Agir ensemble : l'ENISA publie le compte-rendu d'activité de l'exercice Cyber Europe 2014

L'ENISA publie aujourd'hui dans sa version publique le compte-rendu d'activité de l'exercice pan-Européen de cyber-sécurité Cyber Europe 2014 (CE2014). Le rapport, qui a été validé par les États-membres, donne un panorama détaillé de cet exercice de cyber-sécurité très complexe qui a été mené en 2014.

Le principal objectif de Cyber Europe 2014 était d'apprendre aux États-membres à coopérer dans l'éventualité d'une cyber-crise. L'exercice, qui s'est déroulé sur trois phases, a tout d'abord permis de mesurer l'efficacité des procédures de coopération et de remonter des informations en cas de cyber-incident transfrontalier menaçant la sécurité de services et d'infrastructures stratégiques. Il également permis de tester les capacités nationales et les plans de secours en place avec la collaboration des secteurs public et privé.

L'exercice, mis en place tous les deux ans par l'ENISA, a été organisé conjointement par des représentants des pays participants et a nécessité six (6) réunions de préparation à travers l'Europe. Cet exercice, auquel ont participé plus de **1 500 participants** venus de **29 États-membres de l'UE et de l'AELE**, a couvert **pour la première fois l'intégralité des trois (3) phases** de la procédure de réponse aux cyber-incidents – les phases **technique, opérationnelle** et **stratégique**, conçues pour être déployées successivement selon la gravité de l'incident :

- Phase 1 – niveau technique (28-30 avril 2014, **49 heures**) : détection de l'incident, analyse et limitation des dommages, échanges d'information.

- Phase 2 – niveau opérationnel (30 octobre 2014, **10 heures**) : alerte, coopération, limitation des dommages à court terme, développement d'un aperçu collectif de la situation.

- Phase 3 – niveau stratégique - **testé pour la première fois** (25 février 2015) : prise de décisions à partir d'un aperçu collectif de la situation, débats politiques de haut niveau sur les stratégies à adopter pour limiter les dommages à long terme.

Le rapport montre que notre capacité commune à faire face à des incidents de cyber-sécurité de grande échelle en Europe s'est considérablement améliorée depuis 2010, année du premier exercice Cyber Europe. Le partage en temps réel d'informations entre les pays s'est avéré un outil précieux pour accélérer la prise de décisions. Les **Procédures Opérationnelles Standard de l'UE** (POS-UE) créées en complément de ces activités de coopération apportent aux États-membres des consignes à suivre en cas d'incident de cyber-sécurité de grande échelle. Les POS continueront d'être perfectionnées selon les évolutions du contexte politique autour de la cyber-sécurité en Europe.

Le rapport montre que la coopération est essentielle : elle permet de développer une meilleure compréhension des situations, de renforcer la confiance et de répondre plus rapidement en cas de crise. La **Plateforme de Cyber Exercice** (PCE) développée par l'ENISA pour la préparation, la mise en œuvre et l'évaluation de l'exercice s'est avérée être un outil efficace. L'ENISA poursuit actuellement le développement de la PCE afin d'accueillir de nouveaux cyber-exercices et de tester des scénarios techniques. Quatre-vingt dix huit pour cent (**98%**) des participants à la phase technique ont déclaré qu'ils souhaitaient participer à l'exercice suivant.

Udo Helmbrecht, directeur exécutif de l'ENISA, a déclaré : « Nous avons beaucoup appris grâce à Cyber Europe 2014. Ces leçons ont permis d'importantes avancées dans le domaine de la coopération en cas de cyber-crise : un domaine innovant dans lequel l'UE et l'ENISA jouent un rôle de pointe. Nous souhaitons mettre en place notre plan d'action avec le soutien des États-membres, afin d'être encore mieux préparés en cas de cyber-crise au niveau national et européen. »

Le scénario

Le scénario utilisé pour l'exercice Cyber Europe 2014 utilisait une proposition de règlement de l'UE portant sur les **ressources énergétiques**. Pendant la phase technique de l'exercice, les États-membres et les institutions de l'UE devaient faire face à toutes sortes de **cyber-incidents** : **fuites d'information**, informations diffusées en open source, analyse de **logiciels malveillants**, attaques par **déni de service** et autres **attaques répétées et approfondies**. Puis venait la phase opérationnelle de Cyber Europe 2014, avec une aggravation de la situation conduisant à une série de **cyber-attaques de grande échelle**, portant sur des infrastructures critiques et sur différents services en ligne. Enfin, lors de la phase stratégique de l'exercice, la crise passait au niveau supérieur avec plusieurs infrastructures énergétiques sévèrement endommagées en plein hiver, des attaques contre des technologies critiques et une inquiétude montante dans l'opinion publique.

Pour consulter le rapport complet

Pour voir un aperçu rapide de Cyber Europe, vous pouvez consulter cette video réalisée par l'ENISA:

https://www.enisa.europa.eu/media/news-items/preparing-for-the-unknown-a-peek-into-cyber-europe

Interviews et demandes d'information :

Veuillez contacter **Cyber Crisis Cooperation**: c3@enisa.europa.eu