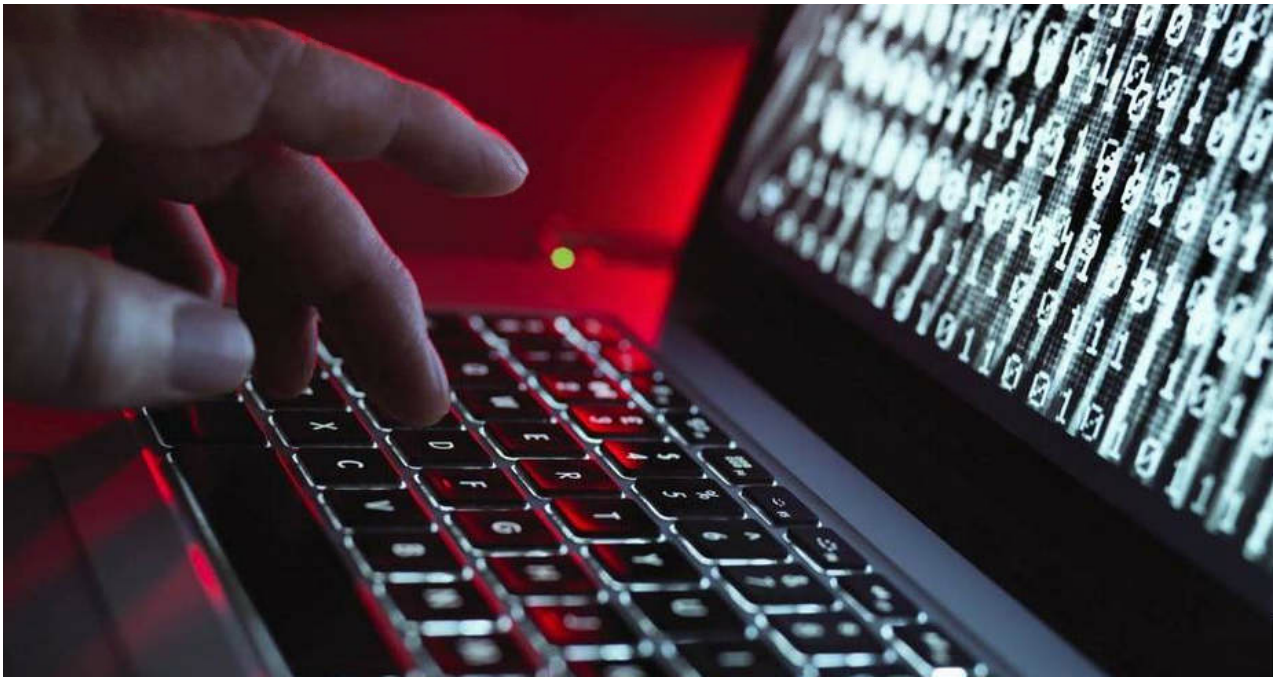
Les Echos EXECUTIVES

Date : 17/08/2021
Heure : 09:57:04
Journaliste : Eric Barbry

business.lesechos.fr
Pays : France
Dynamisme : 1

Visualiser l'article

Cybercriminalité : les entreprises doivent-elles payer les rançons ?



Payer une rançon, c'est nourrir les pirates. Payer, c'est alimenter le cycle infernal.

Opinion | Les entreprises sont de plus en plus nombreuses à être les victimes de logiciels d'extorsion. Doivent-elles payer ? La réponse de l'avocat Eric Barbry.

"Pour ma part, je suis totalement opposée à ce que le paiement des rançons perdure" : voici ce qu'estime la députée LREM Valéria Faure-Muntian, coprésidente du groupe d'études « Assurances » de l'Assemblée nationale , dans une interview à « L'Argus de l'assurance » consacrée aux auditions organisées sur l'assurance cyber en vue de la remise d'un rapport cet automne.

Pour rappel, le rançongiciel (« ransomware », en anglais) est une technique de piratage informatique en plein boom qui consiste à chiffrer les données d'une entreprise ou d'un acteur public et à monnayer les clés de déchiffrement contre une rançon payée en cryptomonnaie. La question de la légitimité du paiement d'une rançon se justifie, mais faut-il y répondre de manière péremptoire et par une interdiction légale de surcroît ?

Nourrir les pirates

Sur le plan de son efficacité d'abord, **en payant l'entreprise est-elle certaine de récupérer ses données ? D'expérience, la réponse est oui** . Cela peut paraître étonnant, mais il y a une forme d'honnêteté chez les voyous. Ne pas redonner accès après paiement d'une rançon reviendrait à mettre un terme à une pratique très lucrative.

Sur le plan éthique ensuite, la question est vite réglée. **Verser une rançon, c'est nourrir les pirates** . Payer, c'est alimenter le cycle infernal. En tarissant la source, il est certain que la pratique s'arrêterait.

Tous droits réservés à l'éditeur

Enfin, sur le plan juridique, on peut se poser la question de la qualification même du règlement de la rançon et d'une certaine forme de complicité vis-à-vis du pirate. Mais difficile d'être à la fois victime et complice ! C'est pourtant la voie que semblent adopter les Américains.

Casquer ou couler ?
Faut-il interdire de payer les rançons ? Il faut avant tout se mettre à la place de la victime. Dans la plupart des cas où le rançonnage est efficace (mauvaise sécurité, mauvaise sauvegarde, absence de tests de restauration régulière, etc.), **l'attaque signe l'arrêt du système d'information de l'entreprise** , c'est-à-dire sa mort technologique ou, dans le meilleur des cas, un coma technique.

Pendant tout le temps du traitement de l'attaque, soit par une remédiation technique soit par le paiement de la rançon, l'activité de l'entreprise est à l'arrêt, comme en témoignent tous les cas médiatisés.

Ne pas payer la rançon implique donc, dans le pire des cas, l'arrêt total de l'entreprise ou, dans le meilleur, une reprise lente et souvent partielle de l'activité, à grand renfort d' **assistance technique dont les coûts sont parfois supérieurs ou égaux à la rançon** demandée.

Alors oui, on peut comprendre et on doit même comprendre que lorsqu'on raisonne en chef d'entreprise, il est préférable de payer une rançon que de déposer le bilan.

Une assurance… sous conditions
Se pose alors la seconde question : doit-on permettre à des assureurs de couvrir ce risque ? Au regard du droit des assurances, à n'en pas douter, le risque peut être couvert. Sur le plan économique, les entreprises ont tout intérêt à bénéficier de ce type de couverture dans la mesure où les sommes en jeu sont parfois considérables. N'oublions pas que le paiement de la rançon n'est jamais systématique. En cas d'attaque, **l'assureur procédera à une balance des intérêts financiers entre le coût de la remise en état et la rançon** .

Mais il existe une autre vertu à l'assurance du « ransomware » : l'amélioration du niveau de sécurité des entreprises. Il ne faut pas croire que l'assurance cyber est un blanc-seing pour les entreprises. Bien au contraire, dans nombre de cas, pour être assurée, l'entreprise devrait mettre en oeuvre des mesures de sécurité particulières et répondre à des questionnaires et des prérequis particulièrement détaillés.

Interdire n'est sans doute pas la bonne issue, mais **conditionner l'obtention d'une assurance à un niveau de sécurité adapté aux menaces** de l'entreprise paraît une solution aussi raisonnable que raisonnée. L'assurance cyber n'est donc pas simplement un moyen de rémunérer les pirates, mais aussi et surtout un formidable accélérateur de la sécurisation des entreprises.

A défaut de permettre aux entreprises de payer les rançons, il faudra alors que l'Etat se mette en ordre de marche pour les protéger par la mise en oeuvre de ressources en amont, mais aussi par la constitution d'un fonds d'aide ou de garantie de nature à combattre ce fléau et à éviter que nos entreprises et acteurs publics ne soient mis à mal.

Eric Barbry *est avocat associé au cabinet Racine, en charge de la pratique « IT et data protection ».*

Tous droits réservés à l'éditeur