Európai Uniós
Kiberbiztonsági Ügynökség
Agamemnonos 14,
Chalandri 15231| Attiki|
Görögország
Tel.: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

Cyber Europe 2022: Az európai egészségügyi ágazat ellenálló képességének tesztelése

Az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) kiberbiztonsági gyakorlatot szervezett az uniós egészségügyi infrastruktúrák és szolgáltatások elleni támadásokra adott válaszok tesztelésére.

Annak érdekében, hogy a polgárok megbízzanak a rendelkezésükre álló egészségügyi szolgáltatásokban és infrastruktúrában, az egészségügyi szolgáltatásoknak minden körülmények között működőképesnek kell lenniük. Ha az Európai Unióban az egészségügyi szolgáltatásokat és infrastruktúrákat jelentős kibertámadások érnék, hogyan történne a reagálás és a koordináció mind nemzeti, mind uniós szinten az incidensek enyhítése és az eszkaláció megelőzése érdekében?

Ez az a kérdés, amelyre a Cyber Europe 2022 egy fiktív forgatókönyv alapján kereste a választ. Az első napon egy manipulált laboratóriumi eredményekből álló dezinformációs kampány és az európai kórházi hálózatok elleni kibertámadás szimulációja volt napirenden. A második napon a forgatókönyv alapján a probléma az egész EU-ra kiterjedő kiberválsággá eszkalálódott, közvetlen fenyegetést jelentve a személyes egészségügyi adatok napvilágra kerülésével, valamint egy másik kampány szimulációjára is sor került, amelynek célja egy beültethető orvostechnikai eszköz hiteltelenné tétele volt egy, az eszközt érintő sérülékenység felhasználásával.

Juhan Lepassaar, az Európai Uniós Kiberbiztonsági Ügynökség ügyvezető igazgatója így nyilatkozott: *„Az előttünk álló kihívások összetettsége mára elérte az összekapcsolt világunk összetettségét. Ezért szilárd meggyőződésem, hogy össze kell gyűjtenünk minden, az EU-ban rendelkezésre álló kiberfenyegetettség-információt, hogy megoszthassuk szakértelmünket és tudásunkat. A Kiberbiztonsági ellenálló-képesség megerősítése az egyetlen előrevezető*

megoldás, ha meg akarjuk védeni egészségügyi szolgáltatásainkat és infrastruktúráinkat, és végső soron valamennyi uniós polgár egészségét."

Az ENISA által szervezett páneurópai gyakorlat az Európai Unió és az Európai Szabadkereskedelmi Társulás (EFTA) 29 országát, valamint az uniós ügynökségeket és intézményeket, az ENISA-t, az Európai Bizottság CERT-EU-csoportot (az európai intézmények, szervek és hivatalok hálózatbiztonsági vészhelyzeteket elhárító csoportja), az Europolt és az Európai Gyógyszerügynökséget (EMA) fogta össze. Az idei Cyber Europe két napja során több mint 800 kiberbiztonsági szakértő vállalt szerepet a rendszerek elérhetőségének és integritásának nyomon követésében.

Megerősíthetjük-e az európai uniós egészségügyi ellátás kiber ellenálló-képességét?

Az összetett gyakorlat résztvevői elégedettek voltak az incidensek kezelésének módjával és a fiktív támadásokra adott válaszokkal.

Most a folyamat és a gyakorlatok különböző aspektusai eredményeinek elemzését kell elvégezni annak érdekében, hogy reális képet kapjunk azokról a potenciális hiányosságokról vagy gyengeségekről, amelyeknél hatásenyhítő intézkedések szükségesek. Az ilyen támadások kezeléséhez különféle szintű kompetenciákra és eljárásokra van szükség, amelyek magukban foglalják a hatékony és összehangolt információcserét, a konkrét incidensekkel kapcsolatos ismeretek megosztását, valamint azt, hogy miként lehet nyomon követni egy olyan helyzetet, amely általánossá vált támadás esetén eszkalálódik. Meg kell vizsgálni az európai uniós szintű CSIRT-hálózat szerepét és a CyCLONe csoport standard működési folyamatait (SOP) is.

A mélyrehatóbb elemzést az úgynevezett after-action jelentésben teszik közzé. A megállapítások alapul szolgálnak majd az egészségügyi ágazat kibertámadásokkal szembeni ellenálló képességének megerősítését célzó jövőbeli iránymutatásokhoz és további fejlesztésekhez az EU-ban.

A Cyber Europe gyakorlatokról

A „Cyber Europe" gyakorlatok során olyan nagyméretű kiberbiztonsági események szimulálására kerül sor, amelyek uniós szintű kiberválsággá növik ki magukat. A gyakorlatok lehetőséget nyújtanak a résztvevőknek, hogy összetett kiberbiztonsági eseményeket vizsgáljanak meg, és komplex üzletmenet-folytonossági és válságkezelési helyzetekre készüljenek fel.

Az ENISA 2010-ben, 2012-ben, 2014-ben, 2016-ban és 2018-ban már szervezett egy-egy páneurópai kibergyakorlatot. Az eseményre általában kétévente kerül sor, de a 2020. évi rendezvényt a Covid19-világjárvány miatt törölték.

A gyakorlatok – amelyekben a legtöbb európai ország részt vesz – nem valósulhatnának meg a részt vevő szervezetek nemzetközi együttműködése nélkül. A gyakorlatok rugalmas tanulási tapasztalatot nyújtanak: egyetlen elemzőtől a teljes szervezetig, részvételi és kívülmaradási forgatókönyvekkel, emellett a résztvevők a gyakorlatot saját igényeik alapján is alakíthatják.

További információk:

Cyber Europe 2022

Kibergyakorlatok – ENISA témakör

Cyber Europe 2018 – Fellépést követő jelentés

Kapcsolat:

A sajtóval és az interjúkkal kapcsolatos kérdések témájában kérjük, hogy a press(at)enisa.europa.eu e-mail-címen keresztül forduljon hozzánk.