Cyber Europe 2018 – Hur kan vi förbereda oss för nästa cyberkris?

EU:s byrå för cybersäkerhet, Enisa, har anordnat en internationell cybersäkerhetsövning

Föreställ dig följande: Det är en vanlig dag på flygplatsen. Plötsligt indikerar incheckningsautomaterna ett systemfel. Smarttelefonernas reseappar slutar att fungera. De anställda vid incheckningsdiskarna kan inte använda sina datorer. Resenärer kan varken checka in sitt bagage eller passera genom säkerhetskontrollen. Det är enorma köer överallt. Alla flygningar anges som inställda på flygplatsens monitorer. Av okänd anledning har bagagehanteringen slutat fungera och mer än hälften av de plan som skulle lyfta blir kvar på marken.

Enligt uppgift ska en radikal gruppering ha tagit kontroll över flygplatsens kritiska system med hjälp av digitala attacker och hybridattacker. De har redan tagit på sig ansvaret för händelsen och använder sina propagandakanaler för att uppmana till handling och locka fler människor att ansluta sig till deras radikala ideologi.

Detta var det intensiva scenario som över 900 europeiska cybersäkerhetsspecialister från 30 länder ställdes inför den 6 och 7 juni 2018, under ”Cyber Europe 2018 (CE2018) – den mest utvecklade cybersäkerhetsövningen i EU hittills.

Tvådagarsövningen anordnades av Enisa vid dess säte i Aten, Grekland, samtidigt som deltagarna antingen stannade kvar på sin vanliga arbetsplats eller samlades i krisenheter. Enisa övervakade övningen via sin cyberövningsplattform (CEP), som tillhandahåller ett ”virtuellt universum” (integrerad miljö) för den simulerade världen, inbegripet incidentunderlag, virtuella nyhetswebbplatser, sociala medier, företagswebbplatser och säkerhetsbloggar.

CE2018-övningen, som anordnades av EU:s cybersäkerhetsbyrå Enisa i samarbete med myndigheter och byråer från hela Europa, syftade till att göra det möjligt för den europeiska cybersäkerhetsgemenskapen att ytterligare stärka sin kapacitet när det gäller att identifiera och ta itu med storskaliga hot och till att ge en bättre förståelse av gränsöverskridande incidenters spridningseffekter.

Framför allt var CE2018 inriktad på att hjälpa organisationer att testa sin interna driftskontinuitet och sina krishanteringsplaner, inbegripet kriskommunikation via medierna, och samtidigt stärka samarbetet mellan offentliga och privata enheter.

Scenariot omfattade tekniska och icke-tekniska incidenter som krävde analys av nätverk och sabotageprogram, kriminaltekniska åtgärder och steganografi. Händelserna i scenariot var avsedda att eskalera till en kris på alla tänkbara nivåer: på organisatorisk, lokal, nationell och europeisk nivå.

– Tekniken erbjuder mängder av möjligheter i alla sektorer av vår ekonomi. Men den medför också risker för företag och medborgare. Europeiska kommissionen och medlemsstaterna måste arbeta tillsammans och utrusta sig med de verktyg som behövs för att upptäcka cyberattacker och skydda nätverk och system säger Mariya Gabriel, kommissionär med ansvar för den digitala ekonomin och det digitala samhället. Det är skälet till att Enisas ”Cyber Europe”-övning såg dagens ljus för åtta år sedan. Den har utvecklats till en betydande cybersäkerhetsövning och blivit ett av EU:s flaggskeppsevenemang som samlar hundratals cybersäkerhetsspecialister från hela Europa. Vi bör bygga vidare på denna framgång och jag är övertygad

om att vi kan utveckla EU:s samarbetsmekanismer ytterligare, särskilt för att kunna hantera storskaliga cyberincidenter.

– Under de senaste tio åren har flygbranschen tagit ett enormt kliv in i teknikåldern. Vi kan nu dra nytta av navigationsappar, incheckning på nätet och automatiserad bagagekontroll. Smart teknik sparar tid och pengar och gör det lättare att resa, konstaterar Udo Helmbrecht, Enisas verkställande direktör. Men parallellt med tekniken utvecklas även cyberhoten. Genom evenemang som Cyber Europe 2018 bidrar vår byrå till att stärka cybersäkerhetsnivån i EU. Europeiska länder och organisationer som arbetar tillsammans som en enhet är det moderna svaret på gränsöverskridande cyberhot. På Enisas och dess personals vägnar vill jag gratulera alla inblandade i Cyber Europe 2018.

I slutändan klarade deltagarna av att hantera incidenterna på ett snabbt och effektivt sätt. Detta visar att den europeiska cybersäkerhetssektorn har mognat under de senaste åren och att de berörda aktörerna är mycket bättre förberedda. Enisa och deltagarna kommer inom kort att följa upp och analysera de åtgärder som vidtagits för att identifiera områden där förbättringar kan göras. En slutrapport kommer så småningom att offentliggöras.

Fakta i korthet

Deltagande länder: 30, Österrike, Belgien, Bulgarien, Kroatien, Cypern, Tjeckien, Danmark, Estland, Finland, Frankrike, Tyskland, Grekland, Ungern, Irland, Italien, Lettland, Litauen, Luxemburg, Malta, Nederländerna, Norge, Polen, Portugal, Rumänien, Slovakien, Slovenien, Spanien, Sverige, Schweiz, Storbritannien

Deltagande organisationer: 30

Antal deltagare: över 900 yrkesverksamma på cybersäkerhetsområdet

Antal angrepp (*injects*): 23 222

Om Cyber Europe-övningar

”Cyber Europe” är simuleringar av storskaliga cybersäkerhetsincidenter som utvecklas till EU-övergripande cyberkriser. Övningarna erbjuder möjligheter att analysera avancerade cybersäkerhetsincidenter, och att hantera komplexa driftskontinuitets- och krishanteringssituationer. Enisa har redan anordnat fyra EU-omfattande cyberövningar under 2010, 2012, 2014 respektive 2016.

Internationellt samarbete mellan samtliga deltagande organisationer är inbyggt i spelet, där flertalet europeiska länder deltar. Det är en övning i flexibelt lärande: genom deltagande med en enskild analytiker eller en hel organisation, och med opt-in och opt-out-scenarier, kan deltagarna anpassa övningen till sina behov.