LE POINT SUR...

SMABTP
BÂTIR L'AVENIR AVEC ASSURANCE

Fiche technique assurance réalisée par SMABTP

mai 2019

Assurance de responsabilité N°67

LES CYBER RISQUES

L'usage généralisé de l'informatique et d'internet dans tous les secteurs de l'économie et dans la vie privée, la multiplicité des échanges électroniques avec les fournisseurs, les clients, les salariés, les partenaires font qu'aujourd'hui aucun professionnel ne peut se considérer à l'abri. Parallèlement, on a pu observer une industrialisation des attaques, plus ciblées, mieux organisées. La diffusion mondiale du virus Wannacry est un exemple probant : en Mai 2017, celui-ci a touché en moins d'une semaine 300 000 ordinateurs répartis dans plus de 150 pays.

Ce fléau concerne désormais toutes les entreprises et pas uniquement les grands groupes des secteurs de la finance !

Selon une enquête produite par la CPME début 2019, 41% des entreprises françaises de 0 à 9 salariés et 44 % des entreprises de 9 à 49 salariés ont subi une ou plusieurs attaques ou tentatives d'attaques informatiques.

QU'EST-CE QUE LA CYBERCRIMINALITÉ ?

Ce sont tous les risques liés à l'utilisation des systèmes informatiques et aux données qu'ils contiennent. On peut parler d'intrusion, de contamination (virus, bombes logiques) ou d'atteinte aux systèmes informatiques réalisée dans un but malveillant qui va cibler tous les outils informatiques que l'entreprise utilise au quotidien pour son activité : ordinateur, serveur, imprimantes, téléphone mobile, tablette…

Elle prend de très nombreuses formes et peut avoir de très lourdes conséquences :

- Dysfonctionnement, voire arrêt, du système de gestion d'une entreprise (plus possible de faire des devis, d'éditer les factures par exemple), d'un site internet, d'un outil de production industrielle
- Vol de données relatives à l'activité, appartenant à des tiers, des collaborateurs, des clients, des fournisseurs
- Demande de rançons, cyber-extorsions et chantage au blocage informatique ou à la diffusion d'informations confidentielles
- Sabotage ou suppression de données, actes de malveillance venant de tiers, de collaborateurs ou d'anciens salariés
- Atteinte à la propriété intellectuelle par la diffusion publique d'informations confidentielles, de brevets…

Les conséquences de ces attaques varient selon leur nature : elles se traduisent le plus souvent par un manque à gagner en termes de chiffre d'affaires, de résultats et par des frais de remise en état des données et des systèmes d'information. Sans parler de la réputation qui peut être entachée. Dans les cas les plus graves, certaines TPE ont même été conduites à la cessation d'activité

COMMENT SE PRÉMUNIR CONTRE LES CYBER RISQUES ?

La prévention : c'est le premier moyen de se protéger

Il convient en premier lieu de mettre en place des règles et moyens de prévention, dont la plupart relèvent du bon sens :

▸ établir des procédures

mettre en place des process de sauvegarde des données, réaliser des sauvegardes régulières…

gérer et contrôler les habilitations et droits d'accès aux systèmes d'informations et aux seuls éléments nécessaires à l'exécution des tâches confiées, mettre en place des règles en matière de mots de passe, élaborer un plan de continuité d'activité, auditer la sécurité des systèmes d'information,

▸ se protéger et sécuriser :

renforcer la sécurité des équipements, notamment ceux connectés à internet,

équiper tous les postes de l'entreprise d'antivirus et tenir à jour ces antivirus, appliquer les correctifs des logiciels,

▸ sensibiliser et former les collaborateurs de l'entreprise :

apprendre à être prudent vis-à-vis des mails douteux, imposer des règles en matière de mots de passe, ne pas les laisser afficher sur un post it aux yeux de tous !

L'entreprise peut aussi souscrire une assurance

En dépit du respect de ces bonnes pratiques, la survenance d'un incident informatique risque toujours de se produire et il existe des solutions de transfert de ce risque à l'assurance via des contrats de Cyber risques comportant 2 volets.

Le premier est une assistance, accessible 24 h/24 et 7 j/ 7, permettant l'intervention d'experts informatiques, d'avocats et de conseils en relation publique pour pallier les difficultés rencontrées. Ces experts informatiques permettront également de recueillir la preuve légale de ce qui s'est passé pour pouvoir porter plainte et faire les recours possibles. C'est aussi le moyen le plus sûr d'avoir accès aux spécialistes maîtrisant la problématique technique rencontrée.

Le second volet, habituel pour un contrat d'assurance, consiste à prendre en charge, tant les conséquences de la responsabilité de l'entreprise que les dommages subis par elle-même, comme :

- les conséquences pécuniaires, y compris les frais de défense, de la mise en cause de la responsabilité de l'entreprise en cas de transmission de virus à des tiers ou en cas de compromission des données personnelles détenues, que ces dernières appartiennent à des employés, des clients ou des fournisseurs.
- les frais de décontamination,
- les frais de reconstitution des données,
- les frais de notification de la compromission à des tiers.

Des garanties complètes permettent à l'entreprise de faire face aux multiples conséquences d'une attaque informatique. C'est pourquoi il est essentiel de parler cyber risque avec votre conseiller et de mettre en place la solution adaptée à vos besoins.

SMA

RETROUVEZ l'intégralité des fiches "Le point sur..."sur le site internet SMA
www.groupe-sma.fr rubrique "l'espace documentaire"