www.alliancy.fr
Pays : France
Dynamisme : 3

Visualiser l'article

[Chronique] Ransomware : faut-il mieux payer un voyou ou laisser crever une entreprise ?

Notre chroniqueur Eric Barbry livre son opinion sur le paiement des rançons pour les entreprises qui subissent une cyberattaque par rançongiciel.

Payer un voyou ou laisser crever une entreprise ? « La question elle est vite répondue ! » (J'espère que vous avez la réf J). Une fois n'est pas coutume, je vais laisser de côté le sujet du RGPD, et plutôt me laisser aller à un petit coup de gueule…

A lire aussi : Est-ce que les cyberassurances facilitent la tâche aux ransomers ?

Quel le motif de mon courroux du jour ? Cette phrase de Madame la Députée LREM Valeria Faure-Muntian, présidente du groupe d'études assurance de l'Assemblée dans une interview consacrée au cycle d'audition engagé à propos de l'assurance cyber en vue de rendre un rapport cet automne.

Elle y affirme : « Pour ma part, je suis totalement opposée à ce que le paiement des rançons perdure ». De quoi parle-t-on ? D'un fléau d'après l'ANSSI qui donne des chiffres catastrophiques sur son site web sur les ransomwares.

Quand les assureurs couvrent le (nouveau) risque du ransomware
En effet les attaques de type rançongiciel en bon français (ransomware, donc) se multiplient. Elles consistent à chiffrer les données d'une entreprise ou d'un acteur public et de monnayer les clefs de déchiffrement contre une rançon payée en crypto monnaie. Evidemment payer la rançon est une horreur et ne fait qu'alimenter la machine.

Mais doit-on pour autant interdire à des assureurs de couvrir ce risque ? De nombreux assureurs proposent en effet des assurances dites « cyber » qui viennent couvrir les risques d'attaques informatiques sous toutes leurs formes.

Visualiser l'article

Ces assurances permettent de couvrir différentes dépenses de l'entreprise ayant subi une attaque comme la gestion de crise (les fameux 72 heures chrono), les dommages et les préjudices causés aux tiers. Mais certains vont un cran plus loin et prennent en charge le paiement de la rançon.

L'objectif n'est pas d'alimenter la fraude informatique mais de procéder à une balance des intérêts entre les coûts de gestion de crise, du forensic, de remédiation, des pertes en tous genres et le montant réclamé par le pirate qui est souvent négociable. Si la balance des intérêts milite en faveur du paiement du montant réclamé par le pirate, la réponse est vite vue : il vaut mieux payer !

Eviter la mort technologique et économique de l'entreprise

Alors oui, on peut trouver que c'est « mal » et considérer que cela participe au développement de cette nouvelle forme de piraterie.

Mais rappelons une évidence : un rançongiciel qui fonctionne, c'est la mort technologique de l'entreprise et de nos jours, la mort technologique, c'est aussi et surtout une mort économique : arrêt d'activité sur une période plus ou moins longue, voir définitive.

Alors entre la peste et le covid, je choisis le vaccin et je préfère encore payer une rançon que de voir disparaitre des entreprises ou mettre à mal des acteurs publics.

Mais au-delà même de sauver des entreprises d'un péril réel et immédiat, ce type d'assurance présente une vraie vertu : l'amélioration de la sécurité informatique des entreprises.

Car ne nous y trompons pas, l'assurance n'est pas un blanc-seing et l'assureur un perdreau de l'année. Dans la plupart des cas, l'assureur va conditionner soit son assurance, soit le niveau de couverture, soit le montant de sa police, soit les trois à un niveau de sécurité pris par l'entreprise et adapté à sa ou ses menaces.

Ainsi donc, l'assurance n'est pas simplement une garantie *ex post* pour l'établissement assuré mais une obligation *ex ante* de prendre des mesures de sécurité qu'il n'aurait peut-être pas prises si l'assureur ne les lui avait imposées.

L'occasion d'une remise en question ?

D'ailleurs la plupart des assurés que je connais ont tous amélioré leur niveau de sécurité par des audits d'une part, un renforcement de leur niveau général de sécurité d'autre part, et surtout, surtout, une meilleure gestion de leurs sauvegardes.

Beaucoup ont également profité de cette occasion pour former leurs collaborateurs aux risques d'attaques dont le télétravail a été un facteur aggravant.

Alors oui, je suis comme tout le monde, je trouve hallucinant de payer une rançon et préfère crier « jamais au grand jamais » ! Mais principe de réalité et de protection des entreprises oblige… il me parait parfois nécessaire passer à la caisse s'il le faut.

Quant à savoir si le paiement d'une rançon est la garantie de retrouver la plénitude de son système d'information, la réponse est « oui ».

Cela peut paraître curieux mais il y a une forme de loyauté chez les voyous. En réalité ce n'est pas vraiment de la loyauté, mais un principe de réalité. S'il était démontré que les voyous après paiement des rançons ne

donnaient pas les moyens de déchiffrer les données, c'est tout le business qui s'écroulerait. Donc oui, dans 100% des cas que je connais, une fois la rançon payée, l'entreprise a pu récupérer ses données.

On peut cependant pendre une autre voie et effectivement interdire de payer les rançons, mais alors il faudra y mettre les moyens :

Moyens d'accompagnement des entreprises qui aujourd'hui à part déposer plainte et s'entendre dire « vous n'êtes pas les seuls et nous n'avons aucune chance de retrouver les attaquants qui sont à l'étranger » …rien ne se passe vraiment ; Avouez que c'est assez démotivant …
Moyens financiers pour assister les entreprises victimes de ce type de fraude par la mise en œuvre d'un fond de garantie par exemple, seul moyen de ne pas les voir mourir.
Personnellement plutôt qu'un fond de garantie et une mise à contribution des contribuables, je préfère que le marché de l'assurance, dont c'est après tout le métier, fasse son œuvre !

Eric Barbry, avocat associé du cabinet Racine

Avocat spécialisé dans le domaine de l'IP/IT & Data Protection au sein du cabinet Racine, je vous propose une nouvelle approche du droit, résolument pratique, basée sur mon expérience professionnelle : celle d'un avocat qui travaille sur le droit des technologies depuis plus de 25 ans.

J'ai souvent envie de pousser des coups de gueules, parfois, moins souvent je l'accorde volontiers, des coups de chapeau…

Je vous propose de partager mes émotions professionnelles tantôt favorables à une nouvelle règlementation, tantôt contre ; critiques (positives ou négatives) à propos de décisions de justices qui bousculent la vie digitale des entreprises.

Sans trahir le moindre secret professionnel il me parait important d'échanger sur les cas d'usage des entreprises confrontées à des nouvelles questions autour de l'usage des nouvelles technologies.

Mon propos se veut pragmatique et tente d'apporter des réponses pratiques pour absorber, aussi sereinement que possible, le choc juridique que constitue la transformation digitale de votre entreprise.

A propos de Racine :

Racine est un cabinet d'avocats français indépendant de droit des affaires qui réunit 200 avocats et juristes, répartis au sein de 7 bureaux.

Racine se caractérise par une approche « full service » en droit des affaires en conseil et contentieux et intervient pour des entreprises, issues de différents secteurs de l'industrie et des services, des organisations professionnelles et interprofessionnelles ainsi que des collectivités publiques.