de procéder rapidement à l'isolement d'un système ou de sections du réseau, de poursuivre l'investigation et de revenir pour l'application des correctifs. C'est un processus pouvant être itératif entre l'investigation de nouvelles failles et l'application des correctifs, jusqu'à la résolution de l'incident. Lors de l'application des correctifs, plusieurs organisations en profitent pour améliorer la sécurité globale de leur organisation.

L'endiguement permet de contenir l'incident rapidement à partir des connaissances acquises lors de l'investigation pour prendre action et éviter que l'incident ne se généralise.

Avant d'agir sur un système, si la **preuve numérique** doit être conservée, il est préférable de faire une copie exacte du système et d'utiliser cette copie pour y apporter les modifications.

Il peut être nécessaire d'**isoler un système** rapidement, par exemple, lorsqu'un système est compromis avec un virus et qu'une communication suspecte est détectée à travers le pare-feu. C'est aussi une façon de s'assurer que les systèmes toujours sains ne soient pas touchés.

- Il s'agit d'une procédure d'urgence et ce choix doit être fait en prenant en considération l'impact sur les services offerts, s'il s'agit d'un serveur Web, par exemple.
- L'isolement peut se faire avec une configuration réseau à partir du pare-feu, du routeur, ou encore en débranchant le câble réseau.
- L'isolement peut rendre l'investigation plus complexe puisque les communications suspectes avec l'externe n'auront plus lieu. Il faut donc procéder à l'analyse avant l'isolement si possible.
- De plus, cela modifie l'état de la machine et doit être dûment noté si la preuve numérique doit être conservée.

Une fois isolé, le système devrait être stabilisé, sauf si une infection est déjà en cours. **L'antivirus permet de faire un premier diagnostic et parfois de désinfecter le système.** Des cas particuliers peuvent demander un antivirus plus précis appelé anti-maliciel ou "*anti-malware*". Cet outil est souvent un excellent complément lors de la désinfection. (Voir fiche « Les outils ».)

Attention à la gestion des changements. Tous changements, mises à jour systèmes et applicatifs peuvent créer une instabilité système et créer un incident. Il est important de procéder aux tests nécessaires de stabilité avant de relancer les services.

Le scan de vulnérabilités permet de voir les faiblesses d'un système et souvent en propose le correctif. C'est un excellent outil pour aider à déterminer les priorités dans l'application des correctifs.

- Les correctifs peuvent être des configurations systèmes, réseau ou applicatives.

L'application des mises à jour applicatives et systèmes peut faire partie des correctifs nécessaires à appliquer. Garder ses systèmes et applications à jour est une excellente façon de se protéger.

Au moment de l'éradication, l'incident devrait être en voie d'être maîtrisé.

Cette étape est effectuée tout juste avant la remise en fonction des systèmes; il faut alors s'assurer que tous soient alors intègres et libres d'infection. Il ne s'agit pas d'une correction temporaire, mais d'une correction permanente des systèmes.

- Les mêmes outils qu'à l'endiguement peuvent être utilisés; cependant, un niveau plus élevé d'assurance sera attendu pour s'assurer qu'aucune vulnérabilité importante ou critique ne perdure sur le système à remettre en ligne afin d'éviter que celui-ci ne soit à nouveau la cible d'une attaque.
- Une nouvelle configuration, un nouveau système ou changement important d'architecture pourrait parfois être requis pour obtenir un degré de sécurité satisfaisant selon l'importance du service affecté.
- L'éradication peut être une étape technique et demander une expertise particulière; il ne faut pas hésiter à consulter un expert lorsque nécessaire.

Recouvrement et leçons apprises

Une fois l'application des correctifs effectuée, c'est la reprise des opérations. Plusieurs bonnes pratiques peuvent être mises en œuvre à ce moment. De plus, la surveillance et les tests de sécurité doivent se poursuivre pour s'assurer que l'attaque est bien terminée.

La reprise des opérations peut se faire rapidement si une copie de sauvegarde est disponible pour le ou les systèmes infectés.

- Si une sauvegarde récente est disponible, il faut s'assurer que celle-ci ne présente pas d'enjeu de sécurité avant de la déployer à nouveau.
- Si possible et nécessaire, déployez l'image de sauvegarde sur un second système afin d'aider à la conservation de la preuve numérique sur le système d'origine. Cela facilitera aussi l'investigation sur le système et la mise en place de son remplaçant.
- Pour les postes de travail, l'utilisation d'une image standard du système est souvent conservée. Si les données sont centralisées sur un serveur interne ou infonuagique et qu'elles n'ont pas été touchées par l'attaque, alors il sera possible de récupérer un poste de travail assez rapidement.
- Pour un équipement réseau tel qu'un pare-feu ou un routeur, la récupération à partir d'une sauvegarde est aussi possible si celle-ci a été faite récemment. Encore une fois, il est essentiel de s'assurer que cette sauvegarde est bien intègre, libre de manipulation malicieuse et fonctionnelle.
- Pour toutes ces manipulations, il faut penser à l'interruption de service, à l'intégrité de la sauvegarde et si l'information incluse est assez récente.

Attention! Plusieurs solutions de sauvegarde sont efficaces pour la sauvegarde, mais très complexes pour la restauration des données. La restauration des sauvegardes devrait être testée régulièrement.

À la suite de la reprise des opérations, il est conseillé d'effectuer un scan de vulnérabilités hebdomadaire sur tous les systèmes de l'environnement.

- Cela permet d'avoir un aperçu des vulnérabilités et de la sécurité des systèmes, de prévenir ou de découvrir de nouvelles attaques.

L'application des mises à jour applicatives et systèmes doit faire partie des opérations quotidiennes pour s'assurer d'une reprise des opérations efficace. Sans ces mises à jour, il est très difficile de garantir la sécurité des systèmes.

L'étape des leçons apprises est essentielle pour s'assurer que le retour à la normale soit complet, efficace et de longue durée. L'objectif est d'apprendre des erreurs et bons coups faits durant l'incident.

- Inclure tous les participants au règlement de l'incident.
- Rassembler toute la documentation produite lors de l'incident.
- Indiquer les améliorations, les défis, les erreurs et les succès.
- Partager cette information avec ses pairs dans l'industrie est aussi une façon bénéfique de s'améliorer et de tisser des liens de confiance.

Bonne pratique

Dans le même ordre d'idées, il est recommandé de procéder à des exercices de « tabletop » afin de simuler des incidents et d'en discuter ou encore de tester les réactions. C'est souvent à ce moment que l'on se rend compte qu'un processus ne fonctionne pas comme prévu ou qu'un élément est absent.

Conservation de la preuve numérique

La conservation de la preuve numérique s'applique principalement dans un cadre légal dans lequel l'organisation voudrait procéder à une poursuite judiciaire en lien avec l'incident vécu. Idéalement, tous les incidents suspects devraient suivre les principes de conservation de la preuve, puisqu'au cours de l'investigation, il pourrait être découvert qu'il s'agit d'une tentative de fraude, de vol ou de nuire à votre organisation. Ce document vous donne les meilleures pratiques à haut niveau; cependant, il peut être judicieux de faire appel à un expert en justice et affaires légales afin de s'assurer que les principes et lois sont correctement appliqués. Dans certains cas, faire appel aux forces de l'ordre pourrait aussi être nécessaire.

La conservation de la preuve débute avec l'importance de la documentation. Celle-ci doit être organisée dès le début de l'incident afin d'y inclure toutes informations pertinentes. Il est conseillé d'utiliser un outil, un formulaire ou un cadre de documentation d'incident afin de s'assurer d'avoir toutes les informations requises. (Voir fiche « Les outils ».) Chaque élément matériel doit aussi être clairement étiqueté et rangé avec un accès limité et documenté pour conserver son intégrité.

Toutes les preuves doivent respecter la chaîne de traçabilité, notamment lorsque les preuves sont partagées. Chaque transfert doit être documenté, incluant la signature de toutes les parties, la date, l'heure, le sujet et les détails techniques s'il s'agit d'équipement ou d'accès système, l'endroit où l'information sera hébergée et le nombre d'accès.

Il faut protéger l'état du système de toute modification pour conserver son intégrité lors de l'enquête. Certains outils d'analyses et d'enquêtes informatiques peuvent être utilisés pour analyser le système sans le modifier et faire une copie exacte du disque dur. (Voir fiche « Les outils ».)

- La copie exacte du disque dur pourra être utilisée pour pousser l'enquête ou faire des tests de correction et de récupération tout en préservant l'état du système d'origine.
- Si requis, isoler le système du réseau et de l'Internet devrait être fait à partir du pare-feu ou du routeur pour éviter toute modification au système. Documenter et bien réfléchir avant d'entreprendre ce changement, puisque les connexions réseau n'auront plus lieu et influencera le système.
- Si le système doit absolument être éteint, il peut être préférable de couper l'alimentation électrique afin de garder son état tel quel plutôt que de fermer le système normalement puisque cela change son état. Évidemment, la coupure de courant devrait être évitée autant que possible puisqu'elle risque aussi d'endommager le système physiquement, mais c'est parfois la meilleure solution.

L'analyse en mémoire vive ou 'RAM' peut être très utile lors d'une enquête. Celle-ci est volatile, c'est-à-dire qu'elle s'efface lorsque l'ordinateur redémarre ou parfois lorsqu'il se met en veille. Tout comme avec le disque dur, l'analyse de la mémoire peut se faire directement sur le système sans perturber son état. Il est cependant conseillé d'en prendre une copie afin d'en faire l'analyse sur un second système avec les outils d'analyse de mémoire. (Voir fiche « Les outils ».) Certaines attaques ne peuvent se trouver qu'en mémoire vive à travers les processus ou fichiers exécutés du système.

Cela permet aussi de voir :

- Certaines communications réseau.
- Ce qui a été copié-collé, incluant certains mots de passe s'il y a lieu.
- Si des lignes de commandes malicieuses ont été exécutées dernièrement.
- Dans des cas plus complexes, si du code a été injecté dans le système afin de l'exploiter.

La conservation de la preuve numérique doit être efficace et simple. S'il est possible d'automatiser le processus d'accès à la preuve par un système informatique, ce processus sera plus facile à suivre et à auditer par la suite. Si ce processus est manuel, celui-ci pourrait être négligé, oublié ou pire, outrepassé.

- Plusieurs enquêtes deviennent très complexes lorsque le volume de renseignements est trop élevé.
- Il peut être judicieux d'avoir une ou plusieurs personnes nommées responsables pour s'assurer que la conservation de la preuve numérique est respectée tout au long du processus. Toute personne manipulant ou ayant accès à de l'information liée à l'enquête devrait être familiarisée avec le processus de conservation de preuve pour en assurer l'intégrité.

Cyberattaques

Maintenant que les étapes de la gestion d'une cyberattaque ont été vues, voyons quelques attaques types. En sécurité, le niveau de risque de chaque étape est calculé par rapport à la probabilité qu'une attaque vous cible, aux répercussions sur votre entreprise, puis aux contrôles de sécurité en place défendant votre organisation. Il ne faut pas oublier que l'exploitation des vulnérabilités se fait souvent à l'aveugle, et que la majorité des attaques sont opportunistes. Si vos défenses sont faibles, cela augmente grandement la probabilité d'une attaque. L'attaquant ou le fraudeur aura donc tendance à choisir des cibles plutôt faciles et évidentes.

Infiltration réseau

L'intrusion dans votre réseau est souvent le début d'une attaque par divers moyens.

Fuite de données

L'extraction de vos données sensibles : base de clients, ventes ou propriété intellectuelle.

Crypto-rançon

Vos données et systèmes ne sont plus accessibles. Vous recevez une demande de rançon!

Hameçonnage

Vous recevez des courriels de fraude sophistiqués demandant vos informations bancaires ou personnelles.

Compromission de boîte courriel

Des fraudeurs ont accès à votre boîte courriel dans le but de détourner des fonds ou de voler de l'information.

Déni de service

Vos systèmes ralentissent ou s'arrêtent complètement, affectant vos opérations et vos services.

Objectifs

Comment détecter

Actions à prendre

Bonnes pratiques

Les phases d'une cyberattaque

Il existe plusieurs types de cyberattaques exploitant différentes stratégies afin d'obtenir un gain ou de tenter de nuire. Selon la société Lockheed Martin, **il y existe 7 phases lors d'une cyberattaque.** Selon l'attaque, certaines seront plus rapides ou lentes que d'autres. Ces phases permettent de mieux comprendre le déroulement d'une attaque et facilitent l'intervention lors de la gestion d'un incident.

1 Reconnaissance

L'attaquant cherche de l'information sur l'organisation. Cette information se trouve principalement dans le domaine du public, ou est facilement accessible. Cette phase devrait permettre d'identifier comment l'attaque sera faite. Voici quelques exemples :

- Adresses courriel des employés.
- Recherche d'information sur l'entreprise.
- Recherche d'information sur les individus.
- Identification de vulnérabilités externes.
- Visite de reconnaissance dans l'entreprise, déguisé en livreur par exemple.

2 Armement

C'est la création ou le choix de l'outil afin d'exploiter la vulnérabilité ou la faille identifiée. L'outil peut aussi bien viser un système en exploitant une faille qu'un être humain en utilisant des techniques d'ingénierie sociale.

3 Livraison

C'est le moment d'envoyer la pièce jointe infectée dans un courriel, le virus ou le ver sur le réseau de l'organisation.

4 Exploitation

C'est l'action d'exploiter la vulnérabilité ou la faiblesse afin d'obtenir un premier gain. Cette étape pourrait permettre plus de droits d'accès sur un système. Dans le cas d'un hameçonnage, ça pourrait être la capture d'authentifiant d'un administrateur système, par exemple.

5 Installation

Une porte dérobée est installée. Même si la vulnérabilité est corrigée, cette porte installée sur un système et accessible depuis l'Internet permettra à l'attaquant d'être persistant et de lancer les prochaines étapes.

6 Commandement et contrôle

À partir de la porte dérobée, l'attaquant a un accès permanent et peut donc obtenir et lancer des ordres à distance selon les droits d'accès acquis sur le ou les systèmes.

7 Actions sur l'objectif

À la dernière étape, l'attaquant utilise la porte dérobée et exécute les commandes voulues afin d'obtenir son gain et d'accomplir son objectif. Il s'agira par exemple :

- De vol de données, pour l'espionnage, la revente ou l'échange contre rançon.
- De chiffrement des données appelé crypto-rançon.
- De modification d'information à leur avantage.
- De vol ou de détournement d'argent, par transfert bancaire par exemple.

De plus, nous allons parler de « APT » pour « Advanced Persistant Threat ». Cela indique un attaquant qui traversera l'ensemble des étapes mentionnées ici, et restera sur le réseau et les systèmes de votre organisation. En établissant une persistance, cela permet à l'attaquant d'agir plus lentement afin d'éviter d'être détecté ou de mettre un œuvre un coup bien plus complexe. Parfois, une attaque persistante peut durer des années avant d'être détectée et mise en échec par l'organisation. Dans ces situations, l'impact sur l'entreprise est souvent très important.

Infiltration réseau

L'infiltration réseau a un sens assez large. Essentiellement, cela signifie qu'un attaquant a réussi ou activement tenté de s'introduire dans le réseau informatique, par exemple en exploitant une faiblesse à partir de l'Internet, de votre site Web ou d'une application ou même en usurpant l'identité d'un employé. Une fois dans le réseau, l'attaquant cherchera à se déplacer en exploitant des vulnérabilités de toutes sortes afin d'atteindre sa cible.

Comment détecter

L'infiltration réseau est souvent l'une des étapes d'une cyberattaque. Celle-ci est généralement difficile à détecter sauf si des systèmes de surveillance sont déjà en place. La découverte pourrait se faire par exemple par la détection de connexions suspectes sur le réseau.

Voici quelques points à surveiller

- **Des connexions inhabituelles** sur le routeur ou le pare-feu, comme la connexion en provenance d'un pays avec lequel vous ne faites pas affaire.
- **Des actions qui sortent de l'ordinaire**, comme un grand transfert de données ou de l'activité en dehors des heures de bureau.
- **La création de comptes utilisateurs récents.**
- **Les fichiers ou de nouveaux logiciels** ajoutés ou effacés sur un système sans raison.

Attention! Les pirates informatiques arrivent aussi à déguiser leurs traces pour rendre leur détection plus difficile. Si l'on suspecte l'intrusion dans un système précis, alors il faut aussi investiguer ce système au moyen des journaux d'événements. Ceux-ci, s'ils n'ont pas été modifiés par l'attaquant, permettraient de valider l'intrusion.

Bonne pratique

Transférer automatiquement tous les journaux d'événements sur un serveur centralisé. Cela facilite l'investigation d'un incident et permet d'investiguer sans se connecter sur le serveur possiblement compromis, simplifiant l'enquête.

Actions à prendre

Une fois l'attaque et la source de la brèche identifiées et investiguées, selon l'ampleur de l'attaque, il faut déclencher le processus de gestion des incidents appropriés selon votre entreprise.

Voici des étapes pouvant aider la prise en charge de ce type d'attaque.

❶ Contenir

- Déconnecter les systèmes potentiellement compromis du réseau et de l'Internet.
- Terminer et bloquer les connexions réseau suspectes.

Si l'investigation précédente est complète, le pirate n'a plus accès au réseau ni aux systèmes.

❷ Conserver

- Faire une copie exacte des systèmes potentiellement touchés. Celle-ci pourra être utilisée pour l'investigation légale s'il y a lieu.

❸ Reprendre et éradiquer

- Si une copie de sauvegarde des systèmes touchés existe, alors celle-ci peut être utilisée afin de relancer une copie du système.
- Avant de remettre le système sur le réseau, il faut s'assurer que celui-ci a été complètement nettoyé.
- **L'utilisation de l'antivirus et d'un scanneur de vulnérabilités est conseillée.** Une investigation plus en détail pourrait être nécessaire.
- Seulement une fois le système validé intègre, alors celui-ci pourra être remis sur le réseau, et Internet s'il y a lieu.

Fuite de données

Le vol de données peut être l'objectif d'une attaque informatique, dans la majorité des cas pour obtenir un gain financier. Les données serviront alors souvent à faire de la fraude par vol d'identité. Il pourrait aussi s'agir de vol de propriété intellectuelle ciblant vos secrets d'entreprise. Le voleur pourrait alors revendre ces renseignements au plus offrant sur Internet, incluant votre liste de clients et vos chiffres de vente. La fuite de données peut aussi provenir de l'interne, c'est-à-dire faite par un employé, un consultant ou un tiers. Une fuite peut aussi survenir suite à une erreur de manipulation, en raison d'un employé voulant travailler de la maison ou partager de l'information à l'externe, ou pour des raisons malveillantes.

Comment détecter

Le vol de données peut être détecté lors de l'extraction ou de la sortie des données de votre réseau. Des systèmes de détection de fuites de données souvent appelées DLP pour « Data Leak Protection» aident la détection et parfois permettent de bloquer la fuite. Sans système DLP, voici des indices à surveiller.

- **Surveiller la consommation Internet** pour un volume anormal, information disponible sur le site de votre fournisseur Internet, sinon à partir de votre routeur ou pare-feu réseau.
- **Surveiller les activités et connexions Internet sortantes en dehors des heures de bureau,** information normalement disponible sur votre routeur ou pare-feu d'entreprise.
- **Valider si votre système de courriels possède déjà des règles de détection ou de prévention de fuites de données** pour les fichiers joints par courriel. On peut créer des alertes facilement.

La fuite peut se produire de différentes façons :

Clé USB, gravure par CD/DVD, pièce jointe par courriel (professionnel ou personnel), site de stockage tel que OneDrive, Dropbox et GoogleDrive, par exemple.

Attention! Si le malfaiteur a voulu cacher ses traces, il est possible qu'il ait eu recours au chiffrement de fichiers. Pour découvrir le contenu, il faut le mot de passe ou trouver le fichier d'origine sur le système utilisé.

Actions à prendre

Prendre le contrôle de l'information

- Si l'information s'est retrouvée sur Internet, il faut alors rapidement en prendre le contrôle et tenter de l'effacer.
- S'il s'agit de l'erreur d'un employé, il est souvent plus rapide de demander à l'employé de l'effacer directement que de communiquer avec les responsables du site web, mais dans certains cas, cela sera requis.
- Pour trouver l'adresse courriel et le numéro de téléphone pour les contacter, il est possible de faire une recherche « WHOIS ». Plusieurs sites Web permettent de faire des recherches de ce type. Au Canada, le site CIRA.CA peut être utilisé.

Bonnes pratiques

- **Pour le travail à distance, un accès sécurisé par VPN (tunnel sécurisé) est à prioriser,** plutôt que d'utiliser des pièces jointes par courriel. Une fois un fichier confidentiel envoyé par courriel, il est difficile d'en garder la trace.
- **S'assurer que les employées comprennent bien ce qui est confidentiel** et l'importance de ne pas sortir l'information de l'entreprise.
- **Fermer les accès de sortie de données lorsque possible** : port USB, graveur CD/DVD, sites de courriels et de stockage pourraient aussi être bloqués si non requis dans le cadre du travail de l'employé.

Crypto-Rançon

Une attaque informatique pourrait inclure le chiffrement des données de l'entreprise. L'objectif du pirate est alors de chiffrer les données pour les rendre inaccessibles à l'entreprise. Une demande de rançon est ensuite envoyée demandant un paiement en échange du mot de passe ou de la clé de déchiffrement. Mais attention : le déchiffrement des données n'est pas toujours un succès, peut demander beaucoup de temps et la rançon peut être très élevée. Dans certains cas, il s'agit d'une demande de rançon de l'ordre de millions de dollars pour les plus grandes entreprises. De plus, payer la rançon revient à financer l'industrie du cybercrime, lui permettant de sophistiquer davantage leurs attaques informatiques !

Comment détecter

La détection d'une attaque de chiffrement est généralement rapide et facile. Les systèmes affectés ne répondront plus, et très souvent un écran affichera la demande de rançon et le processus pour payer; aucune action ne sera possible.

⚠ **Attention** aux fausses demandes de rançon! Il existe plusieurs logiciels malveillants affichant un écran tel que celui-ci mais ne chiffrant pas réellement les données de l'ordinateur. Dans ce cas, redémarrez l'ordinateur avec un antivirus autonome sur une clé USB ou CD. (Voir fiche « Les outils ».)

Bonne pratique

Les logiciels malveillants de chiffrement arrivent souvent par courriels incluant une pièce jointe ou un lien vers un site malicieux. L'infection peut aussi se faire sur un site Web infecté, ou par clé USB.

Pour se protéger, la sauvegarde des données hors réseau, voire hors site, est la meilleure approche. Dans le cas d'une infection majeure, cette sauvegarde sera protégée.

Actions à prendre

❶ **Isoler le système infecté du réseau et de l'Internet** afin d'éviter la réinfection et la propagation.

❷ **Faire une copie du système infecté** est toujours une bonne pratique si une investigation détaillée est nécessaire.

❸ **Investiguer pour trouver la cause de l'infection,** surtout si elle provient d'un autre système ou d'un accès Internet mal protégé.

❹ **Tenter de restaurer vos informations**

- Il faut s'assurer que la sauvegarde n'a pas été infectée. Idéalement, testez-la sur un autre système « vide ».
- Ensuite, utilisez un antivirus pour valider, puis déployez la sauvegarde sur le système touché.
- Si tout va bien, le nouveau système est alors libre de chiffrement.
- Avant de le remettre sur le réseau et sur Internet, il est recommandé d'appliquer toutes les mises à jour du système et l'antivirus.

❺ **Sans sauvegarde ou sauvegarde infectée?**

- Tentez de désinfecter le système. Utilisez un disque de redémarrage pour antivirus. (Voir fiche « Les outils ».)
- Cela permet à la machine de redémarrer sous le contrôle de l'antivirus, de poser un diagnostic et de tenter la désinfection.
- Pour certains logiciels de chiffrement bien connus, une solution de désinfection existe. Il faut alors identifier le logiciel pour faire la recherche de la solution sur Internet.

Hameçonnage

Le terme hameçonnage vient du fait que l'attaquant va aller à la pêche aux informations en sélectionnant une ou plusieurs victimes. Cette méthode peut être faite par téléphone, en personnage (par exemple, livreur de colis), mais très souvent, c'est par courriel que les tentatives d'hameçonnage ont lieu. L'objectif de l'attaque est d'obtenir de l'information sensible. Par exemple, le nom d'utilisateur et mot de passe, la réponse à des questions secrètes ou encore de l'information confidentielle au sujet de la victime ou de son employeur.

Comment détecter

Il n'est pas toujours simple de distinguer un courriel d'hameçonnage d'un vrai courriel. Il y a quelques années, les courriels malicieux étaient bourrés de fautes d'orthographe et souvent rédigés en anglais, et offraient plusieurs indices que la demande ne tenait pas. Maintenant, les fraudeurs vous parleront dans votre langue, sans faute, et avec des sujets qui vous concernent.

Voici quelques questions à se poser afin de tenter d'identifier un courriel malveillant :

Connaissez-vous l'expéditeur du courriel, et ce dernier est-il attendu?

- Un courriel, même d'un ami ou collègue, peut être de l'hameçonnage. Votre contact peut avoir été piraté, et le pirate s'en prend maintenant à vous.

Est-ce que le courriel utilise un ton URGENT, insistant, sans que celui-ci ne soit attendu de votre part ?

- C'est un signe assez commun des courriels d'hameçonnage.

Est-ce que le courriel vous incite à changer votre mot de passe, à payer un compte, à ouvrir une pièce jointe ou à cliquer sur un lien?

- **Attention,** cela est hautement suspect! S'il y a un lien, passer la souris au-dessus sans cliquer permet de valider vers quel site Internet celui-ci est vraiment redirigé.
- **Attention,** si souvent c'est un site inconnu, il peut s'agir aussi d'un site que vous reconnaissez avec une faute de frappe (par exemple, Gooogle.com ou Yahao.ca)!

Actions à prendre

1. Si vous avez reçu un courriel d'hameçonnage, l'idéal est de **le supprimer ou de le signaler à votre équipe informatique**, sinon dans le logiciel de courriel. Il s'agit souvent de faire clic-droit/« signaler comme pourriel ».
2. Si le lien du courriel ou la pièce jointe a été ouvert, alors il faut **isoler l'ordinateur d'Internet et du réseau** et le traiter comme infecté jusqu'à preuve du contraire. Il faut alors **effectuer un scan avec un antivirus** pour s'assurer que l'ordinateur est intègre. **Voir la fiche « Les outils »** pour des conseils là-dessus.
3. Si le courriel redirigeait vers une page pour y mettre un nom d'utilisateur et mot de passe et que la personne l'a fait, il faut les changer immédiatement. Au besoin, désactiver le compte utilisateur sur le réseau est aussi une bonne pratique. Il faut aussi investiguer afin de s'assurer que ces authentifiants n'ont pas déjà été utilisés à des fins malicieuses. Une analyse technique pourrait être requise.

Bonnes pratiques

- La **formation** dans le domaine de l'hameçonnage pour les employés fait une différence lorsqu'il est question de reconnaître une tentative de fraude et d'éviter de cliquer. Faire des campagnes de faux courriels d'hameçonnage aux employés tout en restant éthique par rapport à la vie privée est aussi efficace.
- La meilleure stratégie avec l'hameçonnage est d'**être attentif, de se poser les bonnes questions avant de cliquer** et dans le doute de s'abstenir.

Compromission de boîte courriel

La compromission d'une boîte courriel est une attaque de plus en plus fréquente dans tout type d'entreprise. Cela permet à un fraudeur d'accéder à une boîte courriel et d'en prendre le contrôle. Cela inclut souvent la réception, l'interception et l'envoi de courriels impersonnifiés. De plus, cela inclut l'accès à l'information déjà contenu dans la boîte, sans compter tous les accès possibles avec un changement de mot de passe à partir de cette boîte courriel. L'objectif peut aussi être monétaire, changeant l'information bancaire lors d'un transfert.

Comment détecter

Ce type d'attaque peut être assez difficile à détecter. Souvent, lorsque l'incident est détecté, il est déjà être trop tard, le fraudeur a déjà pris le contrôle des courriels et agit en sa faveur.

Typiquement, **cette attaque se produit suite à de l'hameçonnage**, pour que le fraudeur puisse obtenir le mot de passe de la personne ciblée. Dans d'autres cas, il peut s'agir de la fuite d'un ancien mot de passe réutilisé sur un autre site Web.

Certains indices permettent de découvrir une boîtes courriel compromise :

- Des accès à la boîte courriel en dehors des heures de bureau, à partir de d'autres pays.
- Des courriels en direction de destinataires étrangers, hors du commun.
- De nouvelles règles de boîte courriel redirigeant automatiquement les courriels vers une adresse externe en direction du fraudeur, d'un autre dossier ou de la corbeille.
- La réception de courriels frauduleux à partir de cette boîte courriel.

Actions à prendre

Dès la détection de la compromission de boîte courriel, il faut :

1. **Changer immédiatement le mot de passe ou désactiver la boîte courriel temporairement,** permettant l'investigation.
2. **Comprendre quelles ont été les actions de la personne dont la boîte courriel a été compromise** afin de détecter la source du problème et le corriger. Peut-être faut-il mettre l'ordinateur en quarantaine et s'assurer qu'il n'y a pas d'infection supplémentaire.
3. **Investiguer les actions faites par le fraudeur,** par exemple, l'ajout de nouvelles règles de redirection, et l'envoi de courriels frauduleux.
4. **Investiguer s'il existe d'autres boîtes courriel compromises.**

Bonnes pratiques

L'utilisation du double facteur d'authentification tel que l'ajout d'un jeton numérique lors de la connexion à la boîte courriel en dehors du bureau contribue grandement à diminuer le risque de compromission de boîte courriel. Cette fonction est souvent disponible chez votre fournisseur d'hébergement de courriels.

L'utilisation de mots de passe complexes est aussi importante afin d'éviter ce type de fraude.

L'utilisation d'un mot de passe unique pour chaque service est aussi essentielle. La fuite d'un ancien mot de passe risque d'être utilisée contre vous.

Déni de service

Le but de cette attaque est de rendre les ressources ou les services de l'entreprise hors fonction. Cela peut être le site Web de l'entreprise, le service de courriels, d'impression, souvent l'accès à Internet. Typiquement, l'attaquant va essayer de surcharger un système, par exemple, en envoyant plusieurs requêtes très rapidement à un système pour l'engorger ou des requêtes malformées mettant le système en attente. Ainsi, celui-ci ne pourra plus répondre aux demandes normales. De plus, il est possible que ce type d'attaque soit accompagné d'une demande de rançon.

Comment détecter

- **L'arrêt d'un service ne veut pas dire immédiatement qu'il s'agit d'une attaque de déni de service**. Cependant, les premiers signes pourraient être similaires.
- Il faut alors **investiguer la cause du problème** pour s'avoir s'il s'agit d'un ralentissement causé par une défectuosité, une erreur technique comme une mauvaise configuration, ou tout simplement une utilisation plus élevée qu'à l'habitude.
- **Les services visés sont souvent ceux affectant le plus la compagnie**, comme le site Web, surtout s'il s'agit d'un site transactionnel.
- **Une demande de rançon peut être reçue** par courriel avant l'attaque ou après.

Attention! Plusieurs fausses demandes de rançon existent demandant un paiement sinon quoi une attaque de déni de service aura lieu. Il faut alors tenter de reconnaître la fausse alerte de la vraie menace.

Bonnes pratiques

Les hébergeurs de sites Web ainsi que les fournisseurs d'accès Internet possèdent parfois une protection contre ce type d'attaque.

Pour un hébergement Web à l'interne, plusieurs solutions existent, soit avec l'utilisation de **balanceurs de charge**, permettant de répartir les requêtes, le **pare-feu** pouvant bloquer des requêtes illégitimes, soit une **solution infonuagique** redirigeant et analysant le trafic afin de détecter et d'éviter ce type d'attaque.

Actions à prendre

L'investigation d'un ralentissement ou de l'arrêt d'un système doit être systématique. Il faut investiguer la cause la plus probable selon les signes, très souvent inclus dans des détails techniques. Ainsi, plusieurs questions doivent être posées afin de poser le diagnostic.

Par exemple :

- **Est-ce que l'appareil ou le service affecté a subi un changement technique récemment?**
- **Est-ce que le système pourrait être en sur-demande légitimement (par exemple, vente spéciale)?**

Si effectivement un déni de service est suspecté, l'investigation doit rapidement être faite sur le pare-feu ou le routeur. **Si un nombre anormal de requêtes arrivent d'une seule destination, il est alors facile d'identifier le coupable** et possible de le bloquer rapidement.

Par contre, **les pirates experts vont plutôt distribuer leur attaque et utiliser plusieurs sources pour attaquer.** Il est plus complexe de bloquer ce type d'attaque sans affecter sa propre disponibilité.

Utiliser un service de protection contre ce type d'attaque est souvent la meilleure solution. Ainsi, faire appel à une expertise technique peut être nécessaire.

Les outils

Voici les différents outils devant faire partie de votre trousse pour surveiller, investiguer, corriger et endiguer plusieurs enjeux de sécurité. Il est recommandé de s'assurer de bien comprendre ces outils et d'en avoir l'expertise afin d'être efficace le jour où une investigation ou un incident doit être pris en charge rapidement.

Type	Avantages	Conseils	Caractéristiques
Antivirus	• Offre une protection nécessaire contre les virus et attaques connus. • Fonctionne très bien lorsque la signature de l'attaque est connue.	• Les mises à jour sont essentielles afin d'avoir la base de données des dernières signatures.	• L'antivirus saura mettre en quarantaine et bloquer certaines menaces reconnaissables par une signature.
Disque de redémarrage pour analyse antivirus	• Est parfait pour isoler et investiguer un système rapidement et tenter une désinfection.	• Débrancher le système du réseau le plus tôt possible pour éviter la propagation.	• Permet de démarrer un ordinateur infecté sur un système d'exploitation autonome basé sur un antivirus.
Anti-maliciel (*anti-malware*) **Anti-rançongiciel** (*anti-ransomware*)	• En complément de l'antivirus, l'application se concentre sur les menaces des logiciels malveillants.	• Si intégré dans l'antivirus, doit être un module prouvé efficace contre les menaces de maliciels et de rançongiciels (*malware* et *ransomware*)	• C'est un excellent complément à l'antivirus permettant de détecter et de nettoyer d'autres types d'applications malveillantes.
EDR 'Endpoint Detection & Response'	• En complément à l'antivirus, cela permet une prise en charge plus rapide de l'investigation et de la remédiation des menaces.	• S'assurer de l'intégration dans les outils de journalisation et de détection d'événements journalisés. • Doit inclure la détection d'anomalies en termes de comportement système.	• L'EDR surveille davantage les comportements anormaux et malveillants que l'antivirus traditionnel. C'est un complément très intéressant pour les menaces émergentes.
Logiciel d'investigation numérique	• Facilite la gestion d'incident lorsque la conservation de la preuve numérique doit être faite.	• S'assurer de comprendre et de tester l'outil.	• Cet outil de documentation et d'enquête contribue à respecter la conservation de la preuve s'il est bien utilisé.
Logiciel d'investigation en mémoire **(Expert requis)**	• Facilite et accélère l'investigation en profondeur d'un système.	• Requiert un niveau d'expertise technique dans le domaine.	• Cet outil permettra de voir les informations en mémoire vive, telles que les dernières commandes utilisées, les mots de passe, etc.
Scanneur de vulnérabilités **(Niveau technique)**	• Identifie les vulnérabilités sur les systèmes et applications. Suggère souvent des solutions de correction.	• Attention aux faux positifs. Le volume de vulnérabilités peut être élevé. Il faut avoir l'expertise technique pour distinguer le vrai du faux.	• Un scanneur en ligne (Internet) permet d'identifier des vulnérabilités sur l'infrastructure d'un regard externe (Web et périmètre). • Un scanneur à l'interne permettra de valider un niveau plus détaillé et précis de vulnérabilités.
SIEM '*Security information and event management*'	• Accélère l'investigation et la corrélation d'événements de sécurité journalisés.	• Pour être efficace, un SIEM doit recevoir les bons événements de journalisation. • Des « Use Cases » ou scénarios d'alerte doivent être en place.	• Permet la centralisation de tous les événements de sécurité en un endroit.

Lexique

Chiffrement - *en anglais « Encryption »*
Procédure par laquelle une information est convertie d'une forme à une autre afin d'en dissimuler le contenu et d'en interdire l'accès aux entités non autorisées.

Confidentialité
Caractéristique de l'information sensible protégée contre tout accès non autorisé.

Disponibilité
Caractéristique de l'information ou des systèmes qui sont accessibles aux personnes autorisées au moment où celles-ci en ont besoin.

Faille ou vulnérabilité
Lacune qui émerge en raison d'une négligence ou d'une attaque délibérée. Elle peut aller à l'encontre d'une politique ou d'une loi et est souvent exploitée pour réaliser des actions nuisibles ou criminelles.

Intégrité
Capacité à protéger l'information contre une modification ou une suppression non autorisée.

Pare-feu, Coupe-feu - *en anglais « Firewall »*
Barrière de sécurité placée entre deux réseaux ou avec l'Internet qui contrôle le volume et les types de trafic autorisés à passer d'un réseau à l'autre.

Maliciel
Logiciel malveillant conçu pour infiltrer ou endommager un système informatique. Les maliciels les plus courants sont les virus informatiques, les vers, les chevaux de Troie, les logiciels espions et les logiciels publicitaires.

Rançongiciel, crypto-rançon - *en anglais « Ransomware »*
Type de maliciel qui empêche un utilisateur légitime d'accéder à des ressources (système ou données), et ce, jusqu'à ce qu'il ait payé une rançon.

Routeur
Équipement réseau informatique assurant le routage des paquets. Son rôle est de faire transiter des paquets d'une interface réseau vers une autre, au mieux, selon un ensemble de règles. Certaines règles simples permettent de bloquer ou filtrer les connexions entre les réseaux ou l'Internet.

Source : https://cyber.gc.ca/fr/glossaire

Ressources complémentaires

Cybereco
Trousse de sensibilisation à la sécurité

https://cybereco.ca/trousse-entreprise/

Banque de développement du Canada
Votre liste de vérification pour éviter les failles de sécurité des TI

https://www.bdc.ca/fr/articles-outils/technologie/investir-technologie/pages/securite-informatique-liste-controle-pme.aspx

Centre canadien pour la cybersécurité
Pensez cybersécurité pour les petites et moyennes entreprises

https://www.pensezcybersecurite.gc.ca/fr/ressources/guide-pensez-cybersecurite-pour-les-petites-et-moyennes-entreprises

Centre canadien pour la cybersécurité
Contrôles de cybersécurité de base pour les petites et moyennes organisations

https://cyber.gc.ca/fr/orientation/controles-de-cybersecurite-de-base-pour-les-petites-et-moyennes-organisations

Centre canadien pour la cybersécurité
Élaborer un plan d'intervention en cas d'incident

https://cyber.gc.ca/fr/elaborer-un-plan-dintervention-en-cas-dincident

Références

MICROAGE, Le coût véritable d'une cyberattaque et comment réagir au mieux
https://www.microage.ca/wp-content/uploads/2019/09/Le-cout-veritable-dune-cyberattaque-et-comment-reagir-au-mieux_eBook.pdf

VERIZON, 2020 Data Breach Investigations Report
https://enterprise.verizon.com/resources/reports/dbir/

CANADA, CENTRE CANADIEN POUR LA CYBERSÉCURITÉ, Guide Pensez cybersécurité pour les petites et moyennes entreprises
https://www.pensezcybersecurite.gc.ca/fr/ressources/guide-pensez-cybersecurite-pour-les-petites-et-moyennes-entreprises

CANADA, CENTRE CANADIEN POUR LA CYBERSÉCURITÉ, Contrôles de cybersécurité de base pour les petites et moyennes organisations
https://cyber.gc.ca/fr/orientation/controles-de-cybersecurite-de-base-pour-les-petites-et-moyennes-organisations

WIKIPEDIA, Routeur
https://fr.wikipedia.org/wiki/Routeur

HISCOX, Hiscox Cyber Readiness Report 2019
https://www.hiscox.co.uk/sites/uk/files/documents/2019-04/Hiscox_Cyber_Readiness_Report_2019.PDF

RADIO-CANADA, Les PME québécoises trop vulnérables aux cyberattaques
https://ici.radio-canada.ca/nouvelle/1164074/cyberattaque-cybersecurite-piratage-informatique-pme-entreprises-quebec

STATISTIQUE CANADA, Les défis des entreprises canadiennes quant à la cybersécurité et au cybercrime, 2017
https://www150.statcan.gc.ca/n1/pub/85-002-x/2019001/article/00006-fra.htm

L'INFORMATION D'AFFAIRES D'ICI, Cybersécurité: les PME exposées aux mêmes menaces que les grandes entreprises
https://infodaffaires.com/cybersecurite-les-pme-exposees-aux-memes-menaces-que-les-grandes-entreprises/

LA PRESSE, Attaques contre les PME: un nouveau chien de garde en sécurité informatique
https://www.lapresse.ca/affaires/entreprises/201911/29/01-5251721-attaques-contre-les-pme-un-nouveau-chien-de-garde-en-securite-informatique.php

RADIO-CANADA, Les PME québécoises trop vulnérables aux cyberattaques
https://ici.radio-canada.ca/nouvelle/1164074/cyberattaque-cybersecurite-piratage-informatique-pme-entreprises-quebec

CYBERSEC&YOU, Cybersécurité des PME : comment les accompagner vers la prise de conscience ?
https://www.cybersecandyou.com/cybersecurite-des-pme/

UNIVERSITÉ DU QUÉBEC, L'importance de la cybersécurité pour les PME
https://www.uquebec.ca/reseau/fr/medias/actualites-du-reseau/limportance-de-la-cybersecurite-pour-les-pme

GLOBAL SECURITY MAG, Cybersécurité, les entreprises restent peu préparées malgré l'augmentation du nombre de cyberattaques
https://www.globalsecuritymag.fr/Cybersecurite-les-entreprises,20190423,86425.html

CCI ALPES DE-HAUTE-PROVENCE, Comment réagir en cas d'attaque informatique?
http://www.digne.cci.fr/IMG/pdf/Fiche_23_-_Securite-Comment_reagir_en_cas_d_attaque_informatique.pdf

CSO ONLINE, How to report a data breach under GDPR
https://www.csoonline.com/article/3383244/how-to-report-a-data-breach-under-gdpr.html

SANS, Memory Forensics Analysis Poster
https://digital-forensics.sans.org/media/Poster_Memory_Forensics.pdf

BDC, Votre liste de vérification pour éviter les failles de sécurité des TI
https://www.bdc.ca/fr/articles-outils/technologie/investir-technologie/pages/securite-informatique-liste-controle-pme.aspx

CANADA, CENTRE CANADIEN POUR LA CYBERSÉCURITÉ, Élaborer un plan d'intervention en cas d'incident
https://cyber.gc.ca/fr/elaborer-un-plan-dintervention-en-cas-dincident

CANADA, CENTRE CANADIEN POUR LA CYBERSÉCURITÉ, Contrôles de cybersécurité de base pour les petites et moyennes organisations
https://cyber.gc.ca/fr/orientation/controles-de-cybersecurite-de-base-pour-les-petites-et-moyennes-organisations

NIST, Computer Security Incident Handling Guide
https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

NIST, Guide to Integrating Forensic Techniques into Incident Response
https://csrc.nist.gov/publications/detail/sp/800-86/final

AT&T, Incident Response Steps and Frameworks for SANS and NIST
https://cybersecurity.att.com/blogs/security-essentials/incident-response-steps-comparison-guide

ÉTATS-UNIS, FEDERAL TRADE COMMISSION, Data Breach Response: A Guide for Business
https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business

COMODO, Does paying ransomware work?
https://enterprise.comodo.com/does-paying-ransomware-work.php

FBI, Scams and safety : Ransomware
https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware

LOCKHEED MARTIN, Proactively Detect Persistent Threats

https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

cyber eco