Cyber Europe 2018 – Felkészülés egy lehetséges kiberbiztonsági válsághelyzetre

Az EU kiberbiztonsági ügynöksége (ENISA) nemzetközi kiberbiztonsági gyakorlatot tartott

Képzeljünk el egy átlagos napot a repülőtéren. Majd képzeljük el azt is, hogy hirtelen az önkiszolgáló utasfelvételi automaták rendszerhibát jeleznek. Az utazási appok leállnak a mobilkészülékeken. A check-in pult munkatársai nem tudják használni számítógépeiket. Az utasok nem tudják föladni poggyászaikat, és nem tudnak átmenni a biztonsági ellenőrzésen. Mindenhol sorok kígyóznak. A repülőtéri monitorok szerint az összes járatot törölték. A csomagkiadás ismeretlen okokból leáll; a repülőgépek több mint a fele nem tud felszállni.

Jelentések szerint egy radikális csoport digitális és hibrid támadással átvette az irányítást a repülőtér kritikus rendszerei felett. A támadást a csoport már magára is vállalta. Propagandacsatornáikon keresztül cselekvésre ösztönzik híveiket és minél több további embert kívánnak megnyerni radikális eszméiknek.

Ez volt a forgatókönyve a 2018. június 6-án és 7-én megrendezett „Cyber Europe 2018 (CE2018)" elnevezésű kiberbiztonsági gyakorlatnak, amelyen 30 ország 900 európai kiberbiztonsági szakértője vett részt.

Az eddigi legátfogóbb, kétnapos kiberbiztonsági gyakorlatot az ENISA görögországi székhelyéről, Athénből irányította. A részt vevők egy része saját irodájában, míg más része válságstábba tömörülve vett részt az eseményekben. Az ENISA egy ún. kibergyakorlati platformon keresztül felügyelte a gyakorlatot; ebben a virtuális térben hozták létre a szimulált világ kellékeit, pl. a biztonsági eseménnyel kapcsolatos anyagokat, a virtuális hírportálokat, a közösségi médiacsatornákat, vállalati webhelyeket és biztonságról szóló blogokat.

A gyakorlatot az uniós kiberbiztonsági ügynökség (ENISA) más európai kiberbiztonsági ügynökségekkel és szervekkel együttműködve szervezte. Céljuk egyrészt az volt, hogy az európai kiberbiztonsági közösség növelje kapacitását a kiterjedt fenyegetések beazonosítására és kezelésére, másrészt hogy jobban megértse a biztonsági események más tagállamokba való továbbgyűrűzésének folyamatát.

A CE2018 kiemelt hangsúlyt fektetett arra, hogy segítsen a különböző szervezeteknek tesztelni belső üzletmenet-folytonosságukat és saját válságkezelési terveiket (pl. a válsághelyzeti tömegtájékoztatást), és hogy megerősítse a közszféra és a magánszektor közötti együttműködést.

A forgatókönyv a valós életen alapuló technikai és nem technikai eseményekre épült, amelyek hálózat- és malware-elemzést, kriminalisztikai és szteganográfiai eszközök használatát tették szükségessé. A forgatókönyv eseményei a terveknek megfelelően válsághelyzetbe torkollottak, amely az összes lehetséges szinten (szervezeti, helyi, tagállami és európai szinten) megnyilvánult.

Marija Gabriel, a digitális gazdaságért és társadalomért felelős biztos így fogalmazott: „A technológia számtalan lehetőséget biztosít a gazdaság valamennyi ágazatában. Ám a vállalkozásokra és a lakosságra nézve veszélyt is hordoz magában. Az Európai Bizottságnak és a tagállamoknak közös erővel fel kell vértezniük magukat a védelemhez szükséges eszközökkel, hogy felfedjék a kibertámadásokat és meg tudják védeni hálózataikat és rendszereiket. E gondolattól vezérelve született meg az ENISA első „Cyber

Europe” gyakorlata nyolc évvel ezelőtt. A kezdeményezést az évek során további gyakorlatok követték, melyek ma már jelentős uniós kiberbiztonsági eseményeknek számítanak. Egy-egy gyakorlaton európai kiberbiztonsági szakemberek százai vesznek részt. Építenünk kell erre a sikerre. Biztos vagyok benne, hogy tovább fogjuk tudni fejleszteni az uniós együttműködési mechanizmusokat, különösen amelyek a nagy hatókörű kiberbiztonsági eseményekre való reagálást célozzák.

Az ENISA ügyvezető igazgatója, Udo Helmbrecht elmondta: „Az elmúlt évtizedben a légiközlekedési ágazat hatalmas technológiai fejlődésen ment keresztül. Ma már olyan eszközök állnak a rendelkezésünkre, mint a navigációs alkalmazások, az online utasfelvétel és az automatizált poggyászátvizsgálás. Az intelligens technológiákkal az utasok időt és pénzt takarítanak meg, az életük pedig kényelmesebbé vált. Ugyanakkor nem csak a technológia fejlődik, a kiberveszélyek is fokozódnak. A „Cyber Europe 2018” gyakorlattal és a hasonló eseményekkel ügynökségünk javítja a kiberbiztonság szintjét az EU-ban. Az európai országok és szervezetek egyként való fellépése a korszerű válasz a határokon átívelő kiberveszélyekre. Az ENISA és munkatársai nevében meg szeretném köszönni mindenkinek a munkáját, aki részt vett a „Cyber Europe 2018” gyakorlatban.”

A résztvevők időben és hatékonyan tudták kezelni az eseményeket. Ez azt illusztrálja, hogy az európai kiberbiztonsági ágazat az elmúlt pár évben sokat fejlődött, és hogy az ágazat szereplői ma már sokkal jobban fel vannak készülve egy esetleges támadásra. Az ENISA és a résztvevők hamarosan megkezdik a gyakorlat kiértékelését és az intézkedések vizsgálatát; céljuk, hogy beazonosítsák a javításra szoruló területeket. Az ENISA annak rendje és módja szerint közzé fogja tenni záró jelentését.

Tények dióhéjban

Részt vevő országok: (30) Ausztria, Belgium, Bulgária, Horvátország, Ciprus, a Cseh Köztársaság, Dánia, Észtország, Finnország, Franciaország, Németország, Görögország, Magyarország, Írország, Olaszország, Lettország, Litvánia, Luxemburg, Málta, Hollandia, Norvégia, Lengyelország, Portugália, Románia, Szlovákia, Szlovénia, Spanyolország, Svédország, Svájc, Egyesült Királyság.

Részt vevő szervezetek: 300

Résztvevők száma: több mint 900 kiberbiztonsági szakember

Eseményindító triggerek száma: 23 222

A „Cyber Europe” gyakorlatokról

A „Cyber Europe” gyakorlatok során olyan nagy hatókörű kiberbiztonsági események szimulálására kerül sor, amelyek uniós szintű kiberválsággá növik ki magukat. A gyakorlatok lehetőséget nyújtanak a résztvevőknek, hogy súlyos kiberbiztonsági eseményeket vizsgáljanak meg, és összetett üzletmenet-folytonossági és válságkezelési helyzetekre készüljenek fel. Az ENISA eddig négy páneurópai kibergyakorlatot szervezett (2010-ben, 2012-ben, 2014-ben és 2016-ban).

A gyakorlatok – amelyekben a legtöbb európai ország részt vesz – nem valósulhatnának meg a részt vevő szervezetek nemzetközi együttműködése nélkül. Rugalmas tanulási folyamatról van szó, amelyet a résztvevők saját igényeikhez igazíthatnak: eldönthetik, hogy egyetlen elemzőt vagy egy egész szervezetet vonnak be a feladatba, és hogy a forgatókönyv mely elemeit tartják meg, illetve vetik el.