



Commission européenne
Représentation au Luxembourg

Communiqué de presse

272-2010 – 30 septembre 2010

La Commission va renforcer les moyens de défense de l'Europe contre les cyberattaques

La Commission européenne a dévoilé aujourd'hui deux nouvelles mesures qui doivent permettre à l'Europe de parer aux attaques contre ses systèmes d'information essentiels. Il s'agit d'une proposition de directive sur les mesures contre les nouvelles formes de cybercriminalité, notamment les cyberattaques à grande échelle, complétée par une proposition de règlement destinée à renforcer et à moderniser l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA). Ces deux initiatives sont prévues dans l'[Agenda numérique pour l'Europe](#) et dans le programme de Stockholm pour renforcer la confiance des utilisateurs et la sécurité des réseaux. La proposition de directive prévoit que les auteurs de cyberattaques et les producteurs de logiciels connexes malveillants peuvent être poursuivis et risquent des sanctions pénales plus lourdes. Les États membres seraient également tenus de réagir rapidement aux demandes d'aide urgentes en cas de cyberattaque, ce qui rendrait plus efficace la coopération judiciaire et policière européenne dans ce domaine. Le renforcement et la modernisation de l'ENISA aiderait également l'UE, les États membres et les partenaires privés à développer leur aptitude à prévenir, identifier et combattre les problèmes de cybersécurité, et améliorerait leur état de préparation face à ces défis. Les deux propositions seront soumises au Parlement européen et au Conseil de l'Union européenne pour adoption.

Mme Cecilia Malmström, commissaire chargée des affaires intérieures, a déclaré: «La criminalité innove. À l'aide de logiciels malveillants, il est possible de prendre le contrôle d'un grand nombre d'ordinateurs et de voler des numéros de cartes de crédit, de trouver des informations sensibles ou de lancer des attaques à grande échelle. Il est temps que nous redoublions d'efforts contre la cybercriminalité, à laquelle recourt souvent aussi le crime organisé. Les propositions que nous présentons aujourd'hui constituent une étape importante, car nous criminalisons la création et la vente de logiciels malveillants, et nous améliorons la coopération policière européenne».

Mme Neelie Kroes, vice-présidente de la Commission chargée de la stratégie numérique, a quant à elle déclaré: «Mettre le numérique à la portée de tous les Européens ne sera possible que si les citoyens ont confiance dans les réseaux et se sentent en sécurité lorsqu'ils sont en ligne. Les menaces contre les systèmes informatiques ne connaissent pas de frontières. L'Agence européenne chargée de la sécurité des réseaux et de l'information, une fois modernisée, apportera de nouvelles compétences techniques et encouragera les échanges de bonnes pratiques en Europe. Les institutions de l'UE et les gouvernements doivent coopérer étroitement pour nous aider à comprendre la nature et l'ampleur des nouvelles menaces qui pèsent sur nos systèmes. Nous avons besoin des conseils et du soutien de l'ENISA pour concevoir ensemble des mécanismes de réaction efficaces, afin de protéger nos concitoyens et le commerce électronique».

Alors qu'elle a entrepris d'exploiter au maximum le potentiel des réseaux et des systèmes d'information, l'Europe ne doit pas être plus exposée aux perturbations causées par des accidents ou des phénomènes naturels (comme la rupture de câbles sous-marins) ou par des actes malveillants (comme le piratage informatique ou d'autres types de cyberattaques). Ces derniers pourraient reposer, par exemple, sur l'utilisation d'outils de plus en plus sophistiqués détournant un grand nombre d'ordinateurs et les manipulant simultanément pour en faire une armée de robots sur l'internet (les «botnets») à l'insu de leurs propriétaires. Ces ordinateurs infectés peuvent ensuite être utilisés pour des cyberattaques foudroyantes sur des systèmes informatiques publics ou privés, comme ce fut le cas en Estonie en 2007, où la plupart des serveurs de services publics, mais aussi ceux du gouvernement, du parlement et de la police ont été mis temporairement hors d'état. La fréquence des attaques contre des systèmes d'information n'a cessé d'augmenter depuis l'adoption par l'UE des premières règles sur les [attaques visant les systèmes d'information](#) en février 2005. En mars 2009, les systèmes informatiques d'organismes publics et privés de plus de cent pays ont été attaqués par un réseau d'ordinateurs manipulés qui en extrayaient des documents sensibles et secrets. Dans ce cas également, des logiciels malveillants ont créé des «botnets», soit des réseaux d'ordinateurs infectés qui peuvent être contrôlés à distance pour organiser une attaque coordonnée.

Le train de mesures que propose la Commission permettra à l'Europe de mieux réagir aux perturbations des réseaux informatiques. La proposition de la Commission relative à la cybercriminalité s'appuie sur les règles en vigueur depuis 2005 et introduit de nouvelles circonstances aggravantes et des sanctions pénales plus lourdes, qui sont nécessaires pour combattre plus efficacement les attaques à grande échelle, potentielles et réelles, contre les systèmes d'information.

Cette proposition permettrait en outre d'améliorer la coopération entre les autorités judiciaires et policières des États membres, en prévoyant l'obligation pour ceux-ci de mieux mettre à profit le réseau de points de contacts 24/7 existant en traitant les demandes urgentes dans un délai déterminé.

Enfin, la proposition de directive prévoit la création d'un système de recensement et de localisation des cyberattaques.

Coopération renforcée entre pays et secteurs industriels

Pour mieux coordonner la riposte européenne, la Commission propose un nouveau règlement destiné à renforcer et moderniser l'Agence européenne chargée de la sécurité des réseaux et de l'information ([ENISA](#)), créée en 2004. Cette mesure permettrait de renforcer la coopération entre les États membres, les services répressifs et le secteur industriel. L'ENISA contribuera fortement à accroître la confiance, indispensable au développement de la société de l'information, en améliorant la sécurité et le respect de la vie privée des utilisateurs.

Son nouveau mandat permettrait à l'ENISA de faire participer des États membres et des partenaires privés à des activités conjointes en Europe, notamment des exercices de cybersécurité, des campagnes de sensibilisation et des partenariats public-privé pour des travaux sur la résilience des réseaux, des analyses économiques et une évaluation des risques.

Modernisée, l'ENISA pourrait fonctionner avec davantage de souplesse et mieux s'adapter aux besoins, et elle pourrait fournir une assistance et des conseils aux États membres et aux institutions européennes en matière réglementaire.

Enfin, pour réagir à l'intensité croissante des défis auxquels est confrontée la cybersécurité, la proposition de règlement prévoit d'allonger de cinq ans le mandat de l'ENISA et d'accroître progressivement ses ressources financières et humaines. La Commission propose également que la structure de fonctionnement de l'ENISA soit renforcée, en accordant un rôle de supervision plus étendu à son conseil d'administration, composé de représentants des États membres de l'UE et de la Commission européenne.

Contexte

La proposition de directive relative aux attaques visant les systèmes d'information abroge la décision-cadre 2005/222/JAI du Conseil. Les États membres seraient tenus de se conformer à la nouvelle directive sur la cybercriminalité et de la transposer dans leur législation nationale dans un délai maximal de deux ans à compter de son adoption.

L'ENISA a été créée en 2004, et son mandat actuel expire en mars 2012. La Commission propose de prolonger ce mandat de cinq années supplémentaires. La proposition de règlement a été précédée d'un vaste processus, notamment une évaluation de l'Agence, des recommandations de son conseil d'administration, deux consultations publiques et une étude d'impact comprenant une analyse coûts-avantages.

Pour de plus amples informations

Page d'accueil du site de Mme Cecilia Malmström, commissaire chargée des affaires intérieures:

http://ec.europa.eu/commission_2010-2014/malmstrom/welcome/default_fr.htm

Page d'accueil du site de Mme Neelie Kroes, vice-présidente chargée de la stratégie numérique:

http://ec.europa.eu/commission_2010-2014/kroes/index_en.htm

Salle de presse sur la Société de l'information:

http://ec.europa.eu/information_society/newsroom/cf/menu.cfm

Pour des informations supplémentaires
Ernst Moutschen – 4301 32925
E-Mail: ernst.moutschen@ec.europa.eu