L'Usine Nouvelle,
Le 11 juin 2015,

Les vols de données traqués par Bruxelles

L'Usine Nouvelle n° 3427

Les pirates informatiques lorgnent les informations confidentielles des entreprises. Mais l'Union européenne veille.

Les vols de données personnelles connaissent une recrudescence sans précédent. Ils constituent un véritable danger, tant pour les particuliers que pour les entreprises. Selon une étude du spécialiste de la protection HTTPCS, 72 % des sites français sont particulièrement exposés et vulnérables aux attaques de pirates informatiques. Les risques se sont par ailleurs considérablement accrus avec le développement du cloud computing, consistant à externaliser des données vers des serveurs distants.

Les techniques des pirates informatiques sont connues. Les cybercriminels peuvent agir à l'insu de la victime en insérant un virus dans son ordinateur, capable d'analyser son disque dur et d'isoler ses données personnelles. Ou encore implanter un fichier espion comme le « cheval de Troie » pour enregistrer les frappes du clavier lors de l'accès à un site internet. Une autre technique, dite du phishing ou hameçonnage, consiste à abuser de la crédulité de la victime en lui laissant croire qu'elle s'adresse à un organisme de confiance ? une assistance informatique, une banque ou une administration ? afin de lui soutirer des informations personnelles.

LE MARCHÉ NOIR DES DONNÉES VOLÉES

Les données convoitées par les cybercriminels sont diverses : identité, codes d'accès, mots de passe, adresses électroniques, clés de licence de logiciels, coordonnées bancaires ou postales… Il existe ensuite un véritable marché noir en matière de cybercriminalité. Cette économie souterraine permet aux pirates informatiques de monnayer les données personnelles subtilisées en les revendant via des sites ou forums spécialisés. Les transactions sont souvent réalisées en monnaie virtuelle afin de réduire la traçabilité de l'opération et garantir, dans une certaine mesure, l'anonymat des cybercriminels. Une fois les données personnelles dérobées, les pirates informatiques peuvent également faire chanter la victime pour lui extorquer de l'argent. Il n'est pas rare qu'un cybercriminel contacte l'entreprise spoliée et la menace de divulguer les informations confidentielles subtilisées, si elle refuse de payer la somme exigée.

Les victimes vont toutefois bénéficier d'une meilleure protection juridique pour dissuader et punir les hackeurs. Le Parlement européen et le Conseil de l'Union européenne ont adopté, le 12 août 2013, la directive 2013/40/UE relative aux attaques contre les systèmes d'information. Cette dernière renforce l'arsenal répressif en matière de cybercriminalité. Atteinte à l'intégrité d'un système et de ses données, interceptions illégales d'informations, ou encore utilisation

d’outils informatiques malveillants : autant d’infractions visées par le nouveau texte adopté par l’UE.

UN ARSENAL RÉPRESSIF RENFORCÉ

La législation française reprend déjà la plupart de ses dispositions, mais ne prévoit que des peines maximales en cas d’infraction, qui ne sont par ailleurs jamais appliquées. Pour pallier cette réponse juridique défaillante, la nouvelle directive intègre également des dispositions beaucoup plus sévères en matière de sanctions pénales minimales, appliquées en cas de vol de données. Les états membres de l’Union européenne ont jusqu’au 4 septembre pour appliquer ce nouveau texte.
De leur côté, les entreprises doivent aussi assumer leurs responsabilités. Le règlement européen n° 611 / 2013, entré en vigueur le 25 août 2013, a instauré une procédure d’information en cas de piratage de données à caractère personnel d’un opérateur de télécommunications, ou d’un fournisseur de services internet. après la publication de ce règlement, le législateur français a mis en place une téléprocédure accessible sur le site de la Commission nationale de l’informatique et des libertés (Cnil). L’opérateur concerné a l’obligation de notifier le vol de données à la Cnil et à l’intéressé, dans un délai de 48 heures. En cas de défaillance, il s’expose à une peine d’emprisonnement de cinq ans et à 300 000 euros d’amende.
Cette réglementation devrait bientôt s’étendre à l’ensemble des responsables de traitements de données à caractère personnel. La proposition de règlement relatif à la protection des personnes physiques, dans le cadre du traitement des informations à caractère personnel et de leur libre circulation (règlement général sur la protection des données), a été adoptée par le Parlement européen le 12 mars 2014. Une bonne nouvelle pour les victimes de piratage souhaitant demander réparation.

L’enjeu
Réagir à une intrusion dans le système informatique de l’entreprise et à un vol des données personnelles de ses clients

La mise en Œuvre

- Connaître les moyens des cybercriminels et établir une politique de sécurité des systèmes
- Notifier la Cnil et les personnes concernées par un vol de données
- Prévenir les services de police compétents et déposer une plainte pénale