Cyber Europe 2018 – Forbered dig på den næste cyberkrise

EU-agenturet for cybersikkerhed ENISA har afholdt en international øvelse i cybersikkerhed

Forestil dig, at det er en almindelig dag i lufthavnen. Pludselig kommer der en meddelelse frem på selvbetjeningsautomaterne om systemnedbrud. Rejseappsene på mobiltelefoner holder op med at virke. Medarbejderne ved check-in-skrankerne kan ikke få deres computere til at fungere. De rejsende kan hverken tjekke deres bagage ind eller gå gennem sikkerhedskontrollen. Der er endeløse køer overalt. På skærmene i lufthavnen står der, at alle fly er aflyst. Af ukendte årsager fungerer bagageudleveringen ikke længere og mere end halvdelen af flyene må blive på jorden.

En yderliggående gruppe har angiveligt overtaget kontrollen med lufthavnens mest nødvendige systemer gennem digitale og hybride angreb. Gruppen har allerede taget ansvar for hændelsen og benytter deres propagandakanaler til at opfordre til kamp og tiltrække flere til deres radikale ideologi.

Det var dette intensive forløb, som flere end 900 europæiske eksperter i cybersikkerhed fra 30 lande stod over for den 6. og 7. juni 2018 i løbet af "Cyber Europe 2018" (CE 2018), den hidtil mest udførlige cybersikkerhedsøvelse i EU.

Det var ENISA, som afholdt øvelsen over to dage i sit hovedkvarter i Athen i Grækenland, mens deltagerne enten opholdt sig på deres normale arbejdspladser eller mødtes i kriseceller. ENISA styrede øvelsen via sin platform for cyberøvelser (Cyber Exercise Platform, forkortet CEP), som udgjorde kulissen for et "virtuelt univers" (et integreret miljø) for den simulerede verden. I dette univers var der blandt andet materiale om hændelsen, virtuelle nyhedssider, sociale medier, virksomheders hjemmesider og sikkerhedsblogs.

CE2018 blev afholdt af EU's cybersikkerhedsagentur, ENISA, i samarbejde med cybersikkerhedsmyndigheder og -agenturer fra hele Europa. Hensigten med øvelsen var at give det europæiske cybersikkerhedssamfund mulighed for i højere grad at styrke deres evne til at identificere og håndtere væsentlige trusler og desuden give en bedre forståelse af hændelser, der kan krydse grænser.

Det vigtigste omdrejningspunkt for CE2018 var at hjælpe de berørte organisationer med at afprøve deres interne beredskabs- og krisestyringsplaner, herunder krisekommunikation i medierne, og samtidigt styrke samarbejdet mellem offentlige og private enheder.

Scenariet indeholdt tekniske og ikketekniske hændelser fra det virkelige liv, som alle kræver netværks- og malwareanalyse, kriminalteknisk analyse og steganografi. Hændelserne i løbet af øvelsen var udformet således, at de kunne optrappes til en krise på alle tænkelige planer: organisatoriske, lokale, nationale og europæiske.

Mariya Gabriel, kommissær med ansvar for den digitale økonomi og det digitale samfund, udtaler: "Teknologien byder på utallige muligheder i alle sektorer af vores økonomi, men den medfører også nogle risici for vores virksomheder og for vores borgere. Europa-Kommissionen og medlemsstaterne bliver nødt til at arbejde sammen og sørge for, at de har de rette værktøjer til at opdage cyberangreb og beskytte netværk og systemer. Sådan blev ENISA's øvelse "Cyber Europe" til for otte år siden. Den er nu vokset til en større øvelse i cybersikkerhed og er blevet et vigtigt arrangement i EU, hvor flere end hundrede eksperter i cybersikkerhed fra hele Europa samles. Vi bør bygge videre på denne succes, og jeg er sikker på, at vi kan

videreudvikle EU's samarbejdsmekanismer, især med henblik på at håndtere omfattende cybersikkerhedshændelser."

Professor Dr. Udo Helmbrecht, administrerende direktør for ENISA, forklarer: "I løbet af det sidste årti har flybranchen taget et kæmpestort spring ind i teknologiens tidsalder, der er i konstant udvikling. Vi nyder i dag godt af apps til navigation, check-in på nettet og automatiseret screening af bagage. Intelligent teknologi sparer os tid og penge og gør livet lettere for rejsende. I lighed med at teknologien udvikler sig, udvikler cybertruslerne sig også. Ved at afholde arrangementer som Cyber Europe 2018 styrker vores agentur cybersikkerhedsniveauet i EU. Europæiske lande og organisationer, der arbejder sammen som én enhed, er nutidens svar på cybertrusler uden grænser. På vegne af ENISA og vores medarbejdere vil jeg gerne lykønske alle, som deltog i Cyber Europe 2018".

Alt i alt lykkedes det deltagerne at begrænse hændelserne på en rettidig og effektiv måde. Dette viser, at den europæiske cybersikkerhedsbranche er blevet mere moden i de seneste par år, og at aktørerne er meget bedre forberedt. ENISA og deltagerne vil snart følge op på øvelsen og analysere, hvor man skal sætte ind for at finde de områder, som kan forbedres. På et senere tidspunkt vil ENISA offentliggøre en endelig rapport.

Et hurtigt overblik:

Deltagerlande: 30, Belgien, Bulgarien, Cypern, Danmark, Det Forenede Kongerige, Estland, Finland, Frankrig, Grækenland, Irland, Italien, Kroatien, Letland, Litauen, Luxembourg, Malta, Nederlandene, Norge, Østrig Polen, Portugal, Rumænien Schweiz, Slovakiet, Slovenien, Spanien, Sverige, Tjekkiet, Tyskland, Ungarn,

Deltagende organisationer: rundt regnet, 300

Antal deltagere: flere end 900 eksperter i cybersikkerhed

Antal begivenheder i øvelsen, der sætter noget i gang (injects): 23 222

Om Cyber Europe-øvelserne

"Cyber Europe"-øvelserne er simulationer af væsentlige cybersikkerhedshændelser, som optrappes til cyberkriser i hele EU. Øvelserne giver mulighed for at analysere avancerede cybersikkerhedshændelser og forholde sig til vanskelige beredskabs- og krisestyringssituationer. ENISA har allerede arrangeret fire fælleseuropæiske cybersikkerhedsøvelser i 2010, 2012, 2014 og 2016.

Internationalt samarbejde mellem alle de deltagende organisationer er en naturlig del af rollespillet med deltagelse fra de fleste europæiske lande. Spillet giver erfaring med fleksibel indlæring: fra den enkelte analytiker til hele organisationen, tilvalg og fravalg af scenarier og deltagerne kan tilpasse øvelsen til deres behov.