Directive sur la cybersécurité : Amazon, eBay, Google devront notifier leurs incidents majeurs – Next INpact

Directive sur la cybersécurité : Amazon, eBay, Google devront notifier leurs incidents majeurs

Après des heures de négociations, le Parlement européen et les États membres sont arrivés lundi à un accord sur la future directive NIS (network and information security). Un texte destiné à mieux protéger les opérateurs dits critiques dans toute l'Europe.

Cette future directive sur la cybersécurité visera en effet à imposer des règles harmonisées à tout un ensemble d'opérateurs critiques. Le mouvement sera épaulé par le réseau des Computer Security Incident Response Team (CSIRT) pour discuter des incidents et identifier de possibles réponses coordonnées.

Plusieurs niveaux de reporting selon les acteurs concernés

Ce texte visera avant tout à définir des critères pour savoir qui relève de ces obligations. En tête de liste, on trouvera nécessairement les acteurs de l'énergie, du transport et de la santé. Selon l'eurodéputé Andreas Schwab (EPP), ces entreprises devront répondre à plusieurs mesures de sécurité, mais également notifier aux autorités les incidents de cybersécurité qualifiés « *d'importants.* »

Si les micro entreprises et les PME seront épargnées, les principaux acteurs du Net seront également concernés, mais avec des obligations finalement plus en retrait. Sont cités les marketplaces comme Amazon ou eBay, les moteurs de recherche mais aussi les services de cloud qui devront mettre en place de mesures de sécurité tout en rapportant aux autorités les seuls « *incidents majeurs* » qui viendraient les impacter.

Le flou règne par contre sur les autres plateformes en ligne comme les réseaux sociaux. Selon l'eurodéputé, toutefois, « *cette directive marque le début de la régulation des plateformes. Alors que la consultation de la Commission européenne sur ces acteurs est toujours en cours, les nouvelles règles prévoient déjà des définitions concrètes – une demande du Parlement européen exprimée depuis le début des négociations –*, afin de faire connaître son consentement à l'inclusion des services numériques. »

En aout dernier, l'obligation de reporter aux autorités les incidents de sécurité avait soulevé les inquiétudes des représentants du secteur. Selon l'Afdel, l'association française des éditeurs de logiciels et de solutions Internet, une obligation indifférenciée de reporting « *pourrait porter atteinte à la compétitivité des entreprises du numérique, en particulier des entreprises françaises et européennes du numérique – dont de nombreuses PME, qui n'ont pas toute la capacité d'adaptation des grands groupes internationaux –, sans atteindre les objectifs poursuivis en termes de sécurité* ». L'ASIC, l'association des services Internet communautaires, avait craint pour sa part de voir chaque État membre devenir « *le Directeur des services informatiques de l'ensemble des acteurs du numérique* », du moins si des critères trop larges étaient inscrits en dur dans le texte final.

Le projet de directive doit maintenant être approuvé formellement par la Commission au marché intérieur du Parlement européen et par le Comité des représentants permanents.

Des obligations de reporting préexistent dans certains secteurs et en France

Suite à l'adoption du Paquet Télécom en Europe, rappelons que les opérateurs télécom doivent déjà notifier les fuites de données personnelles aux autorités de contrôle des données personnelles (la CNIL, ici). En France, l'Agence nationale de la sécurité des systèmes d'information chapeaute pour le compte du premier ministre, les règles de sécurité que doivent suivre les OIV, ces opérateurs d'importance vitale dont l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation.

Depuis la loi de programmation militaire de 2013, centrales nucléaires, hôpitaux, sociétés de transports, acteurs des télécoms, etc. ont l'obligation de fournir « *les informations nécessaires pour évaluer la sécurité de ses systèmes d'information, notamment la documentation technique des équipements et des logiciels utilisés dans ses systèmes ainsi que les codes sources de ces logiciels.* »

Réagissez à cet article

Source : http://www.nextinpact.com/news/97630-directive-sur-cybersecurite-amazon-ebay-google-devront-notifier-leurs-incidents-majeurs.htm