

Des mesures renforcées pour la lutte contre la cybercriminalité

Sécurité

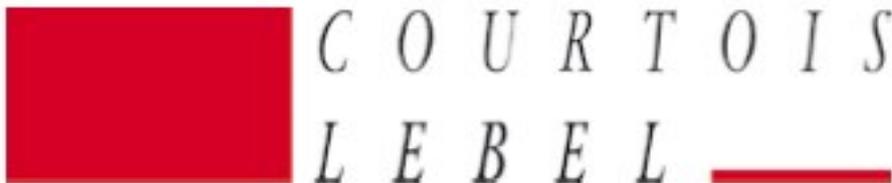
Posté par : JulieM

Publié le : 30/9/2013 13:00:00

Une nouvelle directive européenne (n° 2013-40/UE du 12 août 2013) **relative aux attaques contre les systèmes d'information** est entrée en vigueur le 3 septembre 2013.

Elle remplace et renforce une décision-cadre du Conseil de l'Union (2005/222/JAI) du 24 février 2005, qui avait déjà pour principal objectif de renforcer la coopération entre les autorités judiciaires des États membres grâce à un rapprochement de la législation pénale sanctionnant la cybercriminalité. **Donatienne Blin**, avocat au département Informatique & Réseaux de **Courtois Lebel**, explique quelles vont être ces nouvelles règles.

Les attaques contre les systèmes d'information constituent une menace croissante au sein de l'Union et plus généralement à l'échelle mondiale. Les progrès technologiques permettent aux hackers de construire des méthodes de plus en plus sophistiquées, susceptibles de provoquer des dommages économiques considérables : interruption de l'activité de l'entreprise, perte ou altération de données confidentielles ou personnelles...



L'existence de lacunes et de disparités dans les différentes législations des États membres en matière d'attaques contre les systèmes d'information risque d'entraver la lutte contre la cybercriminalité et de ralentir la coopération policière et judiciaire européenne.

La directive 2013-40/UE renforce donc les mesures mises en place par la décision-cadre de 2005, avec pour objectif de lutter plus efficacement contre les attaques informatiques au niveau européen.

En synthèse, la directive fixe les règles minimales concernant la définition des infractions pénales et les sanctions pénales applicables et améliore la coopération entre les autorités compétentes des États membres.

Les infractions pénales mieux définies

S'agissant de la mise en place de « règles minimales », on citera :

¶ L'adoption de définitions communes s'agissant des éléments constitutifs des infractions pénales suivantes (Art. 3 à 6) :

- accès illégal à un système d'information
- atteinte illégale à l'intégrité d'un système
- atteinte illégale à l'intégrité des données

- interception illégale de ces données ;

§ l'incrimination de la production, de la vente et de l'obtention des outils (programmes) ou dispositifs (code d'accès) connus pour commettre l'une de ces infractions précitées (Art.7) ;

§ l'incrimination du fait « d'inciter à commettre » lesdites infractions, d'y participer ou de s'en rendre complice (Art. 8) ;

§ le principe de « sanctions effectives, proportionnées et dissuasives » à mettre en place par les Etats membres : des peines d'emprisonnement minimum sont imposées par la directive (Art.9) ;

§ la présence de circonstances aggravantes en cas d'attaque de grande ampleur commise par des organisations criminelles (notamment dans le cas des réseaux dit « zombie »), en cas de préjudice grave, lorsque les attaques sont menées contre une « infrastructure critique » d'un Etat membre, ou encore en cas d'usurpation d'identité numérique (Art.9) ;

§ la mise en cause de la responsabilité et la sanction des personnes morales, lorsque les infractions sont commises pour leur compte par toute personne qui exerce un pouvoir de direction (Art.10) ;

§ la responsabilité et la sanction des personnes morales, lorsque « l'absence de surveillance et de contrôle » aura rendu possible l'une des infractions précitées commise pour son compte par ses salariés (Art.10 et 11).

La directive insiste en effet sur le fait qu'il est nécessaire de « garantir des niveaux de protection appropriés contre les menaces et les vulnérabilités pouvant être raisonnablement identifiées » : la responsabilité de la personne morale devra donc être engagée dès lors que celle-ci n'a pas, « de toute évidence », assuré un niveau de protection suffisant contre les cyberattaques commises pour son compte (Considérant 26).

Des dispositions contraignantes pour les entreprises

Les dispositions des articles 10 et 11 sont donc particulièrement contraignantes à l'égard des entreprises, qui il revient d'apporter la preuve de leurs diligences en matière de surveillance et de protection contre les cyberattaques commises par leurs propres salariés.

Pour s'exonérer de leur responsabilité, celles-ci devront donc démontrer cumulativement :

§ que la vulnérabilité ou la menace ne pouvait pas être raisonnablement identifiée ou anticipée (soit au regard de l'Etat de l'art, soit au regard des moyens déployés par l'auteur de l'attaque pour dissimuler ses actes au sein de l'entreprise) ;

§ avoir mis en œuvre en interne des mesures préventives, à la fois juridiques (dispositions spécifiques dans la charte informatique par exemple) et techniques (logiciel de surveillance et de contrôle) de protection contre les cyberattaques susceptibles d'être commises par leurs employés.

La coopération entre Etats membres est renforcée

S'agissant de la coopération entre Etats membres, la directive prévoit :

§ la mise en place de réseaux de coopération et de partenariat pour permettre l'échange d'informations, destinées à prévenir et à combattre la cybercriminalité ;

Il est précisé que les Etats membres doivent désormais disposer d'un point de contact national opérationnel, et recourir, au niveau européen, au réseau existant de points de contact opérationnels (art. 13) ;

Il est précisé que ces réseaux devront être disponibles 24h/24 et 7j/7 ; de plus, des procédures pour répondre aux demandes urgentes sous huit heures devront être mises en place par les Etats membres (Art.13).

La France devra transposer les dispositions imposées par cette directive au plus tard le 4 septembre 2015.