LA SEMAINE DE LA DOCTRINE **LA VIE DES IDÉES**

le club des juristes

LE MOT DE LA SEMAINE

Cybersécurité

www.lexisnexis.fr

1177

L'indemnisation des rançons : un paradoxe insolvable

Valérie Lafarge-Sarkozy, avocat associé Advant Altana, partenaire Club des juristes

Mercredi 7 septembre 2022 dans le cadre du projet de loi d'orientation et de programmation, le ministère de l'Intérieur a présenté en conseil des ministres un rapport recommandant l'indemnisation par les assureurs des rançons payées dans le cadre d'une attaque cyber par *ransomware*, à la condition toutefois qu'une plainte soit déposée par l'entité victime de l'attaque. Cette proposition ne peut pas faire l'unanimité, elle est contraire aux préconisations de l'Agence nationale de la sécurité des systèmes de l'information (ANSSI) et de celles de l'ex députée V. Fauré Muntian dans le rapport parlementaire publié sous sa direction en octobre 2021 qui ont, à juste titre, mis en exergue le financement du terrorisme par le biais des rançons. Il faut donc se convaincre que cette recommandation est adaptée et lui trouver des mérites dont celui de combler le vide juridique quant à la légalité de l'assurabilité des rançons. Vide juridique rappelé dès 2018 dans le rapport sur l'assurance du risque cyber publié par le Club des juristes, sauf à pouvoir démontrer que le piratage a été réalisé par une organisation terroriste, ce qui excluait l'indemnisation à défaut de contrevenir à l'ordre public. Il s'agit également d'une volonté forte de protéger les entreprises et notamment les TPE/PME en les sensibilisant, à cette occasion, à leur exposition à ce risque aux conséquences économiques souvent désastreuses.

54 % d'entre elles ont été attaquées en 2021 et ont par exemple perdu leurs données après que leur système d'information a été piraté et totalement bloqué par un logiciel malveillant codé pour exploiter les failles d'un système d'information (Baromètre annuel du CESIN) réalisé d'après un sondage mené par Opinion Way.

62 % des entreprises attaquées ont payé une rançon en cryptomonnaie malgré le risque de ne pas récupérer les données, lesquelles ne sont pas toujours réutilisables car souvent rendues dans le désordre ou encore chiffrées (sondage Forrester). Ainsi, seules 42 % des entreprises ayant payé la rançon ont récupéré la totalité de leurs données et 68 % d'entre elles se sont à nouveau fait attaquer l'année suivante.

Il s'agit donc d'une forte incitation à la souscription d'une assurance cyber encore mal connue des entreprises, puisqu'elle ne représente que 3 % des cotisations en assurance des dommages des professionnels alors que ce risque est en augmentation constante, suivant en cela la courbe exponentielle de notre dépendance au numérique.

La prise de conscience du risque par la souscription d'une assurance aura la conséquence vertueuse d'être un levier pour contraindre les dirigeants d'entreprises, encore peu concernés par ce risque, à se pencher sur leur système d'information et à en identifier les limites ou les failles via notamment la réponse à un questionnaire de sécurité - l'assurance étant une option qui doit se combiner et s'additionner à des règles strictes de cyber gouvernance.

Conditionner l'indemnisation au dépôt d'une plainte est essentiel car le nombre de plaintes déposées est bien en dessous du chiffre réel des entreprises piratées, lesquelles choisissent souvent de payer la rançon sans déposer de plainte ce qui est un frein majeur à l'identification des pirates informatiques.

Mais le revers de la médaille n'est pas neutre : les compagnies d'assurances, puis leurs assurés vont devenir des cibles privilégiées de ces gangs aux méthodes toujours plus sophistiquées qui vont ainsi avoir des garanties accrues de paiement. Ce sont ces mêmes gangs dont certains sont organisés comme des franchises qui ont créé en 2015 un rançongiciel prêt à l'emploi avec des formules d'abonnement ou de partenariat le RaaS (*Ransomware as a service*).

Enfin, l'effet pervers sera la tentation de céder au chantage des pirates informatiques et ainsi de contribuer à alimenter les activités cybercriminelles (terrorisme, trafic d'armes, de drogues…) en systématisant le paiement des rançons.

Il va falloir trouver le point d'équilibre entre la volonté de ne pas financer les organisations terroristes et celle d'aider les PME/TPE qui sous-estiment encore ce risque d'attaque cyber auquel, lorsqu'il survient, elles sont souvent incapables de résister techniquement et financièrement.

L'enjeu est de taille car il s'agit de la capacité de résilience de nos entreprises face à ce risque cyber qui est omniprésent en France et gagne chaque jour en efficacité et sophistication, c'est donc un enjeu majeur de souveraineté. ■