CONSEIL DE L'UNION EUROPÉENNE

Bruxelles, le 27 mai 2009 (03.06)
(OR. en)

10125/09

TELECOM 115
DATAPROTECT 39
JAI 319
PROCIV 78

NOTE

du:	Groupe "Télécommunications et société de l'information"
au:	Coreper / Conseil
n° prop. Cion:	8375/09 TELECOM 69 DATAPROTECT 24 JAI 192 PROCIV 46
Objet:	Politique européenne en matière de sécurité des réseaux et de l'information - Orientations dans la perspective d'un échange de vues

Dans la perspective du Conseil TTE du 11 juin 2009, les délégations trouveront en annexe pour information les orientations envisagées par la présidence pour servir de base à l'échange de vues que tiendront les ministres.

ORIENTATIONS DANS LA PERSPECTIVE D'UN ÉCHANGE DE VUES SUR

L'AVENIR DE LA POLITIQUE EN MATIÈRE DE SÉCURITÉ DES RÉSEAUX ET DE L'INFORMATION

CONSEIL TTE, 11 JUIN 2009

1. INTRODUCTION

Les réseaux de communication et les systèmes d'information sont devenus le système nerveux de notre société moderne. De nombreux services et processus de notre économie et de notre société dépendent de plus en plus du bon fonctionnement de ce système nerveux, dont la sécurité et la résilience constituent une préoccupation grandissante.

Les risques associés aux technologies de l'information et de la communication représentent un défi constant pour l'Europe, essentiellement en raison de l'évolution permanente des menaces informatiques, de leur complexité croissante et de leur mondialisation. Les interdépendances des infrastructures au niveau mondial, les technologies émergentes, l'omniprésence des technologies de l'information et de la communication, l'absence de normes minimales et la convergence constante des technologies amplifient ce défi.

Les défis posés par la sécurité des réseaux et de l'information nécessiteront une réponse européenne forte et coordonnée. Les récentes cyberattaques prenant individuellement pour cible certains pays ont démontré qu'un pays pris isolément peut être très vulnérable. Une approche à l'échelle européenne qui complète et apporte de la valeur ajoutée aux initiatives nationales est un élément capital de la politique en matière de sécurité des réseaux et de l'information.

2. ENISA – L'AGENCE EUROPÉNNE CHARGÉE DE LA SÉCURITÉ DES RÉSEAUX ET DE L'INFORMATION

En 2004, face aux défis en matière de sécurité auxquels la société de l'information était confrontée, la Communauté européenne a créé l'Agence européenne chargée de la sécurité des réseaux et de l'information[1] (ENISA) aux fins d'assurer un niveau élevé et efficace de sécurité des réseaux et de l'information au sein de la Communauté et de favoriser l'émergence d'une culture de la sécurité des réseaux et de l'information dans l'intérêt des citoyens, des consommateurs, des entreprises et des organismes du secteur public de l'Union européenne.

[1] Règlement (CE) n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information, JO L 77 du 13.3.2004, p. 1.

Le mandat initial de l'ENISA était de cinq ans (2004-2009). Le 24 septembre 2008, le Conseil et le Parlement européen ont adopté un règlement prolongeant ce mandat sans modifications pour une période de trois ans courant jusqu'au 13 mars 2012[1]. Le budget annuel de l'ENISA, qui emploie quelque 50 personnes, avoisine les 8 millions d'euros pour la période 2004-2012.

En vue d'évaluer les solutions envisageables pour l'avenir de l'ENISA après mars 2009, la Commission a chargé un groupe d'experts externes d'évaluer les performances de l'ENISA depuis sa création[2]. En juin 2007, la Commission a élaboré une communication sur l'évaluation de l'ENISA[3] dans laquelle elle présentait une appréciation du rapport du groupe d'experts externes, ainsi que les recommandations du conseil d'administration de l'ENISA. Les résultats essentiels du rapport du groupe d'experts confirmaient la validité du raisonnement politique à la base de la création de l'ENISA et des objectifs initiaux, et notamment sa contribution à la réalisation d'un véritable marché intérieur des communications électroniques.

Le conseil d'administration de l'ENISA a émis des recommandations concernant l'opportunité d'apporter d'éventuelles modifications au règlement ENISA[4]. Les principales recommandations étaient les suivantes: il conviendrait de réviser le règlement ENISA afin de prolonger le mandat de l'agence, il devrait être encore prévu de réviser le mandat à une date déterminée, le champ d'application de l'agence ne devrait pas être matériellement changé et le règlement devrait être révisé pour combiner les articles 2 et 3[5] afin de fixer des objectifs clés basés sur les résultats qui soient réalistes et entrent dans le domaine de compétence de l'agence.

---

1 Règlement (CE) no 1007/2008 du Parlement européen et du Conseil du 24 septembre 2008 modifiant le règlement (CE) no 460/2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information en ce qui concerne sa durée, JO L 293 du 31.10.2008.

2 "Évaluation of the European Network and Information Security Agency", Rapport final du groupe d'experts, IDC EMEA, 8.1.2007. http://ec.europa.eu/dgs/information_society/evaluation/studies/index_en.htm

3 COM(2007) 285 final.

4 Disponible à l'adresse: http://enisa.europa.eu/pages/03_02.htm Ces recommandations sont également abordées dans le document COM(2007) 285 final.

5 Concernant, respectivement, les objectifs et les tâches.

3. CONTEXTE POLITIQUE DE L'ÉCHANGE DE VUES

Le 2 septembre 2008, intervenant devant le Parlement européen réuni en session plénière, la Commission a invité le Parlement européen et le Conseil à ouvrir, début 2009, un débat approfondi sur l'approche européenne de la sécurité des réseaux et sur la manière de faire face aux cyberattaques en se penchant, au cours de leur réflexion, sur l'avenir de l'ENISA.

Le 24 septembre 2008, dans les considérants du règlement prolongeant le mandat de l'ENISA, le Conseil et le Parlement européen appelaient à poursuivre " les discussions concernant l'Agence" et "la réflexion concernant l'orientation générale que doivent suivre les efforts européens visant à accroître la sécurité des réseaux et de l'information."

4. ÉTAPES PRÉPARATOIRES

Pour nourrir ce débat, la première démarche des services de la Commission fut de mener, du 7 novembre 2008 au 9 janvier 2009, une consultation publique sur les objectifs que pourrait se fixer une politique renforcée au niveau de l'UE en matière de sécurité des réseaux et de l'information et sur les moyens à mettre en œuvre pour atteindre ces objectifs. Les services de la Commission ont également organisé, le 15 décembre 2008, un atelier réunissant des experts en sécurité des réseaux et de l'information issus des organes compétents des États membres afin qu'ils discutent de l'évolution des défis qui se posent dans le domaine de la sécurité, des priorités et des objectifs envisageables afin de relever ces défis, ainsi que des instruments et mécanismes nécessaires pour renforcer la politique en matière de sécurité des réseaux et de l'information au niveau de l'UE.

Dans le cadre de la consultation publique sur l'avenir de l'ENISA, une grande majorité des personnes interrogées se sont prononcées en faveur de la prolongation du mandat de l'agence et ont plaidé pour que celle-ci ait un plus grand rôle à jouer dans la coopération européenne en matière de sécurité des réseaux et de l'information et pour que ses ressources soient augmentées.

5. ACTIONS EN COURS DANS LE DOMAINE DE LA PROTECTION DES INFRASTRUCTURES D'INFORMATION CRITIQUES

Dans le contexte de l'initiative générique sur le programme européen de protection des infrastructures critiques (EPCIP), la Commission européenne a récemment adopté une communication relative à la protection des infrastructures d'information critiques (IIC) intitulée "Protéger l'Europe des cyberattaques et des perturbations de grande envergure: améliorer l'état de préparation, la sécurité, et la résilience[1]".

[1] COM(2009)149.

Cette communication propose une série d'actions à mener à brève et moyenne échéance (jusqu'en 2011) dans le domaine de la sécurité et de la résilience des IIC, comme encourager la coopération à l'échelle européenne entre les équipes d'intervention en cas d'urgence informatique nationales ou gouvernementales; engager le secteur privé à partager avec le secteur public les informations et à diffuser les bonnes pratiques; soutenir l'échange d'informations et de bonnes pratiques politiques entre États membres et promouvoir ainsi une coopération européenne plus étroite entre les États membres grâce à des plans nationaux et multinationaux en cas d'urgence et des exercices réguliers portant sur la réaction en cas d'incident de grande envergure affectant la sécurité des réseaux, ainsi que sur la récupération après défaillance grave et continuer à mettre au point des critères d'identification des infrastructures européennes critiques pour le secteur des TIC.

6. LA CONFÉRENCE MINISTÉRIELLE DE TALLIN

Les 27 et 28 avril 2009, une conférence ministérielle consacrée à la protection des infrastructures d'information critiques s'est tenue à Tallin. Cette conférence était organisée par l'Estonie sous les auspices de la présidence tchèque de l'UE.

Dans ses conclusions, la conférence a marqué son soutien à la poursuite des travaux en cours dans le domaine de la protection des infrastructures d'information critiques et a souligné que ces travaux devraient mettre l'accent sur les actions renforçant la sécurité et la résilience des IIC, établissant des partenariats public-privé efficaces au niveau de l'UE et intensifiant la coopération et la coordination tant au niveau de l'UE qu'au niveau international. La conférence a estimé que "les dernières années ont démontré que les cyberattaques ont atteint un degré de complexité sans précédent et qu'elles sont de plus en plus souvent exécutées à des fins lucratives ou pour des raisons politiques" et que "le nombre très élevé de virus, de vers et d'autres types de logiciels malveillants, l'expansion des réseaux de machines zombies et l'augmentation continuelle du pourriel confirment la gravité du problème. Ces menaces requièrent une réponse européenne forte et coordonnée."

En ce qui concerne l'ENISA, la conférence a conclu que l'agence constituait un instrument précieux permettant d'appuyer les efforts de coopération menés à travers l'UE en la matière. Cependant, les nouveaux défis auxquels nous serons confrontés durant de nombreuses années exigent que le mandat de l'agence soit profondément repensé et reformulé afin de mieux mettre l'accent sur les priorités et les besoins de l'UE, de pouvoir y répondre de manière plus souple, de développer des savoirs et des compétences européennes, et de soutenir l'efficacité opérationnelle de l'agence ainsi que son impact général. C'est de cette façon que l'ENISA pourra devenir un atout permanent pour chaque État membre et l'Union européenne dans son ensemble.

La conférence a également conclu qu'un exercice commun au niveau de l'UE dans le domaine de la protection des infrastructures d'information critiques devrait être organisé et avoir lieu avant 2010, conformément au plan d'action de la Commission. Une marque de soutien à cet exercice de la part du Conseil TTE en soulignerait l'importance en tant que premier pas concret vers une coordination et une coopération fortes entre les États membres et en tant que moyen contribuant à recenser les domaines dans lesquels il importe d'agir immédiatement.

7. RÉVISION DU CADRE RÉGLEMENTAIRE POUR LES COMMUNICATIONS ÉLECTRONIQUES

Conformément au nouveau cadre réglementaire pour les communications électroniques, l'ENISA s'est vu attribuer un rôle de soutien aux organes des États membres et à la Commission pour les aspects concernant la sécurité des réseaux et de l'information.

8. QUESTIONS POUVANT SERVIR DE BASE À L'ÉCHANGE DE VUES

1. Quels devraient être les deux ou trois objectifs principaux à moyen ou long terme d'une politique renforcée de l'UE en matière de sécurité des réseaux et de l'information afin d'assurer la coopération transnationale de tous les intervenants et la mise en place d'instruments politiques permanents ou à long terme?
2. Bien qu'une agence semble être un instrument efficace pour renforcer la politique européenne en matière de sécurité des réseaux et de l'information, d'autres moyens devraient-ils être prévus à moyen ou long terme?
3. Comment l'ENISA devrait-elle être réformée afin de mieux se concentrer sur les principaux défis en faisant preuve de davantage de souplesse pour s'adapter à l'évolution des menaces informatiques, en assurant une permanence ou une continuité à long terme, en évaluant ses performances de manière appropriée et en se dotant d'une structure de gouvernance renforcée? Une augmentation des ressources serait-elle nécessaire pour relever ces défis?