Des mesures renforcÃ©es pour la lutte contre la cybercriminalitÃ©
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 30/9/2013 13:00:00

Une nouvelle directive europÃ©enne (nÂ° 2013-40/UE du 12 aoÃ»t 2013) **relative aux attaques contre les systÃ¨mes d'information** est entrÃ©e en vigueur le 3 septembre 2013.

Elle remplace et renforce une dÃ©cision-cadre du Conseil de l'Union (2005/222/JAI) du 24 fÃ©vrier 2005, qui avait dÃ©jÃ pour principal objectif de renforcer la coopÃ©ration entre les autoritÃ©s judiciaires des Ã□tats membres grÃ¢ce Ã un rapprochement de la lÃ©gislation pÃ©nale sanctionnant la cybercriminalitÃ©. **Donatienne Blin**, avocat au dÃ©partement Informatique & rÃ©seaux de **Courtois Lebel**, explique quelles vont Ãªtre ces nouvelles rÃ¨gles.

Les attaques contre les systÃ¨mes d'information constituent une menace croissante au sein de l'Union et plus gÃ©nÃ©ralement Ã l'Ã©chelle mondiale. Les progrÃ¨s technologiques permettent aux hackers de construire des mÃ©thodes de plus en plus sophistiquÃ©es, susceptibles de provoquer des dommages Ã©conomiques considÃ©rables : interruption de l'activitÃ© de l'entreprise, perte ou altÃ©ration de donnÃ©es confidentielles ou personnelles...

L'existence de lacunes et de disparitÃ©s dans les diffÃ©rentes lÃ©gislations des Etats membres en matiÃ¨re d'attaques contre les systÃ¨mes d'information risque d'entraver la lutte contre la cybercriminalitÃ© et de ralentir la coopÃ©ration policiÃ¨re et judiciaire europÃ©enne.

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

En synthÃ¨se, la directive fixe les rÃ¨gles minimales concernant la dÃ©finition des infractions pÃ©nales et les sanctions pÃ©nales applicables et amÃ©liore la coopÃ©ration entre les autoritÃ©s compÃ©tentes des Etats membres.

Les infractions pÃ©nales mieux dÃ©finies

S'agissant de la mise en place de Â« rÃ¨gles minimales Â», on citera :

ï□§ L'adoption de dÃ©finitions communes s'agissant des Ã©lÃ©ments constitutifs des infractions pÃ©nales suivantes (Art. 3 Ã 6) :

- accÃ¨s illÃ©gal Ã un systÃ¨me d'information

- atteinte illÃ©gale Ã l'intÃ©gritÃ© d'un systÃ¨me

- atteinte illÃ©gale Ã l'intÃ©gritÃ© des donnÃ©es

- interception illÃ©gale de ces donnÃ©es ;

ï§ l'incrimination de la production, de la vente et de l'obtention des outils (programmes) ou dispositifs (code d'accÃ¨s) conÃ§us pour commettre l'une de ces infractions prÃ©citÃ©es (Art.7) ;

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

ï§ le principe de Â« sanctions effectives, proportionnÃ©es et dissuasives Â» Ã mettre en place par les Etats membres : des peines d'emprisonnement minimum sont imposÃ©es par la directive (Art.9) ;

ï§ la prÃ©sence de circonstances aggravantes en cas d'attaque de grande ampleur commise par des organisations criminelles (notamment dans le cas des rÃ©seaux dit Â« zombie Â»), en cas de prÃ©judice grave, lorsque les attaques sont menÃ©es contre une Â« infrastructure critique Â» d'un Ã©tat membre, ou encore en cas d'usurpation d'identitÃ© numÃ©rique (Art.9) ;

ï§ la mise en cause de la responsabilitÃ© 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) ;

ï§ la responsabilitÃ© et la sanction des personnes morales, lorsque Â« l'absence de surveillance et de contrÃ´le Â» aura rendu possible l'une des infractions prÃ©citÃ©es commise pour son compte par ses salariÃ©s (Art.10 et 11).

La directive insiste en effet sur le fait qu'il est nÃ©cessaire de Â« garantir des niveaux de protection appropriÃ©s contre les menaces et les vulnÃ©rabilitÃ©s pouvant Ãªtre raisonnablement identifiÃ©es Â» : la responsabilitÃ© de la personne morale devra donc Ãªtre engagÃ©e dÃ¨s lors que celle-ci n'a pas, Â« de toute Ã©vidence Â», assurÃ© un niveau de protection suffisant contre les cyberattaques commises pour son compte (ConsidÃ©rant 26).

Des dispositions contraignantes pour les entreprises

Les dispositions des articles 10 et 11 sont donc particuliÃ¨rement contraignantes Ã l'Ã©gard des entreprises, Ã qui il revient d'apporter la preuve de leurs diligences en matiÃ¨re de surveillance et de protection contre les cyberattaques commises par leurs propres salariÃ©s.

Pour s'exonÃ©rer de leur responsabilitÃ©, celles-ci devront donc dÃ©montrer cumulativement :

ï§ que la vulnÃ©rabilitÃ© ou la menace ne pouvait pas Ãªtre raisonnablement identifiÃ©e ou anticipÃ©e (soit au regard de l'Ã©tat de l'art, soit au regard des moyens dÃ©ployÃ©s par l'auteur de l'attaque pour dissimuler ses actes au sein de l'entreprise) ;

ï§ avoir mis en Å uvre en interne des mesures prÃ©ventives, Ã la fois juridiques (dispositions spÃ©cifiques dans la charte informatique par exemple) et techniques (logiciel de surveillance et de contrÃ´le) de protection contre les cyberattaques susceptibles d'Ãªtre commises par leurs employÃ©s.

La coopÃ©ration entre Etats membres est renforcÃ©e

S'agissant de la coopÃ©ration entre Etats membres, la directive prÃ©voit :

ï§ la mise en place de rÃ©seaux de coopÃ©ration et de partenariat pour permettre l'Ã©change d'informations, destinÃ©es Ã prÃ©venir et Ã combattre la cybercriminalitÃ© ;

ï§ que les Etats membres doivent dÃ©sormais disposer Â« d'un point de contact national opÃ©rationnel Â», et recourir, au niveau europÃ©en, au Â« rÃ©seau existant de points de contact opÃ©rationnels Â» (art. 13) ;

ï§ que ces rÃ©seaux devront Ãªtre disponibles 24h/24 et 7j/7 ; de plus, des procÃ©dures pour rÃ©pondre aux demandes urgentes sous huit heures devront Ãªtre mises en place par les Etats membres (Art.13).

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