La gestion des crises cyber

Sommaire

Si vous souhaitez consulter des articles cités dans ce document, vous pouvez en faire la demande auprès des documentalistes du CRD par mail à crd@ensosp.fr.

Articles:

- Dobigny, Valérie, Grunemwald, Benoît, Jaguenaud, Bernard. « Cyber : le danger vient-il de l'intérieur ? » in *Face au risque*, N°536, Octobre 2017, p. 9 à 17.
  Résumé: Suite à l'explosion des attaques de ransomwares en 2016, ce dossier fait le point sur le risque numérique en présentant les avancées en matière de cybersécurité mais également les défaillances qu'il reste à réguler.

- Dufour, Nicolas. « Fonctionnement d'une cellule de crise cyber » in *Face au risque,* N°580, Mars 2022, p.12 à 14.
  Résumé: L'article présente les différents volets envisagés et les enjeux associés à la mise en place d'une cellule de crise cyber et notamment à partir de l'exemple d'une ETI victime d'un rançongiciel.

- Haas, Patrick. « Gestion de crise : un métier florissant » in *Face au risque*, N°561, Avril 2020, p. 38 à 40.
  Résumé: L'article propose un focus sur la gestion de crise à laquelle les entreprises et organisations sont de plus en plus sensibilisées, en raison des nombreux risques auxquels elles sont exposées (risques sanitaires, cyberattaques, incendies...) et sur le métier florissant de consultant en gestion de crise.

- Kapp, David. « Cyberattaque contre l'entreprise de sécurité Gunnebo » in *Face au risque*, N°572, Mai 2021, p. 13 à 15.
  Résumé: Le 25 août 2020 l'entreprise Gunnebo est piratée par des hackeurs. Ils utilisent un nouveau type de ransomware surnommé " Mount Locker " par les experts. Il cible les grosses entreprises, bloque et encrypte les ordinateurs et oblige la Suède à se doter d'un centre national de cybersécurité en février 2021.

- Kapp, David. « Les cyberattaques montent en gamme » in *Face au risque*, N°574, Juillet-Août 2021, p. 16 à 18.
  Résumé: L'article présente les différents types de cyberattaques qui sont désormais plus élaborées. Elles font appel à de l'ingénierie sociale et nécessitent la formation et l'information des salariés qui peuvent être pris pour cible.

Ouvrages :

- Billois, Gérôme, Cougot, Nicolas, Garnier, Pascal. *Cyberattaques : les dessous d'une menace mondiale*. Vanves : Hachette, 2022, 239 p.
  Résumé : " Hyperconnecté, chacun d'entre nous est une proie des pirates du numérique, capables d'entrer sur nos comptes, de voler nos données personnelles, de bloquer entreprises et gouvernements. Au-delà de simples individus, c'est un réseau complexe de cyberattaquants qui s'est développé à grande échelle. À partir d'histoires saisissantes, vécues sur le terrain, Gérôme Billois décrypte cet écosystème :
  - De l'origine des cyberattaques jusqu'aux événements géopolitiques et économiques majeurs d'aujourd'hui.

- Les profils des cyberattaquants et leurs motivations, entre idéologie, gain financier, espionnage et guerre numérique.
- L'écosystème des attaquants : les chercheurs de failles et les marchés noirs cyber.
- Les défenseurs du numérique : leurs rôles, leurs motivations et leur quotidien, avec en prime les conseils pour sécuriser vos équipements et réagir en cas de problème.
- Le futur de la cyberconflictualité dans un monde toujours plus connecté et complexe géopolitiquement.

Un documentaire captivant et éclairant sur les affrontements entre attaquants et défenseurs du numérique, face à la plus grande menace de la prochaine décennie. "

- Faillet, Caroline, Rosnay, Joël de, etc. *L'art de la guerre digitale : survivre et dominer à l'ère du numérique*. Malakoff : Dunod, 2016, X-226 p.
  Résumé : " Ubérisation, bad-buzz... Engagées dans une guerre digitale dont elles ne maîtrisent ni les armes, ni les techniques de défense, les organisations sont contraintes d'adapter leur arsenal de riposte. À la manière de L'Art de la guerre de Sun Tzu, Caroline Faillet les exhorte à renoncer à l'attaque frontale et propose des stratégies de disruption et d'influence pour renforcer leurs positions et gagner en performance. "

- Weber, Cécile. *Plan de continuité des activités et gestion de crise : résilience, le défi des nouvelles menaces*. La Plaine Saint-Denis : AFNOR, DL 2020, XIV-200 p.
  Résumé: " Comment les entreprises et les organismes publics peuvent-ils faire face à des crises d'ampleur sans précédent, créant complexité et effets dominos, potentiellement dévastateurs ? Dans un environnement de plus en plus instable, les organismes doivent s'engager dans la construction de dispositifs de résilience, véritables leviers stratégiques, pour atténuer les impacts de crises majeures, exposant dangereusement leur fonctionnement, voire leur pérennité. Ce livre-outil décrit tout d'abord la méthodologie de construction du plan de continuité des activités et du plan de gestion de crise, avec une approche volontairement pragmatique, à l'aide d'outils et d'illustrations opérationnels. Il évoque ensuite le nouveau paradigme de résilience qui émerge dans notre société technologique face à des enjeux sociétaux inédits et surtout des menaces systémiques, variées, interconnectées (cyber, climatique, accès aux ressources, géopolitique, sûreté, etc.), amplifiées par une pression médiatique. Cet ouvrage propose, enfin, une approche originale, au travers de dispositifs de résilience " augmentés ", intégrant notamment innovations technologiques, capacités et coopérations audacieuses. "

Mémoires :

- Cuq, Jean-Baptiste, Bianco, Patrick, Carbonnel, Aurélien, Lehmann, Cindy, Witrowski, Hélène, Bchini, Samir. *Anticiper les cybermenaces pour garantir la continuité opérationnelle du SDIS*. Aix-en-Provence : École Nationale Supérieure des Officiers Sapeurs-Pompiers (ENSOSP), 2021, 45 p.
  Rapport de gestion de projet réalisé dans le cadre du module " Manager des risques de la sécurité civile " de la formation d'adaptation à l'emploi de Capitaines FAC 2021-01

- Héritier, Nicolas, Leger, Florent, Maestracci, François-Marie, Seitz, Michel, Noygues, Xavier. *Les cyber attaques dans les SIS : comment réagir ?*. Aix-en-Provence : École Nationale Supérieure des Officiers Sapeurs-Pompiers (ENSOSP), 2021, 124 p.
  Résumé: " Dans notre monde hyper connecté, la problématique des cyberattaques est devenue omniprésente et impose désormais une vigilance permanente notamment pour les services d'incendie et de secours devenus particulièrement vulnérables compte tenu de la sensibilité de leurs missions. Grâce aux partages d'expérience avec les institutions ayant vécu ce type d'attaque et à la richesse des entretiens réalisés avec des personnalités faisant référence au niveau national dans le domaine de la cyber sécurité, nos travaux se sont attachés à développer une analyse du niveau de sensibilité et de prise en considération du risque cyber par les personnels des SIS, qu'ils soient simples utilisateurs, techniciens, ingénieurs informatiques, ou dirigeants. Les aspects purement informatiques et techniques ne sont pas traités dans ce mémoire et peuvent à eux seuls faire l'objet d'un sujet de recherche à part entière. Il nous est apparu nécessaire, dans cette société « cyber sauvage » où une nouvelle forme de criminalité se développe à grande échelle, de comprendre les enjeux de déstabilisation potentielle des SIS, de réfléchir à un outil utile aux services permettant de comprendre les phénomènes en les vulgarisant et en proposant un vade-mecum destiné à la préparation d'une gestion de crise cyber tout en mettant à profit le savoir-faire des sapeurs-pompiers en matière de gestion opérationnelle et de commandement en situation de crise. C'est notre objectif pour augmenter la résilience, consolider notre capacité à assurer les missions des soldats du feu, de l'environnement et plus globalement de la vie. "