CYBER SECURE

Une réponse adaptée pour
la maîtrise de vos risques cyber

assurance citoyenne

Nouveaux risques cyber

Et si cela vous arrivait ?

PIRATAGE
SITE INTERNET

Un domaine viticole de Bourgogne a créé, il y a 4 ans, un site e-commerce afin de vendre son vin à un plus large public. L'entreprise se développe et attire la convoitise. En décembre 2015 – période de commande pour les fêtes, des hackers réussissent à pirater le site Internet et à le mettre hors-service, ce qui entraîne l'arrêt pendant 5 jours de son activité de vente sur Internet représentant 10 % du total de ses ventes.

- **Coût total du sinistre** : 48 000 € avant franchise
- **Prise en charge** : frais d'expertise et d'assistance informatique, frais de remise en état du site Internet, frais de re-référencement, pertes d'exploitation de l'activité Internet.

CYBER-EXTORSION
DE FONDS

En Isère, une entreprise spécialisée dans les études techniques (fluides, électricité, traitement de l'air…) **propose régulièrement ses services dans le cadre de constructions industrielles de grande ampleur**. Son dirigeant, Monsieur X, diplômé d'une grande école d'ingénieur a créé cette structure, après cinq années en tant qu'ingénieur. L'entreprise compte à ce jour 14 salariés dont 12 cadres.

Des hackers ont récupéré l'identité de Monsieur X sur les réseaux sociaux professionnels afin de se faire passer pour lui par mail auprès des salariés de l'entreprise. Le mail frauduleux contenant, en pièce-jointe, un logiciel malveillant (malware) est ouvert par un des salariés.

Son ouverture entraîne l'intrusion dans le système informatique permettant ainsi aux hackers d'accéder aux données comptables et de détourner 100 000 € en modifiant les coordonnées IBAN de RIB.

- **Coût total du sinistre** : 105 000 €
- **Prise en charge** : frais d'expertise et d'assistance informatique, pertes pécuniaires.

RANSOMWARE
CRYPTAGE DONNÉES CLIENTS

Un petit cabinet d'expertise comptable de région parisienne commence à se faire un nom dans le domaine, en axant son développement sur l'accompagnement social des entreprises en plus de l'expertise comptable.

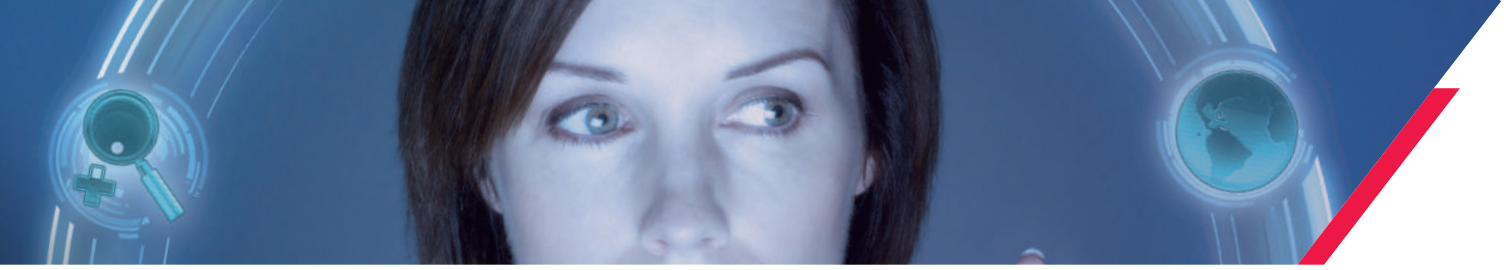
En janvier 2016, le cabinet est « sous l'eau » du fait de la mise en place de la mutuelle santé obligatoire dans les entreprises. C'est le moment choisi par un hacker pour s'infiltrer dans le système d'information du cabinet et ainsi crypter toutes les données clients par le biais d'un cryptolocker.

Le hacker affirme décrypter les données si une rançon de 2 000 € lui est versée. Les 9 salariés du cabinet, tributaires de l'informatique, se retrouvent dans l'impossibilité de travailler pendant plusieurs jours.

- **Coût total du sinistre** : 34 000 €
- **Prise en charge** : frais d'expertise et d'assistance informatique, frais de reconstitution des données, pertes d'exploitation.

☑ **Avec son assureur, l'entreprise a fait le choix de ne pas payer la rançon pour des raisons de moralité**. L'assureur a pris en charge les frais notamment de reconstitution des données et les pertes d'exploitation, bien que ce soit au total plus élevé que le montant de la rançon demandée. Outre la raison d'éthique, c'est aussi plus sûr et plus efficace que de payer une rançon à l'efficacité incertaine.

☑ **Suite à cette attaque, l'entreprise a suivi les recommandations de son assureur pour s'équiper en prévention d'un outil de détection comportementale des logiciels suspects** (solution SES proposée par Stormshield, filiale d'AIRBUS D&S, partenaire d'AXA), de façon à ne plus jamais avoir de cryptolocker.



MALVEILLANCE INTERNE
AVEC VOL DE DONNÉES

Un cabinet médical réunissant quatre médecins et une infirmière a mis en place une plateforme d'appels afin d'enregistrer les demandes de consultations. Deux réceptionnistes se relayent dans la prise de RDV et ont accès à toutes les données (historique de santé et informations médicales) des patients via le serveur du cabinet.

En avril dernier, un des réceptionnistes n'obtient pas satisfaction sur une requête faite auprès de son responsable et démissionne. Afin de « faire payer » son employeur, ce « petit génie de l'informatique », introduit dans le système informatique un logiciel malveillant via une clé USB.

Le logiciel remonte au poste administrateur et récupère l'ensemble des données médicales des patients. Le but pour l'ancien salarié étant de diffuser purement et simplement les informations sur Internet et ainsi mettre en péril le cabinet médical.

- **Coût total du sinistre** : 77 000 € avant franchise
- **Prise en charge** : frais d'expertise et d'assistance informatique, frais de notification clients (10 € par client), frais de nettoyage des données et noyage des informations, frais de protection juridique.

☑ **L'action pilotée par l'assureur a permis de ne pas effacer les preuves de la malversation lors de l'intervention des experts informatiques**. Cela a ainsi permis d'être plus efficace dans l'action judiciaire intentée envers l'ancien salarié de façon à lui demander réparation et SURTOUT dédouaner l'entreprise de sa responsabilité notamment vis-à-vis de la CNIL.

☑ **L'ancien salarié a été condamné** à 3 ans de prison dont 2 avec sursis ainsi qu'au remboursement de 70 000 € de dommages et intérêts.

USURPATION
D'IDENTITÉ

Une entreprise du bâtiment est victime d'une usurpation d'identité destinée au détournement de sa clientèle. En effet, en effectuant une recherche sur le moteur Internet de Google, elle s'est aperçue qu'un concurrent a référencé son entreprise sur son site Internet.

L'intégralité de ses coordonnées professionnelles, à l'exception de son numéro de téléphone a été reprise par ce dernier. Au surplus, en cliquant sur le lien « demander un devis », c'est l'adresse du contact commercial de ce concurrent qui s'affiche.

Notre assuré sollicite l'assistance de son juriste de la protection juridique.
Le juriste a alors adressé une lettre de mise en demeure en mettant en cause le tiers sur le fondement des articles L 226-4-1 du Code pénal et de l'article 38 de la loi informatique et libertés. Il lui a alors indiqué faire constater ces pratiques par voie d'huissier et saisir la juridiction compétente à défaut de prompt règlement amiable.

Peu de temps après, le concurrent a procédé à la désactivation de son inscription sur l'annuaire.

DÉNIGREMENT
SUR INTERNET

Un office notarial de 8 personnes constate en juin 2016 un dénigrement de son activité sur Internet. Il sollicite l'assistance de sa protection juridique afin qu'un noyage des propos diffamatoires soit effectué.

Le juriste de la protection juridique a saisi une société spécialisée dans l'e-réputation afin qu'il soit procédé :
- à une analyse de l'atteinte à l'e-réputation consistant à définir la date d'origine de l'atteinte, à trouver l'endroit où s'exerce le préjudice (site, blog...), à déterminer les circonstances du préjudice et rechercher l'auteur de l'atteinte à l'e-réputation ;
- au nettoyage des informations ;
- ou à défaut, au noyage des informations.

La partie adverse refuse de procéder au retrait des propos dénigrants.

La société spécialisée dans l'e-réputation a alors noyé ces informations moyennant la somme de 900 €.

Cette action a été précédée d'un constat d'huissier, notre assuré souhaitant engager une action en justice pour contraindre le forum à supprimer les messages litigieux (bien que noyés) et obtenir une indemnisation pour le préjudice causé.
Le juriste a saisi un avocat. L'action judiciaire est en cours...

Avant que ça ne vous arrive...

... Souscrivez Cyber Secure auprès de votre intermédiaire AXA pour bénéficier

☑ d'une solution simple et complète adaptée aux PME **pour faire face aux nouvelles menaces informatiques**

☑ d'une assistance téléphonique **dédiée aux risques cyber**, disponible **24h/24, 7j/7**

☑ du **service crise majeure en inclusion** qui prévoit des conseils en communication de crise d'une agence spécialisée en cas de mise en cause médiatique de votre entreprise

Réf. 971087 10 2016 - AGI - Crédits photos : Photononstopo

réinventons / notre métier