Cvičení Cyber Europe 2018 – Příprava na příští kybernetickou krizi

Agentura EU pro kybernetickou bezpečnost ENISA uspořádala mezinárodní cvičení

Na letišti probíhá běžný každodenní provoz. Najednou se na monitorech automatizovaných odbavovacích kiosků objeví zpráva o selhání systému. Aplikace v chytrých telefonech přestanou fungovat. Zaměstnanci na odbavovacích přepážkách ztratili přístup do počítače. Cestující nemohou odbavit svá zavazadla ani projít bezpečnostní kontrolou. Všude se začínají tvořit dlouhé fronty. Na monitorech jsou všechny lety zobrazeny jako zrušené. Z neznámých důvodů přestal fungovat výdej zavazadel a více než polovina letadel nemůže vzlétnout.

Prostřednictvím digitálních a hybridních útoků převzala údajně kontrolu nad kritickými systémy letiště radikální skupina, která se již k útoku přihlásila. Šíří také svou propagandu, vyzývá k akci a snaží se skrze svou radikální ideologii nalákat další adepty.

S tímto fiktivním útokem se během cvičení Cyber Europe 2018 (CE2018), které se konalo ve dnech 6. a 7. června, muselo vypořádat více než 900 evropských odborníků na kybernetickou bezpečnost z 30 zemí. Jednalo se o doposud nejkomplexnější celoevropské cvičení v oblasti kybernetické bezpečnosti.

Dvoudenní cvičení organizovala agentura ENISA ve svém sídle v Aténách. Jeho účastníci buď zůstali na svém pracovišti, nebo se shromáždili v tzv. krizových buňkách. Agentura celé cvičení řídila prostřednictvím své platformy pro kybernetická cvičení (CEP), která nabízí virtuální integrované prostředí včetně materiálu o incidentech, virtuálních zpravodajských internetových stránek, sociálních médií, firemních internetových stránek a bezpečnostních blogů.

Účelem cvičení CE2018, které uspořádala agentura ENISA ve spolupráci s příslušnými orgány a agenturami z celé Evropy, bylo posílit schopnosti těchto orgánů a agentur při odhalování a řešení rozsáhlých hrozeb a zúčastněným umožnit lépe pochopit způsob přeshraničního šíření incidentů.

Cvičení se však zejména zaměřilo na to, aby pomohlo organizacím otestovat interní postupy k zajištění kontinuity provozu a plány krizového řízení, včetně mediální komunikace v případě krize, a zároveň posílit spolupráci mezi veřejnými a soukromými subjekty.

Scénář fiktivního útoku obsahoval incidenty technické i netechnické povahy inspirované reálnými událostmi, které vyžadovaly analýzu sítě a malwaru, forenzní analýzu a použití steganografie. Incidenty byly koncipovány tak, aby se vystupňovaly do podoby krize na všech možných úrovních — organizační, místní, celostátní i evropské.

Marija Gabrielová, komisařka pro digitální ekonomiku a společnost, zdůraznila: „Technologie nabízejí nesčetné příležitosti ve všech odvětvích ekonomiky. Mohou však pro naše podniky a občany představovat i riziko. Evropská komise a členské státy proto musí spolupracovat a vybavit se nezbytnými nástroji k odhalování kybernetických útoků a na ochranu sítí a systémů. Tak se před osmi lety zrodilo cvičení Cyber Europe, které se postupně rozrostlo a stalo se prestižní akcí, jež se účastní stovky odborníků z celé Evropy. Měli bychom proto na tento úspěch navázat. Jsem přesvědčena, že mechanismy spolupráce v rámci EU můžeme i nadále rozvíjet, zejména abychom byli schopni reagovat na kybernetické incidenty velkého rozsahu.“

Prof. Dr. Udo Helmbrecht, výkonný ředitel agentury ENISA, doplnil: „Za posledních deset let učinilo odvětví letecké dopravy obrovský skok a posunulo se do věku neustále se vyvíjejících technologií. Můžeme nyní využívat například výhod navigačních aplikací, online odbavování a automatizované kontroly zavazadel. Inteligentní technologie šetří čas a peníze a usnadňují cestujícím život. Ale stejně rychle, jako se vyvíjejí technologie, se vyvíjejí i kybernetické hrozby. Díky akcím, jako je Cyber Europe, zvyšuje naše agentura úroveň kybernetické bezpečnosti v EU. Spolupráce mezi evropskými zeměmi a organizacemi představuje moderní reakci na kybernetické hrozby, před kterými nás hranice států neochrání. Jménem agentury ENISA a jejích zaměstnanců bych chtěl všem, kdo se na cvičení Cyber Europe 2018 podíleli, poblahopřát.“

Účastníci dokázali odvrátit všechny hrozby včas a efektivně. To dokazuje, že evropského odvětví kybernetické bezpečnosti v posledních několika letech vyspělo a jednotlivé subjekty jsou mnohem lépe připraveny. Zástupci agentury ENISA a účastníci cvičení se již brzy sejdou, aby zanalyzovali přijatá opatření a identifikovali oblasti, které by se daly dále vylepšit. Agentura poté zveřejní závěrečnou zprávu.

Fakta a čísla

Zúčastněné země: 30; Rakousko, Belgie, Bulharsko, Chorvatsko, Kypr, Česká republika, Dánsko, Estonsko, Finsko, Francie, Německo, Řecko, Maďarsko, Irsko, Itálie, Lotyšsko, Litva, Lucembursko, Malta, Nizozemsko, Norsko, Polsko, Portugalsko, Rumunsko, Slovensko, Slovinsko, Španělsko, Švédsko, Švýcarsko a Spojené království

Zúčastněné organizace: 300

Počet účastníků: více než 900 odborníků na kybernetickou bezpečnost

Počet komponentů fiktivního scénáře: 23 222

Cvičení Cyber Europe

Jedná se o simulaci závažných incidentů v oblasti kybernetické bezpečnosti a modelování krizové situace v celé EU. Cvičení umožňují tyto incidenty analyzovat a optimalizovat postupy k zajištění kontinuity provozu a řešení krizových situací. Doposud proběhla čtyři celoevropská kybernetická cvičení, a sice v letech 2010, 2012, 2014 a 2016.

Cvičení se účastní většina evropských zemí a mezinárodní spolupráce všech zúčastněných organizací je jejich neodmyslitelnou součástí. Celý proces, během kterého účastníci získávají praktické poznatky, je velmi flexibilní. Za daný subjekt se může zúčastnit jeden analytik či celá organizace a účastníci si mohou vybrat scénáře, do kterých se chtějí zapojit.