REP : INTERVIEW
Brune Poirson

PANORAMAS
VÉRANDAS ET PERGOLAS
STORES

REPORTAGE
CES

PREVIEW
FENSTERBAU FRONTALE

verre& protections mag

N°116 • FÉVRIER-MARS 2020

vitrages menuiseries stores portes volets contrôles d'accès

17 € — ISSN 1773-1933

Cette rubrique est proposée en partenariat avec le Cabinet Seiler, expert en assurances spécialisé dans les domaines du vitrage et de la menuiserie.

GROUPE SEILER ASSUREUR CONSEIL
www.groupeseiler.com

Il y a du **virus** dans l'air…

Les cyberattaques ne sont plus réservées aux multinationales mais menacent désormais les menuiseries ou les miroiteries de tailles plus modestes et bien moins armées que les groupes mondialisés. Voici un état des lieux des moyens pour s'en prémunir.

Alors que le monde est tourné vers la Chine et tremble devant l'éventualité d'une crise sanitaire majeure liée à la propagation du coronavirus, Bouygues, le géant français du BTP, a à son tour été frappé par une attaque virale d'un autre type.
Bien entendu, il faut toutes proportions garder entre un évènement qui alarme la communauté mondiale et un autre qui ne mobilise que les services informatiques d'une entreprise.
Toutefois, on observe pour ces deux évènements une curieuse double analogie tant sur le mode de propagation que sur les mesures mises en œuvre entre :

- Un monde géographique et des modes d'échanges d'information ouverts.
- Les mesures de confinement de population et les décisions de coupure des systèmes d'information.

Si les sociétés de renom sont les plus visibles et donc les plus exposées, elles disposent également de moyens financiers, techniques et humains pour mieux se protéger et mettre en œuvre des plans de gestion de crise et de continuité d'activité prévus à l'avance.
En effet, en matière de virus de type ransomware ou rançongiciel dont il est question et dont l'objet est de faire peser une menace de destruction ou de cryptage des données de l'entreprise ciblée pour obtenir le paiement d'une rançon, la capacité de réaction est un élément clé.
Ainsi Bouygues a-t-il été en mesure de couper sans délai ses systèmes d'information pour éviter la propagation du virus.

Cyberattaques : quelques données clé

Dans son dernier rapport l'ANSSI (Agence nationale de sécurité des systèmes d'information) relève que l'année 2018 a vu la multiplication d'attaques par rançongiciel impactant des entreprises et institutions dans le monde entier.
Elles dépassent désormais en nombre celles impactant les particuliers, et représentent actuellement **la menace informatique la plus sérieuse pour les entreprises et institutions.**

> 60 % des PME mettent la clé sous la porte après une attaque.

Sur les nombreuses attaques de ce type en France, l'ANSSI a traité 69 incidents en 2019 sur son périmètre, et en distingue 2 typologies :

- La grande majorité des attaques par rançongiciels s'avère être opportunistes et profitent de la faible maturité en sécurité numérique de leurs victimes.
- De plus en plus de groupes cybercriminels ciblent spécifiquement des entreprises financièrement solides (attaques dites **"Big Game Hunting"**).

Les actions malveillantes sont réalisées par des groupes d'attaquants aux ressources financières et aux compétences techniques importantes, et présentent un niveau de sophistication s'apparentant à des opérations d'espionnage institutionnel.
Alors que les montants habituels de rançons s'élèvent à quelques centaines ou milliers de dollars, celles demandées lors des attaques "Big Game Hunting" sont à la mesure de la cible et peuvent atteindre **des dizaines de millions de dollars.**
Depuis fin 2019, l'ANSSI constate également que certains groupes cybercriminels cherchent à faire pression sur leurs victimes en divulguant des données internes préalablement prélevées du système d'information infecté.
On parle alors de compromission informatique, l'objectif étant d'atteindre la réputation de l'entreprise ciblée, en démontrant que sa capacité à garantir l'intégrité et la confidentialité des données qui lui sont confiées est défaillante.
Dans ce cadre, on peut citer les cas d'Altran en janvier 2019, Fleury Michon en avril 2019, Ramsay Générale de Santé en août 2019, ou encore le CHU de Rouen en novembre 2019 (source ANSSI).
Le prestataire spécialisé Accenture relève, lui, qu'alors que le nombre de cyberattaques a diminué au cours de la dernière année (passant de 232 en 2018 à 206 en 2019), 40 % des incidents de sécurité proviennent d'attaques indirectes de cybercriminels ciblant les systèmes d'information de tierce partie (partenaires, sous-traitants, prestataires,...).
Ces cyberattaques à l'encontre de l'écosystème de partenaires sont considérées comme "cachées". Si on tient compte de ces évènements indirects, il y a lieu de constater que le nombre moyen de cyberattaques visant une entreprise serait en augmentation de 25 % sur une année.

Un risque avéré à prendre en compte

On le constate, le Cyber Risk s'est installé durablement comme une des menaces majeure pour les acteurs économiques.
Les outils numériques sont au cœur de la vie de chaque entreprise (e-mails, site internet, stockage de données, etc.). Ils accompagnent le développement de votre activité professionnelle mais vous exposent à de lourdes menaces.
La prise en compte et maîtrise de ces risques est donc un facteur essentiel de continuité de votre entreprise.

Établir une cartographie de son risque "Cyber"

Vous devez ainsi vous poser quelques questions, notamment :

- Mes données sont-elles susceptibles d'intéresser un tiers, la concurrence ?
- Mon système d'information est-il correctement protégé ?

• Quel serait l'impact d'une cyberattaque privant temporairement, partiellement ou totalement mon entreprise de l'accès à ses systèmes d'information ?
• Dans quels délais et par quels moyens puis-je réagir en cas d'incident ?
Comme les études ci-avant évoquées l'ont montré, les PME-PMI constituent soit des cibles d'opportunité du fait de leur niveau de sécurité plus limité soit des cibles indirectes du fait de leurs relations économiques avec des sociétés de premier plan.

Les TPE-PME représentent en effet 77 % des victimes d'attaques numériques en France.
Au sein de 66 % d'entre elles, ne disposant pas d'équipe dédiée aux questions informatiques, le chef d'entreprise endosse cette responsabilité.
Les TPE-PME ne sont en général pas assurées pour les incidents numériques.

Protéger votre entreprise

La sûreté informatique de votre entreprise passe donc d'abord par une démarche d'analyse de votre exposition à ces risques spécifiques puis par la mise en place d'une politique de prévention adaptée.
Ce process doit être porté par une personne de l'entreprise, clairement identifiée, en charge de la mise en place et du suivi de cette politique de management du cyber risque.

Cette politique doit reposer sur 3 piliers :
- les facteurs humains et organisationnels :
  – Gestion des sauvegardes, des mots de passe, consignes en cas de connexion externe, charte informatique.
  – Mise à jour du système d'exploitation.
  – Culture de la vigilance (clés USB, téléchargements, verrouillage des sessions en cas d'absence, ouverture de mail).
- des outils de protection (antivirus, pare-feu, cryptage des données sensibles, protection des accès distants et des matériels nomades).
- une anticipation de la gestion de crise par des outils.

Quelle que soit son origine, l'incident numérique menace le système informatique des entreprises, ce qui entraîne une série de conséquences sur leur capital immatériel ou sur celui de tiers (données, image de marque, propriété industrielle).
A cause d'une baisse ou d'une interruption d'activité : 60 % des PME mettent la clé sous la porte après une attaque.

Examiner les conditions de transfert du risque vers l'assurance

Aussi et au-delà de l'attention qu'il faut apporter à ces protections, il faut analyser les conditions de transfert du risque vers l'assureur tout

en étant conscient que les contrats d'assurance classiques (multirisques, bris de machines, responsabilité civile) ne couvrent pas ce type d'événements.
Des réponses accessibles et simples existent désormais au travers de contrats d'assurance spécifiques présentés dans un format (garanties, prestations de services, tarifs) adapté aux PME-PMI et TPE.
Leur objet est à la fois de réparer les conséquences des incidents numériques, de les protéger contre l'extension des risques et permettre la pérennité de leur activité.
Ils garantissent les dommages subis ou causés par l'entreprise suite à une atteinte à son système informatique ou à ses données.

Le champ des garanties proposées est donc double :
Dommages et pertes
Le contrat prend en charge plusieurs types de frais pouvant s'avérer particulièrement onéreux pour une entreprise (frais d'expertise informatique ou de reconstitution des données, coûts liés à la notification, pertes d'exploitation...).
La prestation se caractérise donc par une grande réactivité pour faire face au plus vite aux incidents détectés et parer dès l'origine à toute extension du risque.
Cet accompagnement est disponible 24h/24 et 7j/7 et prend la forme :
- de la mise à disposition d'un expert informatique faisant partie d'un réseau de professionnels en sécurité informatique en capacité d'intervenir sur toute la France, et qui va prendre en charge l'ensemble de la prestation technique liée à l'incident numérique (diagnostic technique, mesures conservatoires et prestations liées à la restauration et la reconstitution des données).
- d'une assistance pour la mise en œuvre des notifications réglementaires impliquées par le RGPD (Règlement général sur la protection des données de l'UE) en vigueur depuis mai 2018 qui fait obligation, sous peine de sanctions financières lourdes, à toutes les entreprises quels que soient leur taille et leur secteur d'activité. en cas d'atteinte à des données à caractère personnel, de notification dans des délais très courts :
  – Aux autorités administratives compétentes ;
  – Aux personnes physiques concernées (clients, salariés).
- d'une prestation spécialisée en cas d'atteinte à la réputation.
  Mise à disposition d'une agence de communication si besoin pour éviter la perte de confiance des clients et la dégradation de l'image de votre entreprise.
- d'une assistance technique en cas de tentative de cyber extorsion. L'assureur, dans la plupart des cas, la prendra en charge.
- d'une indemnisation pour les pertes d'exploitation et frais supplémentaires, si cette attaque engendre une perte de chiffre d'affaires.

Responsabilité civile
Le contrat offre également une protection en cas de dommages causés à des tiers (clients, fournisseurs, sous-traitants...), consécutivement à des incidents numériques subis par l'entreprise assurée.

En conclusion, le lecteur a bien perçu que les risques se déplacent des actifs matériels (bâtiments, marchandises...) vers les actifs immatériels sur lesquels se concentrent désormais et de façon durable les actes de malveillance.
L'heure est donc à une prise de conscience et à une action résolue pour mieux appréhender et se protéger contre ces risques, qui ne peuvent plus être maintenant qualifiés seulement d'émergents.
Retrouvez tous ces conseils et d'autres bonnes pratiques dans le guide édité par la Confédération des petites et moyennes entreprises (CPME) et l'Agence nationale de la sécurité des systèmes d'information (ANSSI) : www.ssi.gouv.fr ■