Agence de l'Union européenne
pour la cybersécurité
Agamemnonos 14,
Chalandri 15231| Attiki| Grèce
Tél.: +30 28 14 40 9711
Adresse électronique:
info@enisa.europa.eu
www.enisa.europa.eu

Cyber Europe 2022 teste la résilience du secteur européen de la santé

L'Agence de l'Union européenne pour la cybersécurité (ENISA) vient d'organiser un exercice de cybersécurité afin de tester la capacité de réaction aux attaques contre les infrastructures et les services de santé de l'UE.

Afin de garantir la confiance des citoyens dans les infrastructures et les services médicaux dont ils disposent, les services de santé devraient fonctionner à tout moment. Si les services et infrastructures de santé en Europe faisaient l'objet d'une cyberattaque majeure, comment réagir et assurer la coordination tant au niveau national qu'au niveau de l'UE pour atténuer les incidents et prévenir les escalades?

C'est à cette question que Cyber Europe 2022 a cherché à répondre à l'aide d'un scénario fictif. La première journée a été marquée par une campagne de désinformation faisant circuler des résultats de laboratoire manipulés et par une cyberattaque ciblant les réseaux hospitaliers européens. Au deuxième jour, le scénario s'est transformé en une crise informatique à l'échelle de l'UE, avec la menace imminente de la divulgation de données médicales à caractère personnel associée à une nouvelle campagne de désinformation visant à discréditer un dispositif médical implantable par le biais d'une revendication de vulnérabilité.

Le directeur exécutif de l'Agence de l'Union européenne pour la cybersécurité, **Juhan Lepassaar**, a déclaré: *«La complexité de nos défis s'élève désormais à la mesure de la complexité de notre monde connecté. C'est pourquoi je crois fermement que nous devons rassembler toute l'intelligence dont nous disposons dans l'UE pour partager notre expertise et nos connaissances. Le renforcement de notre résilience en matière de cybersécurité est la seule voie à suivre si nous voulons protéger nos services et infrastructures de santé et, en fin de compte, pour protéger la santé de tous les citoyens de l'UE.»*

L'exercice paneuropéen organisé par l'ENISA a réuni au total 29 pays de l'Union européenne et de l'Association européenne de libre-échange (AELE), ainsi que les agences et institutions de l'UE, l'ENISA, la CERT-UE de la Commission européenne, Europol et l'Agence européenne des médicaments (EMA). Plus de 800 experts en cybersécurité se sont mobilisés pour contrôler la disponibilité et l'intégrité des systèmes au cours des deux jours de cette dernière édition de Cyber Europe.

Pouvons-nous renforcer la cyber-résilience des soins de santé de l'UE?

Les participants à cet exercice complexe se sont satisfaits de la manière dont les incidents ont été traités et de la réponse apportée aux attaques fictives.

Désormais, l'analyse du processus et des résultats des différents aspects des exercices doit encore être effectuée afin de parvenir à une compréhension réaliste des lacunes ou des faiblesses potentielles qui pourraient nécessiter des mesures d'atténuation. Pour faire face à de telles attaques, différents niveaux de compétences et de processus doivent être engagés, il s'agit d'établir un échange d'informations efficace et coordonné, le partage de connaissances sur des incidents spécifiques et la manière de surveiller une situation sur le point de s'aggraver en cas d'attaque généralisée. Le rôle du réseau des CSIRT au niveau de l'UE et les processus opérationnels standard du groupe CyCLONe doivent également être examinés.

L'analyse approfondie de cet exercise sera publiée dans le rapport de suivi. Les conclusions serviront de base aux futures orientations et aux améliorations supplémentaires à apporter afin de renforcer la résilience du secteur des soins de santé face aux cyberattaques dans l'UE.

Au sujet des exercices Cyber Europe

Les exercices «Cyber Europe» sont des simulations de cyberincidents de grande ampleur qui s'aggravent pour devenir des cybercrises à l'échelle de l'UE. Ces derniers permettent d'analyser les incidents de cybersécurité les plus avancés et de faire face à des situations complexes en matière de gestion de crise et de continuité opérationnelle.

L'ENISA a déjà organisé cinq exercices paneuropéens de cybersécurité en 2010, 2012, 2014, 2016 et 2018. L'événement a généralement lieu tous les deux ans, mais l'édition 2020 a été annulée en raison de la pandémie de COVID-19.

La coopération internationale entre toutes les organisations participantes est inhérente aux règles de l'exercice et la plupart des pays européens y ont pris part. Il s'agit d'une expérience d'apprentissage souple, qui peut être adaptée à un analyste unique mais aussi à une organisation entière, avec des scénarios de participation et de non-participation, et où les participants peuvent adapter l'exercice à leurs besoins.

Autres informations

Cyber Europe 2022

Exercices de cybersécurité – thème de l'ENISA

Cyber Europe 2018 – rapport de suivi

Contacts:

Pour toute question relative à la presse et aux entretiens, veuillez contacter:
press(at)enisa.europa.eu