Agentschap van de Europese
Unie voor cyberbeveiliging
Agamemnonos 14,
Chalandri 15231| Attiki|
Griekenland
Tel. +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

Cyber Europe 2022: Testen van de weerbaarheid van de Europese gezondheidszorgsector

Het Agentschap van de Europese Unie voor Cyberbeveiliging (ENISA) heeft een cyberbeveiligingsoefening georganiseerd om het weerwoord van aanvallen op de infrastructuur in de gezondheidszorg en -diensten in de EU te testen.

Om het vertrouwen van de burgers in de beschikbare medische diensten en infrastructuur te waarborgen, moeten de gezondheidsdiensten te allen tijde functioneren. Als gezondheidsdiensten en diens infrastructuur in Europa het doelwit zouden zijn van een grote cyberaanval, hoe zouden we daar op reageren en hoe zouden we zowel op nationaal als Europees niveau dit coördineren, om de gevolgen van een dergelijk incident het hoofd te bieden en escalatie te voorkomen?

Dit is de vraag die tijdens Cyber Europe 2022 getracht is te beantwoorden aan de hand van een fictief scenario. Dag één stond in het teken van een desinformatiecampagne over gemanipuleerde laboratoriumresultaten en een cyberaanval op Europese ziekenhuisnetwerken. Op dag twee escaleerde dit scenario tot een Europease cybercrisis waarbij openbaarmaking van medische persoonsgegevens dreigde, en werd tevens een nieuwe desinformatie campagne gelanceerd die erop was gericht een implanteerbaar medisch hulpmiddel met beweringen over vermeende risico's in diskrediet te brengen.

Juhan Lepassaar, uitvoerend directeur van het Agentschap van de Europese Unie voor Cyberbeveiliging, verklaarde: *"De complexiteit van onze uitdagingen staan inmiddels in gelijke verhouding tot de complexiteit van onze digitaal verbonden wereld. Daarom is het mijnsinziens dringend noodzakelijk om alle inlichtingen te verzamelen waarover we in de EU beschikken, om zo onze expertise en kennis te bundelen. Alleen door onze weerbaarheid op het gebied van cyberbeveiliging te verhogen kunnen we onze gezondheidsdiensten en -infrastructuur en uiteindelijk de gezondheid van alle EU-burgers beschermen."*

Aan de door ENISA georganiseerde pan-Europese cyberoefening namen in totaal 29 landen uit zowel de Europese Unie als de Europese Vrijhandelsassociatie (EVA) deel, naast de EU-agentschappen en -instellingen, ENISA, de Europese Commissie, CERT-EU, Europol en het Europees Geneesmiddelenbureau (EMA). In de twee dagen van deze editie van Cyber Europe stonden meer dan 800 deskundigen op het gebied van cyberbeveiliging paraat om de beschikbaarheid en integriteit van de systemen te bewaken.

Kunnen we de cyberweerbaarheid van de gezondheidszorg in de EU versterken?

De deelnemers die betrokken waren bij de complexe oefening toonden zich tevreden over de manier waarop de incidenten werden aangepakt en op fictieve aanvallen werd gereageerd.

Nu moet een analyse worden gemaakt van het proces en van de resultaten van de verschillende onderdelen van de oefeningen om een realistisch inzicht te krijgen in eventuele lacunes of zwakke punten die mogelijk passende maatregelen vereisen. Bij het aanpakken van dergelijke aanvallen zijn diverse competenties en processen vereist, waaronder efficiënte en gecoördineerde informatie uitwisseling en het delen van kennis omtrent de specifieke incidenten en over hoe de situatie moet worden gemonitord als escalatie dreigt in het geval van een massale aanval. Daarnaast wordt de rol van het CSIRT-netwerk op EU-niveau en de standaardwerkwijzen (SOP's) van EU-CyCLONe geëvalueerd.

De grondige analyse zal worden gepubliceerd in de vorm van een 'after-action report'. De bevindingen zullen als basis dienen voor toekomstige richtsnoeren en verdere verbeteringen om de gezondheidssector weerbaarder te maken tegen cyberaanvallen in de EU.

Over de Cyber Europe-oefeningen

Cyber Europe-oefeningen zijn simulaties van grootschalige cyberbeveiligingsincidenten die escaleren tot EU-brede cybercrises. De oefeningen bieden de mogelijkheid om geavanceerde cyberincidenten te analyseren en complexe uitdagingen op het gebied van bedrijfscontinuïteit en crisisbeheer het hoofd te bieden.

ENISA heeft vijf eerdere pan-Europese cyberoefeningen georganiseerd in 2010, 2012, 2014, 2016 en 2018. Het evenement vindt gewoonlijk om de twee jaar plaats, maar de editie van 2020 werd geannuleerd vanwege de COVID-19-pandemie.

Internationale samenwerking tussen de deelnemende organisaties is een essentieel onderdeel van de simulatie, waaraan de meeste Europese landen deelnemen. Cyber Europe biedt flexibele leermogelijkheden voor zowel één of meer analisten alswel gvoor de gehele organisatie, met verschillende opt-in- en opt-outscenario's, zodat deelnemers de oefening kunnen aanpassen aan hun behoeften.

Meer informatie:

Cyber Europe 2022

Cyber Exercises – ENISA topic

Cyber Europe 2018 – After Action Report

Contactpersonen:

Voor de beantwoording van persvragen en aanvragen voor interviews kunt u contact met ons opnemen via press(at)enisa.europa.eu