Cyber Europe 2018 — Подготовка за следващата киберкриза

Агенцията на ЕС ENISA организира международно учение по киберсигурност

Представете си: обикновен ден на летището. Внезапно на машините за автоматична регистрация се показва съобщение за срив на системата. Приложенията за пътуване на смартфоните не работят. Служителите на гишетата за регистрация на пътниците не могат да изпълняват задачите си на своите компютри. Пътниците не могат да регистрират багажа си, нито пък да преминат през проверката за сигурност. Навсякъде се оформят огромни опашки. На мониторите на летището всички полети са обявени за анулирани. По неизвестни причини обработката на багажи е преустановена, а повече от половината полети не могат да бъдат осъществени.

Според съобщения радикална групировка е установила контрол над критичните системи на летището чрез компютърни и хибридни атаки. Тя вече е поела отговорност за инцидента и използва пропагандните си канали, за да разпространи призив за действие и да привлече повече хора да приемат нейната радикална идеология.

Това бе динамичният сценарий, пред който бяха изправени 900 европейски специалисти в областта на киберсигурността от 30 страни на 6 и 7 юни 2018 г. по време на Cyber Europe 2018 (CE2018) — най-сложното до момента учение в областта на киберсигурността в ЕС.

Двудневното учение бе ръководено от централата на ENISA в Атина (Гърция), а участниците се намираха на своите работни места или бяха събрани в кризисни центрове. ENISA контролираше учението чрез платформата за кибернетични учения (CEP), която осигури виртуално пространство (интегрирана среда) за симулацията, включително материали за инцидента, виртуални новинарски уебсайтове, канали на социални медии, уебсайтове на компании и блогове в областта на сигурността.

Целта на организираното съвместно от ENISA и органи и агенции в областта на киберсигурността от цяла Европа учение CE2018 бе да се даде възможност на европейската общност в тази сфера да укрепи допълнително капацитета си за откриване на широкомащабни заплахи и справяне с тях, както и за по-добро разбиране на трансграничния ефект на инцидентите.

Най-важна бе целта на CE2018 да се помогне на организациите да изпробват непрекъснатостта на дейността си и своите планове за управление на кризи, включително за комуникация с медиите при кризи, като в същото време се засили сътрудничеството между публичните и частните субекти.

В сценария бяха включени свързани с реалния живот инциденти с технически и нетехнически характер, изискващи мрежов анализ и анализ на зловреден софтуер, компютърна криминалистика и стеганография. Сценарият бе замислен така, че инцидентите да прераснат в криза на всички възможни равнища: организационно, местно, национално и европейско.

Мария Габриел, комисар по въпросите на цифровата икономика и цифровото общество, заяви: „Технологиите предоставят безкрайни възможности във всички сектори на нашата икономика. Съществуват обаче и рискове за нашите предприятия и граждани. Европейската комисия и страните членки трябва да работят заедно и да се снабдят с необходимите инструменти за откриване на кибератаки и защита на мрежите и системите. Така се стигна до първото учение на ENISA – Cyber Europe, преди осем години. То прерасна в голямо учение по киберсигурност и се превърна във

водеща проява на ЕС, в която участват стотици специалисти в тази област от цяла Европа. Трябва да използваме този успех. Уверена съм, че можем да развием още повече механизмите за сътрудничество на ЕС, по-специално що се отнася до реакцията при мащабни кибернетични инциденти“.

Проф. д-р Удо Хелмбрехт, изпълнителен директор на ENISA, поясни: „През последното десетилетие авиационният сектор направи огромен скок в ерата на технологиите. Вече можем да използваме навигационни приложения, онлайн регистрация при пътувания, автоматизирана проверка на багажа. Интелигентните технологии спестяват време и пари и улесняват пътниците. Развиват се обаче не само технологиите, но и кибернетичните заплахи. Чрез прояви като Cyber Europe 2018 нашата агенция укрепва равнището на киберсигурността в ЕС. Европейските страни и организации трябва да работят съвместно, като едно цяло — това е съвременният отговор на кибернетичните заплахи, които не познават граници. От името на ENISA и нейния персонал бих искал да поздравя всички, които участваха в Cyber Europe 2018“.

В крайна сметка участниците успяха да вземат навременни и ефективни мерки за смекчаване на последиците от инцидентите. Това показва, че европейският сектор на киберсигурността е претърпял развитие през последните няколко години и участниците в него са много по-добре подготвени. ENISA и участниците скоро ще предприемат последващи действия във връзка с ученията и ще анализират предприетите мерки, за да преценят в кои области могат да бъдат направени подобрения. ENISA ще публикува заключителен доклад своевременно.

Фактите накратко

Участващи страни: [30], Австрия, Белгия, България, Хърватия, Кипър, Чешката република, Дания, Естония, Финландия, Франция, Германия, Гърция, Унгария, Ирландия, Италия, Латвия, Литва, Люксембург, Малта, Холандия, Норвегия, Полша, Португалия, Румъния, Словакия , Словения, Испания, Швеция, Швейцария, Великобритания

Участващи организации: приблизително 30
Брой на участниците: над 900 специалисти в областта на киберсигурността

Брой на симулираните инциденти: 23 222

За ученията Cyber Europe

Ученията Cyber Europe представляват симулации на мащабни кибернетични инциденти, ескалиращи в кибернетични кризи на равнище ЕС. Ученията дават възможност за анализиране на високотехнологични кибернетични инциденти и за справяне със сложни ситуации, свързани с непрекъснатостта на дейността и управлението на кризи. ENISA вече организира четири общоевропейски кибернетични учения — през 2010 г., 2012 г., 2014 г. и 2016 г.

Международното сътрудничество между участващите организации е характерна особеност на ученията, в които участват повечето европейски страни. Това е гъвкав процес на учене: за самостоятелни анализатори или цели организации, с възможности за участие или неучастие. Участниците могат да адаптират ученето към своите нужди.