(r) assuré d'entreprendre

LE RENDEZ-VOUS EXPERT DE LA PETITE ENTREPRISE

(r)assurez-vous face aux CYBER RISQUES EN ENTREPRISE

LIVRE BLANC
« ASSURÉ D'ENTREPRENDRE » – N° 8

INTRO

Cryptage malveillant de vos données informatiques, revente de vos secrets de fabrication, prise de contrôle de votre site internet… Vous croyez que ces actions sont tout juste sorties d'un film de cinéma ? Ou qu'elles ne concernent que les autres entreprises, les plus grosses ? Détrompez vous !
Aujourd'hui, avec l'essor des nouvelles technologies, du numérique et l'usage grandissant des smartphones et autres tablettes, qui permettent certes à votre entreprise de capter et fidéliser de nouveaux clients ou d'améliorer vos process de fabrication, vous multipliez par la même occasion les failles potentielles.

Vos systèmes d'information et vos données informatiques, qui drainent une grosse partie de la richesse de votre entreprise, peuvent en effet faire l'objet d'une attaque. Et dans cette histoire, toutes les entreprises sont visées, des plus petites, souvent les plus fragiles où la sécurité des réseaux n'est pas nécessairement une priorité, aux plus grosses qui détiennent de nombreuses informations et donc monnayables.

Ces cyber risques peuvent avoir des répercussions graves sur votre activité et votre image, et doivent vous inciter à vous méfier dès à présent.
Au travers de ce guide, tentez de mieux comprendre ce que sont ces cyber risques, ce qu'ils recouvrent et quelles sont leurs conséquences… Ainsi, vous pourrez envisager de mettre en place des actions et des outils efficaces pour faire baisser ce risque et limiter ses conséquences.

SOMMAIRE

« CYBER RISQUES » : DE QUOI PARLE-T-ON ?

Sous la notion de cyber risques se cache en réalité une large variété de situations.

Il n'existe pas de définition légale de ce que sont les cyber risques. Mais de manière synthétique, on peut dire que ce sont :
- les risques liés à l'utilisation des systèmes d'information connectés à un réseau ouvert
- ou encore les conséquences des atteintes aux données et aux systèmes d'information.

ILS PEUVENT AVOIR DES SOURCES DIFFÉRENTES, C'EST À DIRE ÉMANER :

- de la sphère internet elle-même, via des hackers ou la « cyber mafia »
- du monde économique, comme un concurrent, un collaborateur, un sous-traitant, ou un acteur de l'intelligence économique
- de la sphère politique : d'un état ou d'activistes, voire de terroristes
- des attaques émanant d'autres sites internet, comme par exemple :
  – le déni de services = saturer votre système d'information par un volume très important de requêtes rendant le système incapable de fonctionner
  – le hameçonnage = courriel semblant provenir d'une personne de confiance pour soutirer des informations confidentielles
  – le cybersquatting = déposer un nom de domaine qui contient le nom d'une marque connue vous appartenant pour récupérer un trafic illégitime.

ILS SE PRÉSENTENT SOUS DIVERSES FORMES, TELLES QUE :

- un virus, une intrusion ou une mauvaise utilisation du système d'information qui affectent directement votre site internet,
- une atteinte à votre e-réputation, c'est-à-dire une atteinte à votre réputation sur internet
- l'ingénierie sociale : pratique qui consiste à exploiter les failles humaines et sociales de l'entreprise à laquelle est lié le système informatique visé en abusant de sa confiance, de son ignorance ou de sa crédulité.

LE TÉMOIGNAGE DE L'EXPERT

« L'un des risques les plus élevés en entreprise actuellement est le cryptovirus : vous recevez un mail anodin avec un fichier en attachement. On vous indique de cliquer sur ce fichier, et ce faisant vous attirez un virus qui va chiffrer vos données. Vous ne pourrez plus y accéder sans acheter la clé de déchiffrement auprès de pirates pour 1 bitcoin (aujourd'hui autour des 1 000 euros).

En deuxième place des risques les plus répandus, on trouve les APT (Advanced Persistent Threats), qui explorent la sociologie, la psychologie des personnes de l'entreprise, via les réseaux sociaux le plus souvent, pour connaître la structure et les vulnérabilités du système d'information. Au bout de quelques mois, s'il y a un intérêt, un virus est envoyé pour récupérer les informations les plus sensibles, et ce pillage peut durer des mois. C'est une forme de cyber espionnage : l'entreprise perd tous ses secrets de fabrication, ses brevets non encore publiés, ses fichiers clients…

En troisième position, il y a les attaques sur les infrastructures techniques comme l'empoisonnement de l'eau, la coupure de la connexion internet, de l'électricité… »

GÉRARD PELIKS,
EXPERT EN SÉCURITÉ DE L'INFORMATION,
PRÉSIDENT DE L'ASSOCIATION CYBEREDU

ZOOM – STATISTIQUES

Selon un rapport de PWC* d'octobre 2015 : le nombre de cyber-attaques a progressé de **38 %** dans le monde en 2015. En France, les entreprises ont subi en moyenne **21 incidents par jour,** soit + 51% en un an, ce qui fait de notre pays celui où les cyber-attaques ont le plus augmenté en 2015 !

En France, les sources de ces incidents sont le plus souvent :

- des salariés en poste (34,2%)
- d'anciens salariés (28,2%)
- des prestataires de services (23,7%)
- d'anciens prestataires de services (17,5%)
- des fournisseurs (17,5%)

Avec une croissance forte des fournisseurs et des prestataires de services.

Certains secteurs sont plus exposés que d'autres. C'est le cas du secteur des finances, du e-commerce, des hôtels, des agences de voyages, du secteur de la santé et de l'éducation.

REMARQUE :

Les premières cibles sont les TPE-PME : plus de 75 % des intrusions malveillantes par Internet visent les PME, selon le baromètre Sage 2016 des Directeurs Financiers.

POURQUOI ?

Les TPE-PME sont un moyen d'atteindre les grands comptes soit d'autres entreprises plus importantes (avec lesquelles elle sont en lien) car elles ont généralement moins de moyens financiers à consacrer à la sécurité informatique…

LE TÉMOIGNAGE DE L'EXPERT

« Les motivations des attaquants sont variées. Ils n'attaquent pas que pour l'argent, ils agissent aussi par idéologie ou pour se venger.

Par exemple, le CNES* envoie des fusées qui font des trous dans la couche d'ozone, celui-ci peut se faire attaquer par des groupes comme Anonymous, défenseurs, pour un temps, de l'environnement.

Autre exemple : un collaborateur qui s'est fait licencier peut attaquer son ancienne entreprise non pas pour de l'argent, mais pour lui nuire. »

GÉRARD PELIKS,
EXPERT EN SÉCURITÉ DE L'INFORMATION,
PRÉSIDENT DE L'ASSOCIATION CYBEREDU

* CNES : Cente national d'études spatiales

* PWC : PricewaterhouseCoopers

QUELS SONT LES FACTEURS DE RISQUES ?

Bien sûr le développement des nouvelles technologies, et notamment l'échange de données à distance, au sein même des entreprises ou avec des tiers (clients, partenaires …) est favorable à la prolifération de ces risques.

On peut citer, par exemple :

- **Le Cloud,** l'informatique « dans les nuages », qui permet de stocker ses données et ses logiciels à distance et de les récupérer via internet.
  Il est certes très pratique, mais cette sous-traitance implique une grande confiance dans le prestataire qui doit être capable d'assurer, la disponibilité, la confidentialité et la sécurité de vos données. Dans ce cadre, il faut également s'assurer que vos données restent en France* sous peine de se voir appliquer une législation étrangère peu protectrice en cas de problème.

- **L'interdépendance des systèmes,** qui permet aux entreprises de communiquer entre elles par l'intermédiaire de réseaux informatiques (Internet, extranet, messageries électroniques) via des normes communes et souvent des logiciels libres où là aussi l'échange de données se fait avec plus ou moins de sécurité.

- **Le BYOD, pour « Bring Your Own Device »,** qui signifie « Apportez votre propre périphérique ». C'est le fait pour les collaborateurs de l'entreprise d'utiliser leurs appareils personnels sur leur lieu de travail : smartphone, tablette, ordinateur… avec le risque que cela comporte d'ouvrir son réseau sur le monde extérieur via des machines pas ou peu protégées.

- **Les objets connectés,** ces objets « intelligents » qui communiquent pour transmettre des informations à des systèmes distants, comme les montres, les automobiles, les baskets… Ils se multiplient dans notre quotidien et donc aussi sur les lieux professionnels et conversent avec les réseaux extérieurs.

CONCRÈTEMENT, QU'EST-CE QUE CELA PEUT IMPLIQUER POUR VOTRE ENTREPRISE ?

Vous pouvez :

- subir une perte, voire une destruction de vos données informatiques, qu'il s'agisse de vos fichiers clients, de vos secrets de fabrication…
- voir vos données, parfois personnelles ou confidentielles, divulguées avec à la clé vos produits contrefaits et perdre en performance si on utilise vos données,
- être en situation de déni de service et ne plus pouvoir fonctionner pendant plusieurs jours.

LE TÉMOIGNAGE DE L'EXPERT

« Les PME, surtout les plus petites, sont souvent mal préparées et démunies face aux cyber risques, alors que c'est vital pour elles de les prendre en compte. Généralement, celui qui gère la sécurité informatique dans l'entreprise, quand quelqu'un la gère, c'est le patron lui-même, qui fait ça le dimanche et qui ne s'y connaît par forcément.. Alors pourtant que les conséquences sont graves et peuvent aller jusqu'à la perte de confiance des clients et la fermeture de l'entreprise.»

GÉRARD PELIKS,
EXPERT EN SÉCURITÉ DE L'INFORMATION,
PRÉSIDENT DE L'ASSOCIATION CYBEREDU

* Le transfert de données hors de l'UE est par principe interdit, sauf autorisation de la CNIL ou sous réserve des exceptions prévues.

LES CONSÉQUENCES ET IMPACTS DES CYBER ATTAQUES

Les cyber attaques peuvent revêtir des formes variées, en voici les conséquences :

> UNE SITUATION DE CRISE

L'attaque laisse une situation qu'il faut rapidement prendre en main pour remettre en route et en sécurité le réseau informatique, gérer la communication en interne et vis-à-vis des personnes victimes, mettre en place des procédures pour faire face aux recours éventuels, gérer la notification éventuelle des violations aux autorités compétentes (ANSSI, CNIL,)…

À NOTER

La gestion de cette crise peut être assurée soit en interne, soit par un prestataire externe, disposant d'une infrastructure appropriée, qui mettra en place un plan de gestion de crise, une cellule de crise, voire un centre d'appels dédié aux clients et un site internet prenant le relais en cas de défaillance du site principal de l'entreprise.

> DES COÛTS FARAMINEUX

Les pertes financières consécutives à une cyber attaque peuvent être rapidement exorbitantes, qu'il s'agisse de reconstituer les données perdues ou volées, de combler les pertes d'exploitation, de restaurer sa réputation en faisant intervenir une agence spécialisée, des frais de justice, ou d'expertise technique…

> L'ATTEINTE À LA RÉPUTATION DE VOTRE ENTREPRISE

Voir leurs données divulguées à droite à gauche, n'est pas du meilleur effet auprès de vos clients ni même du grand public, surtout si les réseaux sociaux s'emparent du sujet. Votre réputation peut rapidement être mise à mal : votre entreprise n'est pas sérieuse, votre système informatique n'est pas fiable, vous n'avez pas mis en place les garde-fous pour empêcher la situation, le problème risque de se reposer…

> LA MISE EN CAUSE DE VOTRE RESPONSABILITÉ CIVILE ET PÉNALE

C'est la conséquence la moins évidente pour les petites entreprises et pourtant la plus lourde : en tant que collecteur des données personnelles de vos clients ou de vos salariés, si ces données sont volées, votre responsabilité aussi peut être engagée. C'est en effet de la responsabilité des entreprises de garantir et d'assurer la sécurité et la confidentialité de ces données et vous n'êtes pas à l'abri qu'on porte plainte contre vous !

LE TÉMOIGNAGE DE L'EXPERT

« Si les conséquences sont bien-sûr financières, juridiques et pénales, elles peuvent aussi être psychologiques… Une entreprise fait du business car ses clients ont confiance en elle. Si cette confiance s'envole, c'est fini pour l'entreprise. Inspirer la confiance est l'un des biens les plus précieux de l'entreprise. Elle peut le perdre suite à une cyberattaque. Et pour l'instant, seuls l'administration et les opérateurs d'importance vitale sont obligés de déclarer les cyber attaques qu'ils subissent, à l'ANSSI*, mais bientôt sans doute, les PME le devront aussi auprès d'organismes officiels qui recenseront ces attaques… entraînant une meilleure connaissance des dangers du cyberespace. »

Le saviez-vous ?

« Le coût moyen d'une cyber attaque en France s'élève en 2016 à 773 000 euros, d'après une étude de NTT Communications. Elle était de 250 000 euros il y a 3 ans. Ça croît très rapidement. »

GÉRARD PELIKS,
EXPERT EN SÉCURITÉ DE L'INFORMATION, PRÉSIDENT DE L'ASSOCIATION CYBEREDU

* ANSSI : Agence Nationale pour la Sécurité des Systèmes d'Information

COMMENT LUTTER CONTRE LES CYBER RISQUES ?

Heureusement, différents moyens existent pour anticiper, limiter et réparer les conséquences des cyber attaques.

LE TÉMOIGNAGE DE L'EXPERT

« La sécurité informatique c'est très technique mais aussi de plus en plus juridique. Si certains collaborateurs commettent des irrégularités, la loi est là pour réprimer leurs agissements, que ce soit suivant le Code civil ou le Code pénal. D'où l'importance de sensibiliser le personnel aux cyber risques !

Les articles 323-1 à 323-7 du Code pénal, qui datent des années 1990 sont toujours valables. Pénétrer dans un système d'information (un STAD* comme il est écrit dans le code pénal) sans permission est passible de 2 ans de prison et de 60 000 euros d'amende. S'y maintenir est plus grave, le perturber est encore plus grave, et si cela est effectué par une personne morale, c'est encore plus grave.

Si vous laissez partir des données à caractère personnel liées au personnel ou aux clients par exemple, vous aurez aussi des problèmes avec la CNIL. Dans ce cas, l'entreprise, du statut de victime passe à celui de responsable. Elle subit un dommage, le vol des données, mais peut également se voir reproché le fait de ne pas avoir tout fait pour les protéger).

GÉRARD PELIKS,
EXPERT EN SÉCURITÉ DE L'INFORMATION,
PRÉSIDENT DE L'ASSOCIATION CYBEREDU

* STAD : Système de Traitement Automatisé de Données

CE QUI DIT LA LOI

Deux grands axes composent l'arsenal juridique français :

- **La protection des données à caractère personnel**

Les fournisseurs d'accès à internet (FAI) et les opérateurs de téléphonie ont l'obligation de notifier auprès de la CNIL* toute violation de données à caractère personnel : destruction, perte, altération, divulgation, accès non autorisé à des données à caractère personnel faisant l'objet d'un traitement dans le cadre de la fourniture au public de services de communications électroniques.

Attention : cette obligation est étendue à tous les professionnels, pour toute violation de données personnelles en 2018 avec un alourdissement des sanctions jusqu'à 2 % du chiffre d'affaires mondial annuel de l'exercice précédent ou 10 M d'euros (nouveau règlement européen sur la protection des données voté en 2016 et applicable en 2018). Cette notification, s'accompagne d'une communication aux personnes concernées, si cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés, sauf notamment si le professionnel a mis en œuvre les mesures de protection techniques et organisationnelles appropriées (par exemple, chiffrement des données, rendant les données incompréhensibles à une personne non autorisée).

- **La fraude informatique**

Une loi de 1988 insérée dans le Code Pénal (Art. 323-1 et suivants) prévoit plusieurs peines, allant de 2 ans à 7 ans d'emprisonnement et de 60 000 à 300 000 euros d'amende en fonction du degré de gravité de l'action, pour les personnes qui accèdent ou se maintiennent frauduleusement dans un système de traitement automatisé de données, en suppriment ou en modifient le contenu, en faussent le fonctionnement, en reproduisent les données, etc.

À NOTER

Un professionnel est responsable de la sécurité des données de ses clients et prospects cf. art 34 de la loi Informatique et Libertés.

* CNIL : Commission Nationale de l'Informatique et des Libertés

ÉVALUER SES RISQUES

Il est indispensable d'auditer régulièrement votre système d'information et de traitement de données, pour lister, analyser et classifier les risques, identifier les personnes qui peuvent être exposées aux risques, mesurer la solidité et l'efficacité des mesures déjà prises via des tests ou des simulations d'intrusion…

Cet audit peut être fait en interne si vous disposez d'une équipe ou d'un collaborateur dédié à la gestion de la sécurité des systèmes d'information, ou en faisant appel à un prestataire extérieur.

LE CONSEIL DE L'EXPERT

« Il ne faut pas hésiter à solliciter des prestataires spécialisés qui vont auditer le système d'information de l'entreprise, voir quels sont les gisements d'informations sensibles, vérifier s'ils sont bien sécurisés, ce qu'il faut faire pour mieux les sécuriser, rencontrer le personnel pour étudier leurs comportements… Un regard extérieur est toujours préférable à un regard intérieur qui peut en voir beaucoup moins… »

GÉRARD PELIKS,
EXPERT EN SÉCURITÉ DE L'INFORMATION,
PRÉSIDENT DE L'ASSOCIATION CYBEREDU

BON À SAVOIR

Comment choisir un prestataire spécialisé ?

Le prestataire choisi devra analyser les risques que votre entreprise peut encourir et mettre en place les outils et les actions nécessaires pour les contrer.

Pour cela, il est indispensable de choisir un prestataire :

- capable de vous donner un aperçu de l'impact financier des risques encourus et de vous adresser des conseils personnalisés, en fonction de votre univers, de votre organisation…
- qui pourra intervenir sur le long terme, afin d'adapter régulièrement le dispositif de sécurité,
- disponible 24h/24, 7j/7 pour faire face aux attaques, quel que soit le moment où celles-ci surviennent car on sait que la rapidité est un élément clé pour limiter les conséquences.
- qui vous propose éventuellement d'installer un capteur indépendant. Celui-ci permet d'enregistrer les incidents et de dresser un historique en cas de sinistre.

FAIRE DE LA PRÉVENTION

Plusieurs actions peuvent être mises en place en amont pour éviter, limiter ou retarder les conséquences d'une cyber attaque dans votre entreprise :

> SENSIBILISER VOTRE PERSONNEL

Le « maillon faible » ce n'est pas forcément votre logiciel mais ce peut être votre personnel, qui sans être malveillant peut être naïf ou inconscient des risques ! Il faut donc impérativement, quelle que soit sa fonction, du simple collaborateur jusqu'au dirigeant, l'informer sur les risques existants et sur les bonnes pratiques à adopter.

Par exemple, vous pouvez rappeler la politique de sécurité des systèmes d'informations et des chartes TIC qui peuvent s'imposer à vos collaborateurs en la joignant au règlement intérieur de votre entreprise.

> COMPARTIMENTER L'INFORMATION

Séparer les informations sensibles du reste, pour mieux les sécuriser, car il n'est pas possible de tout sécuriser.

Par exemple, séparez la bureautique des systèmes de contrôles industriels parce que les attaquants s'introduisent souvent par la bureautique pour ensuite dérégler le reste.

> CHIFFRER LES INFORMATIONS SENSIBLES...

... avec des algorithmes suffisamment solides et des clés suffisamment longues. Il faut également mettre en place des contre-mesures de base bien configurées : antivirus, firewall…
Et si vous ouvrez votre réseau informatique aux collaborateurs qui sont à l'extérieur, il faut mettre en œuvre des systèmes d'identification et d'authentification forts.

> AUDITER OU FAIRE AUDITER RÉGULIÈREMENT...

... votre réseau informatique pour avoir une vue d'ensemble, pouvoir mettre à jour vos solutions et repérer rapidement s'il y a un problème.

LE RÔLE DE L'ASSUREUR

Aujourd'hui, toute entreprise peut être victime d'une cyber attaque… Or, on l'a vu, les conséquences peuvent être désastreuses pour votre entreprise, et notamment pour sa trésorerie.

Certains dommages peuvent être couverts, mais seulement partiellement, par votre Assurance Responsabilité Civile ou votre multirisques professionnelle.

Vous avez donc tout intérêt à faire appel à votre assureur pour souscrire une assurance spécifique, qui vous permettra d'avoir de l'aide pour faire face aux atteintes à vos systèmes d'informations et à vos données résultant notamment d'actes de malveillance, et de prendre les mesures nécessaires pour limiter les conséquences de ces atteintes sur votre activité professionnelle.

Assurez-vous que votre assurance Cyber risques vous donne les moyens de :

> GÉRER LA CRISE

En cas d'attaque, une garantie d'assistance vous permet généralement de réaliser un état des lieux de la situation informatique pour identifier l'origine et la nature des attaques et les éventuelles failles de votre système d'information.

> FINANCER VOS FRAIS ET PERTES

Sont généralement couverts :
- les frais d'experts informatiques pour sécuriser votre réseau,
- les frais de communication en cas d'atteinte à votre réputation,
- les frais de reconstitution de vos données (dans les limites de garanties indiquées au contrat) dont le coût de remplacement des logiciels, d'achat de licences et de transfert des données vers tout nouveau fournisseur informatique.

> INDEMNISER LES LÉSÉS, SI VOTRE RESPONSABILITÉ CIVILE EST MISE EN CAUSE

Si la responsabilité civile de votre entreprise est engagée suite à la perte de données à caractère personnel ou à leur utilisation frauduleuse, ses conséquences financières sont couvertes.

LE TÉMOIGNAGE DE L'EXPERT

« Si vous vous sentez isolé sur ce sujet, sachez que différentes structures existent et peuvent aider les entreprises.

Par exemple, la gendarmerie a une cellule spéciale composée de gendarmes spécialisés dans les NTIC*.

A Paris et dans la grande couronne, c'est la BEFTI (brigade d'enquête sur les fraudes aux technologies de l'information), de la préfecture de police de Paris qui peut être sollicitée.

Il y a aussi l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) présente sur toute la France, de même que l'agence nationale de la sécurité des systèmes d'information (ANSSI).

La CNIL donne aussi des conseils sur la protection des données à caractère personnel et la DGSI* propose des sensibilisations en entreprises.

La sécurité c'est un problème d'expertise ! »

GÉRARD PELIKS,
EXPERT EN SÉCURITÉ DE L'INFORMATION,
PRÉSIDENT DE L'ASSOCIATION CYBEREDU

* NTIC : Nouvelles Technologies de l'Information et de la Communication
* DGSI : Direction Générale de la Sécurité Intérieure

EXEMPLES

LA BASE CLIENTS D'UNE ENTREPRISE A ÉTÉ PIRATÉE. LES DONNÉES CLIENTS, DONT LES COORDONNÉES BANCAIRES, ONT ÉTÉ UTILISÉES FRAUDULEUSEMENT NOTAMMENT POUR DES ACHATS EN LIGNE.

Un contrat d'assurance cyber risques peut vous permettre :

- de financer la mise en place ou de bénéficier d'une plateforme de gestion de crise chargée d'identifier les causes du piratage et d'établir des préconisations destinées à renforcer la sécurité informatique de l'entreprise,
- de bénéficier d'une prise en charge des frais d'avocats et d'une assistance juridique pendant l'enquête,
- de financer les frais de restauration des données clients,
- d'indemniser les clients ayant subi un détournement de fonds.

UNE ENTREPRISE EST VICTIME DE VOLS D'ORDINATEURS. DES DONNÉES SONT VOLÉES ET REVENDUES. LA CRÉDIBILITÉ DE L'ENTREPRISE EST REMISE EN CAUSE.

Un contrat d'assurance cyber risques peut vous permettre :

- de financer le recours à un expert informatique chargé d'identifier la faille du système informatique,
- de financer les frais de ressaisies manuelles des données à partir des archives papier de l'entreprise
- de bénéficier d'une prise en charge des frais de communication visant à restaurer l'image de l'entreprise.

FAQ

« JE VIENS D'INTRODUIRE UNE CLÉ USB VIRUSÉE… UN CLIENT M'A ENVOYÉ UN MAIL AVEC UNE PIÈCE JOINTE CONTENANT UN VIRUS… SUIS-JE COUVERT EN CAS DE SOUSCRIPTION D'UNE ASSURANCE CYBER RISQUES ? »

Tout acte de malveillance externe atteignant le système d'information et les données est généralement garanti dès lors qu'il résulte d'un virus ou d'un maliciel, peu importe le fait que le préposé ait ouvert la pièce jointe ou introduit la clé USB avec un virus.

Ce qui est la plupart du temps essentiel au titre des conditions d'octroi de cette garantie, c'est qu'un antivirus soit installé et à jour.

« MON SYSTÈME D'INFORMATION EST ALTÉRÉ SUITE À UNE ATTAQUE DE CELUI D'UN PRESTATAIRE, COMMENT SUIS-JE COUVERT EN CAS DE SOUSCRIPTION D'UN CONTRAT D'ASSURANCE CYBER RISQUES ? »

Si le système d'information du prestataire subit une attaque, il peut en résulter deux situations :

- Du fait de l'attaque, votre système d'information est altéré :
Le contrat d'assurance interviendra généralement pour prendre en charge les frais de décontamination de maliciel, les frais de reconstitution des données suite à incident de sécurité et les frais supplémentaires d'exploitation suite à une atteinte aux données et au système d'information.

- Du fait de l'attaque, les données de votre entreprise dans le système d'information du prestataire sont altérées :
Votre assureur prendra la plupart du temps en charge les frais supplémentaires d'exploitation suite à une atteinte aux données, en particulier les frais de réversibilité et de transfert des données gérées par un fournisseur informatique tiers (data center, hébergeur, fournisseur de cloud) chez un nouveau fournisseur en cas d'indisponibilité provisoire ou définitive du fournisseur tiers à la suite de la survenance de l'événement assuré.

EN CONCLUSION

Il subsiste certaines limites...
En effet, les utilisateurs d'internet avec qui vous êtes en relation, qu'il s'agisse de vos clients, de vos fournisseurs… sont libres de choisir leur niveau de protection, et beaucoup pensent que les mesures de protection prises par les autres suffisent.
Vous pouvez aussi être confrontés à des vendeurs de logiciels de sécurité ne sachant pas ou ne voulant pas dire quel niveau de sécurité est garanti par leur matériel…

Quoi que vous fassiez, le risque existera toujours. Vous ne pouvez que le diminuer voire l'assurer, mais pas l'annuler.
Et encore parle-t-on ici des risques connus… mais de nouveaux procédés d'attaques apparaissent tous les jours !

ATTENTION AUX IDÉES REÇUES !

« MON SYSTÈME INFORMATIQUE EST TRÈS FIABLE AVEC TOUTES LES SÉCURITÉS »

Aucun système n'est fiable à 100% !

Les institutions et les très grandes entreprises sont victimes d'attaques malgré les budgets de sécurité informatique très importants qu'elles investissent…
Sachez que votre entreprise est responsable de la sécurité des données à caractère personnel vis-à-vis des titulaires de ces données et vis-à-vis des autorités de régulation telles que la CNIL.
Il est préférable de disposer d'une couverture d'assurance contre ces cyber risques permettant au moins d'être accompagné pour la gestion de crise. En outre, en cas de responsabilité d'un prestataire externe, par exemple, il peut être appréciable d'être indemnisé par votre assureur et de le laisser se retourner contre le prestataire pour faire son propre recours…

« JE NE TRAITE PAS DE DONNÉES SENSIBLES »

Toutes les entreprises et tous les professionnels peuvent être amenés à gérer des flux de données, plus ou moins sensibles. (Exemple : paiement par carte bancaire, site internet...)

Le développement des échanges de données, qu'elles soient à caractère personnel, de santé, confidentielles, bancaires ou financières, s'est accompagné en parallèle d'un développement des obligations réglementaires et administratives qui y sont liées et sont parfois spécifiques à certains métiers !
Dès à présent, on observe que toute violation de données, sensibles ou pas, entraîne des conséquences qui peuvent affecter votre réputation et votre image de professionnel, ainsi que la responsabilité de votre entreprise si vos clients sont affectés par cette violation.

BIOGRAPHIE DE L'EXPERT

GÉRARD PELIKS,
EXPERT EN SÉCURITÉ DE L'INFORMATION, PRÉSIDENT DE L'ASSOCIATION CYBEREDU

Gérard Peliks a fait 40 ans de carrière auprès de grosses entreprises (Thales, Digital Equipement, Airbus Defense & Space, CNES, EADS…) comme expert en sécurité. Parallèlement, il donnait des cours sur la cyber criminalité et la cyber sécurité pour ses clients et dans des écoles d'ingénieurs. Aujourd'hui, Gérard Peliks donne toujours des cours et est directeur adjoint du MBA management de la sécurité des données numériques à l'Institut Léonard de Vinci. Il est aussi président de l'atelier sécurité du Forum Athéna, qui organise de grands événements sur la cyber sécurité. Enfin, il fait partie de la réserve citoyenne de cyber défense comme lieutenant colonel dans la gendarmerie. Depuis peu, il a été nommé président de Cyberedu, une association créée par l'ANSSI pour sensibiliser les enseignants en informatique afin qu'ils incluent dans leurs cours un enseignement sur la cybersécurité.

Gérard Peliks : gerard.peliks@forumatena.org

POUR ALLER PLUS LOIN : QUELQUES CONTACTS

- **Brigade d'enquête sur les fraudes aux technologies de l'information (BEFTI)**
  122/126, rue du Château des Rentiers – 75013 Paris
  Tél. : 01 55 75 26 19

- **Agence nationale de la sécurité des systèmes d'information (ANSSI)**
  51, boulevard de La Tour-Maubourg – 75700 Paris 07 SP
  Tél. : 01 71 75 84 05

- **Commission nationale de l'informatique et des libertés (CNIL)**
  8, rue Vivienne – CS 30223 – 75083 Paris cedex 02
  Tél : 01 53 73 22 22
  www.cnil.fr

- **Direction générale de la Sécurité intérieure (DGSI)**
  84 Rue de Villiers – 92300 Levallois-Perret
  Tél. : 01 77 92 50 00

- **Cyberedu, association pour l'intégration de la cybersécurité dans les formations en informatique**
  www.cyberedu.fr

NOTES

Une édition

assurédentreprendre.fr

Édité par Gan Assurances. Document non contractuel.
Dépôt légal : ISBN n° 979-10-96702-00-8 9791096702008. Achevé de rédiger en septembre 2016. Mis à jour en janvier 2017.
Gan Assurances – Société anonyme au capital de 109 817 739 euros (entièrement versé)
RCS 542 063 797 Paris – APE : 6512Z
Siège social : 8-10, rue d'Astorg – 75008 Paris – www.ganassurances.fr
Direction Qualité / Réclamations – Gan Assurances – Immeuble Michelet
4-8, cours Michelet – 92082 La Défense CEDEX – E-mail : reclamation@gan.fr
Entreprise régie par le Code des assurances et soumise à l'Autorité de contrôle prudentiel
et de résolution (APCR),
61, rue Taitbout – 75009 Paris.