FRANCE ASSUREURS
FAIRE AVANCER LA SOCIÉTÉ EN CONFIANCE

DOCUMENT DE POSITION

POUR ACCÉLÉRER LA CYBER-RÉSILIENCE DE L'ÉCONOMIE FRANÇAISE

Synthèse

La crise du Covid-19 a accéléré l'expansion du risque cyber et l'explosion des cyberattaques a mis en lumière la **vulnérabilité de l'ensemble des acteurs économiques** (entreprises, collectivités territoriales, associations, hôpitaux**) en termes de sécurité informatique**. Le **risque cyber** s'est révélé **difficile à évaluer et protéiforme**. Il est donc nécessaire **d'améliorer la connaissance de ce risque majeur**.

Depuis 2020, les assureurs ont alerté les pouvoirs publics sur le niveau insuffisant de sécurité informatique des entreprises, et notamment des TPE et PME, les conduisant à être plus exigeants pour couvrir le risque cyber.

Les assureurs considèrent la **prévention du risque cyber comme un préalable indispensable pour se prémunir contre les attaques potentielles**. La maîtrise du risque cyber ne passe pas par l'assurance mais par la prévention.

Le cadre réglementaire actuel n'est pas propice au développement de ce marché, puisque les règles du remboursement par l'assureur d'un rançongiciel ne sont pas clairement fixées. Au regard des débats actuels, les assureurs souhaitent donc que les pouvoirs publics français et européens s'expriment clairement sur la légalité de l'assurabilité du remboursement des rançons.

Analyse

L'émergence du risque cyber a fait éclore des premières actions de prévention en lien avec les pouvoirs publics pour atténuer ce risque. Les assureurs sont membres du dispositif cybermalveillance.gouv.fr depuis ses débuts en 2017.

Depuis le déclenchement de la crise sanitaire, les cyberattaques par rançongiciel ont été multipliées par 4 en 2020, et cette tendance se poursuit pour 2021 avec une hausse de 60 %, selon l'Agence nationale de la Sécurité des systèmes d'information (ANSSI). Les tentatives d'hameçonnage ont augmenté de 400 % dès la première semaine du confinement[1] en mars 2020, et les règles de base de cybersécurité ont souvent été oubliées.

Plus récemment, en septembre 2021, les assureurs ont signé avec la Gendarmerie nationale et AGEA, la Fédération nationale des syndicats d'agents généraux d'assurance, un partenariat inédit pour former et sensibiliser les agents généraux d'assurance au risque cyber, grâce aux équipes d'experts de la gendarmerie. C'est une étape importante pour la diffusion de conseils de prévention, notamment à destination des TPE et des PME à grande échelle et au niveau local.

Cependant, il y a un vrai sujet autour de l'indemnisation des rançons dont le cadre réglementaire doit être clarifié tant à un niveau national qu'européen. Une interdiction nationale ne résoudrait pas le problème de la distorsion de concurrence entre entreprises victimes selon qu'elles sont établies dans un Etat membre qui autorise ou non l'assurabilité du risque de rançongiciel. Les TPE et les PME sont les plus vulnérables. Il s'agit d'un sujet de **souveraineté économique** puisque 50 % des PME qui ont subi une cyberattaque paralysante disparaissent dans les six mois qui suivent[2].

[1] Jean-Jacques Latour, responsable de Cybermalveillance.gouv.fr - Le Figaro - avril 2021.

[2] Bâtir et promouvoir une souveraineté numérique nationale et européenne, Assemblée nationale, juin 2021.

Proposition des assureurs

Pour accélérer **la « cyber-résilience » de l'économie française**, et le transfert du risque aux assureurs, les assureurs proposent :

1. **Développer la culture du risque cyber** au sein de l'ensemble des acteurs économiques pour **protéger les entreprises contre les conséquences financières de la survenance d'une attaque cyber** :
   - **sensibiliser à la gravité du risque cyber** auprès d'une cible complète (dirigeants, collaborateurs, mais également les maires et leurs services techniques) ;
   - **définir** des **règles de sécurité informatique à respecter** ;
   - **mettre en place un cadre normatif de certification pour la sécurité informatique** ;
   - **élaborer un socle minimum de prévention/protection** cyber par typologie d'entreprise (TPE, PME, ETI) et par niveau d'exposition aux risques cyber ;
   - **développer les filières** de **prestataires informatiques labellisés** Experts Cyber[3].

2. Obtenir une position claire de l'État français et l'UE sur la **légalité de l'assurabilité** du remboursement des rançons**.**

3. Dans l'attente de ces textes, dès lors qu'un assureur décide de couvrir le remboursement des rançons, il s'engagerait à **respecter des bonnes pratiques tant en matière de souscription que d'indemnisation**, dans le respect du droit de la concurrence.

4. Une **collaboration doit être bâtie entre assureurs et autorités judiciaires et policières pour encadrer au mieux le paiement de rançons** (information systématique d'une entité de la police judiciaire, du parquet de Paris, communication des adresses IP de paiement).

[3] Label Expert Cyber de cybermalveillance.gouv.fr.