enisa
European Network and Information Security Agency

Cyber Europe 2012

Principales conclusions et recommandations

Décembre 2012

Remerciements

L'ENISA tient à remercier toutes les personnes et toutes les organisations qui ont contribué à cet exercice. Nous exprimons tout particulièrement notre reconnaissance à l'égard des planificateurs de l'exercice, des moniteurs et des modérateurs nationaux.

À propos de l'ENISA

L'Agence européenne de la sécurité des réseaux et de l'information (ENISA) est un centre d'expertise en matière de sécurité des réseaux et des informations au service l'UE, de ses États membres, du secteur privé et des citoyens européens. En collaboration avec ces groupes, l'ENISA travaille au développement de conseils et de recommandations en matière de bonnes pratiques pour la sécurité des informations. L'Agence aide les États membres de l'UE à mettre en œuvre une législation communautaire pertinente et œuvre à l'amélioration de la résilience des infrastructures et des réseaux d'information vitaux en Europe. L'ENISA vise à renforcer l'expertise existante des États membres de l'UE en soutenant le développement de communautés transfrontalières déterminées à améliorer la sécurité des réseaux et des informations dans toute l'UE. Pour plus d'informations sur l'ENISA et ses activités, visitez le site web: www.enisa.europa.eu.

Suivez-nous sur Facebook Twitter LinkedIn Youtube et RSS feeds

L'équipe de projet ENISA

Panagiotis TRIMINTZIOS, ENISA
Razvan GAVRILA, ENISA
Maj Ritter Klejnstrup, ENISA

Données de contact

Pour toute question concernant le présent rapport ou toute autre demande générale sur le programme «Résilience», écrire à l'adresse de contact électronique suivante: resilience at enisa.europa.eu

Table des matières

À propos de Cyber Europe 2012

Le 4 octobre 2012, plus de 500 professionnels de la cyber-sécurité venus de toute l'Europe ont participé à Cyber Europe 2012, le deuxième cyber-exercice paneuropéen.

L'exercice était basé sur des activités extensives tant au niveau national qu'européen visant à améliorer la résilience des infrastructures d'information vitales. Ainsi, Cyber Europe 2012 constitue une étape marquante dans les efforts consentis pour renforcer, dans toute l'Europe, la coopération, l'état de préparation et la réaction en matière de cyber-crise.

En 2009, la Commission européenne a publié une communication relative à la protection des infrastructures d'information critiques (CIIP) – «Protéger l'Europe des cyberattaques et des perturbations de grande envergure: améliorer l'état de préparation, la sécurité et la résilience» (COM/2009/149). Cette communication a ouvert la voie au premier cyber-exercice paneuropéen, organisé le 4 novembre 2010. La Commission européenne est allée de l'avant avec son Agenda numérique pour l'Europe (2010) et sa communication de 2011 relative à la protection des infrastructures d'information critiques – «Réalisations et prochaines étapes: vers une cybersécurité mondiale» (COM/2011/163). En s'appuyant sur ces efforts, Cyber Europe 2012 a élargi son champ d'action, son envergure et sa complexité.

Cyber Europe 2012 avait trois objectifs:

1. Tester l'efficacité et les capacités d'évolution des mécanismes, des procédures et des flux d'information pour la coopération des pouvoirs publics en Europe.
2. Explorer la coopération entre les acteurs publics et privés en Europe.
3. Identifier les lacunes et les défis sur la façon dont les incidents cybernétiques à grande échelle pourraient être traités plus efficacement en Europe.

Vingt-neuf États membres de l'UE (Union européenne) et de l'AELE (Association européenne de libre-échange) étaient impliqués dans la manifestation; 25 d'entre eux ont participé activement à l'exercice, tandis que les quatre autres étaient présents en tant qu'observateurs. En outre, plusieurs institutions de l'UE ont également participé à l'exercice. Globalement, 339 organisations ont participé à Cyber Europe 2012, qui a ainsi rassemblé au total 571 acteurs actifs. À la suite d'une recommandation clé de Cyber Europe 2010, les acteurs du secteur privé ont pris part à cet exercice. Les acteurs publics et privés ont coopéré au niveau national, tandis que les pouvoirs publics mettaient en place une coopération transfrontalière. La plupart des acteurs (88 %) ont émis une opinion positive sur l'exercice (cf. Figure 1).

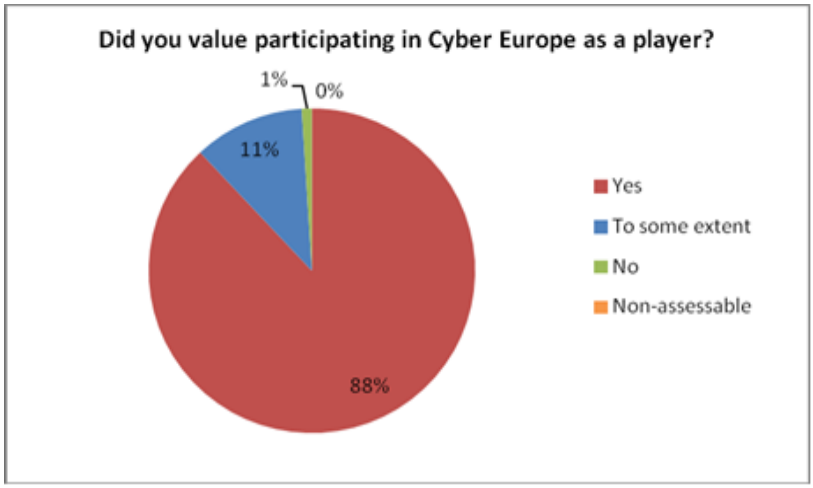


Figure 1: Évaluation de la satisfaction des participants

Avez-vous apprécié votre participation à Cyber-Europe?
Oui
Dans une certaine mesure
Non
Sans opinion

Le processus de planification

Le déroulement de Cyber Europe 2012 a été facilité par l'Agence européenne de la sécurité des réseaux et de l'information (ENISA) et soutenu sur le plan technique par le Centre commun de recherche (CCR) de la Commission européenne. Des représentants des 25 pays participants et les institutions de l'Union européenne ont participé à la planification de l'exercice. L'organisation du processus de planification a été répartie entre plusieurs ateliers.

Le scénario

Le scénario de l'exercice consistait à simuler une série de cyber-incidents à grande échelle survenant en Europe et affectant tous les pays participants: des adversaires fictifs s'associent pour lancer une cyber-attaque massive contre l'Europe, principalement au travers d'attaques de «déni de service coordonné» (DDoS) contre des services publics électroniques. Les services touchés étaient des services d'e-gouvernement et des services financiers en ligne (e-banking, etc.).

Ces cyber-incidents – un défi pour les participants des secteurs public et privé – impliquent la nécessité d'une coopération transfrontalière. Les acteurs, qui avaient reçu des informations sur le scénario (intrants) par courriel, devaient collaborer en utilisant des procédures et des structures standard afin d'évaluer la situation et de convenir d'un mode d'action. La Figure 2 illustre le grand nombre de courriels d'information échangés pendant l'exercice.

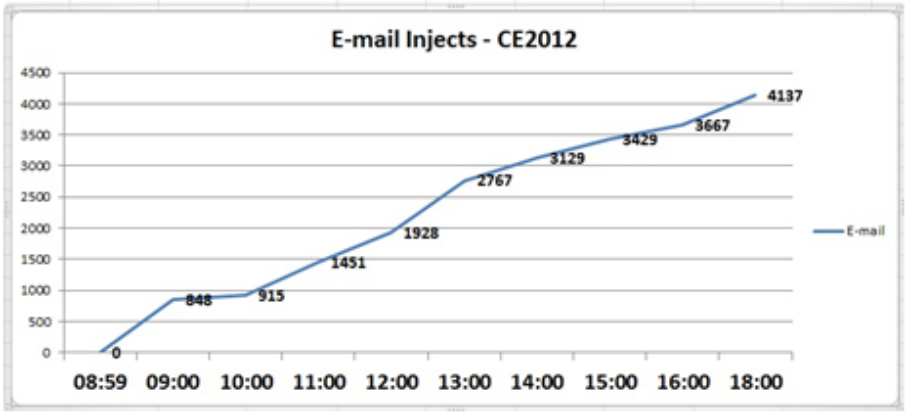


Figure 2: Courriels d'information envoyés pendant l'exercice

Courriels d'information – CE2012

Les acteurs

Le scénario de l'exercice impliquait de nombreux acteurs différents. Au total, 571 personnes membres de 339 organisations venant de toute l'Europe ont pris part à l'exercice. Vingt-cinq pays y étaient impliqués, ainsi que les institutions de l'Union européenne. Les organisations impliquées étaient issues des groupes suivants: agences et organisations de cyber-sécurité, ministères concernés, responsables de services d'e-gouvernement, établissements financiers, fournisseurs d'accès internet (ISP) et opérateurs de services de télécommunications. La

Figure 3 indique la répartition des acteurs.

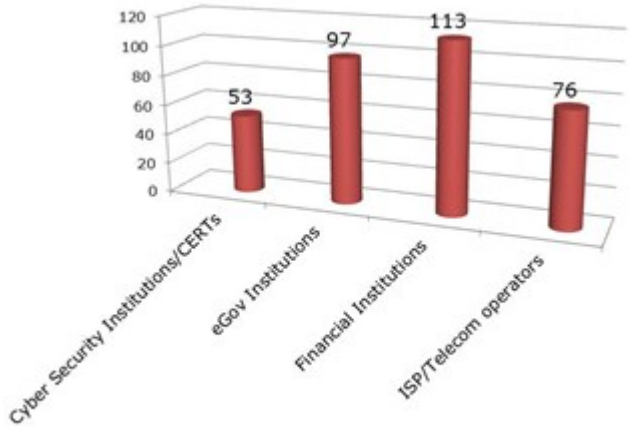


Figure 3: Répartition des organisations ayant participé activement au CE2012

- Institutions de cyber-sécurité/CERT (Computer emergency response team- Équipe d'intervention en cas d'urgence informatique)
- Services d'e-gouvernement
- Établissements financiers

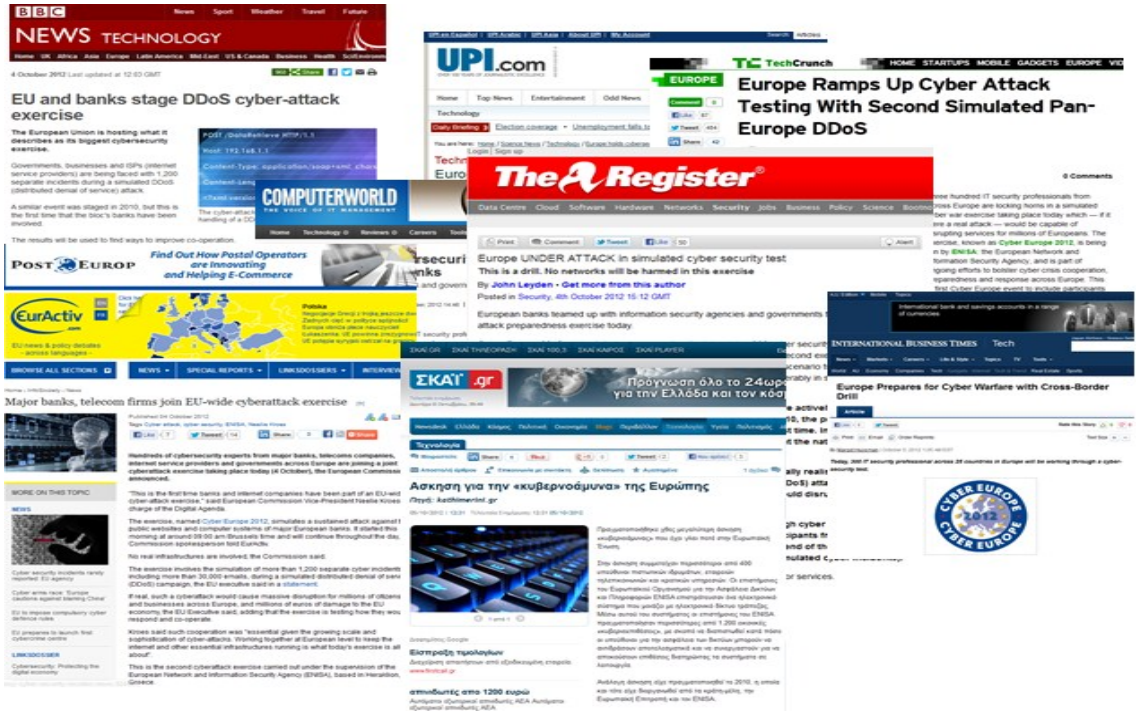
- Fournisseurs d'accès internet/Opérateurs de télécommunications

Couverture médiatique

Cyber Europe 2012 a eu un retentissement considérable dans les médias mondiaux. Plus de 600 articles ont été publiés en 19 langues.

De nombreux articles ont cité la vice-présidente de la Commission européenne responsable de l'Agenda numérique, Neelie Kroes, qui a déclaré que «*Travailler ensemble, au niveau européen, pour maintenir l'internet et les autres infrastructures essentielles en état de fonctionner: voilà le but de l'exercice d'aujourd'hui*.»

En outre, Cyber Europe 2012 a été mentionné dans les médias sociaux dans plus de six langues. La compilation des messages médiatiques contenue dans l'illustration ci-dessous montre certains des articles publiés au sujet de Cyber Europe 2012.



Principales conclusions

Cyber Europe 2012 a conduit à une série de conclusions importantes concernant la coopération nationale, la coopération internationale et les cyber-exercices, qui sont résumées ci-dessous:

La coopération au niveau national

- Les pays participants, prenant très au sérieux les incidents de cyber-sécurité, ont réagi aux défis en renforçant leurs cellules nationales de réponse aux crises et/ou en activant des structures de crise nationales.
- La coopération et les échanges d'informations ont été fréquents au niveau national entre acteurs publics et privés pendant l'exercice.

- Certains pays ont connu des défis en matière de prise de décision dans le cadre de la gestion d'une crise, même si cette question ne faisait pas partie des objectifs de l'exercice (par ex., certaines de ces décisions doivent être prises à des plus niveaux stratégiques pendant une crise).
- Les structures de coopération public–privé diffèrent d'un pays à l'autre. Au niveau national, des procédures publiques et privées parallèles et qui parfois se chevauchent ont créé de temps à autre des problèmes de coopération public–privé au sein des pays.
- L'inclusion d'organisations du secteur privé en tant qu'acteurs au niveau national a permis une amélioration considérable par rapport à l'exercice Cyber Europe précédent.

La coopération au niveau international

- Cyber Europe 2012 s'est avéré être une excellente occasion d'explorer, comprendre et évaluer les mécanismes européens de cyber-coopération existants. L'exercice a renforcé la communauté européenne de gestion des cyber-incidents.
- Tous les pays participants se sont pleinement impliqués dans la phase de coopération internationale de l'exercice. De nombreuses interactions bilatérales et multilatérales ont eu lieu au niveau international au cours de l'exercice.
- Disposer d'une série de procédures opérationnelles et d'outils de communication standardisés a favorisé la bonne connaissance des structures et de la situation pendant la simulation de la cyber-crise.
- Des imperfections ont été repérées dans les procédures opérationnelles, notamment en termes de capacité d'évolution, du fait du grand nombre de pays et d'institutions participants.
- Il s'est avéré qu'une bonne connaissance des procédures et des flux d'informations était cruciale pour la mise en place d'une capacité de réaction rapide et efficace à travers l'ensemble de l'Europe.
- Disposer d'infrastructures techniques et d'outils de pointe appropriés s'est avéré crucial pour garantir l'efficacité de la coopération.
- Cyber Europe 2012 a contribué à établir la confiance entre les pays, ce qui est capital lorsqu'il s'agit de déployer des activités d'atténuation efficaces et rapides en cas de cyber-crise réelle. L'exercice a favorisé la création de nouvelles relations et renforcé les relations existantes.

Cyber-exercices

- La communauté européenne de gestion des cyber-incidents estime que les exercices paneuropéens sont un outil important d'évaluation et d'amélioration des cadres existants de coopération en matière de cyber-crise.
- Cyber Europe 2012 s'est avéré extrêmement utile pour tester les mesures d'urgence et les niveaux de préparation nationaux.
- Les cyber-exercices sont très utiles pour établir la confiance parmi les différentes cyber-communautés.
- La réussite d'un exercice efficient, complexe et à grande échelle nécessite une planification efficace.

Recommandations

Cyber Europe 2012 a permis de formuler les recommandations suivantes:

- Cyber Europe 2012 s'est avéré être un outil précieux d'amélioration de la gestion paneuropéenne des cyber-incidents. Il est donc important de poursuivre les efforts et d'accroître l'ampleur du cyber-exercice européen. Les États membres de l'UE et les pays de l'AELE sont invités à coopérer en faveur de nouveaux cyber-exercices paneuropéens et nationaux afin de renforcer la gestion transnationale des cyber-incidents. Le Guide des bonnes pratiques pour les exercices nationaux[1], élaboré par l'ENISA, apporte un soutien supplémentaire dans ce domaine.
- Les futurs cyber-exercices devraient explorer les dépendances intersectorielles et être davantage axés sur des communautés spécifiques.
- Cyber Europe 2012 a été l'occasion de renforcer la coopération au niveau international et la communauté européenne de gestion des cyber-incidents. Resserrer les liens de la coopération internationale est essentiel si l'on veut faciliter l'échange de bonnes pratiques en matière de cyber-exercices et l'organisation de conférences, et capitaliser l'expérience et l'expertise acquises. Ces efforts contribueront à consolider une communauté capable de gérer les cyber-crises transnationales.
- Les États membres de l'UE et les pays de l'AELE doivent continuer à améliorer l'efficacité, la capacité d'expansion et la connaissance pratique des mécanismes existants, des procédures et des flux d'informations relatifs à la coopération au niveau national et avec d'autres pouvoirs publics en Europe. Les enseignements tirés de Cyber Europe 2012 fournissent un excellent point de départ pour ce faire.
- Tous les acteurs intéressés par le domaine de la coopération internationale en matière de cyber-crise doivent être formés à l'utilisation des procédures afin de pouvoir travailler correctement avec celles-ci.
- L'implication d'organisations du secteur privé en tant qu'acteurs a ajouté de la valeur à cet exercice. Par conséquent, les États membres de l'UE et les pays de l'AELE doivent envisager l'implication du secteur privé dans les futurs exercices.
- La communauté européenne de gestion des cyber-incidents pourrait être renforcée grâce à la contribution d'autres secteurs européens vitaux (par ex.: la santé, les transports) pertinents pour le traitement des crises à grande échelle.

Des informations complémentaires sur la coopération et les exercices de cyber-crise sont disponibles sur le site web de l'ENISA à l'adresse: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation

[1] *http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/exercises (en anglais)*

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu