16/12/2011

www.enisa.europa.eu

Protéger le cyber-espace: réaliser des échanges transfrontaliers d'informations entre les «pompiers numériques»

L'ENISA, l'Agence européenne de cyber-sécurité, a publié une étude consacrée aux aspects juridiques et règlementaires du partage d'informations et de la collaboration transfrontalière entre les CERT (Équipes d'interventions en cas d'urgence informatique) nationales/gouvernementales en Europe. Le rapport analyse les conséquences de ces aspects sur le partage transfrontalier d'informations entre les CERT. La conclusion est qu'il existe un équilibre subtil entre les enquêtes, la gestion et l'atténuation des incidents informatiques, tout en respectant les droits et les devoirs prévus par certains cadres juridiques et règlementaires, qui concernent notamment la protection des données et les dispositions concernant la vie privée.

Les CERT sont essentielles dans la coordination transfrontalière des incidents informatiques et, pour jouer ce rôle crucial, elles doivent échanger des informations. L'échange transfrontalier d'informations exige d'examiner des facteurs juridiques complexes. Les CERT situées dans différents pays doivent se conformer à différentes bases juridiques pour demander et transmettre des informations à d'autres équipes. En outre, les informations échangées peuvent être des données personnelles et donc être soumises à des dispositions spécifiques concernant la vie privée. Par ailleurs, les CERT, y compris les CERT nationales/gouvernementales, ont des mandats différents. L'étude identifie ces facteurs juridiques et règlementaires, et donne une évaluation de leurs conséquences sur le partage transfrontalier d'informations entre CERT. Entre autres, l'une des constatations de cette étude est que, en pratique, la protection des données, la rétention des données et l'obligation de travailler avec l'application de la loi sont les défis les plus importants de la coopération transfrontalière entre CERT.

Le Directeur Exécutif de l'ENISA, le Professeur Udo Helmbrecht, a commenté: *«Les CERT doivent agir de manière équilibrée et subtile entre les enquêtes, la gestion et l'atténuation des incidents, tout en protégeant la vie privée, les données et l'intégrité. Clairement, l'échange transfrontalier d'informations ne devrait pas être considéré comme un risque aux droits fondamentaux, car ces échanges sont une condition préalable pour assurer une réponse efficace aux incidents cyber-TIC, mais aussi pour protéger ces mêmes droits. Une mauvaise cyber-sécurité peut en effet compromettre l'exercice des droits de l'homme.»*

Des exemples de recommandations en termes de politique à moyen/long terme comprennent:

- La clarification des différences entre les divers cadres juridiques nationaux ;

- L'adoption d'une législation européenne qui prenne en compte la portée des CERT nationales/gouvernementales;
- La précision d'un seuil pour les incidents exigeant le partage d'informations et l'intervention des CERT nationales/gouvernementales;
- L'explication de la raison pour laquelle les CERT doivent traiter les données personnelles pour les autorités concernées afin de clarifier les circonstances dans lesquelles ces données doivent être partagées au-delà des frontières;
- L'inclusion d'informations sur les bases juridiques pour les demandes d'informations.

Pour consulter **LE RAPPORT COMPLET**

Contexte: Communication sur la protection des infrastructures informatiques 2011 de la Commission européenne

Pour toute demande d'interview, veuillez contacter: Ulf Bergstrom, Porte-parole de l'ENISA, press@enisa.europa.eu, Portable: + 30-6948-460-143, ou Silva Portesi, Expert, CERTrelations Q enisa.europa.eu

Veuillez noter: traduction. La version anglaise est la seule version officielle.
www.enisa.europa.eu/media/enisa-en-francais/
www.enisa.europa.eu