Агенция на Европейския съюз
за киберсигурност
Agamemnonos 14,
Chalandri 15231| Attiki| Гърция
Тел.: +30 28 14 40 9711
Ел. поща: info@enisa.europa.eu
www.enisa.europa.eu

Cyber Europe 2022: Тестване на устойчивостта на европейския сектор на здравеопазването

Агенцията на Европейския съюз за киберсигурност (ENISA) организира учение в областта на киберсигурността, за да тества реакцията на здравните инфраструктури и услуги на ЕС срещу кибер атаки.

За да се гарантира доверието на гражданите в медицинските услуги и инфраструктура, които са на тяхно разположение, здравните услуги следва да функционират по всяко време. Ако здравните услуги и инфраструктури в Европа са обект на мащабна кибератака, как бихме реагирали и координирали както на национално равнище, така и на равнище ЕС, за да намалим ефекта от инцидентите и да предотвратим ескалация?

Това е въпросът, чийто отговор се търси на „Cyber Europe 2022“ чрез въображаем сценарий. Първият ден включваше кампания за дезинформация с манипулирани лабораторни резултати и кибератака, насочена срещу европейските болнични мрежи. На втория ден сценарият се превърна в киберкриза в целия ЕС с непосредствена заплаха от разпространение на лични медицински данни и друга кампания за компрометиране на имплантируемо медицинско изделие с твърдение за уязвимост.

Изпълнителният директор на Агенцията на ЕС за киберсигурност **Юхан Лепасар** заяви: *„Сложността на нашите предизвикателства сега е пропорционална на сложността на нашия свързан свят. Ето защо твърдо вярвам, че трябва да обединим всички способности, с които разполагаме в ЕС, за да споделим своя експертен опит и знания. Укрепването на устойчивостта на нашата киберсигурност е единственият път напред, ако искаме да защитим нашите здравни услуги и инфраструктури, и в крайна сметка здравето на всички граждани на ЕС.“*

Общоевропейското учение, организирано от ENISA, събра общо 29 държави както от Европейския съюз и Европейската асоциация за свободна търговия (EACT), така и от агенциите и институциите на ЕС, ENISA, CERT-EU на Европейската комисия, Европол и Европейската агенция по лекарствата (EMA). Над 800 експерти в областта на киберсигурността бяха в действие, за да наблюдават непрекъснатостта на дейността и целостта на системите през двата дни на това най-скорошно издание на Cyber Europe.

Можем ли да укрепим киберустойчивостта на здравеопазването в ЕС?

Участниците, включили се в сложното учение, са доволни от начина, по който са третирани инцидентите, и от реакцията на фиктивни атаки.

Сега е необходимо да се извърши анализ на процеса и на резултатите от различните аспекти на ученията, за да се постигне реалистично разбиране на потенциалните пропуски или слабости, които може да изискват защитни мерки. Справянето с такива атаки изисква различни равнища на компетентност и процеси, които включват ефикасен и координиран обмен на информация, споделяне на знания относно конкретни инциденти и начини за наблюдение на ситуация, която предстои да ескалира, в случай на всеобща атака. Трябва да се разгледа и ролята на мрежата на ЕРИКС на равнище ЕС и стандартните оперативни процеси (СОП) на групата CyCLONe.

По-задълбоченият анализ ще бъде публикуван в доклада за резултатите от действията. Констатациите ще послужат като основа за бъдещи насоки и допълнителни подобрения за укрепване на устойчивостта на сектора на здравеопазването срещу кибератаки в ЕС.

За ученията Cyber Europe

Ученията Cyber Europe представляват симулации на мащабни кибер инциденти, ескалиращи в кибер кризи на равнище ЕС. Ученията дават възможност за анализиране на високотехнологични кибер инциденти и за справяне със сложни ситуации, свързани с непрекъснатостта на дейността и управлението на кризи.

ENISA вече организира пет общоевропейски учения в областта на кибер пространство през 2010 г., 2012 г., 2014 г., 2016 г. и 2018 г. Обикновено проявата е на всеки две години, но изданието за 2020 г. беше отменено поради пандемията от COVID-19.

Международното сътрудничество между всички участващи организации е характерна особеност на ученията, в които участват повечето европейски страни. Това е гъвкав образователен опит: от един анализатор до цяла организация, със сценарии за участие и неучастие, при които участниците могат да приспособят упражнението към своите нужди.

Допълнителна информация

Cyber Europe 2022

Киберучения — тема ENISA

Cyber Europe 2018 — Доклад за последващи действия

За контакти:

За въпроси, свързани с пресата, и интервюта се свържете с press(at)enisa.europa.eu.