

18/04/2011

www.enisa.europa.eu

## L'agence européenne ENISA publie son [rapport final](#) et [un clip vidéo](#) sur 'Cyber Europe 2010', le premier exercice pan-européen de cyber-sécurité pour les organismes publics

L'agence de cyber-sécurité de l'UE, l'ENISA, a publié son [rapport final](#) sur le premier exercice pan-européen de cyber-sécurité pour les organismes publics, 'Cyber Europe 2010'. Ce rapport souligne la nécessité d'augmenter le nombre d'exercices de cyber-sécurité à l'avenir et de favoriser une plus grande collaboration entre les États membres, ainsi que l'importance du rôle de garant de la sécurité informatique incombant au secteur privé. L'ENISA a également publié un clip vidéo en ligne afin d'étayer ce rapport.

Pour accéder à la version multimédia de ce communiqué de presse, veuillez cliquer [ici](#).

Il est prioritaire pour l'UE et son 'Stratégie numérique pour l'Europe' de réaliser des exercices à l'échelle européenne pour assurer la cyber-sécurité, afin de garantir que les entreprises et les particuliers soient protégés quand ils sont connectés à Internet.

L'exercice 'Cyber Europe 2010' a eu lieu le 4 novembre 2010. Son objectif était de déclencher la communication et la collaboration entre les pays dans l'éventualité de cyber-attaques à grande échelle. Plus de 70 experts des organismes publics participants ont collaboré pour contrer plus de 300 cyber-attaques simulées visant à paralyser Internet et les services en ligne essentiels à travers l'Europe. Au cours de l'exercice, une perte simulée de connectivité Internet entre les pays a eu lieu, nécessitant une coopération transfrontalière pour éviter un crash total (simulé) du réseau.

L'exercice a été évalué à trois niveaux :

1. National ;
2. Pan-européen ; et
3. Global.

**Les principaux constats** de ce rapport incluent les éléments suivants :

- Les organismes informatiques des États membres communiquent de nombreuses façons différentes. Une harmonisation des procédures d'opération standards conduirait à des communications plus sécurisées et efficaces entre les organismes.

- La capacité des participants à trouver des points de contact pertinents dans les organisations montrait des divergences. En cas de véritable crise, quelque 55 % des pays n'étaient pas confiants quant à leur capacité à identifier rapidement le contact adéquat, même avec les annuaires disponibles.

- L'avis des participants au sujet des points de contact était équitablement partagé : environ la moitié préférait un 'Point de contact unique' (PDCU), tandis que les participants restants préféraient des 'Points de Contact multiples' (PDCM). Un PDCU serait plus facile ; cependant, en étant réaliste, il existe aujourd'hui de multiples points de contact.

Disposer de PDCM permet également d'éviter qu'il y ait un unique point de défaillance.

18/04/2011

[www.enisa.europa.eu](http://www.enisa.europa.eu)

Le rapport fournit également les **principales recommandations** suivantes:

- L'Europe devrait continuer à réaliser des exercices sur la Protection des infrastructures informatiques essentielles (PIIE) : 86 % des participants ont trouvé ce 'galop d'essai' soit 'très', soit 'extrêmement' utile.
- Le secteur privé peut offrir de la valeur pour les futurs exercices en augmentant les niveaux de réalisme.
- Les 'leçons identifiées' devraient être échangées avec ceux qui organisent d'autres exercices (nationaux ou internationaux).
- Il est important que les États membres soient bien organisés au niveau interne, par exemple en développant et en testant des exercices et plans d'urgence nationaux. Les pays européens sont organisés au niveau national de diverses façons. Compte tenu des différences en termes de structures et de processus, il est vital de savoir qui contacter. Le dialogue sur la nécessité d'un PDCU ou de PDCM au niveau européen devrait se poursuivre, et l'ENISA peut agir en qualité de coordinatrice.
- Un itinéraire pour les exercices pan-européens devrait être créé. Cela inclurait une définition des structures et procédures standards pour les événements à grande échelle

"Le rapport Cyber Europe identifie la façon dont nous pouvons rendre nos activités économiques et sociales en ligne plus sûres. L'ENISA est dédiée à la réalisation d'exercices, de processus et de plans européens visant à protéger l'infrastructure des technologies de l'information et des communications, dont nous dépendons de plus en plus", a déclaré [le Prof. Udo Helmbrecht, Directeur Exécutif de l'ENISA](#).

Un clip vidéo sur '[Cyber Europe 2010](#)' est disponible ici.

**Informations contextuelles:**

[Le Plan d'action de Protection des infrastructures informatiques essentielles](#) (PIIE)

La [Stratégie numérique](#)

et les récentes [Communications sur la PIIE](#) en date du 30/03/2011

**Rapport complet.**

Pour toute interview, ou pour de plus amples détails, veuillez contacter : Ulf Bergstrom, Porte-parole, ENISA, [press@enisa.europa.eu](mailto:press@enisa.europa.eu), Mobile : +30-6948-460-143, ou Panagiotis Trimintzios, Expert, ENISA, [panagiotis.trimintzios@enisa.europa.eu](mailto:panagiotis.trimintzios@enisa.europa.eu).

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