Cyber Europe 2018 – Bereid je voor op de volgende cybercrisis

Het EU-agentschap voor cyberveiligheid ENISA organiseerde een internationale cyberbeveiligingsoefening

Stel: Het is een normale dag op de luchthaven. Plotseling vertonen de geautomatiseerde incheckautomaten systeemstoringen. Reisapps op smartphones werken niet meer. De werknemers aan de check-in-balies kunnen hun computers niet meer bedienen. Reizigers kunnen hun bagage niet inchecken of door de veiligheidscontrole gaan. Overal staan lange rijen. Alle vluchten worden op de schermen in de luchthaven als geannuleerd weergegeven. Om onbekende redenen loopt de bagageband niet meer en moet meer dan de helft van de vluchten aan de grond blijven.

Een radicale groepering heeft naar verluidt de controle van de kritische systemen van de luchthaven door middel van digitale en hybride aanvallen overgenomen. Ze hebben de verantwoordelijkheid voor het incident al opgeëist en gebruiken hun propagandakanalen om een oproep tot actie te verspreiden en meer mensen van hun radicale ideologie te overtuigen.

Dit was het intense scenario waar meer dan 900 Europese specialisten op het gebied van cyberbeveiliging uit 30 landen op 6 en 7 juni 2018 mee te maken hadden tijdens 'Cyber Europe 2018' (CE2018) – tot op heden de breedste cyberbeveiligingsoefening van de EU.

De oefening van twee dagen werd georganiseerd door ENISA in haar hoofdkwartier in Athene, Griekenland, terwijl de deelnemers ofwel op hun gebruikelijke werkplek bleven of samenkwamen in crisiscellen. ENISA controleerde de oefening via haar platform voor oefeningen op cybergebied (CEP), dat zorgde voor een 'virtueel universum' (geïntegreerde omgeving) voor de gesimuleerde wereld, met inbegrip van materiaal over de incidenten, virtuele nieuwswebsites, socialemediakanalen, websites van bedrijven en blogs over beveiliging.

CE2018 werd georganiseerd door het EU-agentschap voor cyberveiligheid ENISA in samenwerking met autoriteiten en agentschappen voor cyberbeveiliging uit heel Europa. De bedoeling ervan was om de Europese cyberbeveiligingsgemeenschap in staat te stellen de capaciteiten op het gebied van het identificeren en aanpakken van grootschalige bedreigingen te versterken en een beter inzicht van grensoverschrijdende incidentbesmetting te geven.

Bovenal was CE2018 met name gericht op het helpen van organisaties bij het testen van hun interne bedrijfscontinuïteit en crisismanagementplannen, waaronder crisiscommunicatie in de media, terwijl het ook de samenwerking tussen particuliere en overheidsinstanties versterkte.

Het scenario bevatte op het echte leven geïnspireerde technische en niet-technische incidenten die netwerk- en malware-analyse, forensisch onderzoek en steganografie (een vorm van cryptografie) vereisten. De incidenten in het scenario zijn ontworpen om te ontaarden in een crisis op alle mogelijke niveaus: organisatorisch, lokaal, nationaal en Europees.

Mariya Gabriel, commissaris voor Digitale Economie en Samenleving: "Technologie biedt talloze kansen in alle sectoren van onze economie. Maar er kleven ook risico's aan voor bedrijven en burgers. De Europese Commissie en de lidstaten moeten de handen ineenslaan en zichzelf voorzien van de nodige instrumenten om cyberaanvallen op te sporen en netwerken en systemen te beschermen. Dit is waarom de 'Cyber

Europe'-oefening door ENISA acht jaar geleden in het leven werd geroepen. Het is uitgegroeid tot een belangrijke cyberbeveiligingsoefening en is een EU-vlaggenschipevenement geworden, dat honderden deskundigen op het gebied van cyberbeveiliging uit heel Europa samenbrengt. We moeten op dit succes voortbouwen en ik ben ervan overtuigd dat we de samenwerkingsmechanismen van de EU verder kunnen ontwikkelen, vooral om op grootschalige cyberincidenten te reageren."

Prof. Dr. Udo Helmbrecht, uitvoerend directeur van ENISA: "In de afgelopen tien jaar heeft de luchtvaartsector een enorme sprong in het evoluerende technologietijdperk gemaakt. Navigatie-apps, online inchecken, en automatische screening van bagage brengen ons grote voordelen. Slimme technologie bespaart tijd, geld, en maakt het leven van de reiziger gemakkelijker. Cyberdreigingen evolueren echter mee met de technologie. Aan de hand van evenementen zoals Cyber Europe 2018 versterkt ons agentschap het niveau van cyberbeveiliging in de EU. Europese landen en organisaties die samenwerken als één geheel, dat is de moderne respons op grenzeloze cyberdreigingen. Namens ENISA en zijn personeel zou ik graag iedereen die betrokken is bij Cyber Europe 2018 bedanken."

Uiteindelijk konden de deelnemers de incidenten tijdig en doeltreffend inperken. Hieruit blijkt dat de Europese cyberbeveiligingssector zich in de laatste jaren ontwikkeld heeft en dat de betrokkenen veel beter voorbereid zijn. ENISA en de deelnemers zullen binnenkort passende maatregelen nemen naar aanleiding van deze oefening en de ondernomen acties analyseren om vast te stellen op welke gebieden nog verbetering mogelijk is. ENISA zal te zijner tijd een eindverslag publiceren.

De feiten op een rijtje

De deelnemende landen: Oostenrijk, België, Bulgarije, Kroatië, Cyprus, Tsjechië, Denemarken, Estland, Finland, Frankrijk, Duitsland, Griekenland, Hongarije, Ierland, Italië, Letland, Litouwen, Luxemburg, Malta, Nederland, Noorwegen, Polen, Portugal, Roemenië, Slowakije , Slovenië, Spanje, Zweden, Zwitserland, Verenigd Koninkrijk

Deelnemende organisaties: ongeveer, 300

Aantal deelnemers: meer dan 900 professionals op het gebied van cyberbeveiliging

Aantal 'injects' (gesimuleerde incidenten): 23 222

Over Cyber Europe-oefeningen

'Cyber Europe'-oefeningen zijn simulaties van grootschalige cyberbeveiligingsincidenten die escaleren tot EU-brede cybercrises. De oefeningen bieden mogelijkheden om geavanceerde cyberincidenten te analyseren, en om met complexe situaties van bedrijfscontinuïteit en crisisbeheer om te gaan. ENISA heeft reeds vier pan-Europese cyberoefeningen georganiseerd, namelijk in 2010, 2012, 2014 en 2016.

Internationale samenwerking tussen alle deelnemende organisaties is inherent aan de gameplay, met de deelname van de meeste Europese landen. Het is een flexibele leerervaring: van een enkele analist tot een hele organisatie, opt-in en opt-out scenario's – de deelnemers kunnen de oefening aan hun behoeften aanpassen.