La cybersécurité a-t-elle une obligation de résultat ?

La cybersécurité a-t-elle une obligation de résultat ?

Obligation de résultat ou obligation de moyens : qu'est-ce que cela implique en matière de cybersécurité ? Olivier Iteanu, avocat à la Cour (www.iteanu.com), nous livre son analyse et revient sur la sanction infligée à Orange par la Cnil.

Chacun conviendra qu'il est absurde de considérer que la sécurité en général, et plus particulièrement celle attachée aux systèmes d'information, soit soumise à une obligation de résultat. Aucune technologie, aucun système de défense n'est capable de garantir une fiabilité à 100 % contre toute attaque. L'éditeur d'une solution ou le prestataire qui prétendrait le contraire serait tout simplement un menteur. L'esprit humain est ainsi fait, et c'est tant mieux, qu'un jour ou l'autre, l'attaquant, venu de l'extérieur ou plus encore, de l'interne, trouve le moyen de contourner les meilleures protections techniques et organisationnelles mises en place.
Le pendant de l'obligation de résultat ou son contraire, est l'obligation de moyens. Dans le cas de l'obligation de moyens, si l'attaque a causé des dommages à des tiers, ceux-ci ne peuvent se retourner contre le maître du système attaqué pour obtenir réparation que si une négligence ou une faute prouvées peut être retenue contre lui. Dans le cas de l'obligation de résultat, le tiers n'aura qu'à démontrer l'existence de l'attaque et son dommage, pour engager la responsabilité du maître du système, sans même avoir à démontrer que ce dernier a commis une faute. Evidemment, on comprend ici que les conséquences de l'un ou de l'autre régime juridique sont radicalement différentes.
On est en droit de se demander si le système plein de bon sens de l'obligation de moyens en matière de cybersécurité, n'est pas remis en cause par une décision récente de la Commission Nationale de l'Informatique et des Libertés du 7 août 2014, qui a sanctionné Orange pour manquement à l'obligation de sécurité prévue à la Loi informatique et libertés.
http://www.cnil.fr/fileadmin/documents/approfondir/deliberations/Formation_contentieuse/D2014-298_avertissement_ORANGE.pdf

Que dit la loi ?
Pour mémoire, la Loi du 6 janvier 1978 en son article 34 prévoit que « Le responsable du traitement est tenu de prendre toutes précautions utiles (…) pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. » Le défaut de prendre « toutes précautions utiles » est sanctionné des peines maximales de 5 ans de prison et de 300 000 € d'amende par l'article 226-17 du Code pénal. Et comme la matière informatique et libertés prévoit une double peine aux contrevenants à la Loi, la Cnil peut également prendre une sanction dite administrative à l'encontre du responsable du traitement défaillant. Les sanctions de la Cnil peuvent être pécuniaires, jusqu'à 300 000 € en cas de récidive et portent surtout atteinte à l'image du condamné, car ces sanctions sont publiques, donnent lieu à publication, et sont régulièrement reprises par la presse et les médias.

Orange attaqué… et condamné
Une décision récente de la Commission Nationale de l'Informatique et des Libertés du 7 août 2014 a sanctionné Orange pour manquement à l'obligation de sécurité prévue à la Loi informatique et libertés. Dans l'affaire jugée, Orange était alertée en mars 2014 par un client et découvrait que le serveur d'un prestataire de l'opérateur « chargé de réaliser certaines campagnes de marketing direct » par courriel avait été piraté. Plus de 1,3 millions de clients d'Orange étaient impactés par cette attaque. L'enquête révélait qu'Orange avait confié à un premier prestataire la mission de réaliser des campagnes de emailing auprès de ces clients. Ce prestataire avait lui-même sous-traité la prestation à un prestataire secondaire. C'est ce dernier qui était piraté.

Le lien de désinscription, qui se trouvait au bas du courriel de prospection, menait par une modification de l'URL aux 700 fichiers de prospects et de clients d'Orange, permettant à l'indélicat à les aspirer. Le 25 avril 2014, Orange notifiait la faille de sécurité à la Cnil comme elle y est contrainte depuis le Paquet Télécom d'août 2011 et un Règlement 611/2013 de la Commission européenne du 24 juin 2013. Le 5 mai 2014, la presse s'emparait de l'affaire. Une semaine plus tard, la Cnil diligentait sur deux jours un contrôle dans les locaux d'Orange qui révélait les circonstances dans lesquelles les 700 fichiers de clients et prospects avaient été aspirés. Orange déposait une plainte pénale. Mais Orange était également convoquée devant la formation contentieuse dite restreinte de la Cnil, qui lui infligeait un avertissement public le 9 août 2014 pour manquement à l'obligation de sécurité.

Orange se trouvait donc à la fois victime et responsable. Ce qui nous interpelle dans cette décision, ce sont les motifs retenus par la Cnil pour sanctionner Orange. Le premier grief est que selon l'autorité française, Orange « n'a pas fait réaliser d'audit de sécurité sur la version de l'application technique spécifiquement développée par son prestataire secondaire. » Face à la généralité de l'obligation imposée par la Cnil, on cherche désespérément la base légale à ce grief. Mais à supposer celui-ci fondé, on peut penser que le prestataire secondaire a, quant à lui et en sa qualité de professionnel, procédé à cet audit. Tenir Orange, le client dans cette relation, responsable au motif qu'elle n'a pas procédé à cet audit devrait glacer le sang de tous les clients utilisateurs. Le second motif nous paraît, quant à lui, lunaire. La Cnil reproche à Orange d'avoir « communiqué de manière non sécurisé les mises à jour de ses clients » à ses prestataires. L'enquête avait certes révélé qu'Orange avait transmis les 700 fichiers de ses clients et prospects par simple courriel, mais la même enquête a établi que ce n'est pas durant cette communication que les fichiers ont été captés. Cette communication ne serait donc pas en cause. Enfin, la Cnil reproche à Orange « qu'aucune clause de sécurité et de confidentialité des données n'était imposée à son prestataire secondaire »,c'est-à-dire au sous-traitant du sous-traitant d'Orange, c'est-à-dire la société avec laquelle elle n'a pas de contrat … C'est compte tenu de ces « défaillances » que la Cnil entre en voie de condamnation à l'encontre d'Orange.

Cette décision nous amène à deux commentaires sous formes de conclusions.
D'une part, il y a un auteur à cette infraction, « quelque part dans le monde » qui a accédé illicitement aux serveurs et a procédé à l'aspiration des fichiers. Les adresses IP relevées par les serveurs du prestataire attaqué ont désigné des pays lointains. Dans ce genre d'affaires, l'enquête judiciaire est souvent en panne. L'enquête bute en effet sur des difficultés de coopérations policières et judiciaires en termes de délais, de paperasserie et de coûts quasi insurmontables, sans compter que certains pays ne coopèrent tout simplement pas. Dans ce contexte, le seul condamné de l'histoire a toutes les chances d'être la victime, Orange. Il y a tout de même ici quelque chose de choquant sur le fond. En outre, c'est Orange qui a notifié elle-même la faille à la Cnil par application de la Loi certes. Si chaque notification donne lieu à condamnation de son auteur, ceux-ci risquent désormais de réfléchir à deux fois avant de se lancer dans ce qui apparaît comme « la gueule du loup ».

D'autre part, les griefs retenus à l'encontre d'Orange nous paraissent d'une interprétation des plus sévères des précautions utiles de l'article 34 de la Loi de 1978 et surtout très généraux, laissant dans le désarroi et l'insécurité juridique tous utilisateurs des systèmes d'information et de leurs services. Enfin, faire tenir Orange responsable des agissements du sous-traitant de son sous-traitant paraît déraisonnable.

En conclusion, on a le sentiment ici que le cri des victimes et des médias a couvert tout raisonnement juridique. Il fallait un responsable. L'auteur de l'infraction introuvable, c'est sur la victime qu'on se rabat. C'est un mode de fonctionnement regrettable sur le plan des principes et qui ne devrait pas se généraliser.

A défaut, oui, la cybersécurité deviendrait synonyme d'obligation de résultat.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.solutions-logiciels.com/actualites.php?titre=La-cybersecurite-a-t-elle-une-obligation-de-resultat-&actu=15232
par Juliette Paoli