Cyberattaque d'un établissement : quelle conduite en pratique ?

Serge Houtain

Regional computer crime unit (RCCU) – Police judiciaire fédérale Mons-Tournai – Mons – Belgique

✉ **Serge Houtain** – 1er Commissaire, chef de service – RCCU – Police judiciaire fédérale Mons-Tournai – Avenue Melina Mercouri B6-B8 – 7000 Mons – Belgique – E-mail : Serge.Houtain@police.belgium.eu

Introduction

Partant du principe que vous serez un jour ou l'autre victime d'une cyberattaque, nous abordons ci-après des recommandations et bonnes pratiques afin de vous préparer à cet « événement indésirable » et gérer la crise qui en découlera.

Déroulement d'une cyberattaque

Une cyberattaque comporte quatre grandes phases (Figure 1) : identification de la cible et phase de reconnaissance passive ou active par le cybercriminel via les noms de domaines[1], les requêtes Whois[2], archive.org[3], les serveurs DNS[4], adresses e-mails, publications en ligne, réseaux sociaux, etc. ; compromission initiale ou intrusion par (*spear*[5]) *phishing*, dit hameçonnage, exploitation des réseaux sociaux, kits d'exploits[6], *malwares* (logiciels malveillants), RAT[7] ; établissement de la persistance et mouvements laté-

1- p. ex : chwapi.be, chu-lyon.fr.
2- Whois est un service qui permet de récupérer des informations sur les titulaires de domaines sur internet et d'adresses IP (*Internet protocol*).
3- Organisme à but non lucratif consacré à l'archivage du web qui agit comme une bibliothèque numérique. Ces archives sont constituées de clichés instantanés (copies de pages web, etc.).
4- Le serveur DNS (*Domain name system*, système de noms de domaines) traduit des demandes de noms de domaines en adresses IP pour éviter à l'utilisateur de mémoriser des milliers d'adresses IP. Il est en effet plus facile de saisir « amazon.fr » dans le navigateur que 108.174.10.10.
5- Lance (pour parler d'un hameçonnage ciblé).
6- Un exploit ou code d'exploitation est un élément de programme permettant d'exploiter une faille de sécurité dans un système informatique (source : Wikipédia).
7- *Remote access tools* ou outils de prise de contrôle à distance.

Résumé

La bonne question à se poser : non pas SI vous subirez une cyberattaque, mais QUAND cela arrivera-t-il ? Anticiper pour vous préparer à faire face à une situation de crise est la première chose à faire. Comment ? Notamment en mesurant les différents impacts d'une cyberattaque sur la disponibilité, la confidentialité, et l'authenticité de vos données. Pour cela, l'analyse de risques est primordiale, tout comme le plan de sécurité, le plan de continuité d'activités. Inventoriez vos actifs (les valeurs à protéger), préparez vos check-lists, votre plan de communication, les listes de contacts, vérifiez et testez vos back-up, définissez clairement les rôles de chacun(e). Recensez les partenaires externes pouvant apporter une aide, comme votre fournisseur internet, une société de cybersécurité, les autorités (Cert.be, enquêteurs spécialisés de la police ou de la gendarmerie, Anssi). N'oubliez pas les sous-traitants de la chaîne logistique. Enfin, ne perdez pas de vue l'impact psychologique que peut engendrer une cyberattaque sur différentes catégories de personnel.

Mots-clés : Cybersécurité – Systèmes d'information – Gestion du risque – Gestion de crise.

Abstract

Your facility falls victim to a cyberattack: what practical response?

The issue to consider is not "IF you fall victim to a cyberattack" but "WHEN you will fall victim to a cyberattack..." The first thing to do is anticipate and prepare yourself to face a crisis. How? By evaluating the different impacts a cyberattack could have on the availability, confidentiality and authenticity of your data. This is why risk analysis is crucial, as are security plans and activity maintenance plans. Take stock of your assets (the values to protect), prepare your checklists, your communication plan, the lists of contacts, check and test your backups, clearly define the role of each person. List outside partners who might help: your internet access provider for instance, or a cybersecurity company, as well as the appropriate authorities (in French-speaking countries: CERT.be, special units of the police and Gendarmerie, Anssi). Do not forget supply-chain subcontractors. Last but not least, do not forget the potential psychological impact that cyberattacks can have on different categories of staff.

Keywords: *Cybersecurity – Information systems – Risk management – Crisis management.*

raux (renforcement des accès, augmentation des privilèges, collecte de mots de passe et de *hashes*[8]) ; exfiltration des données (via RAT, FTP[9], e-mails). Assez souvent, une cyberattaque majeure se déclenche en soirée, à la veille d'un week-end (prolongé), lorsqu'il n'y a pas ou plus de personnel informatique présent en nombre au sein de l'infrastructure.

Prévention

« *Si vis pacem, para bellum*[10] ». Vous devez anticiper et vous préparer à faire face à une situation de crise qui va durer de quelques heures dans le meilleur des cas à quelques mois pour une cyberattaque majeure.

Appréciez le risque

Globalement, la question à se poser est : que devons-nous protéger en priorité ? Il faut se concentrer sur les conséquences d'une attaque (impact) afin de déterminer le niveau de risque et les contrôles de sécurité à mettre en place en priorité, notamment les risques possibles en termes de confidentialité, d'intégrité, de disponibilité et d'authenticité des données, qui sont un bon point de départ **(Figure 2)**. Qu'est-ce qui est confidentiel ? Par exemple les données à caractère personnel, les identifiants et les mots de passe, les adresses e-mail, les dossiers médicaux numérisés. Que ne doit-on pas perdre ? Par exemple les dossiers médicaux numérisés, les données à caractère personnel. Qu'est-ce qui est irremplaçable ? Par exemple les dossiers médicaux numérisés. Qu'est-ce qui pourrait causer le plus grand dommage ? Par exemple la perte des dossiers médicaux numérisés. Qu'est-ce qui pourrait affecter notre réputation ? Par exemple la perte de données à caractère personnel, des dossiers médicaux numérisés ou des données financières. Les risques sont les conséquences et l'impact potentiel des vulnérabilités non traitées. L'impossibilité d'accéder à des dossiers médicaux numérisés peut compromettre le pronostic vital de certains patients. Pourquoi le patient est-il hospitalisé ? Quels sont les médicaments à prescrire, quels sont les soins urgents à prodiguer ? Le patient a-t-il des allergies à certains médicaments ?

8- Un « *hash* » est l'empreinte numérique d'un fichier. Il permet notamment de vérifier l'authenticité de ce fichier.
9- *File transfer protocol* : logiciel permettant le transfert de fichiers entre périphériques (p. ex. : d'un ordinateur vers un serveur et inversement).
10- Si tu veux la paix, prépare la guerre.

Figure 1 – Phases d'une cyberattaque.

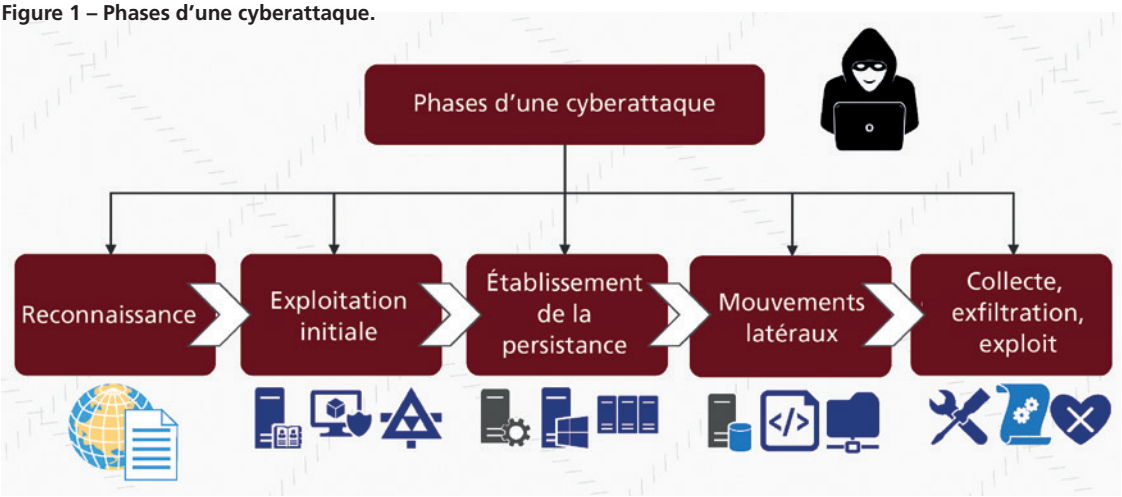
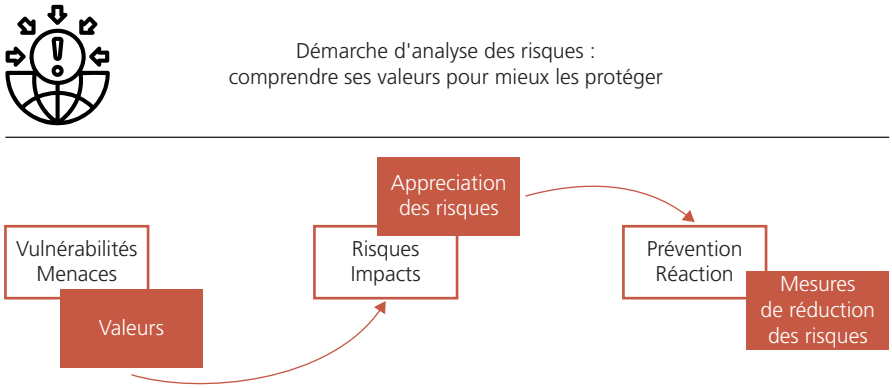


Figure 2 – Analyse de risques.



Si le médecin n'est plus en mesure de le savoir, la situation peut devenir critique. Un risque peut être accepté, quand l'impact et la probabilité sont trop insignifiants pour prendre d'autres mesures, évité, en prenant les mesures adéquates pour ce faire, transféré, en déléguant à une tierce partie la gestion de son impact – il peut s'agir d'une assurance (risque financier) ou d'un fournisseur de services (p. ex. : *cloud computing*[11]) –, ou encore atténué, si vous mettez en place des contrôles suffisants afin de le réduire à un niveau acceptable. Ne sous-estimez pas le travail que cela implique, car même si un projet (comprenant une application informatique) semble simple, les risques associés peuvent être importants. Il n'y a pas de corrélation entre la taille d'un projet et les risques qui y sont associés. L'analyse des risques[12] conduit à l'établissement d'une matrice des risques **(Figure 3)**. Afin de vérifier l'exactitude et l'exhaustivité de votre analyse, celle-ci doit être vérifiée par différentes personnes de votre organisation. Le résultat de votre analyse de risques influencera, entre autres, votre plan de sécurité. Pour arriver à ce plan, vous devez hiérarchiser les mesures de sécurité nécessaires qui doivent être établies afin d'obtenir un plan d'implantation qui devra être approuvé par la direction.

Ayez un registre de tous vos actifs

L'objectif est d'avoir une connaissance à jour de tous les appareils informatiques utilisés et des données à votre disposition. Cette compréhension vous aide à identifier les vecteurs d'attaque possibles et les actifs (valeurs à protéger) essentiels de votre organisation. En cas d'incident, le registre des actifs peut vous aider à détecter l'origine du problème et potentiellement le fournisseur à contacter. Pour cela, vous devez tenir à jour un inventaire de vos actifs informatiques tels que les périphériques réseau, les serveurs connectés à internet, les postes de travail, les appareils mobiles et les appareils des utilisateurs. Cet inventaire vous permet de comprendre l'étendue de vos actifs essentiels, de vérifier vos contrats de maintenance et d'identifier les ressources qui ne sont plus utilisées mais qui n'ont pas encore été déclassées (p. ex. un VPN[13] géré par un fournisseur internet qui n'est plus opérationnel). Pour l'identification des actifs essentiels, il peut être utile de relier cet inventaire informatique aux activités et aux processus clés.

Modélisez les menaces

Sachant que le risque zéro n'existe pas, il convient de trouver un équilibre entre le risque et les moyens à mettre en œuvre pour s'en protéger (*risque = vulnérabilités x menaces x conséquences*). N'oubliez pas vos partenaires externes dans votre analyse, comme les sous-traitants et les fournisseurs dont les actions peuvent avoir un impact sur votre cybersécurité. Identifiez les menaces potentielles de la chaîne logistique avec ces partenaires. La sous-traitance représente un risque en matière de cybersécurité. Une faille chez un fournisseur peut être synonyme de fuite de données confidentielles avec des répercussions légales ou de fonctionnement sur votre organisation.

Établissez des check-lists de sécurité

Voici quelques check-lists à établir tant que la situation est sous contrôle, c'est-à-dire avant l'attaque de votre infrastructure informatique et la désorganisation ou le blocage de vos activités de soins :

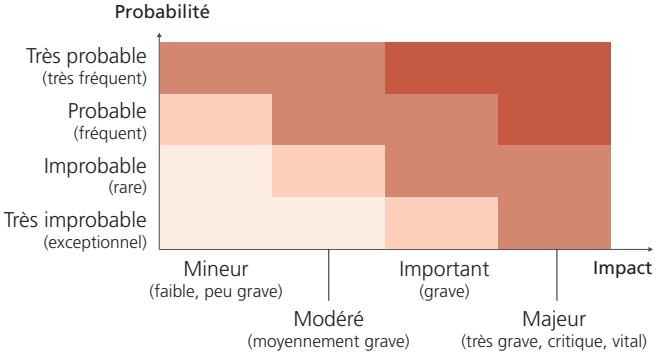
Acteurs et calendrier

- Quelles personnes doivent-elles être informées de l'incident ? Préciser les noms, adresses e-mail, numéros de téléphone, appartenances à un groupe ou à une société tierce (p. ex. : fournisseur d'accès internet, fournisseurs de la chaîne logistique, entreprises de cybersécurité, etc.).
- Qui est désigné comme coordinateur principal de la réponse à l'incident ?
- Qui est autorisé à prendre des décisions commerciales dans les services affectés (p. ex. : achat en urgence de matériel, d'un logiciel) ?
- Par quels mécanismes l'équipe communique-t-elle lors de la gestion de l'incident (courriel, conférence téléphonique, etc.) ? Quelles sont les capacités de chiffrement à utiliser ?
- Quel est le calendrier des mises à jour régulières internes ? Qui en est responsable ?
- Quel est le calendrier des mises à jour régulières externes ? Qui est chargé de les diriger ?
- Qui procédera à l'examen « sur le terrain » de l'infrastructure informatique concernée ?

11- Informatique en nuage, ou dématérialisée.
12- Conseil : une analyse de risque peut être réalisée à l'aide de l'application *open source* Monarc. Accessible à : https://www.monarc.lu/ *(Consulté le 18-02-2022)*.

13- *Virtual private network* (réseau privé virtuel), soit un tunnel sécurisé (chiffré) à l'intérieur d'un réseau informatique.

Figure 3 – Matrice des risques.



- Qui assurera l'interface avec les équipes juridiques, de direction, de relations publiques et autres équipes internes concernées ?

Plan de communication

- Destinataires : la communication visera le personnel de l'organisation mais sans doute également le public.
- Médias : cette communication peut être faite au travers de différents canaux tels que communiqués de presse, informations en continu sur un forum, etc.
- Moyens techniques : tenez compte du fait que vous n'aurez peut-être plus d'accès à internet, plus de possibilité d'utiliser l'e-mail ou les téléphones VoIP[14].

Évaluation de la situation

- Quelle est la nature du problème tel qu'il a été observé jusqu'à présent ?
- Comment, quand et par qui le problème a-t-il été détecté ?
- Quelles sont les composantes de l'infrastructure de sécurité disponibles dans l'environnement concerné (pare-feu, anti-virus, etc.) ?
- Quel est le niveau de sécurité des composants de l'infrastructure informatique concernée ? À quelle date, le cas échéant, les vulnérabilités ont-elles été évaluées ?
- Quels groupes ou organisations ont-ils été touchés par l'incident ?
- D'autres incidents de sécurité ont-ils été observés récemment dans l'environnement ou l'organisation concernés ?
- Dans un premier temps, et pour conserver l'empreinte (numérique) de l'attaquant, évitez de prendre des mesures qui permettent d'accéder à de nombreux fichiers (p. ex. : logs[15]) ou d'installer des outils.
- Examinez les journaux du système, de la sécurité et des applications pour détecter les événements inhabituels.
- Examinez les détails de la configuration du réseau et des connexions ; notez les paramètres, sessions ou ports actifs et anormaux.
- Examinez la liste des utilisateurs pour des comptes qui n'appartiennent pas à l'organisation ou qui auraient dû être désactivés.
- Consultez la liste des processus en cours d'exécution ou des tâches planifiées.
- Recherchez les programmes inhabituels configurés pour s'exécuter automatiquement au démarrage du système.
- Vérifiez les paramètres ARP[16] et DNS, regardez le contenu du fichier *hosts*[17] pour des entrées suspectes.
- Recherchez des fichiers inhabituels et vérifiez l'intégrité des fichiers de l'OS[18] et des applications.
- Utilisez un renifleur de réseau (p. ex. Wireshark[19]), s'il est présent dans le système ou disponible à l'extérieur, pour observer toute activité inhabituelle.
- Examinez les problèmes récemment signalés, la détection des intrusions et les alertes connexes pour le système.

En cas (de suspicion) d'incident

- Faites appel à un spécialiste de la réponse aux incidents et informez votre responsable.
- Ne paniquez pas et ne laissez pas vos collègues vous mettre la pression ; concentrez-vous pour éviter des erreurs d'inattention.
- Si vous arrêtez une attaque en cours, débranchez le système du réseau ; ne redémarrez pas et ne mettez pas le système hors tension.
- Prenez des notes détaillées pour suivre ce que vous avez observé, quand et dans quelles circonstances.
- Avertissez les autorités (RGPD) : en cas d'incident majeur, ou de perte ou vol de données à caractère personnel, le *Data protection officer* (DPO) (ou délégué à la protection des données) de l'organisation a l'obligation légale d'en avertir les autorités compétentes, l'Autorité de protection des données[20] (APD) en Belgique ou la Commission nationale de l'informatique et des libertés (Cnil) en France, sous peine d'amendes ou de poursuites judiciaires. Il est en principe obligatoire d'avertir chaque personne (par courrier recommandé) dont des données à caractère personnel ont été dérobées.

Gérez vos sauvegardes

Conservation et protection

- Protégez vos sauvegardes au même titre que vos données originales en effectuant, par exemple, plusieurs sauvegardes de vos données sur différents supports.
- Conservez également une sauvegarde dans un lieu différent de celui où sont stockées les données originales pour vous prémunir en cas de sinistre.
- Si vous estimez que vos données sont suffisamment

14- *Voice over internet protocol* (voix sur protocoles internet) ou communication vocale ou multimédia via internet.
15- Fichiers contenant l'enregistrement de tous les événements ayant affecté un processus particulier (application, activité d'un réseau informatique…) (source : Wikipédia).
16- *Address resolution protocol* (protocole de résolution d'adresse), utilisé pour associer l'adresse de protocole de couche réseau (typiquement une adresse IPv4) d'un hôte distant, à son adresse de protocole de couche de liaison (typiquement une adresse MAC [*Media access control*, contrôle d'accès au support] de carte réseau).
17- Le fichier *hosts* se comporte comme un annuaire en faisant correspondre un nom de domaine (p. ex. : chawpi.be) à une adresse IP.
18- *Operating System* (P. ex. : MS-Windows, GNU/Linux, MacOS).
19- Accessible à : https://www.wireshark.org/download.html *(Consulté le 18-02-2022).*
20- Anciennement Commission de la protection de la vie privée.

sensibles pour les chiffrer ou en limiter l'accès, ou si un règlement vous y oblige, faites de même avec vos sauvegardes.
- Veillez à disposer de sauvegardes non connectées en permanence au système informatique.

Vérification

Assurez-vous régulièrement que votre sauvegarde fonctionne en effectuant une restauration. C'est un élément souvent négligé ! Effectuez des tests de restauration périodiquement peut vous aider à évaluer votre objectif de temps de restauration. L'exécution d'un test de restauration est le moyen le plus rapide de vous assurer que votre support est totalement fonctionnel et que vos données sont correctement stockées.

Stockage des supports

Tout comme les supports qui permettent de stocker les données originales, les supports sur lesquels sont réalisées les sauvegardes peuvent être endommagés. C'est l'une des raisons les plus courantes pour lesquelles les sauvegardes et les restaurations échouent. C'est particulièrement fréquent lors de l'utilisation de bandes magnétiques, de CD ou de DVD (pour autant que ces supports soient encore utilisés). Assurez-vous de suivre les précautions appropriées pour le stockage de ces supports et souvenez-vous que certains ont une date de péremption. Vérifiez leur état afin de prévenir toute défaillance.

Plan de continuité d'activité

Le plan de continuité d'activité (PCA), sur-ensemble du *Disaster recovery plan*[21], décrit exhaustivement les étapes à effectuer, les personnes à contacter et les moyens de mitigation rapide pour revenir à une situation stable (même en mode dégradé). Un PCA bien testé et diffusé auprès de tous les collaborateurs permet de revenir plus vite et plus sereinement à un mode normal (ou presque) de travail, sans perte de temps concernant « qui fait quoi à quel moment ».

Continuité d'activité dans le cloud

Le *cloud computing* et les solutions « *cloud* » procurent un faux sentiment de sécurité quand il s'agit de la continuité d'activité. Bien que votre fournisseur de *cloud computing* propose souvent des solutions de continuité d'activité pour des services standardisés tels que la gestion des courriels ou des documents, et même pour les serveurs virtuels, ces solutions dépendent entièrement de la connectivité internet. Lors de la rédaction du PCA, une attention particulière doit être accordée à l'accès à internet dans un environnement *cloud*.

21- Plan de reprise après sinistre.

Appel à des sociétés de cybersécurité

Faites auditer votre système informatique par des sociétés externes. Cependant, ne croyez jamais un expert qui vous dit au premier contact qu'il dispose des connaissances pour protéger votre organisation à 100% : c'est illusoire. Le niveau de sécurité se conçoit après une analyse des risques complète. L'analyse des risques est un sujet vaste. Retenez dans un premier temps que c'est toujours une question d'équilibre à trouver entre la valeur de ce que vous souhaitez protéger et le budget que vous acceptez de consacrer à cette protection. Comme mentionné dans le premier article[22], n'hésitez pas à faire appel à des pirates éthiques pour tester vos défenses (logiques et physiques). Organisez ponctuellement des campagnes de *phishing* pour vérifier que votre personnel est suffisamment sensibilisé à ce type d'attaque. N'oubliez pas de rappeler les techniques d'ingénierie sociale permettant de collecter des informations sensibles avec un simple téléphone.

Soutien psychologique

Outre l'aspect purement technique, une cyberattaque majeure avec arrêt total de l'activité hospitalière durant plusieurs jours et une remise en fonction du système informatique qui pourrait durer plusieurs mois constituent des éléments déstabilisants pour certains membres du personnel (notamment du département informatique). Pensez dès lors à prévoir un plan de suivi et de soutien psychologique pour ces personnes.

Assistance des forces de police

En Belgique, une structure hospitalière victime d'une cyberattaque peut faire appel à une *Regional computer crime unit* (RCCU) pour le dépôt de plainte, mais aussi pour obtenir une assistance pour la recherche de l'origine de la cyberattaque et des auteurs. Au besoin, la RCCU fera elle-même appel à des renforts en interne (*Task force*, FCCU[23]) et prendra contact avec le Cert.be[24] (branche opérationnelle du Centre pour la cybersécurité Belgique – CCB) ainsi qu'avec d'autres partenaires (Europol, Interpol, équipe de négociateurs, services de renseignement). Il existe une RCCU au sein de chaque police judiciaire fédérale (PJF) dans chaque arrondissement judiciaire. Les zones de polices locales (en première ligne) savent comment contacter une RCCU. En France, la Gendarmerie nationale dispose de correspondants en technologies numériques au sein des brigades territoriales pour les premiers contacts (C-Ntech), et d'enquêteurs spécialisés dans les nouvelles technologies (N-tech,

22- Houtain S. Cybersécurité : ne vaut-il pas mieux prévenir que guérir, Risques & Qualité 2022;(19)1:12-16.
23- *Federal computer crime unit.*
24- *Computer emergency response team fédérale*, équipe d'intervention d'urgence informatique belge.

équivalents des professionnels du RCCU) dans les différents départements. Il existe également le Centre de lutte contre les criminalités numériques (C3N), basé à Pontoise et jouant le rôle de service central pour la Gendarmerie. La sous-direction de la lutte contre la cybercriminalité (SDLC), basée à Nanterre, dispose d'autres ressources opérationnelles pouvant s'avérer utiles, comme les enquêteurs de la Police nationale spécialisés en cybercriminalité (ICC[25]). Si les auteurs ne sont pas identifiés immédiatement, la coopération internationale entre les services de sécurité et le monde judiciaire permet parfois d'obtenir des résultats positifs[26], et ce, même si les enquêtes durent souvent très longtemps. Il ne faut donc jamais hésiter à contacter la police ou la gendarmerie en cas de cyberattaque. ■

25- Investigateur en cybercriminalité.

26- Exemple récent, le démantèlement du groupe cybercriminel REvil. Accessible à : https://bit.ly/3J7ilzD *(Consulté le 18-02-2022)*.

Pour en savoir plus

- Pernet C. Sécurité et espionnage informatique - Connaissance de la menace APT (*Advanced persistent threat*) et du cyberespionnage. Paris : Éditions Eyrolles, 2014, ISBN 978-2-212-13965-5.
- Bilet V, Liottier M. Survivre à une cyberattaque. Versailles : VA Éditions, 2018, ISBN 979-10-93240-42-8.
- Ghernaouti S. Cybersécurité : analyser les risques, mettre en œuvre les solutions. 6e édition. Malakoff : Éditions Dunod, 2019, ISBN 978-2-10-079054-8.
- Agence Nationale de la sécurité des systèmes d'information (Anssi). Guide d'hygiène informatique. Renforcer la sécurité de son système d'information en 42 mesures. Paris, 2017. 72 pages. Accessible à : https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf *(Consulté le 25-01-2022)*.

Citation
Houtain S. Cyberattaque d'un établissement : quelle conduite en pratique ? Risques & Qualité 2022;(19)1:17-22.

Historique
Reçu 7 février 2022 – Accepté 14 fevrier 2022 – Publié 21 mars 2022

Financement : l'auteur déclare ne pas avoir reçu de financement.

Liens d'intérêt : l'auteur déclare ne pas avoir de lien d'intérêt.