Press Release

30/10/2014

www.enisa.europa.eu

Le plus grand exercice de cyber sécurité en Europe a lieu aujourd'hui

@Enisa_EU #CyberSecurity #CyberEurope2014

Plus de 200 organisations et 400 professionnels de la cyber-sécurité originaires de 29 pays européens sont en train de tester leur réactivité face aux cyber-attaques lors d'une simulation d'une journée organisée par l'Agence européenne de cyber-sécurité (ENISA). Pour Cyber Europe 2014, des experts des secteurs publics et privés dont des agences de cyber-sécurité, des équipes d'intervention en cas d'urgence informatique, plusieurs ministères, des sociétés de télécommunications, des entreprises du domaine de l'énergie, des institutions financières et des fournisseurs d'accès à internet mettent à l'épreuve leurs procédures et leurs capacités dans le cadre d'une simulation à grande échelle.

#CyberEurope2014 est le plus important et le plus complexe exercice de ce type jamais organisé en Europe. Plus de 2000 cyber incidents différents seront traités, tels que des attaques de déni de service sur les services en ligne, rapports de renseignements et comptes rendus médiatiques des opérations de cyber-attaques, défiguration de sites web (attaques visant à modifier l'aspect d'un site), exfiltration d'informations sensibles, attaques d'infrastructures critiques comme celles des réseaux énergétiques ou de télécommunications – afin de tester la coopération au sein de l'UE et les procédures progressives. Il s'agit d'un exercice distribué impliquant plusieurs centres dans toute l'Europe, coordonnés par un centre principal de contrôle de l'exercice.

D'après la Vice-présidente de la Commission Européenne, @NeelieKroesEU: « la sophistication et le nombre de cyber-attaques augmentent de jour en jour. Elles ne peuvent être contrecarrées si les États travaillent seuls ou en petit groupes. Je suis heureuse que les États membres de l'UE et de l'EFTA collaborent avec les institutions européennes par le biais de l'ENISA. Seul ce genre d'effort commun permettra à l'économie et la société actuelles d'être protégées. »

Le Directeur exécutif de l'ENISA, le Professeur Udo Helmbrecht, ajoute : "Il y a cinq ans aucune procédure n'existait afin de mener une coopération entre les États membres de l'UE lors d'une cyber-crise. Aujourd'hui, nous avons mis en place collectivement les procédures nécessaires pour dissiper une cyber-crise au niveau européen. Le résultat de l'exercice d'aujourd'hui nous dira où nous en sommes et nous permettra d'identifier les prochaines étapes à entreprendre pour continuer à nous améliorer.

Press Release

30/10/2014

www.enisa.europa.eu

L'exercice #CyberEurope2014 testera entre autres les procédures destinées à partager des informations opérationnelles sur les cyber-crises en Europe, à améliorer les capacités nationales de réponse aux cyber-crises, à explorer les effets d'échanges multiples et parallèles entre le privé et le public ainsi qu'au sein du privé au niveau national et international. L'exercice testera également les Procédures opérationnelles permanentes de l'UE (EU-POP), un ensemble de directives pour partager des informations opérationnelles concernant les cyber-crises.

Contexte

Selon le rapport de l'ENISA sur les menaces cybernétiques (2013), les agents menaçants ont amélioré leurs attaques et leurs outils. Il est maintenant clair que la maturité en termes d'activité cybernétique n'est plus un privilège réservé à une poignée de pays. Au contraire, de nombreux pays ont développé des capacités pouvant être utilisées pour infiltrer toutes sortes de cibles, gouvernementales comme privées, pour atteindre leurs objectifs.

En 2013, les attaques visant le web en général exécutées depuis internet ont augmenté de 25% et le nombre de fuites de données était en hausse de 61% comparé à 2012. Chacune des huit fuites de donnés les plus importantes a entrainé la perte de dizaines de millions d'enregistrements de données et 552 millions d'identités ont été exposées. Selon les estimations du secteur, la cybercriminalité et l'espionnage ont représenté entre 300 milliards et 1 billion de dollars de pertes générales en 2013.

L'exercice

Cet exercice simule des crises de grande ampleur touchant des infrastructures d'information critiques. Des experts de l'ENISA vont rédiger un compte rendu présentant leurs principales conclusions une fois l'exercice terminé.

#CyberEurope2014 est un exercice biannuel de cyber-sécurité à grande échelle. Organisé tous les deux ans par l'ENISA, il compte cette année 29 pays européens parmi ses participants (26 membres de l'UE et 3 membres de l'EFTA) ainsi que des institutions européennes. Il se déroule en 3 phases durant l'année : une phase technique impliquant la détection de l'incident, l'enquête, l'atténuation du problème et des échanges d'informations (terminée en avril) ; une phase

opérationnelle/tactique comprenant le déclenchement de l'alerte, l'évaluation de la crise, la coopération, la coordination, l'analyse tactique, le conseil et les échanges d'informations au niveau opérationnel (aujourd'hui) et enfin, début 2015, une phase stratégique qui examinera le processus de décision, l'impact politique et les affaires publiques. Cet exercice n'affectera pas les infrastructures, systèmes et services d'information critiques.

Dans la Stratégie de cybersécurité pour l'UE et le projet de Directive pour un niveau élevé commun de sécurité des réseaux et de l'information, la Commission européenne appelle au développement de plans d'urgence nationaux et d'exercices réguliers testant la réponse à un incident de grande ampleur touchant la sécurité des réseaux et la capacité de reprise après un incident. Le nouveau mandat de l'ENISA met aussi en lumière l'importance des exercices de réduction des risques en termes de cyber sécurité dans le but d'améliorer la confiance dans les services en ligne dans toute l'Europe. Les ébauches de Procédures opérationnelles permanentes de l'UE (EU-SOPs en anglais) ont été testées ces trois dernières années, également durant CE2012.

Liens utiles

La cyber sécurité dans l'Agenda Digital

Les exercices de cyber crise de l'ENISA

Le briefing de l'ENISA sur CE2014

Communiqué de presse CE2014 Exercice de niveau technique : TLEx

Neelie Kroes - Suivey Neelie sur Twitter

Contacts

Email: comm-kroes@ec.europa.eu, c3e@enisa.europa.eu

Tel: +32.229.57361 Twitter: @RyanHeathEU, @enisa_eu