CyberEurope 2018 – Se préparer à la prochaine crise

L'agence de l'UE pour la cybersécurité, l'ENISA, a organisé un exercice international de cybersécurité

Imaginez ce scénario: Une journée normale à l'aéroport. Soudain, les bornes d'enregistrement automatique connaissent une défaillance du système. Les applications de voyage pour smartphone ne fonctionnent plus. Les préposés aux comptoirs d'enregistrement ne peuvent plus utiliser leur ordinateur. Les voyageurs ne peuvent ni faire enregistrer leurs bagages ni passer les contrôles de sécurité. Les files d'attente s'allongent partout. Tous les vols sont annulés sur les écrans d'affichage. Pour des raisons inconnues, le service de reprise des bagages a cessé de fonctionner et plus de la moitié des vols doivent rester au sol.

On rapporte qu'un groupe radical a perpétré des attaques numériques et hybrides contre les systèmes critiques de l'aéroport pour en prendre le contrôle. Ce groupe a déjà revendiqué l'incident et utilise ses canaux de propagande pour diffuser un appel à l'action et faire du prosélytisme.

Tel est l'intense scénario auquel ont dû faire face plus de 900 spécialistes européens de la cybersécurité dans 30 pays, les 6 et 7 juin 2018, à l'occasion de «CyberEurope 2018» (CE2018), le plus abouti des exercices de cybersécurité réalisés dans l'Union jusqu'à présent.

L'exercice de deux jours était orchestré par l'ENISA depuis son siège à Athènes, en Grèce, tandis que les participants sont soit restés sur leur lieu de travail habituel soit se sont rassemblés au sein de cellules de crise. L'ENISA a supervisé l'exercice par l'intermédiaire de sa plateforme pour les exercices de cybersécurité (Cyber Exercise Platform - ECP), qui a fourni un «univers virtuel» (environnement intégré) pour la simulation du monde, y compris le matériel relatif aux incidents, des sites web d'information virtuels, des réseaux sociaux, des sites web d'entreprises et de blogs sur la sécurité.

Organisé par l'agence de l'UE pour la cybersécurité, l'ENISA, en collaboration avec les agences et autorités chargées de la cybersécurité de l'ensemble de l'Europe, CE2018 visait à permettre à la communauté de la cybersécurité européenne de renforcer davantage ses capacités de détection des menaces à grande échelle et de réaction face à celles-ci, ainsi qu'à mieux comprendre la contagion transfrontière en cas d'incident.

Plus important encore, CE2018 a essentiellement servi à aider les organisations à tester leurs plans internes de continuité des activités et de gestion des crises, y compris la communication des médias en cas de crise, tout en renforçant la coopération entre les entités publiques et privées.

Le scénario comprenait des incidents techniques et non techniques inspirés de la réalité, qui nécessitaient de procéder à une analyse des réseaux et des logiciels malveillants, et de recourir à la criminalistique et à la stéganographie. Les incidents prévus dans le scénario visaient à provoquer une escalade aboutissant à une crise à tous les niveaux possibles: organisationnel, local, national et européen.

La commissaire pour l'économie et la société numériques, Mariya Gabriel, a déclaré: «Les technologies offrent d'innombrables possibilités dans tous les secteurs de notre économie. Mais elles comportent aussi des risques pour nos entreprises et nos citoyens. La Commission européenne et les États membres doivent coopérer et se doter des outils nécessaires pour détecter les cyberattaques et protéger les réseaux et les

systèmes. C'est dans ce contexte que l'exercice «CyberEurope» organisé par l'ENISA a vu le jour il y a huit ans. Il s'est transformé en un vaste exercice de cybersécurité et est devenu un événement phare de l'UE qui rassemble des centaines de spécialistes de la cybersécurité venus de toute l'Europe. Nous devons nous appuyer sur ce succès et je suis convaincue que nous pouvons approfondir encore les mécanismes de coopération de l'UE, en particulier pour faire face aux cyberincidents de grande ampleur.»

M. Udo Helmbrecht, directeur exécutif de l'ENISA, a précisé: «Au cours de la dernière décennie, le secteur de l'aviation a fait un énorme bond dans l'ère des technologies en pleine évolution. Nous bénéficions aujourd'hui des avantages des applications de navigation, de l'enregistrement en ligne et du contrôle automatisé des bagages. Les technologies intelligentes permettent d'économiser du temps et de l'argent, et elles facilitent la vie des voyageurs. Mais à mesure que les technologies évoluent, les cybermenaces font de même. Grâce à des événements tels que «Cyber Europe 2018», notre agence renforce le niveau de cybersécurité dans l'Union. La collaboration des organisations et pays européens, rassemblés en une entité, constitue la riposte moderne aux cybermenaces. Au nom de l'ENISA et de son personnel, je tiens à féliciter toutes les personnes ayant pris part à CyberEurope 2018.»

Finalement, les participants sont parvenus à atténuer les effets des incidents avec diligence et efficacité. Cela montre que le secteur de la cybersécurité en Europe a mûri au cours des dernières années et que les intervenants sont beaucoup mieux préparés. L'ENISA et les participants feront bientôt le bilan de l'exercice et analyseront les mesures prises afin de pointer les domaines susceptibles d'améliorations. L'ENISA publiera un rapport final en temps utile.

Données en bref

Pays participants: 30, Autriche, Belgique, Bulgarie, Croatie, Chypre, République tchèque, Danemark, Estonie, Finlande, France, Allemagne, Grèce, Hongrie, Irlande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Pays-Bas, Norvège, Pologne, Portugal, Roumanie, Slovaquie, Slovénie, Espagne, Suède, Suisse, Royaume-Uni

Organisations participantes: environ 30

Nombre de participants: plus de 900 professionnels de la cybersécurité

Nombre d'éléments déclencheurs: 23 222

Au sujet des exercices de cybersécurité en Europe

Les exercices «CyberEurope» sont des simulations de cyberincidents de grande ampleur qui dégénèrent en cybercrises à l'échelle de l'UE. Ils sont l'occasion d'analyser les incidents affectant les éléments de cybersécurité les plus avancés et de faire face à des situations complexes en matière de gestion de crise et de continuité des activités. L'ENISA a déjà organisé quatre exercices paneuropéens de cybersécurité en 2010, 2012, 2014 et 2016.

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: les participants peuvent adapter l'exercice à leurs besoins, en choisissant de faire intervenir un seul analyste ou toute une organisation, et en retenant ou excluant certains scénarios.