+ PANORAMA GARDE-CORPS

VERRE & PROTECTIONS mag

SPÉCIAL TERTIAIRE

N°98 JUILLET 2017

vitrages menuiseries stores portes volets contrôles d'accès

Actu

Création de deux Unions distinctes à la FFPV

Vitrage

Inauguration de la nouvelle ligne "float" d'Aniche

Menuiserie

Une étude confirme l'efficacité du remplacement des fenêtres et volets

Protection

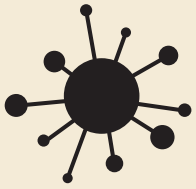
Étude TBC : reprise pour le marché des portes d'entrée en 2017

17 € – ISSN 1773-1933

*Posez votre question, un **expert en assurances** y répondra. Tel est le fonctionnement des plus simples de cette rubrique que nous proposons à nos lecteurs en partenariat avec **le Cabinet Seiler,** expert en assurances et spécialisé dans les domaines du vitrage et de la menuiserie.*

www.groupeseiler.com

Wanna Cry!*



LA QUESTION DE NOTRE LECTEUR

« Je suis responsable façade et, comme tout le monde, j'ai énormément d'échanges sur le net. Compte tenu de toute l'actualité, sommes-nous vraiment menacés par la cybercriminalité ? Quelles précautions puis-je prendre ? En quoi mon assureur peut-il m'aider pour me protéger ? »

LA RÉPONSE DE L'EXPERT

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 nouvelles menaces : les risques numériques.
La maîtrise de ces risques est un gage de continuité de votre entreprise.
Les incidents numériques sont en hausse constante et concernent toutes les entreprises, quels que soient leur taille et leur secteur d'intervention.

Qu'est ce que le risque numérique ?

C'est l'ensemble des événements, malveillants ou non, susceptibles d'altérer les données ou les systèmes d'information :

- Logiciels criminels ;
- Vols et fuites de données ;
- Erreurs diverses ;
- Attaques des applis Web ;
- Attaques par DoS2 - L'attaque par déni de service, ou DoS (en anglais Denial of Service), vise à perturber, ou paralyser totalement, le fonctionnement d'un serveur informatique en le saturant ;
- Cyber-espionnage ;
- Fraude à la carte bancaire...

"Wanna cry", qui signifie "envie de pleurer" est le nom d'une cyber attaque mondiale qui a eu lieu en juin dernier.

En quoi êtes-vous concerné par les cyber-risques ?

Vous devez vous poser quelques questions, notamment :

- Mes données sont-elles susceptibles d'intéresser un tiers, la concurrence ? Mon système d'information est-il correctement protégé ?
- En cas de cyber attaque, mon entreprise serait-elle affectée si je ne pouvais plus accéder à mon système d'information ou à mes données ? Une baisse significative d'activité est-elle à craindre ?
- Un arrêt total, mettant en péril l'existence même de mon entreprise, peut-il être envisagé ?
- Ai-je mis en place un plan de continuité d'activité en cas d'indisponibilité de mon système d'information ou de mes données ?
- Qui contacter en cas de cyber attaque pour gérer cette crise ?

Si vous n'avez pas de réponse satisfaisante à ces questions notamment, **vous êtes vulnérables.**
Si vous êtes vulnérables, **vous devez vous protéger**...

Cette protection passe par un audit attentif de vos pratiques.

Les TPE-PME sont les cibles privilégiées de cyber-risques aux conséquences lourdes pour leur activité

La majorité des PME ne pensent pas être exposées car elles estiment exercer une activité non ciblée, être dans une struc-

CHIFFRES MARQUANTS

- +140 % de cyberattaques
- Les TPE-PME représentent 77% des victimes d'attaques numériques en France
- 38% de nos ordinateurs personnels stockent des fichiers illicites à notre insu
- 47% des entreprises ont éprouvé des intrusions suite à des brèches présentes dans des appareils mobiles
- 38% des victimes d'une attaque DDoS ont été dans l'incapacité de poursuivre leur activité principale
- + 17% d'infections touchant les terminaux

Source : http://lenetexpert.fr.

ture trop petite, procéder à un faible usage d'Internet et bénéficier de protections fiables.
Pourtant, au regard de la fréquence déclarée des sauvegardes et des antivirus utilisés, l'étude menée par l'Ifop en juin 2016 sur les cyber-risques révèle un niveau de protection limité.
Les TPE-PME se caractérisent par une vulnérabilité accrue par rapport aux grandes entreprises. Leurs moyens en matière de sécurité informatique sont limités. 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, face auxquels elles éprouvent le besoin d'une solution simple et d'une relation de proximité.

Seule 1 entreprise sur 3 se dit consciente d'être exposée aux cyber-risques.

Protéger votre entreprise

La sûreté informatique de votre entreprise passe d'abord par une démarche d'analyse de votre exposition à ces nouveaux risques, 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 ;
- des outils de protection ;
- une anticipation de la gestion de crise par des outils.

Exemples de bonnes pratiques et d'outils à mettre en œuvre pour réduire votre risque cyber

- **Mettre à jour** votre système d'exploitation et ses logiciels ;
- Effectuer des **sauvegardes** a minima de façon hebdomadaire ;
- **Se méfier des clefs USB** et disques durs externes : échanges via clef USB ou moyens similaires à proscrire ou mise en place d'une procédure de scan anti-virus ;
- **Protéger et détruire** les données sensibles (broyeur, destruction des disques durs lors d'échange de matériel) ;
- **Verrouiller votre session** dès que vous vous absentez ;
- Installer, utiliser et mettre à jour une suite de **sécurité antivirus** ;
- Choisir des **mots de passe complexes** avec des majuscules, minuscules, chiffres, caractères spéciaux... ;
- Utiliser un logiciel de **gestion de mots de passe** préconisé par l'ANSSI **(Agence nationale de la sécurité des systèmes d'information) ou la CNIL (Keepass, Zenyway...) et désactiver celui des navigateurs ;
- Imposer le **changement régulier** des mots de passe ;
- **Chiffrer** les données sensibles sur vos ordinateurs ;
- Ne jamais **cliquer sur un lien** dans un e-mail vous demandant de vous identifier ;
- Ne jamais ouvrir les pièces jointes avec les **extensions** .pif, .bat, .com, .exe, .lnk... ;
- **Interdiction de téléchargement** de logiciels ou contenus non autorisés ;
- Ne saisir vos **données personnelles** que sur des sites sécurisés (identifiables par la présence d'un cadenas) ;

- **Consignes de travail en déplacement** ou en dehors du bureau (accès à distance) ;
- **Protection contre le vol des outils nomades d'informations et de leurs données** (chiffrement des supports, interdiction de laisser les ordinateurs portables dans les voitures).

➔ 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

Celles-ci sont à reprendre dans une Charte informatique, document à faire signer par tout le personnel

Les protections usuelles ne suffisent plus face à des risques numériques en constante mutation.
Les formes des cyberattaques évoluent tous les jours : les virus, fléaux majeurs il y a quelques années, sont aujourd'hui supplantés par les ransomwares (prise d'otage des données personnelles) ou des attaques sophistiquées exploitant les failles des logiciels informatiques.

La plupart des entreprises n'ont souvent pas conscience d'être victimes, **les atteintes étant bien souvent non détectables immédiatement.** Leurs effets peuvent être lents et progressifs, parfois sur plusieurs années.
Par ailleurs, le système informatique peut aussi constituer **une porte d'entrée pour attaquer l'un des clients ou des fournisseurs.**
Conséquences : de la perte de chiffre d'affaires à l'arrêt de l'activité.
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).
Baisse ou interruption d'activité : 60 % des PME mettent la clé sous la porte après une attaque.

Aussi et au-delà de l'attention qu'il faut apporter à ses 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 polices d'assurance spécifiques jusqu'à présent destinées aux Sociétés du CAC 40 sont maintenant disponibles dans un format (garanties, prestations de services, tarif) adapté aux PME-PMI et TPE.
Leur fonction est à la fois de réparer les conséquences des incidents numériques et de les défendre contre l'extension des risques et assurer la pérennité de leur activité.
Ces contrats 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 & 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 **réactivité assurée dès le premier appel**, 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 à votre disposition dans 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). Limitée jusqu'à présent aux opérateurs de l'internet, **la réglementation européenne va étendre l'obligation de notification à toutes les entreprises quels que soient leur taille et leur secteur d'activité.**
  En cas d'atteinte à des données à caractère personnel, celles-ci seront tenues à compter de mai 2018 d'informer dans des délais très courts :
  – Les autorités administratives compétentes ;
  – Les personnes physiques concernées, par ex. vos clients.
  À compter de mai 2018, date d'entrée en application du règlement européen, le non-respect de cette obligation vous expose à de lourdes sanctions financières ;

- **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 de dégradation de l'image de votre entreprise ;
- **D'une assistance technique en cas de tentative de cyber extorsion :** une rançon peut vous être réclamée pour déchiffrer vos fichiers suite au cryptage de vos données. 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 peuvent être maintenant qualifiés d'émergents. ■