

## Cyber Europe 2018 – Fiți pregătiți pentru următoarea criză informatică

### Agenția UE pentru Securitate Cibernetică – ENISA – a organizat un exercițiu de securitate cibernetică la nivel internațional

Să ne imaginăm următoarea situație: E o zi normală la aeroport. Dintr-o dată, toate mașinile automate de înregistrare a pasagerilor și a bagajelor afișează un mesaj de defecțiune a sistemului. Aplicațiile de călătorie de pe telefoanele inteligente nu mai funcționează. Agenții de la ghișeele de înregistrare nu își pot utiliza calculatoarele. Călătorii nu își pot înregistra bagajele și nici nu pot trece prin controalele de securitate. Se formează cozi de așteptare peste tot. Pe monitoarele aeroportului, toate zborurile sunt afișate ca fiind anulate. Din motive necunoscute, serviciul de recuperare a bagajelor nu mai funcționează și mai mult de jumătate din curse trebuie să rămână la sol.

Se raportează că un grup radical a preluat controlul asupra sistemelor critice ale aeroportului prin intermediul unor atacuri digitale și hibride. Acesta a revendicat deja atacul și își utilizează canalele de propagandă pentru a difuza un apel la acțiune și a determina mai multe persoane să adopte ideologii radicale.

Acesta a fost scenariul intens cu care s-au confruntat peste 900 specialiști europeni în materie de securitate cibernetică din 30 de țări la 6 și 7 iunie 2018, în timpul exercițiului „Cyber Europe 2018” (CE2018) — cel mai elaborat exercițiu de securitate cibernetică din UE până în prezent.

Exercițiul, care a durat două zile, a fost organizat de ENISA la sediul său de la Atena, Grecia, în timp ce participanții fie au rămas la locul lor obișnuit de muncă, fie s-au reunit în celule de criză. ENISA a controlat exercițiul prin intermediul platformei sale de exerciții cibernetică, care a pus la dispoziție un „univers virtual” (mediu integrat) pentru simularea respectivei dimensiuni, inclusiv materialul legat de incidente, site-uri web de știri virtuale, platforme de comunicare socială, site-uri web ale întreprinderilor și bloguri de securitate.

Organizat de către Agenția UE pentru Securitate Cibernetică ENISA în colaborare cu autoritățile și agențiile de securitate cibernetică din întreaga Europă, exercițiul CE2018 urmărea să permită comunității europene a securității cibernetică să își consolideze și mai mult capacitățile de identificare și combatere a amenințărilor la scară largă, precum și să asigure o mai bună înțelegere a contagiunii transfrontaliere în caz de incidente.

Și mai important, obiectivul central al CE2018 a fost acela de a sprijini organizațiile să își testeze planurile interne de continuitate a activității și de gestionare a crizelor, inclusiv comunicarea mass-media în situații de criză, consolidând în același timp cooperarea între entitățile publice și cele private.

Scenariul a cuprins incidente tehnice și de alt tip inspirate din viața de zi cu zi, care necesitau realizarea unor analize ale rețelelor și ale programelor malware, precum și recurgerea la criminalistică și steganografie. Incidentele din scenariu au fost concepute astfel încât să conducă la o situație de criză la toate nivelurile posibile: organizațional, local, național și european.

Mariya Gabriel, comisarul pentru economie digitală și societate digitală, a precizat: „Tehnologia oferă nenumărate oportunități în toate sectoarele economiei noastre, dar presupune și riscuri pentru întreprinderile și cetățenii noștri. Comisia Europeană și statele membre trebuie să conlucreze și să se

doteze cu instrumentele necesare pentru a detecta atacurile cibernetice și a proteja rețelele și sistemele. Acesta este modul în care s-a născut exercițiul „Cyber Europe” al ENISA, în urmă cu opt ani. El s-a transformat cu timpul într-un exercițiu de securitate cibernetică major și a devenit un eveniment emblematic al UE, care reunește sute de specialiști în materie de securitate cibernetică din întreaga Europă. Ar trebui să valorificăm acest succes și am convingerea că putem dezvolta în continuare mecanismele de cooperare ale UE, în special pentru a răspunde incidentelor informatice la scară largă.”

Prof. Dr. Udo Helmbrecht, directorul executiv al ENISA, a explicat: „În ultimul deceniu, sectorul aviației a făcut un salt uriaș către era în continuă schimbare a tehnologiei. Suntem acum în măsură să ne bucurăm de beneficiile aplicațiilor de navigație, ale înregistrărilor online și ale controlului automat al bagajelor. Tehnologiile inteligente contribuie la realizarea de economii de timp și de bani și facilitează viața călătorilor. Cu toate acestea, pe măsură ce tehnologia evoluează, evoluează și amenințările cibernetice. Prin intermediul unor evenimente precum Cyber Europe 2018, agenția noastră consolidează nivelul securității cibernetice din UE. Țările și organizațiile europene care lucrează împreună ca o singură entitate constituie răspunsul modern la amenințările informatice fără frontiere. În numele ENISA și a personalului acesteia, aș dori să îi felicit pe toți cei implicați în Cyber Europe 2018.”

La final, participanții au fost în măsură să atenueze incidentele în timp util și în mod eficace. Acest lucru demonstrează că sectorul european al securității cibernetice a evoluat în ultimii ani și că actorii implicați sunt mult mai bine pregătiți. ENISA și participanții vor efectua în curând o evaluare a exercițiului și vor analiza acțiunile întreprinse pentru a identifica domeniile care ar putea fi îmbunătățite. ENISA va publica un raport final în timp util.

### **Date pe scurt**

Țările participante: 30: Austria, Belgia, Bulgaria, Croația, Cipru, Republica Cehă, Danemarca, Estonia, Finlanda, Franța, Germania, Grecia, Ungaria, Irlanda, Italia, Letonia, Lituania, Luxemburg, Malta, Țările de Jos, Norvegia, Polonia, Portugalia, România, Slovacia, Slovenia, Spania, Suedia, Elveția, Regatul Unit

Organizațiile participante 300

Numărul de participanți: peste 900 specialiști în materie de securitate cibernetică

Numărul de evenimente declanșatoare: 23 222

### **Informații despre exercițiile Cyber Europe**

Exercițiile „Cyber Europe” sunt simulări ale unor incidente de securitate cibernetică la scară largă care se transformă în crize cibernetice la nivelul întregii UE. Exercițiile oferă ocazia de a analiza incidente grave de securitate cibernetică și de a rezolva situații complexe de continuitate a activității și de gestionare a crizelor. ENISA a organizat deja patru exerciții cibernetice paneuropene – în 2010, 2012, 2014 și 2016.

Cooperarea internațională între toate organizațiile participante este inerentă exercițiului, majoritatea țărilor europene participând la acesta. Exercițiul este o experiență de învățare flexibilă: participanții își pot personaliza exercițiul în funcție de nevoile lor, fiind posibilă includerea sau excluderea anumitor scenarii, precum și participarea unui singur analist sau a unei întregi organizații, cu toate opțiunile intermediare.

