FICHE « Pour approfondir » : **Cybersécurité des entreprises :**

comment mieux protéger les TPE et les PME ?

*Le coût mondial de la cybercriminalité est évalué à 6 000 milliards de dollars pour l'année 2021. Rapporté à l'échelle d'un pays, le coût du cyberrisque est au niveau de la troisième économie mondiale. Selon un récent rapport du Sénat, les en*treprises, particulièrement les TPE [Très Petites Entreprises] et les PME [Petites et Moyennes Entreprises], sont souvent exposées à des incidents de cybersécurité.

Le développement du e-commerce depuis quelques années et le recours massif au télétravail, du fait de la crise sanitaire, ont accru les risques de cyberattaques.

Un **rapport d'information relatif à la cybersécurité des entreprises**, remis au Sénat le 10 juin 2021, dresse le bilan de cette menace et de sa prise en compte par les entreprises et les pouvoirs publics. Face à ce constat, le rapport propose également un certain nombre de réponses afin de mieux aider les TPE et les PME à faire face à la cybercriminalité.

1 - Un enjeu majeur longtemps négligé

Plusieurs facteurs ont accéléré et banalisé la cybercriminalité :

- la numérisation de l'économie (e-commerce, télétravail, déploiement de la fibre) ;
- la professionnalisation de la cybercriminalité (plateformisation, cryptomonnaies...) ;
- la difficulté de la prévention et de la répression (manque de coordination internationale) ;
- l'exploitation de failles dans le cyberespace à des fins **géopolitiques.**

Toutes les entreprises sont concernées par les cyberattaques qui peuvent conduire à leur fermeture. Chaque utilisateur d'un outil numérique peut être le point d'entrée d'une attaque.

Longtemps, les petites et moyennes entreprises(TPE et PME) ne se sont pas senties concernées. Le basculement a eu lieu avec l'arrivée de **plus de 8 millions de salariés en télétravail** au printemps 2020. Les services informatiques mettent désormais en place le concept **zero trust** (confiance zéro) : aucun utilisateur sur un réseau n'est totalement digne de confiance. **La notation ESG (environnement, sécurité, gouvernance) prend en compte la cybersécurité.**

L'**Agence nationale de la sécurité des systèmes d'information (ANSSI)** assure la protection des **opérateurs d'importance vitale (OIV)**. Ces entreprises sont protégées de manière satisfaisante, du fait de leur importance. En revanche, ce dispositif public ignore les TPE, les PME et les ETI qui ne sont pas identifiées comme étant d'importance vitale.

La protection de ces entreprises est d'autant plus importante que les évolutions à venir sont imminentes : internet des objets (IoT), ordinateur quantique, intelligence artificielle...

2 - Comment aider les TPE et les PME à faire face à la cybercriminalité ?

Les grandes entreprises et les entreprises de taille intermédiaire (ETI) ont pris des mesures afin de se protéger. Cela a eu pour effet de **détourner la cybercriminalité vers les plus petites entreprises.** Malgré une grave **pénurie mondiale d'expertise humaine,** le marché de la cybersécurité est particulièrement porteur puisqu'il représente **13 milliards d'euros de chiffre d'affaires** sur le sol national.

Le rapport propose trois axes afin de développer le cercle vertueux de la cyberprotection :

1. **tester** et renforcer la résistance et la résilience des entreprises ;
2. **alerter**, conseiller et former sur les différentes menaces ;
3. **protéger** les TPE, PME et ETI grâce à des outils adaptés (cybercampus, formation des magistrats, procédures pénales adaptées...).

Le rapport présente 22 propositions afin de renforcer la cybersécurité des TPE, PME et ETI. Les principales sont :

promouvoir le dispositif cybermalveillance.gouv.fr ;

- ouvrir un guichet de recueil anonymisé des cyberattaques ;
- inclure la cybersécurité dans les schémas régionaux de développement économique ;
- renforcer la réponse pénale à la cybercriminalité ;
- accélérer le projet de règlement européen sur la preuve électronique (*"e-evidence"*) ;
- permettre un remboursement par les assurances du recours aux services de prestataires labellisés Expert Cyber ;
- sensibiliser les PME sur la responsabilité personnelle des dirigeants en cas de cyberattaque ;
- accorder aux TPE et PME la protection de **l'article L212-1 du code de la consommation sur les clauses abusives pour les contrats conclus en matière de cybersécurité.**

Source : **https://www.vie-publique.fr/en-bref/280574-cybersecurite-des-entreprises-mieux-proteger-les-tpe-pme**
juillet 2021 (+précisions et mises à jour personnelles)