LA PRÉVENTION DES RISQUES EN ENTREPRISE

Prévenir et gérer les cyber-risques

Livre Blanc n°5

Manuel Dorne, plus connu sous le pseudonyme de Korben, *est un blogueur français spécialisé dans l'informatique, la cybersécurité et la culture geek. Il écrit sur son blog Korben.info pour plus d'un million de lecteurs par mois et participe à plusieurs podcasts dont Le Rendez-Vous Tech. Entrepreneur, il est cofondateur de la société RemixJobs, portail d'emploi spécialisé dans les métiers du Web et YesWeHack, plate-forme dédiée à la cybersécurité.*

Préface

Avec l'augmentation de la présence des petites et grandes entreprises sur Internet, les risques en matière de cybercriminalité n'ont jamais été aussi élevés. Les grands groupes comme les PME sont dans le collimateur des cybercriminels et malheureusement, quand le couperet tombe, il est trop tard. La cybersécurité est donc un enjeu stratégique à ne pas négliger si l'on veut que l'entreprise perdure. Et il sera toujours plus coûteux d'intervenir après un incident que de manière préventive en anticipant les risques.

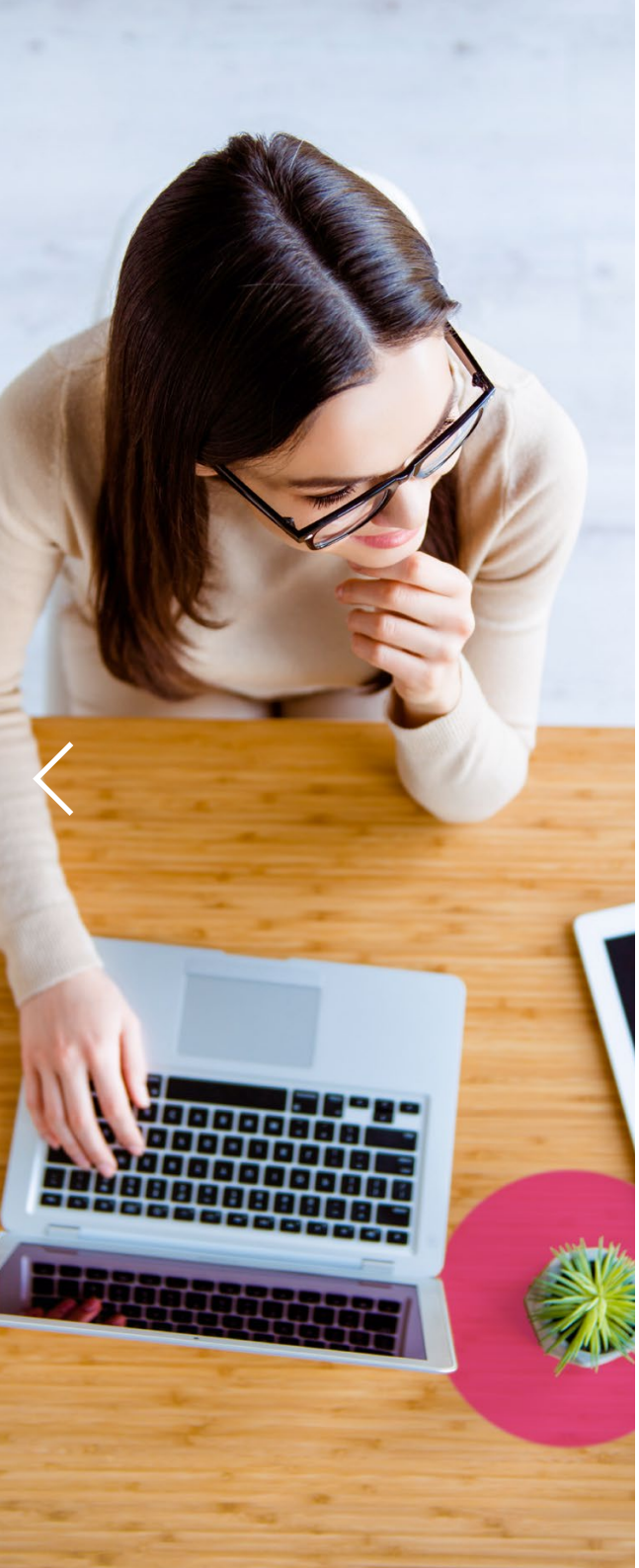
En effet, les répercussions suite à une mauvaise gestion des risques cyber sont nombreuses, imprévisibles et il est difficile de les chiffrer en amont.

Toutefois, résumer la cybersécurité à un panel de solutions techniques à mettre en place est une vision trop simpliste de celle-ci. La cybersécurité est un ensemble d'outils, de techniques, de connaissances et de bonnes pratiques qui permettent de réduire au maximum les risques.

Chacun doit se sentir concerné par sa propre cybersécurité et c'est en formant un bloc solide, cohérent et conscient que nous pourrons résister au mieux aux attaques et faire monter le niveau de sécurité global.

Ce livre blanc est donc un bon point de départ pour comprendre les risques auxquels vous êtes exposés et il saura vous donner les pistes pour prévenir les plus courants. Bonne lecture à tous !

Korben



SOMMAIRE

COMPRENDRE LES CYBER-RISQUES

QUELS ENJEUX POUR VOTRE ENTREPRISE ?

175 milliards de téraoctets : c'est le volume de données qui devrait être stocké en 2025 dans le monde entier[1]. Cette perspective s'annonce réjouissante pour les hackers. Mais pour les entreprises, cibles potentielles, elle rappelle l'importance des questions de cybersécurité. Et les enjeux sont d'autant plus forts que la dépendance aux outils numériques continue de grandir parmi les professionnels, que le recours au Cloud se généralise et que les objets connectés se multiplient.

AVANT TOUTE CHOSE, QU'EST-CE QUE LES CYBER-RISQUES ?

Les cyber-risques désignent **toute atteinte aux systèmes informatiques (SI) et de communication, ainsi qu'aux données** stockées ou en transfert. Ces sinistres, de nature à bloquer le fonctionnement de l'entreprise, peuvent être le fait :

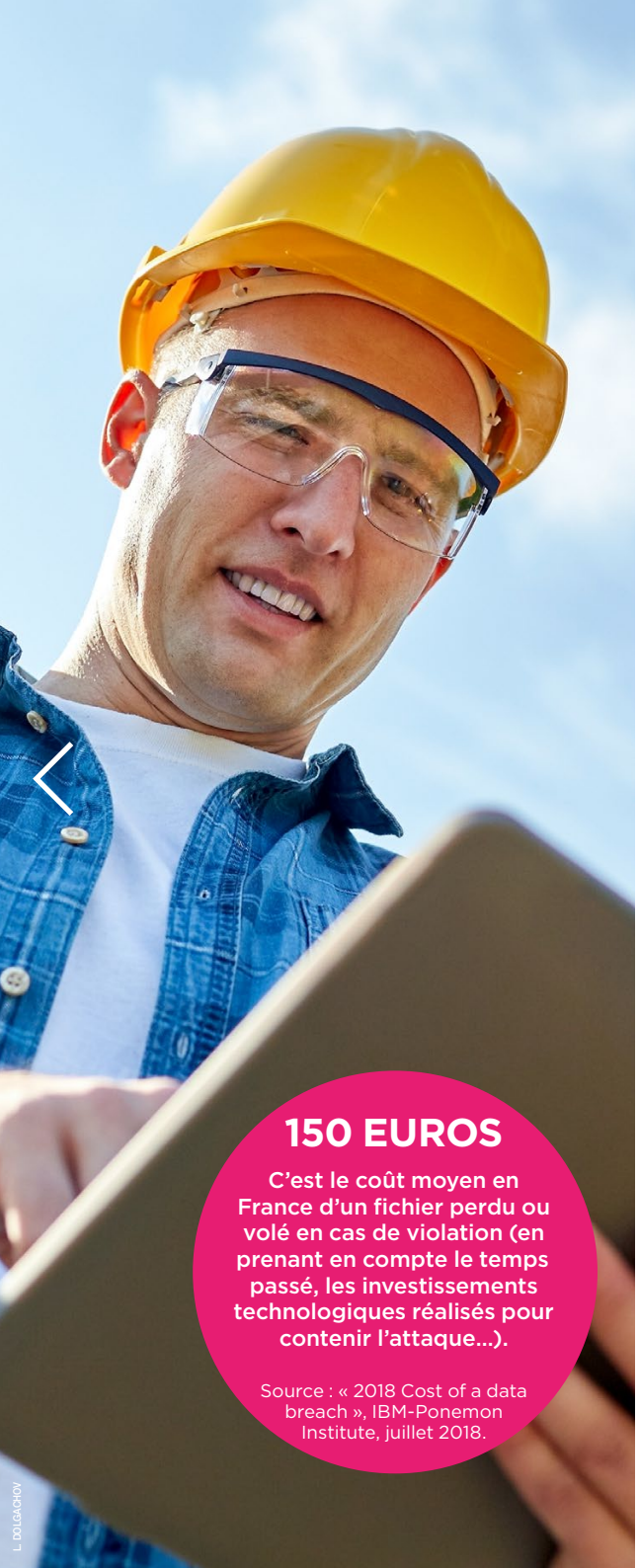
- d'actes malveillants, réalisés essentiellement à des fins pécuniaires (dérober ou bloquer des informations pour les revendre ou exiger des rançons…). Mais certains pirates peuvent aussi avoir pour seul objectif de saboter l'activité d'une société en provoquant l'arrêt de la production et en nuisant à son image ;
- d'erreurs humaines involontaires ;
- de dysfonctionnements techniques (panne, bug…).

Plus précisément, les cyberattaques peuvent prendre différentes formes : hameçonnage*, fraude informatique, rançongiciel*, déni de service*… Mais elles ont toutes en commun de commencer le plus souvent par un simple mail, premier vecteur de propagation des attaques informatiques[2].

De fait, cette menace mérite une grande attention : **en janvier 2019, 80 % des entreprises déclaraient avoir été victimes d'au moins une attaque au cours des 12 derniers mois.** 59 % d'entre elles ont même constaté un impact sur leur business (ralentissement ou arrêt de la production, indisponibilité du site web…). Un chiffre en hausse de 10 points sur un an[3].

(1) « Data Age 2025 » IDC – Seagate, novembre 2018.
(2) « Rapport Cisco Cybersécurité 2019 ».
(3) « Baromètre de la cybersécurité des entreprises », Cesin - Opinion Way, janvier 2019.
* Rendez-vous page 25 pour une définition de ce terme.

> « Les coûts liés aux activités cybercriminelles représentent environ 600 milliards de dollars par an. En mettant cela en face de l'économie mondiale d'Internet, estimée à plus de 4 billions de dollars par an, le cybercrime peut être considéré comme une « taxe invisible » de 14 % par an. »
>
> *Korben*
> Source : « L'impact économique du cybercrime », McAfee 2018.



150 EUROS

C'est le coût moyen en France d'un fichier perdu ou volé en cas de violation (en prenant en compte le temps passé, les investissements technologiques réalisés pour contenir l'attaque…).

Source : « 2018 Cost of a data breach », IBM-Ponemon Institute, juillet 2018.

L. DOUGKOV

UN ENJEU FINANCIER POUR L'ENTREPRISE

Le système d'information de votre entreprise est atteint ? **Vous allez devoir engager des actions sans attendre pour limiter la propagation des dommages** et permettre la reprise de l'activité au plus vite. La gestion du sinistre représente donc d'abord un enjeu financier direct puisqu'il va s'agir de sécuriser les données, d'informer les clients, de faire appel à des avocats et à des experts en relation publique... À cela s'ajoute la perte de chiffre d'affaires susceptible d'être enregistrée en attendant le rétablissement complet du système. Un rétablissement dont le délai est estimé en moyenne à 69 jours une fois la violation de données détectée(1).

Au-delà des conséquences immédiates et pour une évaluation juste du coût des risques cyber, il faut aussi prendre en compte les impacts indirects (sur une durée plus ou moins longue selon l'ampleur de la crise), comme la perte de confiance de la part des clients et des partenaires, les sanctions financières appliquées en cas de défaut de sécurité, la divulgation d'informations portant atteinte à votre compétitivité... Au total, en moyenne, **les entreprises françaises évaluent leurs pertes à 9,36 % de leur chiffre d'affaires en cas de violation de sécurité(2).**

UN ENJEU POUR L'IMAGE DE VOTRE ENTREPRISE ?

Les consommateurs sont aujourd'hui soucieux de la protection de leurs données. C'est un fait que l'on doit en partie à l'actualité récente, ponctuée d'événements au retentissement mondial : les vagues massives de cyberattaques en 2017 (WannaCry, NotPetya), le scandale Cambridge Analytica (début 2018)... Désormais, 2 citoyens sur 3 dans le monde se disent méfiants envers l'utilisation de leurs données personnelles. Seuls 36 % ont un sentiment de sécurité vis-à-vis du traitement de ces informations par les différents types d'organisations (entreprises, gouvernement...)(3).

Autrement dit, la confiance de vos clients, lorsqu'elle vous est accordée, constitue **un capital précieux mais aussi fragile.**

À l'heure des réseaux sociaux, toute violation de votre système d'information peut avoir des retombées dévastatrices sur l'image de marque de votre entreprise. Un cabinet de conseil en a fait l'expérience en 2017, quand des pirates informatiques ont utilisé l'identifiant et le mot de passe d'un compte administrateur pour accéder aux serveurs mails et à certaines informations sensibles. Dans cette opération, plusieurs clients ont vu leurs données compromises. Précisons que cette société était experte... en cybersécurité. Sa crédibilité se trouva mise en doute, en particulier pour la faiblesse des mécanismes de protection qui avait permis cette intrusion.

(1) « 2018 Cost of a data breach », IBM-Ponemon Institute, juillet 2018.
(2) « Rapport Risk:Value 2018 », NTT Security.
(3) « Rapport Global Citizens Data Privacy », Ipsos et Forum économique mondial, janvier 2019.

> « En plus des aspects techniques, il faudra aussi tenir compte des coûts en ressources humaines, des impacts directs sur le chiffre d'affaires, des retombées en termes d'image de marque ou dans la presse, voire de l'évolution du cours en bourse pour les entreprises cotées, et bien sûr des impacts juridiques liés. »
> *Korben*

V. MERKUSHEV

UN ENJEU LÉGAL, NOTAMMENT VIS-À-VIS DES DONNÉES PERSONNELLES

Le 25 mai 2018 est entré en vigueur le RGPD (Règlement Général sur la Protection des Données). Il concerne toutes les entreprises dès lors qu'elles manipulent des données personnelles, c'est-à-dire relatives aux personnes physiques identifiées ou identifiables, directement (par leur nom…) ou indirectement (par un numéro de téléphone, un numéro client…).

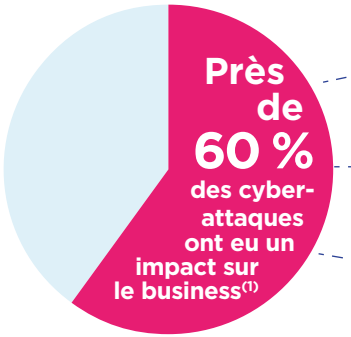
Ce règlement vise à renforcer les droits des utilisateurs (droits d'accès aux données, d'opposition, d'effacement, de portabilité…). Il entend, par ailleurs, **responsabiliser les acteurs impliqués dans le traitement des données personnelles.** À cette fin, il oblige les entreprises mais aussi leurs sous-traitants à prouver leur « accountability », c'est-à-dire à mettre en place des procédures internes destinées à démontrer le respect des règles.
Le RGPD prévoit aussi la réalisation d'une Analyse d'Impact relative à la Protection des Données (AIPD) si leur traitement est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes concernées.
Enfin, autre point notable : si vous constatez une violation de sécurité, vous devez en informer la CNIL et selon les cas, les usagers touchés.
L'absence de conformité au RGPD vous expose à **des sanctions pouvant atteindre 20 millions d'euros ou 4 % de votre chiffre d'affaires annuel mondial.**

UN DPO POUR VEILLER À VOTRE CONFORMITÉ AU RGPD ? **Le délégué à la protection des données (appelé également DPO) fait partie des nouveautés introduites par le RGPD. Sa désignation est obligatoire pour certaines entreprises (comme celles qui réalisent un suivi régulier des personnes à grande échelle) et reste simplement recommandée à toutes les autres.**
Son rôle : conseiller les dirigeants sur leurs obligations légales en matière de protection des données, contrôler le respect de la réglementation, mais aussi coopérer avec l'autorité de contrôle, à savoir la CNIL.

> « Malheureusement, quand le couperet tombe, il est souvent trop tard. Et, pour les plus petites entreprises, qui sont aussi les plus fragiles, cela peut prendre des années pour se relever, voire signer leur arrêt de mort. »
> *Korben*

CYBER-RISQUES : UNE MENACE À PRENDRE EN COMPTE DANS TOUTES LES ENTREPRISES

8 ENTREPRISES SUR 10 SUBISSENT AU MOINS 1 ATTAQUE PAR AN[1]



- Un ralentissement de production
- Une indisponibilité du site web
- Un retard de livraison...

1 200 à 1 300
NOTIFICATIONS DE VIOLATIONS DE DONNÉES PERSONNELLES EN FRANCE, DEPUIS L'ENTRÉE EN VIGUEUR DU RGPD[2]

LES ATTAQUES LES PLUS FRÉQUENTES[1]

CHAQUE MINUTE, **9** NOUVEAUX LOGICIELS MALVEILLANTS DÉTECTÉS[3]

À L'ORIGINE DES VIOLATIONS DE DONNÉES... :

- **48 %** LES ACTES MALVEILLANTS
- **27 %** L'ERREUR HUMAINE (SALARIÉ, FOURNISSEUR...)
- **25 %** LA DÉFAILLANCE DU SYSTÈME[4]

Sources :

(1) « Baromètre de la cybersécurité des entreprises », Cesin - Opinion Way, janvier 2019.
(2) CNIL, janvier 2019.
(3) « Malware report 1er semestre 2018 », G DATA, septembre 2018.
(4) « 2018 Cost of a data breach », IBM-Ponemon Institute, juillet 2018.

SY_SARAYUT

PRÉVENIR LES RISQUES INFORMATIQUES

L'HAMEÇONNAGE ET LE HARPONNAGE

L'une des premières cyberattaques remonterait à 1988, quand le ver* informatique Morris a mis hors service, en 24 heures, 6 000 machines connectées à Internet(1). Depuis, les pirates informatiques n'ont cessé de se distinguer par leur inventivité, comme le prouvent les 2 millions de nouveaux types de logiciels malveillants* identifiés au cours du seul 1er semestre 2018(2). Pour vous aider à y voir plus clair, voici un panorama des principaux risques cyber et les mesures à mettre en place pour les combattre, en commençant par l'hameçonnage.

DE QUOI PARLE-T-ON ?

L'hameçonnage* (ou « phishing » en anglais) et le harponnage* (ou « spear-phishing » en anglais) consistent à **dérober des données personnelles (mots de passe, identifiants bancaires…) en apaisant la méfiance de la victime**. Pour y parvenir, les pirates se font passer pour des tiers de confiance dont la légitimité n'est pas discutable : administration, banque, assurance, opérateur téléphonique, fournisseur d'énergie…

HAMEÇONNAGE ET HARPONNAGE : ATTENTION À NE PAS CONFONDRE ! Tandis que le premier repose sur des envois massifs, le second est, lui, personnalisé. D'où sa redoutable efficacité.

La prise de contact peut s'effectuer par différents biais : un courriel ou un message via les réseaux sociaux ou les messageries instantanées qui renvoie sur une page de site web aux couleurs d'une entreprise ou d'une administration… Mais l'approche est toujours la même. Il s'agit de contraindre la victime à rapidement fournir les données réclamées, sans réfléchir :

- soit en l'appâtant — trop perçu à récupérer auprès d'une administration, par exemple ;
- soit en l'inquiétant — codes d'accès perdus par une banque, amende à régler sans délai auprès de l'administration…

Ce type d'attaque s'est propagé en même temps que s'est développé l'usage des courriels et d'internet, jusqu'à devenir celui le plus fréquemment rencontré par les entreprises(3).

LES CYBERATTAQUES À SURVEILLER EN 2019 ?

- **Le piratage des données hébergées dans le Cloud**
- **Le cryptojacking (les pirates génèrent de la cryptomonnaie à partir des terminaux des internautes, en tâche de fond, sans leur consentement)**
- **Les campagnes de harcèlement et d'extorsion menées contre les entreprises par des robots, via les réseaux sociaux**

Source : « Prévisions 2019 en matière de menaces », McAfee Labs, décembre 2018.

(1) « The Morris Worm, 30 years since first major attack on the internet », FBI.gov, 2 novembre 2018.
(2) « Malware report 1er semestre 2018 », G Data, septembre 2018.
(3) « Baromètre de la cybersécurité des entreprises », Cesin - Opinion Way, janvier 2019.
* Rendez-vous page 25 pour une définition de ce terme.

Prévenir les risques informatiques

UN EXEMPLE DE TENTATIVE D'HAMEÇONNAGE

Un salarié d'une entreprise de logistique reçoit un mail d'un expéditeur qu'il croit être son fournisseur. Il ouvre la pièce jointe, porteuse d'un programme malveillant. Le système d'information, dont certains logiciels n'ont pas été mis à jour, se trouve paralysé. La société ne peut plus assurer les livraisons de marchandises de ses clients. Il est nécessaire de faire appel à des prestataires extérieurs et de réutiliser d'anciens logiciels, pour redémarrer l'activité en mode dégradé.

RECONNAÎTRE LES TENTATIVES D'HAMEÇONNAGE

Quelques bons réflexes méritent d'être rappelés à vos salariés :

- **jamais une administration ou une entreprise ne demande d'informations personnelles sensibles par courriel, SMS ou téléphone.** Si cela arrive, il ne faut surtout pas les communiquer et contacter directement l'organisme concerné (sans utiliser les coordonnées fournies dans le courriel ou le SMS douteux) ;

- si le courriel renvoie vers un site internet dont vous doutez de l'authenticité, **aucune opération ne doit être effectuée sans avoir vérifié que l'adresse Internet (nom + extension) est conforme à celle consultée habituellement**. Pour le savoir, il suffit d'ouvrir une seconde page dans le navigateur et de rechercher le site de l'institution en question en utilisant un moteur de recherche.

COMMENT RÉAGIR ?

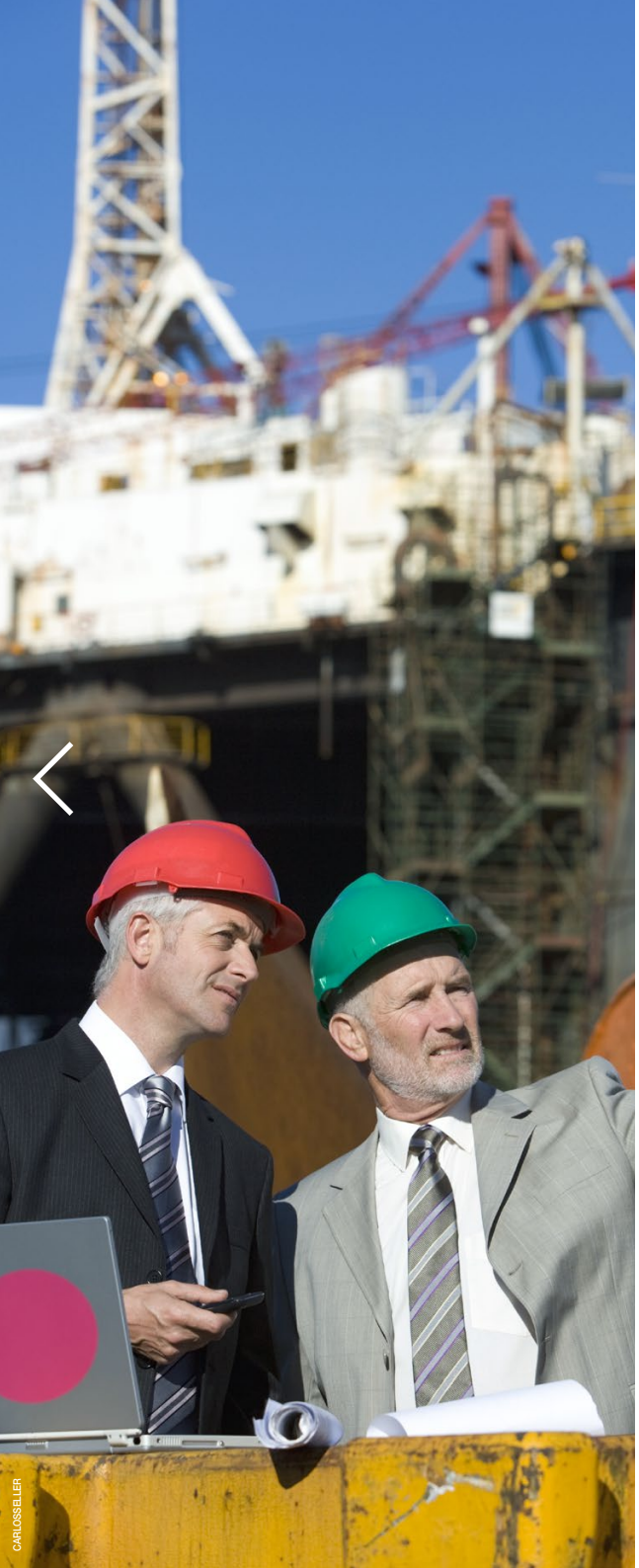
Vous vous êtes fait dérober des données sensibles. Vous devez immédiatement :

- faire opposition s'il s'agit de données bancaires et alerter la direction financière de l'entreprise ;
- prévenir le directeur des systèmes d'information (DSI) si l'accès au réseau est compromis ;
- contacter votre Agent Général MMA si vous avez une assurance Cyber-risques MMA ;
- déposer une plainte.

3 ENTREPRISES SUR 10 VICTIMES DE VOL D'IDENTIFIANTS[1]

Les combinaisons de mails et de mots de passe sont une cible de choix pour les cybercriminels. En effet, il n'est pas rare, par souci de facilité, de réutiliser les mêmes identifiants pour différents comptes. Alors pour éviter la multiplication des attaques informatiques à l'encontre de vos données, pensez à utiliser des codes uniques pour chacune de vos applications personnelles et professionnelles.

(1) « Baromètre de la cybersécurité des entreprises », Cesin - Opinion Way, janvier 2019.


CARLOSSELLER

LA FRAUDE INFORMATIQUE

Souvent dévastatrice, la fraude informatique consiste le plus souvent à usurper l'identité d'une personne de confiance après une utilisation non autorisée d'un système d'information, afin d'obtenir le versement d'une somme d'argent importante.

DE QUOI PARLE-T-ON ?

Pour une entreprise, il s'agit des pertes de fonds lui appartenant ou qui lui sont confiés en raison de son activité professionnelle.
Ces pertes de fonds sont consécutives à une fraude, un détournement, une escroquerie, avec une utilisation non autorisée du système d'information de l'entreprise.

Pour préparer leur attaque, les malfaiteurs :

- **lancent une campagne de harponnage***, pour récupérer des identifiants ou installer un programme malveillant qui permettra de s'introduire dans le système informatique de l'entreprise. Objectif : dérober des informations — factures en cours, coordonnées des partenaires, RIB, numéros de carte bancaire… —, voire pirater des boîtes mails ;
- **étudient la société et son fonctionnement** à travers son organigramme, ses partenaires ou encore l'emploi du temps du dirigeant :
  - en effectuant de simples recherches en ligne, sur les sites d'actualité, les réseaux sociaux… ;
  - et/ou en téléphonant, en prétextant un sondage par exemple.

* Rendez-vous page 25 pour une définition de ce terme.

UN EXEMPLE DE FRAUDE INFORMATIQUE

Une société du secteur pétrolier est avertie par son expert-comptable d'un mouvement bancaire suspect. Elle constate en effet un virement depuis sa banque vers un compte qu'elle ne connaît pas, un nouveau bénéficiaire ayant donc été créé à son insu, suivi d'un virement.
Après investigations, il s'avère que des hackers ont trompé l'une des personnes de cette société en lui envoyant un mail frauduleux. Cette personne, en ouvrant la pièce jointe du courriel, a ainsi permis l'installation d'un logiciel malveillant* sur son poste informatique, permettant l'accès non autorisé au système d'information de l'assuré.
Les pirates ont alors pu saisir un ordre de virement du compte bancaire de la société vers leur compte.

AVEZ-VOUS PENSÉ À INTÉGRER LE CYBER-RISQUE DANS VOTRE PCA ?

Si un incident se produit, vous pourrez retrouver dans votre Plan de Continuité d'Activité (PCA) toutes les mesures à déployer pour réagir rapidement et de manière adéquate, maintenir votre activité et restaurer vos capacités de fonctionnement. Pour plus d'informations, reportez-vous au livre blanc « Établir un PCA » de MMA.

Prévenir les risques informatiques

COMMENT LIMITER LES RISQUES LIÉS À L'USURPATION D'IDENTITÉ ?

- **Sensibilisez les salariés** en leur présentant la mécanique de ce type de fraude ainsi qu'aux techniques d'hameçonnage* et de harponnage*. Les consignes de sécurité devant être plus que jamais appliquées pendant les périodes creuses de congés, notamment lorsque des collaborateurs prennent temporairement le relais de collègues absents ;
- En cas de mail douteux, **saisissez vous-même l'adresse de votre destinataire,** plutôt que de faire « répondre à » ;
- **Assurez la confidentialité des organigrammes** (et a minima, en extraire le nom et les coordonnées des responsables financiers et comptables) ;
- **Ne communiquez pas l'agenda des dirigeants** afin d'éviter que les fraudeurs profitent de leur absence pour agir ;
- **Limitez la communication de l'entreprise** autour de ses partenariats et de ses grands projets ;
- **Mettez en place une procédure de validation** comme par exemple, contacter directement le chef d'entreprise, un cadre... quand la demande est insolite et/ou portée par un interlocuteur inconnu faisant preuve d'insistance, de flatterie, d'intimidation... ;
- **Prévoyez un protocole de double signature** pour tout virement supérieur à une certaine somme ;
- **Assurez aux salariés qu'aucune sanction ne sera prise** à leur encontre s'ils venaient à différer l'exécution d'un ordre afin de vérifier qu'il émane vraiment d'un dirigeant ou d'un fournisseur.

* Rendez-vous page 25 pour une définition de ce terme.

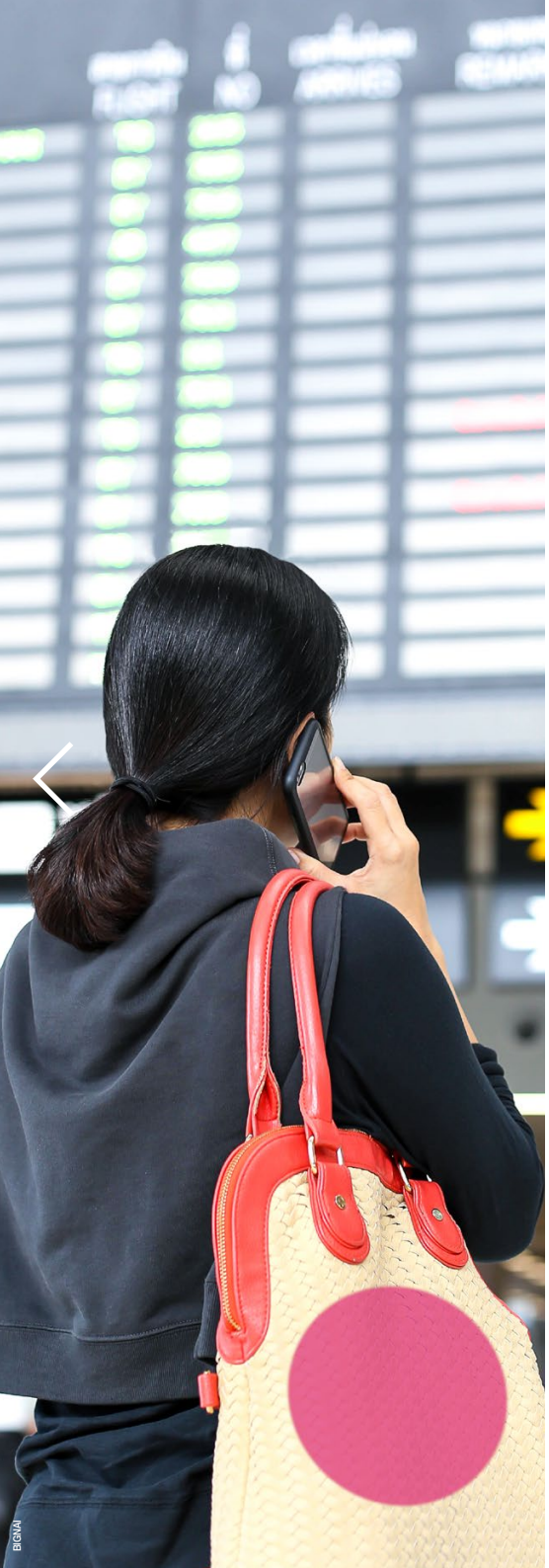
COMMENT RÉAGIR ?

Si le virement vient d'être effectué, il n'est peut-être pas trop tard.
Les banques disposent, en effet, d'une possibilité de rappel des fonds durant les premières heures qui suivent l'ordre. Sans attendre, il faut ainsi :

- alerter votre banque, y compris en dehors des heures d'ouverture, via leur numéro d'urgence ;
- saisir les autorités : la police dispose de services spécialisés ;
- le cas échéant, bloquer les coordonnées bancaires frauduleuses qui auraient pu être enregistrées dans vos logiciels ;
- contacter votre Agent Général MMA si vous avez une assurance Cyber-risques MMA. Il vous accompagnera dans la mise en place des premières mesures d'urgence et vous aidera à revenir au plus vite à un fonctionnement normal.

ON CHERCHE À VOUS MANIPULER !

La fraude informatique, mais aussi les campagnes d'hameçonnage* figurent parmi les exemples les plus connus « d'ingénierie sociale* » (« social engineering » en anglais), une technique qui consiste pour un escroc à manipuler psychologiquement ses cibles pour gagner leur confiance.



LES RANÇONGICIELS

Les rançongiciels* ont bénéficié d'une publicité particulière en 2017, lorsqu'une vague d'attaques spectaculaire a touché indifféremment les entreprises, les hôpitaux, les particuliers... partout dans le monde. Un bon prétexte pour rappeler que cette menace touche en réalité plus de 4 entreprises sur 10[1].

DE QUOI PARLE-T-ON ?

Les rançongiciels sont un type particulier de logiciel malveillant* qui, une fois installé sur une machine, chiffre les données qu'elle abrite pour les rendre inaccessibles. Une demande de rançon sera alors adressée à la victime par le pirate, en échange d'un code permettant de « libérer » les informations retenues en otage.

Comme les autres virus*, les rançongiciels peuvent « s'attraper » en cliquant sur une pièce jointe ou un lien internet, en affichant une page web piratée ou via l'exploitation d'une faille de sécurité détectée par les pirates dans l'un de vos logiciels (navigateur, système d'exploitation...). Leur propagation se trouve facilitée depuis quelques années par **des kits prêts à l'emploi, vendus sur le Darkweb*** (« Ransomware as a Service »).

En 2017, la gendarmerie a recueilli 218 plaintes présentant 28 rançongiciels différents[2]. En 2018, 44 % des entreprises déclaraient avoir fait face à cette menace[3]. Contrairement aux premiers rançongiciels qui opéraient par vagues massives et non ciblées, les pirates informatiques semblent maintenant s'intéresser en priorité aux entreprises jugées rentables, autrement dit les plus susceptibles de payer la rançon.

RANÇONGICIELS, VERS, VIRUS... : MÊME FAMILLE !

Les virus*, les vers*, les rançongiciels*, les chevaux de Troie... sont ce qu'on appelle des « logiciels malveillants » (ou « malware » en anglais). En un mot, ce sont des programmes développés pour nuire à un tiers (chiffrement et vol de données, espionnage...) et propagés à l'aide de campagnes d'hameçonnage* ou de harponnage* le plus souvent. Une pratique tend à se généraliser : l'attaque sans fichier (« fileless attack » en anglais), qui ne nécessite plus de télécharger un fichier exécutable infecté. Leur détection n'en est alors que plus difficile.

GARE AU « SHADOW IT* » !

Lorsque des salariés jugent votre politique sécuritaire trop excessive ou vos solutions techniques inadaptées, ils peuvent être tentés de recourir à des outils de contournement, autrement dit d'utiliser des logiciels non autorisés et non testés par votre DSI. C'est ce qu'on appelle le « shadow it ». Cette pratique n'est pas sans présenter un danger sur votre système d'information. Pour en limiter le développement, il est conseillé de rester à l'écoute des besoins de vos collaborateurs et de veiller à trouver le bon curseur entre sécurité et confort d'utilisation.

(1) « Baromètre de la cybersécurité des entreprises », Cesin - Opinion Way, janvier 2019.
(2) « Etat de la menace liée au numérique en 2018 », Ministère de l'intérieur, mai 2018.
(3) « Baromètre de la cybersécurité des entreprises », Cesin - Opinion Way, janvier 2019.
* Rendez-vous page 25 pour une définition de ce terme.

QUELQUES MILLIERS D'EUROS

C'est le montant moyen des rançons demandées par les pirates informatiques, selon MMA.

Prévenir les risques informatiques

UN EXEMPLE D'ATTAQUE PAR RANÇONGICIEL*

Un aéroport britannique fait l'objet d'une attaque d'un rançongiciel. Pendant deux jours, les écrans d'affichage en temps réel sont hors service, pour limiter la propagation des dommages et réparer le SI. Le personnel doit recourir à des tableaux blancs pour informer les voyageurs sur le statut de leurs vols.

DES ACTIONS DE PRÉVENTION

Pour limiter les risques d'être victime d'un rançongiciel, vous devez :

- **mettre régulièrement à jour les systèmes d'exploitation,** les antivirus et les pare-feu* ;
- ne jamais ouvrir des courriels dont la provenance ou la forme est douteuse. Les courriels sont le mode de contamination « favori » des rançongiciels ;
- interdire l'installation de logiciel sans l'accord de la DSI ;
- éviter de naviguer sur des sites non sûrs ;
- **effectuer des sauvegardes régulières des données de l'entreprise sur des supports non connectés** en permanence aux machines. En cas d'attaque, vous pourrez ainsi effectuer un formatage et réinstaller les données ;
- limiter les droits d'accès des machines sur les serveurs de l'entreprise, un ordinateur infecté pourra ainsi, plus difficilement, contaminer votre SI.

* Rendez-vous page 25 pour une définition de ce terme.

COMMENT RÉAGIR ?

Si votre entreprise est victime d'une attaque de rançongiciel, il est conseillé :

- de déconnecter immédiatement du réseau toute machine infectée ;
- d'alerter sans attendre les services informatiques internes ou votre prestataire ;
- de sauvegarder les fichiers importants sur un support isolé. Prendre soin de ne pas écraser la dernière sauvegarde au cas où les fichiers en cours de copie seraient altérés ou déjà infectés ;
- de ne pas payer la rançon ;
- d'alerter votre Agent Général MMA si vous avez une assurance Cyber-risques MMA ;
- de porter plainte.

BESOIN D'UNE MISE À NIVEAU SUR LES QUESTIONS DE CYBERSÉCURITÉ ?

Vous trouverez en ligne de nombreuses ressources à destination des chefs d'entreprise comme des salariés :
- le MOOC de l'ANSSI sur la sécurité du numérique ;
- les kits de sensibilisation disponibles sur le site cybermalveillance.gouv.fr.

Par ailleurs, MMA, en lien avec des entreprises spécialisées dans le domaine, peut aussi vous accompagner dans la mise en place d'actions de formation. N'hésitez pas à vous rapprocher de votre Agent Général MMA !

LE DÉNI DE SERVICE

L'objectif premier des pirates qui lancent une attaque en déni de service est de nuire au bon fonctionnement d'un serveur informatique en le bombardant de requêtes. Le service rendu par la machine ciblée peut alors être fortement dégradé, voire totalement indisponible.

DE QUOI PARLE-T-ON ?

Une attaque par déni de service peut provenir d'une source unique ou de plusieurs machines. On parle alors de déni de service distribué. Dans cette hypothèse, la plus fréquente, le pirate va agir en 2 temps :

- d'abord en contaminant un maximum d'ordinateurs connectés à Internet avec un programme malveillant spécifique ;
- ensuite, en lançant l'attaque en direction du serveur. À ce moment-là, toutes les machines contaminées, constituant un réseau appelé « réseau de machines zombies » ou « botnet », lui adresseront simultanément des requêtes afin de le « noyer ».

Sans surprise, **plus le réseau de machines zombies est important, plus l'attaque sera massive et dévastatrice.**
Un déni de service peut temporairement affecter le fonctionnement d'un site Internet, sans parler des conséquences en termes d'image et de notoriété.
La motivation des pirates informatiques est notamment financière, la victime se voyant demander de payer une somme d'argent pour faire cesser les attaques. En 2017, 1 800 attaques de ce type auraient été enregistrées(1) chaque jour. Les secteurs les plus touchés étant les plate-formes d'e-gaming et le e-commerce.

UN EXEMPLE D'ATTAQUE PAR DÉNI DE SERVICE

Un hébergeur web est victime d'une attaque soudaine qui rend ses serveurs indisponibles pendant quelques minutes. Sa responsabilité civile est mise en cause, les sites internet de ses clients se trouvant eux aussi hors service.

QUELQUES MESURES PRÉVENTIVES

Il est très difficile de prévenir un déni de service. Toutefois, quelques solutions techniques permettent de limiter l'impact des attaques :

- utiliser des pare-feu* et les répartiteurs de charge ;
- utiliser des matériels de filtrage spécifiques programmés pour se déclencher en cas de variation significative et imprévue du trafic ;
- recourir aux services de protection anti-déni de service proposés par votre hébergeur.

VOUS POURRIEZ PARTICIPER À UN DÉNI DE SERVICE…
Si elles venaient à être contaminées, les machines de votre entreprise pourraient se transformer en machines zombies et prendre part à un déni de service. Dans cette hypothèse, l'entreprise pourrait voir sa responsabilité engagée. Bien protéger chaque ordinateur (antivirus, filtrage du trafic en sortie…) est donc indispensable.

COMMENT RÉAGIR ?

Plusieurs actions doivent être menées en cas d'attaque de déni de service :

- identifier les équipements visés et si possible, la source de l'attaque afin de la bloquer ;
- solliciter l'hébergeur ou le fournisseur d'accès pour filtrer le trafic en amont ;
- prévenir votre service de communication pour qu'il participe à la gestion de crise ;
- alerter votre Agent Général MMA si vous avez une assurance Cyber-risques MMA ;
- porter plainte.

(1) « Les années passent, pas la menace : les attaques DDoS observées par OVH en 2017 », 25 janvier 2018.
* Rendez-vous page 25 pour une définition de ce terme.

VOTRE SI RÉSISTERAIT-IL À UNE CYBERATTAQUE ?

Ne vous posez plus la question ! Faites appel à une société spécialisée en cybersécurité. Elle réalisera des tests d'intrusion* pour détecter toute faille de sécurité et vous permettre d'effectuer les correctifs nécessaires avant qu'un (vrai) pirate informatique ne la repère.

M. PABA

LE VOL DE DONNÉES, EN PARTICULIER PENDANT UN DÉPLACEMENT

Télétravail, déplacements professionnels, utilisation des outils personnels à des fins professionnelles (et vice-versa)… : les nouveaux usages au sein du monde de l'entreprise représentent un défi de taille, celui de devoir sécuriser chacun des supports (ordinateurs, tablettes, smartphones…) pour garantir l'intégrité du SI.

DE QUOI PARLE-T-ON ?

Le vol de données est loin d'être un risque anecdotique. **Au cours du 1er semestre 2018, 3,3 milliards de données à caractère médical, bancaire… auraient été volées,** compromises ou perdues. Soit une hausse de 72 % par rapport à la même période en 2017. Les actes malveillants externes en seraient les principaux responsables(1).

À cet égard, la tendance à travailler en mobilité, depuis n'importe où, suppose une attention particulière. En effet, en déplacement, la tentation est grande de se connecter aux réseaux wi-fi publics de l'aéroport, de la gare, de l'hôtel… Or, les dangers sont réels. Le plus courant étant l'attaque dite de « l'homme du milieu », à travers laquelle le pirate intercepte les données échangées entre deux systèmes (par exemple, entre votre navigateur et le site internet consulté). Et cela, sans que vous ne vous en rendiez compte.

Une autre habitude, de plus en plus répandue, appelle également à la vigilance : celle qui consiste à utiliser ses terminaux personnels à des fins professionnelles, et vice-versa.
Tout l'enjeu est ici d'**éviter la fuite de données en raison de la perte ou du vol de l'ordinateur d'un collaborateur,** de la propagation d'un virus* au SI de l'entreprise depuis un outil personnel insuffisamment sécurisé…

QUE DEVIENNENT VOS DONNÉES, UNE FOIS DÉROBÉES ? Les pirates informatiques réutilisent les données pour lancer des campagnes d'hameçonnage* ou de harponnage*. Ou ils peuvent sinon se rendre sur le Darkweb*, sur le marché noir des données, où numéros de cartes bancaires et de Sécurité sociale, adresses mails… se monnaient en bitcoins.

UN EXEMPLE DE VOL DE DONNÉES

En attendant son train, un collaborateur se connecte au réseau wi-fi de la gare. Ou du moins au réseau qu'il croit être celui de la gare. En réalité, il s'agit d'un routeur portant un nom aux apparences légitimes, piloté par un pirate informatique. Ce dernier peut alors intercepter ses codes d'accès et envoyer de faux emails pour demander le versement de sommes d'argent ou obtenir des informations confidentielles.

(1) « Data Breaches Compromised 3.3 Billion Records in First Half of 2018 », Gemalto, 23 octobre 2018.
* Rendez-vous page 25 pour une définition de ce terme.

AUREMAR

Prévenir les risques informatiques

DES RÈGLES BASIQUES POUR LIMITER LES FAILLES DE SÉCURITÉ

Pour garder la maîtrise sur votre système d'information et les données de votre entreprise, vous pouvez sensibiliser vos salariés à quelques bonnes pratiques :

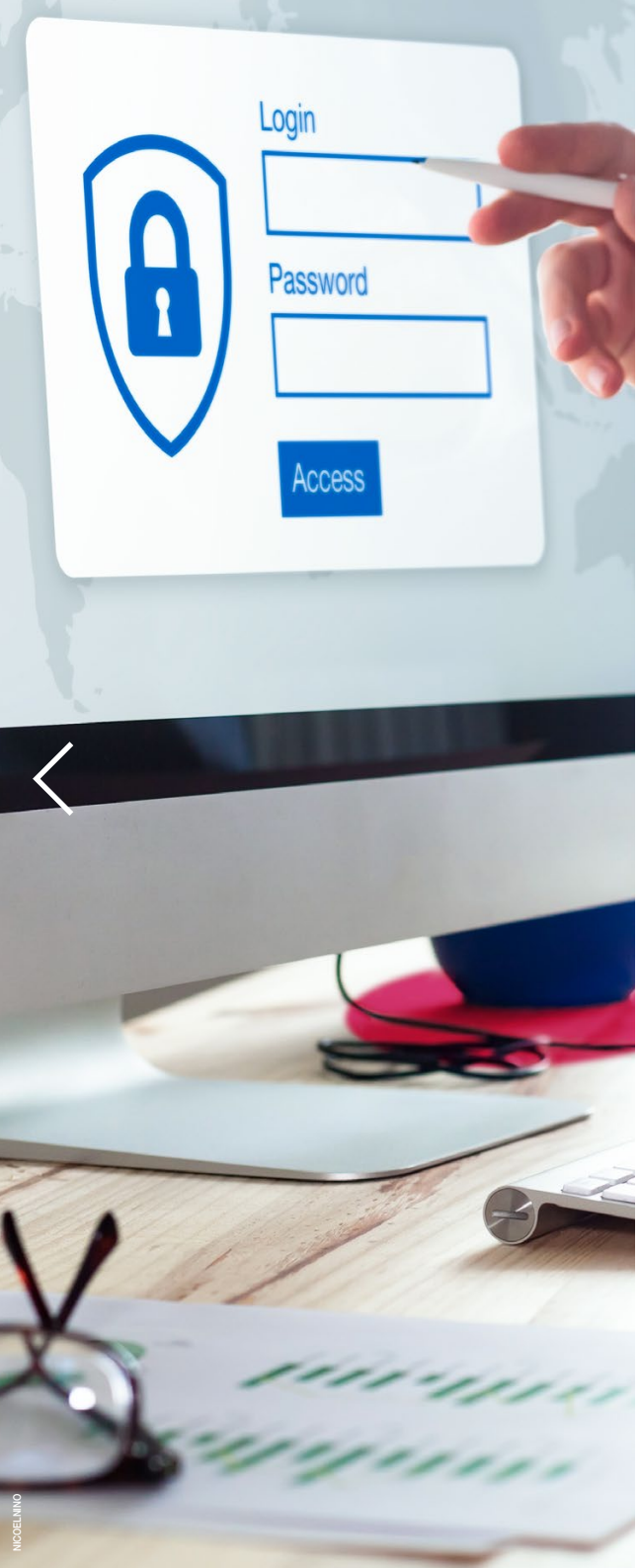
- **ne prenez avec vous que les données strictement nécessaires** à votre déplacement. Et avant de partir, pensez à en faire une sauvegarde que vous conserverez en lieu sûr ;
- **cryptez les dossiers et informations confidentielles** pour en empêcher la lecture en cas de vol des terminaux ;
- plus que jamais, protégez-vous à l'aide de mots de passe forts (au moins 8 caractères), que vous changerez à votre retour au cas où ils auraient été dérobés à votre insu ;
- avant de télécharger une nouvelle application, vérifiez les autorisations d'accès aux données demandées ;
- ne pré-enregistrez pas les mots de passe dans vos navigateurs (le cas échéant, effacez-les avant de partir) ;
- pour éviter l'installation de logiciels malveillants*, **évitez de connecter à votre machine des équipements appartenant à des tiers.** Prenez plutôt avec vous une clé USB, dédiée à ce déplacement, pour réaliser les échanges de document ;
- si vous utilisez le poste d'un client pour vous connecter à une application, n'oubliez pas de fermer votre session avant de partir ;
- désactiver le wi-fi public et le bluetooth.

COMMENT RÉAGIR ?

- En cas de violation de données avérée ou suspectée, mais aussi de vol de matériel : prévenez immédiatement votre DSI ;
- Contactez votre Agent Général MMA si vous avez une assurance Cyber-risques MMA.

> « La cybersécurité est un processus qui se met en place sur le long terme et qui s'entretient afin de défendre au mieux l'intégrité du capital informationnel de l'entreprise. Depuis de nombreuses années, sur mon site Korben.info, je sensibilise et je démystifie les bonnes pratiques en matière de cybersécurité pour les PME et les particuliers. Je suis convaincu que la sécurité informatique passe aussi par l'information et la sensibilisation de tout un chacun aux bonnes pratiques. »
>
> *Korben*

LES SOLUTIONS MMA



UNE ASSURANCE SUR-MESURE POUR COMPLÉTER VOS ACTIONS DE PRÉVENTION

Sauvegarde des données, gestion des mots de passe, formation des salariés… : en dépit de toutes les mesures de prévention adoptées, le risque zéro n'existe pas en matière de sécurité informatique. Plusieurs raisons à cela : les outils de protection sont rendus rapidement obsolètes par des menaces qui changent constamment de visage, au fur et à mesure où sont détectées de nouvelles failles ; les salariés ne respectent pas toujours les recommandations (à peine 1 sur 2 selon une étude du Cesin(1)), et cela malgré les actions de sensibilisation. Dans ces conditions, il est conseillé de souscrire une assurance adaptée afin d'être protégé en cas d'atteinte à votre SI.

L'ASSURANCE CYBER-RISQUES MMA, UNE OFFRE SUR-MESURE POUR RÉPONDRE AUX SPÉCIFICITÉS DE VOTRE ENTREPRISE

Votre entreprise est exposée à différents risques de sinistres :

- actes de cybercriminalité (hameçonnage*, rançongiciel*, déni de service*, vol de données, fraude avec utilisation non autorisée du SI et détournement de fonds…) ;
- erreurs de manipulation (écrasement de données, mauvaise utilisation du SI…) ;
- dysfonctionnements du SI (bug, panne de matériel, défaillance liée à l'environnement…).

Avec l'assurance Cyber-risques MMA, vous êtes couvert en cas de sinistres immatériels susceptibles de bloquer le fonctionnement de votre système d'information.
Différentes garanties permettent de prendre en charge les dommages subis à la fois par votre entreprise et par des tiers.

À NOTER : pour vous proposer la protection la plus efficace, un audit est réalisé au moment de la souscription. Il permet d'évaluer vos besoins selon votre activité, la nature des risques auxquels vous êtes exposés, les impacts financiers possibles, les actions de prévention déjà mises en place…

POUR AFFINER VOS ACTIONS…

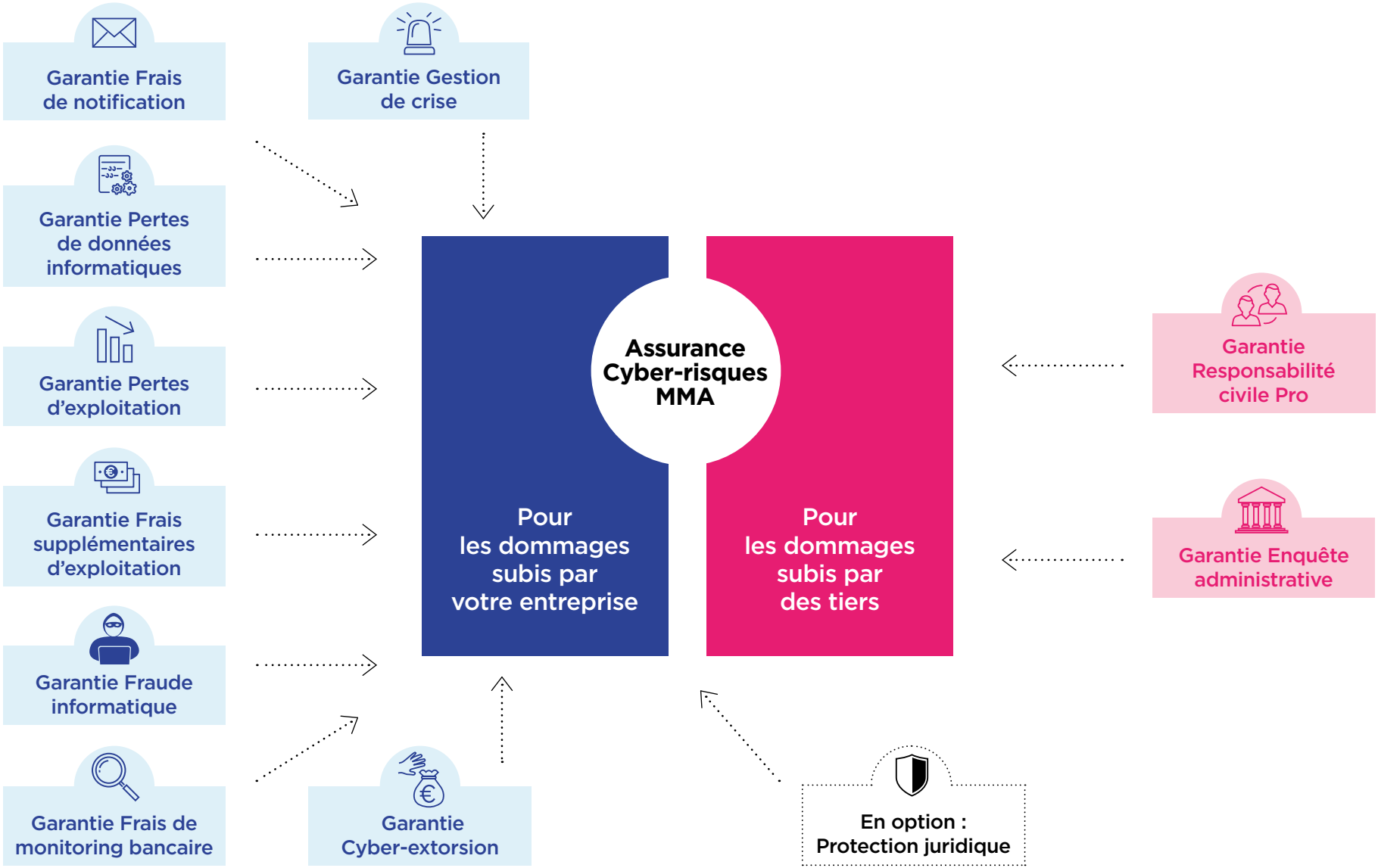
MMA vous propose 2 prestations d'audit(2) :

- **une évaluation menée sur la base d'un questionnaire,** pour identifier les risques majeurs et les processus critiques. Vous obtiendrez une fiche de synthèse précisant l'exposition au risque cyber de votre entreprise, les impacts à prévoir et les mesures préventives à mettre en place ;
- **un audit expert avec plan de recommandations,** réalisé par le biais de questionnaires, d'analyses in situ, de tests d'intrusion*… Des comptes-rendus d'entretiens, des rapports d'audit et/ou des tableaux de synthèse des scénarii d'attaque vous sont remis avec les recommandations correspondantes. Peuvent être également inclus dans la prestation, le suivi des plans d'actions, des rapports d'évolution, un audit annuel de suivi…

Pour en savoir plus, contactez votre Agent Général MMA

(1) Baromètre de la cybersécurité des entreprises, Cesin – Opinion Way, janvier 2019.
(2) Prestations payantes gérées par l'intermédiaire de Covéa Solutions Prévention (contrats de prestations de service indépendants du contrat d'assurance).
* Rendez-vous page 25 pour une définition de ce terme.

L'ASSURANCE CYBER-RISQUES MMA EN UN COUP D'ŒIL



CHRISTIAN42

RÉPARER LES DOMMAGES SUBIS PAR VOTRE ENTREPRISE

LIMITER LA PROPAGATION DES DOMMAGES AU PLUS VITE, AVEC LA GARANTIE « GESTION DE CRISE »(1)

Vous constatez un dysfonctionnement ? MMA est à vos côtés tout au long de l'incident, de la mise en place des premières mesures d'urgence à la gestion de la sortie de crise. **L'objectif de cette garantie de base de l'assurance Cyber-risques : vous aider à revenir au plus vite à un fonctionnement normal.**

En pratique, vous disposez d'une ligne directe pour joindre la **plate-forme d'assistance MMA, disponible 24 h/24, 7 jours/7.** Vous serez mis en contact rapidement avec un expert. Son rôle : déterminer la nature du problème, ses causes probables et ses conséquences, mais surtout identifier les solutions adéquates et coordonner leur mise en œuvre (avec l'aide de vos prestataires informatiques habituels ou le cas échéant avec une entreprise partenaire MMA).

Au-delà des aspects techniques à résoudre, cette garantie prévoit également la **prise en charge des frais destinés à sortir de la crise :** honoraires d'avocat, ouverture d'une hotline (pour répondre aux questions des clients), recours à un prestataire extérieur ou à un sous-traitant, frais d'e-réputation…

RESPECTER VOS OBLIGATIONS LÉGALES, AVEC LA GARANTIE « FRAIS DE NOTIFICATION »(1)

Des données à caractère personnel, stockées par votre entreprise, ont été atteintes (vol, détournement…) ? **Le RGPD vous oblige à déclarer l'incident à la CNIL, et selon les cas, à informer les personnes concernées elles-mêmes.** MMA peut prendre en charge vos différents frais de notification : envoi de recommandés, recours à un prestataire pour l'envoi d'un email…

CONNAÎTRE VOS DROITS ET PRÉVENIR LES LITIGES, AVEC L'OPTION « PROTECTION JURIDIQUE »

La mise en conformité de votre entreprise avec le RGPD suscite des préoccupations nouvelles : quelles procédures mettre en œuvre ? Comment démontrer votre respect des règles ? Quelles clauses insérer dans les contrats de vos sous-traitants ? Quelles durées de conservation des factures ? Quels sont les droits de vos clients ? Etc. Grâce à l'option « Protection juridique » proposée notamment dans les contrats Multirisque Pro MMA, une équipe de juristes experts est à votre disposition pour vous informer à titre préventif sur l'ensemble de vos droits et obligations. Et si vous faites l'objet d'une attaque, elle vous accompagne dans les démarches à entreprendre auprès de vos clients ainsi qu'en cas de procédure entamée par la CNIL.

RELANCER VOTRE ACTIVITÉ, AVEC LA GARANTIE « PERTES DE DONNÉES INFORMATIQUES »(1)

Votre SI est à l'arrêt à la suite d'une erreur de manipulation d'un salarié ou d'une défaillance technique, un virus* limite l'accès à vos fichiers… : **MMA peut couvrir les frais destinés à reconstituer vos données.** Selon la situation, il peut s'agir :

- d'effectuer une duplication à partir de vos sauvegardes ;
- de réinstaller des logiciels ;
- de ressaisir vos informations ;
- de vérifier la validité des données restaurées…

(1) Nos prises en charge sont faites en application des garanties ou options souscrites et des conditions, limites, exclusions de garanties et du montant des franchises qui sont précisées dans les Conditions Générales, Conditions Particulières du contrat Assurance Cyber-risques MMA. Pour en savoir plus, contactez votre Agent Général MMA.

Les + MMA

- Une solution sur-mesure, avec un service d'assistance disponible 24 h/24, 7 j/7
- En cas de sinistre, une mise en contact rapide avec un expert informatique chargé de coordonner les actions de sortie de crise

LIMITER L'IMPACT D'UN SINISTRE SUR VOTRE CHIFFRE D'AFFAIRES, AVEC LA GARANTIE « PERTES D'EXPLOITATION »(1)

Un bug technique vous oblige à fermer votre boutique en ligne, un malware* bloque le SI de votre site de production… Lorsqu'un sinistre immatériel ralentit voire interrompt votre activité, les conséquences peuvent être lourdes sur votre productivité.
Dans une telle situation, MMA vous verse une indemnité pour **compenser la baisse de votre chiffre d'affaires et payer vos charges fixes,** et ainsi retrouver la situation financière qui était la vôtre avant l'incident.

FAIRE FACE AUX IMPRÉVUS, AVEC LA GARANTIE « FRAIS SUPPLÉMENTAIRES D'EXPLOITATION »(1)

Une attaque ou un dysfonctionnement informatique se produit, et c'est l'ensemble de votre entreprise qui est impactée. La garantie « Frais supplémentaires d'exploitation » est là pour **rembourser les frais nécessaires au maintien de votre activité,** jusqu'au rétablissement de votre système d'information. Par exemple :

- le paiement d'heures supplémentaires à vos salariés, contraints de réutiliser d'anciens logiciels moins performants ;
- la location de matériel de remplacement…

À NOTER : le montant de votre indemnisation est calculé par un expert, selon votre secteur d'activité et sur la base de différents critères, notamment comptables comme les comptes d'exploitation…

GÉRER UN DÉTOURNEMENT D'ARGENT, AVEC LA GARANTIE « FRAUDE INFORMATIQUE »(1)

Avec la garantie « Fraude informatique », **vous êtes indemnisé pour vos pertes financières consécutives** à un détournement de fonds, une fraude, une escroquerie, un acte de sabotage, un vol… Le sinistre pouvant aussi bien être la conséquence d'une utilisation non autorisée du SI, interne comme externe.

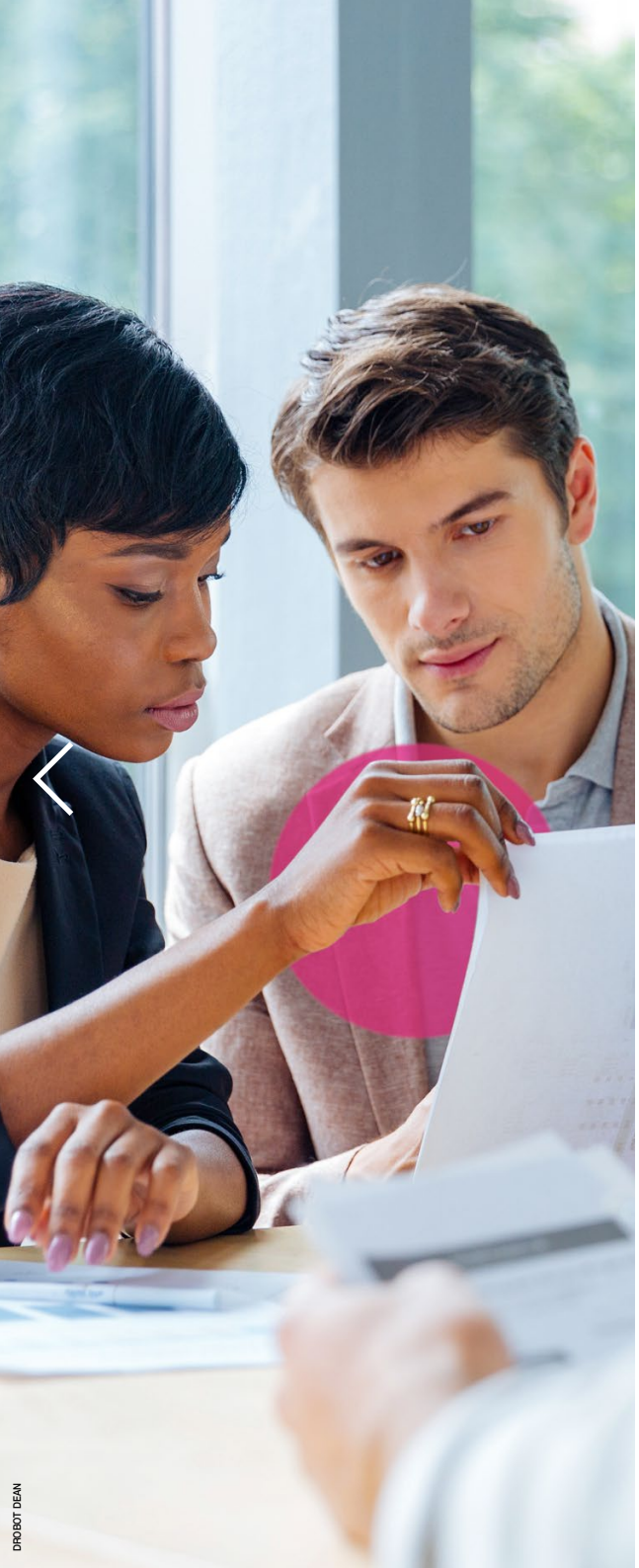
SUIVRE LES CONSÉQUENCES D'UN VOL DE DONNÉES, AVEC LA GARANTIE « FRAIS DE MONITORING BANCAIRE »(1)

Les données bancaires de vos clients ont fait l'objet d'une attaque ? Les comptes en banque susceptibles d'être piratés doivent faire l'objet d'une surveillance, afin de **détecter tout mouvement financier suspect durant la période qui suit le sinistre.** Une surveillance dont le coût est couvert par la garantie « Frais de monitoring bancaire ».

ÊTRE REMBOURSÉ POUR LE PAIEMENT D'UNE RANÇON, AVEC LA GARANTIE « CYBER-EXTORSION »(1)

Vous êtes victime d'un rançongiciel* et vos données, rendues inaccessibles, seront débloquées par les hackers sous réserve de vous acquitter d'une certaine somme. Si aucune autre solution technique ne permet de retrouver vos fichiers, **MMA vous rembourse le montant de la rançon,** à condition d'avoir eu l'accord préalable de votre Agent Général MMA.

(1) Nos prises en charge sont faites en application des garanties ou options souscrites et des conditions, limites, exclusions de garanties et du montant des franchises qui sont précisées dans les Conditions Générales, Conditions Particulières du contrat Assurance Cyber-risques MMA. Pour en savoir plus, contactez votre Agent Général MMA.



DROBOT DEAN

GÉRER LES DOMMAGES SUBIS PAR DES TIERS

RÉPARER LES PRÉJUDICES, AVEC LA GARANTIE « RESPONSABILITÉ CIVILE PRO »

La garantie « Responsabilité civile pro » permet de réparer les dommages subis par vos clients, vos prestataires ou tout autre tiers[1] lorsqu'ils ont fait l'objet :

- d'une **atteinte aux données**. Par exemple, vous travaillez sur un projet industriel, un pirate informatique a dérobé vos données, parmi lesquels des plans de conception ; le prestataire qui les avait réalisés doit engager des frais pour les produire de nouveau ;
- d'une **intrusion à votre réseau.** Par exemple, vous êtes hébergeur de sites internet et l'indisponibilité de vos services, suite à une panne, ont empêché vos clients de réaliser des ventes en ligne ;
- d'un **préjudice médiatique.** Par exemple, une mauvaise instruction donnée à votre SI a conduit à une erreur de logistique et à la commercialisation de produits défectueux dans les point de vente d'un client ; l'information est divulguée dans les médias, portant atteinte à l'image de votre partenaire. Avec l'option protection juridique, MMA prend en charge des heures de consultation d'un communicant pour analyser la situation, recommander et suivre des actions de communication en interne et en externe.

(1) Nos prises en charge sont faites en application des garanties ou options souscrites et des conditions, limites, exclusions de garanties et du montant des franchises qui sont précisées dans les Conditions Générales, Conditions Particulières du contrat Assurance Cyber-risques MMA. Pour en savoir plus, contactez votre Agent Général MMA.

ASSURER LA DÉFENSE DE VOS INTÉRÊTS, AVEC LA GARANTIE « ENQUÊTE ADMINISTRATIVE »

Une autorité administrative a lancé une enquête à l'encontre de votre entreprise, afin de vérifier votre conformité avec la règlementation. MMA vous aide à protéger vos intérêts en couvrant vos frais d'honoraires d'avocat ou encore de recours à un expert pour réunir les preuves nécessaires à votre dossier.

RESSOURCES ET INFORMATIONS UTILES

- **www.cybermalveillance.gouv.fr,** pour accéder à un kit de sensibilisation ;
- **Le site internet de l'ANSSI,** pour connaître les principales menaces et bonnes pratiques ;
- **Signal-spam.fr,** pour signaler les mails frauduleux ;
- **Le centre de contact Info Escroqueries,** joignable au 0805 805 817, pour obtenir des conseils ;
- **www.internet-signalement.gouv.fr,** pour signaler tout comportement illicite ;
- **Le site internet Connexion Pro de MMA,** pour vous informer sur les cyber-risques.

Lexique

Darkweb : pages Internet accessibles uniquement via des navigateurs spéciaux. Elles sont notamment le lieu d'activités illégales (vente de données, de drogues…).

Déni de service (DoS) : action (malveillante ou accidentelle) qui a pour résultat de bloquer ou de ralentir un système d'information. Si elle est lancée à partir de plusieurs machines, on parle alors de « Déni de service distribué » (DDoS).

Hameçonnage (ou « phishing » en anglais) : technique qui consiste, pour les pirates informatiques, à envoyer un mail aux couleurs d'un partenaire ou d'un prestataire de confiance, dans le but de dérober des informations.

Harponnage (ou « spear-phishing » en anglais) : une déclinaison de l'hameçonnage, qui s'appuie sur une connaissance de la cible et une personnalisation du message.

Homme du milieu (ou « man in the middle » en anglais) : technique à travers laquelle un pirate informatique intercepte les données échangées entre deux parties, à leur insu.

Ingénierie sociale (ou « social engineering » en anglais) : manipulation psychologique exercée dans le but d'obtenir la confiance de la victime et de lui soutirer des informations, de l'argent…

Logiciel malveillant (ou « malware » en anglais) : programme informatique destiné à nuire à un système informatique. Il peut prendre la forme par exemple d'un rançongiciel ou encore d'un botnet.

Pare-feu (ou « firewall » en anglais) : outil permettant de protéger les ordinateurs connectés à un réseau. Il protège d'attaques externes (filtrage entrant) et souvent de connexions illégitimes à destination de l'extérieur (filtrage sortant).

Rançongiciel (ou « ransomware » en anglais) : logiciel malveillant qui crypte les données de ses cibles, avant de demander le paiement d'une rançon pour le déblocage des informations retenues en otage.

Réseau de machines zombies (ou « botnet » en anglais) : ensemble de machines infectées par un logiciel malveillant et utilisées par les pirates informatiques, le plus souvent dans le cadre d'attaque DoS.

Shadow IT : logiciels installés sur des ordinateurs professionnels sans l'autorisation préalable de la DSI.

Test d'intrusion (ou « pentest » en anglais, pour « penetration test ») : attaque menée contre son propre réseau, afin d'en détecter les failles de sécurité.

Ver : logiciel malveillant qui se caractérise par sa capacité à se propager et s'exécuter en toute autonomie, sans programme hôte (tel qu'un fichier exécutable).

Virus : logiciel malveillant qui se diffuse à partir de programmes hôtes (tel qu'un fichier exécutable).

MMA met à votre disposition une collection de livres blancs

Ils vous permettent de mieux comprendre les risques auxquels vous pourriez être confronté en tant que chef d'entreprise. Vous trouverez des conseils de prévention et des solutions adaptées pour bien protéger votre activité.

LB n°5_Cyber-risques - 03/2019 - Crédits photos : Adobe stock.