

29/11/2012

EPR23/2012

www.enisa.europa.eu

Nouveau rapport sur les moyens de renforcer la coopération entre les équipes d'intervention d'urgence informatique de l'UE (CERT) et les forces de l'ordre

L'Agence européenne ENISA lance un nouveau Guide des Bonnes Pratiques sur la coopération et la coordination entre équipes d'intervention d'urgence informatique de l'UE (CERT) et les forces de l'ordre (LEA). Le rapport établit que la coopération est essentielle dans la lutte contre la cybercriminalité. L'étude se concentre sur l'identification des lacunes actuelles et sur les synergies possibles et suggère cinq recommandations sur la manière d'améliorer la coopération.

La société et l'économie numériques européennes sont de plus en plus dépendantes de l'espace informatique. Dans le même temps, les cyber-attaques contre des Infrastructures Critiques telles que les systèmes d'énergie, d'eau et de transport, les cyber-incidents, et la cybercriminalité, tels que les attaques botnet et le piratage, mettent la société de l'information en péril. En outre, la plupart des citoyens - 59% - ne se disent pas suffisamment informés sur les risques liés à la cybercriminalité.

La nouvelle étude de l'ENISA estime que la collaboration entre les CERT et les LEA est entravée par leurs différences culturelles inhérentes. Les CERT sont généralement techniques, informelles et axées sur le traitement des problèmes du système d'information. Les LEA, par comparaison, agissent lorsqu'ils soupçonnent qu'un crime a été commis. Le rapport identifie également un certain nombre d'obstacles juridiques et réglementaires. Plus précisément, l'étude a identifié un écart entre une plus grande prise de conscience des lois nationales, par rapport à une petite prise de conscience des cadres juridiques internationaux (directives de l'UE ou la Convention sur la cybercriminalité du Conseil de l'Europe). Un certain nombre de facteurs opérationnels ont également été identifiés comme entravant l'échange d'informations et la collaboration. Les experts qui ont participé à l'étude ont reconnu que l'information sur les rôles et les paramètres de la coopération étaient les questions les plus importantes. Elles ont été suivies par les préoccupations à propos de la bureaucratie, des politiques et des procédures différentes ou inconnues, du manque de normes communes et de clarté sur ce que fait l'autre partie avec les informations délivrées et des détails insuffisants ou inadaptés.

Le rapport formule cinq recommandations clés pour surmonter ces obstacles :

- la formation,
- l'amélioration des structures pour favoriser le partage d'informations,
- la facilitation de la collaboration,
- le développement de bonnes pratiques et
- l'harmonisation et la clarification des aspects juridiques et réglementaires.

ENISA is a Centre of Expertise in Network and Information Security in Europe

Securing Europe's Information Society

Suivez les cyber affaires européennes de sécurité de l'ENISA sur [Facebook](#), [Twitter](#), [LinkedIn](#) [YouTube](#)

& [RSS feeds](#)



29/11/2012

EPR23/2012

www.enisa.europa.eu

Ces recommandations portent sur le développement de la formation entre les CERT et les LEA, l'établissement de compétences de base, les capacités et les procédures, les bonnes pratiques sur la rédaction d'un protocole d'entente (MoU) et des accords de partage de preuves et des précisions supplémentaires pour les CERT sur les problèmes de protection des données.

Le directeur exécutif de l'ENISA le professeur [Udo Helmbrecht](#) a commenté:

«Les équipes d'intervention d'urgence informatique de l'UE (CERT) et les forces de l'ordre couvrent des aspects cruciaux, mais différents de la cyber-sécurité. Leur coopération est vitale pour bien protéger nos citoyens et notre économie numérique. Cependant, jusqu'à présent, peu de recherches ont été faites sur la façon de relier ces deux domaines. Cette étude contribue à une meilleure lutte contre la cybercriminalité en identifiant les défis de collaboration et les moyens de les surmonter. »

Pour le rapport [complet](#)

Pour le contexte : [COM/2011/163](#), ([Flash Eurobaromètre sur la cybersécurité](#)) 2012

Pour obtenir un entretien : Ulf Bergstrom, Porte-parole, à press@enisa.europa.eu, +30 6948 460 143, ou Jo De Muynck, Expert national détaché, à opsec@enisa.europa.eu

Veillez noter: traduction. La version anglaise est la seule version officielle

www.enisa.europa.eu/media/enisa-en-francais/

www.enisa.europa.eu

