Les entreprises européennes bientôt obligées de signaler toute cyber-attaque ? | Le Net Expert Informatique

	Les entreprises européennes bientôt obligées de signaler toute cyber-attaque ?

Les entreprises du domaine des nouvelles technologies opérant en Europe pourraient devoir systématiquement reporter toute intrusion sur leurs installations informatiques. Une directive devrait étendre cette obligation au secteur du numérique. Depuis 2013, l'Europe mène des discussions autour d'un texte visant à obliger les entreprises des secteurs de l'énergie, des transports, de la santé ou des services financiers à implémenter des mesures de sécurité minimales pour leurs installations informatiques. Baptisée NIS (pour Network and Information Security), cette directive implique surtout à ces mêmes professionnels de rapporter aux autorités compétentes tout incident informatique (cyber-attaque, intrusion, perte de données…).
Selon Reuters, cette directive pourrait être étendue à de nouveaux secteurs, à savoir à l'ensemble du domaine des nouvelles technologies. A terme, **ces sociétés qu'elles soient majeures ou non pourraient être soumises à ce devoir de divulgation en cas d'attaque informatique**.
A ce jour, certaines obligations incombent déjà aux opérateurs de réseaux d'importance vitale (eau, électricité…) mais également aux opérateurs de télécommunications. Ces derniers doivent par exemple signaler à la Cnil d'éventuelles pertes ou fuites concernant les informations personnelles de leurs clients.
Ce type d'obligation pourrait donc être étendu à davantage de sociétés. Ce volet doit toutefois être discuté devant les institutions communautaires ainsi que les Etats membres. Ces derniers devraient faire part de leurs critiques au sujet d'une extension trop large de ce texte à l'ensemble du secteur du numérique.

Un débat encore vif et des critiques toujours présentes
La question de la communication en cas de faille de sécurité reste majeure. Les exemples de fuites de données massives, comme celui de Sony, ont montré l'importance de tenir informer les personnes concernées mais aussi les autorités, pour qu'elles puissent éventuellement agir.
En Europe, et notamment en France, la question reste également pertinente. Comme nous le rapportions suite à une conférence sur le sujet, certaines entreprises préfèrent rester discrètes quant à leurs dispositifs et les relations entre « hackers blancs » peuvent rapidement tourner à l'incompréhension.
C'est pourquoi de nombreux professionnels, ou leurs représentants, critiquent une extension trop large des obligations de notification des failles de sécurité. Ces derniers craignent que ce type de contrainte nuise à la compétitivité des entreprises, ou n'entraîne un jeu du chat et de la souris peu profitable aux professionnels.

Source : http://pro.clubic.com/it-business/securite-et-donnees/actualite-776250-directive-nis.html
Par Olivier Robillart