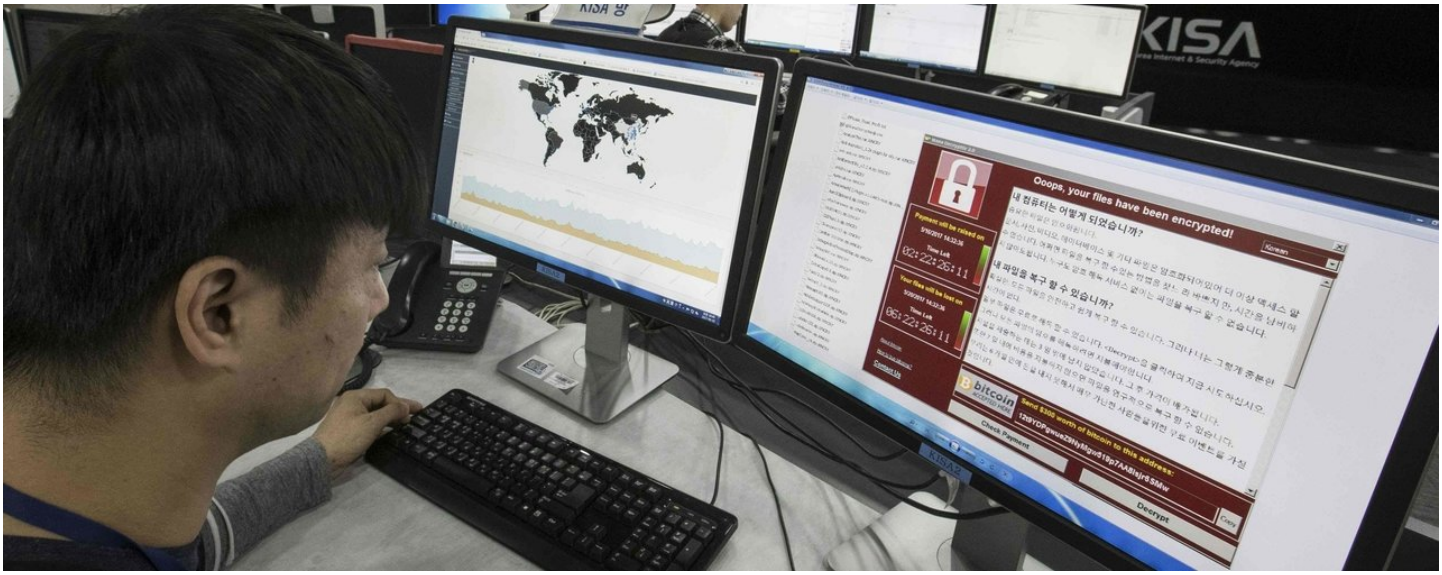

Agence de sécurité de l'Internet en Corée du Sud. Séoul, 15 mai 2017. © AFP/Yonhap

OPINION

Le paradoxe des cyberattaques: la responsabilité des victimes

Les entreprises cibles d'une cyberattaque réussie s'exposent au final à un risque de sanctions significatives, explique l'avocat Adrien Alberini

3 minutes de lecture

Technologies

Adrien Alberini, Dr. en droit, LL.M. Avocat, sigma legal
Publié dimanche 21 mai 2017 à 18:50, modifié dimanche 21 mai 2017 à 18:50.

Les médias ont largement relayé l'information de l'attaque informatique à large échelle perpétrée en fin de semaine dernière. En bref, il apparaît que l'attaque a pris la forme pernicieuse d'un ransomware, c'est-à-dire d'un cryptage de données couplé à une demande de rançon, sous la menace d'une destruction des données concernées. Il semble en outre que l'attaque ait visé des entreprises qui utilisaient encore l'ancien système d'exploitation Windows XP, système pour lequel Microsoft avait cessé de proposer des mises à jour depuis peu.

Cette situation complexe donne lieu à ce qu'on peut qualifier de «paradoxe de la cyberattaque»: quand bien même cela peut paraître à première vue surprenant, les entreprises cibles d'une cyberattaque réussie s'exposent au final à un risque de sanctions significatives! Ce paradoxe s'explique en réalité par le renforcement du droit de la protection des données. Ce droit impose des exigences toujours plus élevées tant en amont des cas de violation de données personnelles (data breach) qu'en aval, c'est-à-dire lorsque la violation s'est produite. Exigences qu'il n'est pas facile de respecter, d'où le risque de responsabilité pour les entreprises victimes d'une cyberattaque.

La Suisse dans le sillage de l'Europe

En bref, une réglementation modernisée en matière de protection des données – couramment abrégée le GDPR (General Data Protection Regulation) – entrera en vigueur l'année prochaine dans l'UE. Cette révision vise précisément à adapter le droit de la protection des données à l'évolution des nouvelles technologies de l'information. La Suisse suit cette vague; une révision de la Loi fédérale sur la protection des données est actuellement en discussion. On relèvera encore que les entreprises suisses sont assez largement tenues de se conformer au GDPR, dès lors que cette réglementation s'applique (extra-territorialement) en cas de traitement de données de personnes qui résident dans l'UE.

Le GDPR impose aux personnes qui traitent des données personnelles de garantir une sécurité adéquate de ces données à l'aide de «mesures techniques et organisationnelles appropriées», notion complexe que la réglementation européenne ne définit malheureusement pas de manière précise. On trouvera dans la réglementation à tout le

moins quelques recommandations, telles que l'utilisation de solutions de cryptage ainsi que de back up qui permettent de restaurer rapidement les données. En pratique, on recommande aux entreprises de respecter par exemple un code de conduite adopté par une organisation professionnelle ou d'adhérer à un système de certification en matière de cybersécurité.

Double notification

A noter encore que, selon le GDPR, les mesures techniques et organisationnelles doivent être régulièrement réexaminées et actualisées. Ce point paraît particulièrement pertinent et délicat en lien avec les attaques récentes qui, comme indiqué plus haut, semblent avoir été possibles en raison du fait que les entreprises victimes utilisaient encore Windows XP, alors que Microsoft n'offrait plus de mises à jour pour ce système d'exploitation.

C'est surtout en cas de violation de données personnelles que le GDPR va plus loin que la réglementation existante et élève le niveau d'exigences à respecter. En substance, une double notification est imposée à l'entreprise victime de l'attaque: une notification à l'autorité de contrôle (dans le très court délai de 72 heures après la prise de connaissance de la violation!) et une notification aux personnes concernées. Certaines exceptions sont prévues, étant toutefois précisé que les conditions à remplir pour en bénéficier doivent être appréciées avec prudence dans chaque cas d'espèce. Il va pratiquement sans dire que la mise en œuvre concrète de ce type de notifications n'est pas aisée, lorsque l'on sait que ce sont parfois les données de milliers d'utilisateurs qui sont en jeu...