COMMISSION EUROPEENNE

COMMUNIQUE DE PRESSE

Bruxelles, le 7 février 2013

Un plan de cybersécurité de l'UE pour protéger l'internet ouvert et les libertés en ligne

La Commission européenne a publié, en liaison avec la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité, une stratégie en matière de cybersécurité ainsi qu'une proposition de directive de la Commission concernant la sécurité des réseaux et de l'information (SRI).

La stratégie de cybersécurité «Un cyberespace ouvert, sûr et sécurisé», expose la vision globale de l'Union européenne en ce qui concerne les meilleurs moyens de prévenir les perturbations et attaques visant le cyberespace et de s'y opposer. Elle vise à promouvoir les valeurs européennes que sont la liberté et la démocratie et à faire en sorte que l'économie numérique puisse se développer en toute sécurité. Des mesures spécifiques sont prévues pour accroître la résilience des systèmes informatiques, faire reculer la cybercriminalité et renforcer la politique internationale de l'UE en matière de cybersécurité et de cyberdéfense.

La vision de l'UE en matière de cybersécurité s'articule autour de cinq priorités:

- parvenir à la cyber-résilience,
- faire reculer considérablement la cybercriminalité,
- développer une politique et des moyens de cyberdéfense en liaison avec la politique de sécurité et de défense commune (PSDC),
- développer les ressources industrielles et technologiques en matière de cybersécurité,
- instaurer une politique internationale de l'Union européenne cohérente en matière de cyberespace et promouvoir les valeurs essentielles de l'UE.

La politique internationale de l'UE en matière de cyberespace encourage le respect des valeurs essentielles de l'Union, définit des règles pour un comportement responsable et prône l'application dans le cyberespace de la législation internationale existante tout en aidant les pays hors UE à renforcer leurs capacités en matière de cybersécurité et en promouvant la coopération internationale dans ce domaine.

L'UE a réalisé des progrès décisifs en ce qui concerne la protection contre la cybercriminalité, notamment en créant un Centre européen de lutte contre la cybercriminalité (IP/13/13), en proposant des mesures législatives relatives aux attaques visant les systèmes d'information (IP/10/1239) et en lançant l'Alliance mondiale contre les abus sexuels commis contre des enfants via internet (IP/12/1308). La stratégie vise également à mettre en place et à financer un réseau de centres d'excellence de lutte contre la cybercriminalité qui faciliteront la formation et le renforcement des capacités.

La proposition de directive sur la SRI est un volet essentiel de la stratégie globale. Elle obligerait tous les États membres, les facilitateurs de services internet clés et les opérateurs d'infrastructures critiques telles que les plateformes de commerce électronique et les réseaux sociaux, ainsi que les acteurs économiques des secteurs de l'énergie, des transports, des services bancaires et des soins de santé à garantir un environnement numérique offrant des gages de sécurité et de confiance dans toute l'UE. La proposition de directive prévoit notamment les mesures suivantes:

(a) les États membres doivent adopter une stratégie de SRI et désigner des autorités nationales compétentes en la matière, qui disposeront de ressources financières et humaines suffisantes pour prévenir et gérer les risques et incidents de SRI et intervenir en cas de nécessité,

(b) un mécanisme de coopération entre les États membres et la Commission doit être instauré pour diffuser des messages d'alerte rapide sur les risques et incidents au moyen d'une infrastructure sécurisée, pour collaborer et organiser des examens par les pairs,

(c) les opérateurs d'infrastructures critiques de secteurs tels que les services financiers, les transports, l'énergie et la santé, les facilitateurs de services internet clés (notamment les magasins d'applications en ligne, les plateformes de commerce électronique, les passerelles de paiement par internet, les services informatiques en nuage, les moteurs de recherche ou les réseaux sociaux) ainsi que les administrations publiques doivent adopter des pratiques en matière de gestion des risques et signaler les incidents de sécurité significatifs touchant leurs services essentiels.

Mme Neelie Kroes, vice-présidente de la Commission responsable de la stratégie numérique, a déclaré:

«Plus on recourt à l'internet, plus on se montre exigeant en ce qui concerne sa sécurité. Un internet sûr, c'est la garantie que nos libertés, nos droits et nos possibilités d'activité économique sont protégés. Il est temps d'agir, et il faut le faire de manière coordonnée. Le coût de l'inaction est plus élevé que celui de l'action.»

Catherine Ashton, haute représentante de l'Union européenne pour les affaires étrangères et la politique de sécurité et vice-présidente de la Commission européenne, a déclaré à ce sujet:

«Pour que le cyberespace reste libre et ouvert, les normes, principes et valeurs que l'UE défend hors ligne doivent aussi s'appliquer en ligne. Les droits fondamentaux, la démocratie et l'État de droit doivent donc être protégés dans le cyberespace. L'UE s'emploie, avec ses partenaires internationaux, la société civile et le secteur privé, à promouvoir ces droits sur le plan mondial.»

Mme Cecilia Malmström, membre de la Commission chargée des affaires intérieures, a pour sa part déclaré:

«Cette stratégie met en exergue les actions concrètes que nous allons engager pour faire reculer considérablement la cybercriminalité. Beaucoup de pays n'ont pas les outils nécessaires pour enquêter sur la cybercriminalité organisée et la combattre. Tous les États membres devraient mettre en place de véritables unités anticybercriminalité nationales qui pourront bénéficier du savoir-faire et de l'assistance du Centre européen de lutte contre la cybercriminalité (EC3)».

Contexte

Les incidents de cybersécurité, dont l'ampleur, la fréquence et la complexité ne cessent de croître, ignorent les frontières. Ils peuvent porter un grand préjudice à la sécurité et à l'économie. Il faut redoubler d'efforts en ce qui concerne la prévention, la coopération et la transparence sur les cyberincidents.

En effet, les actions entreprises jusqu'à présent par la Commission européenne et certains États membres étaient trop fragmentées pour régler ce problème de plus en plus préoccupant.

La cybersécurité en chiffres aujourd'hui

- On estime à 150 000 le nombre de virus en circulation et à 148 000 le nombre d'ordinateurs dont la sécurité est compromise chaque jour.
- Selon le Forum économique mondial, la probabilité d'une grave défaillance des infrastructures d'information critiques dans les dix années à venir est de 10 %, et le préjudice qui en résulterait pourrait être de 250 milliards de dollars.
- La cybercriminalité est responsable d'une bonne partie des incidents de cybersécurité. Symantec estime le montant des pertes subies chaque année par les victimes des cybercriminels dans le monde entier à 290 milliards d'euros et, selon une étude de McAfee, le produit de la cybercriminalité atteindrait 750 milliards d'euros par an.
- Le sondage Eurobaromètre de 2012 sur la cybersécurité a révélé que 38 % des internautes de l'UE avaient modifié leur comportement en raison d'inquiétudes liées à la sécurité: 18 % sont moins susceptibles de faire des achats en ligne et 15 % sont moins susceptibles d'utiliser les services bancaires en ligne. Il a également montré que 74 % des personnes interrogées considéraient que les risques étaient en augmentation, 12 % avaient déjà été victimes de fraude en ligne et 89 % évitaient de divulguer des informations personnelles.
- 56,8 % des personnes qui se sont exprimées dans le cadre de la consultation publique sur la SRI ont indiqué avoir été confrontées, pendant l'année écoulée, à des incidents liés à la cybersécurité ayant eu une incidence grave sur leurs activités.
- Dans le même temps, les données recueillies par Eurostat montraient que, à la date de janvier 2012, seules 26 % des entreprises de l'UE avaient une politique de sécurité informatique en bonne et due forme.

Liens utiles

Foire aux questions MEMO/13/71

Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé

Proposition de directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union

Donnez votre avis

Mots-clé: # cybersecurity

Site web de Mme Neelie Kroes (en anglais et néerlandais)

Suivez Mme Neelie Kroes sur Twitter

Site web du SEAE

Suivez le SEAE sur Twitter

Site internet de Mme Cecilia Malmström

Suivez Mme Neelie Kroes sur Twitter

Site web du Centre européen de lutte contre la cybercriminalité d'Europol (EC3) (en anglais)

Alliance mondiale contre les abus sexuels commis contre des enfants via internet.

Contacts :
Ryan Heath (+32 2 296 17 16), Twitter: @RyanHeathEU
Michele Cercone (+32 2 298 09 63)
Maja Kocijancic (+32 2 298 65 70)
Michael Mann (+32 2 299 97 80)