CERT BG
COMPUTER EMERGENCY RESPONSE TEAM
BULGARIA

Екип за реагиране при инциденти в компютърната сигурност

Мониторинг на актуалните киберновини – към 10.12.2020 г.

Съдържание

Задвижване на глобалната екосистема на възможностите за реагиране при инциденти: нови проучвания вече са на разположение

Агенцията на Европейския съюз за киберсигурност публикува две проучвания за разработване и подкрепа на екипи за реагиране при инциденти по време на 12-тата среща на CSIRTs мрежата.

10 декември 2020 г.

12-ата среща на CSIRTs мрежата, проведена по-рано тази седмица, даде възможността Агенцията на Европейския съюз за киберсигурност да представи следните две нови ръководства, посветени на подобряването на работата на екипите за реагиране при инциденти:

- Как да настроите CSIRT и SOC - Ръководство за добри практики
- Секторни възможности на CSIRT - Състояние и развитие в сектора на енергетиката и въздушния транспорт

Събитието, организирано от германското председателство на Съвета на Европейския съюз, събра членове на мрежата на CSIRT (състояща се от държавите-членки на CSIRT и CERT-EU), за да обсъдят възможностите за оперативно сътрудничество в ЕС, както е определено от Директивата за мрежова и информационна сигурност .

Ролята на CSIRTs мрежата е да осигури форум, където националните и секторни CSIRTs на всички държави-членки и CERT-EU могат да си сътрудничат, да обменят информация и да работят за изграждането на доверие. Те са посветени на подобряването на начина, по който се обработват трансграничните инциденти и как да се реагира координирано на конкретни инциденти. ENISA осигурява секретариата на CSIRTs мрежата и активно подкрепя сътрудничеството между членовете на мрежата и организацията на техните срещи.

За кого са предназначени проучванията?

И двете проучвания са предназначени за екипи за реагиране при инциденти. Първото е проведено, за да се проучат начини за това как да се създадат и подобрят екипи. Вторият се фокусира върху тенденциите в реагирането на инциденти в енергийния и въздушния транспорт (IR) и предлага прозрения за текущите предизвикателства и пропуски.

Как да настроите CSIRT и SOC - Ръководство за добри практики

Заплахите за киберсигурност се увеличават и стават все по-сложни. Един от най-ефективните начини за противодействие на тези заплахи е чрез създаване на глобална екосистема от екипи за реагиране при инциденти на компютърната сигурност (CSIRTs) и оперативни центрове за сигурност (SOC).

Целта на тази екосистема е да улесни комуникацията и споделянето на информация, за да отговори ефективно на киберзаплахите. Това може да се постигне чрез осигуряване на подходящи рамки, като същевременно се увеличи броят на CSIRT и SOC по целия свят и се развие зрелостта на съществуващите CSIRT и SOC.

ENISA подпомага държавите-членки на ЕС с техните възможности за реагиране при инциденти, като им предоставя различни ресурси като документи, инструменти, материали и насоки. Повече от 40 екипа от цял свят са допринесли за съдържанието на изследването.

Методология

Изследването е разработено въз основа на ориентиран към резултатите подход. Представен е със структура, предназначена да предоставя насоки за различните етапи от създаването на CSIRT или SOC организация. Читателят ще бъде насочен към това върху какво да се съсредоточи на всеки етап от процеса, като създаване и подобряване.

Тази публикация ще бъде от особен интерес за тези, които възнамеряват да създадат CSIRT или SOC. Също така ще помогне на онези, които търсят насоки за възможни подобрения според различните видове CSIRT и SOCs, които вече са създадени и функционират. Ръководството се основава на съществуващата работа на ENISA, особено в областта на зрелостта и обучението.

Секторни възможности на CSIRT - Състояние и развитие в сектора на енергетиката и въздушния транспорт

Цифровата инфраструктура, информационните и комуникационни технологии са от решаващо значение за нашите общества и икономики. И енергийният, и въздушният транспорт са изправени пред значителни заплахи с потенциално катастрофални финансови и обществени последици. Ето защо те изискват солидни възможности за реагиране при инциденти (IRC).

И двата сектора идват с големи вериги за доставки и множество заинтересовани страни (публични органи, регулатори, професионални асоциации, големи индустрии, МСП и др.). През последните години те предприеха стъпки за структуриране и укрепване на способността им да се изправят срещу киберзаплахи и да реагират на киберинциденти. Създаването на ISAC за насърчаване на обмена на информация на секторно ниво е отлична илюстрация на това развитие.

Контекст и обхват на изследването

Тази публикация осигурява продължение на работата по секторния IRC на европейско ниво след публикуването на „Доклад за състоянието на развитието на реагирането при инциденти в държавите-членки на ЕС за 2019 г.“.

Чрез предоставяне на обширен анализ на последните промени и развитие на IR способностите (IRC) в секторите на въздушния транспорт и енергетиката в държавите-членки, изследването има за цел да увеличи разбирането и познанията за развитието на IRC при днешните обстоятелства. За тази цел проучването е проведено в светлината на неотдавнашните промени, свързани с пандемията Covid-19 и в контекста на предстоящото преразглеждане на Директивата за МИС.

Препоръки

Изследването е представено като моментна снимка на текущата ситуация в района. Предлагат се общи препоръки относно способностите, разпоредбите и сътрудничеството. По-специално, проучването подчертава общо осем ключови констатации по теми като създаване и организация на секторни CSIRT, специфични услуги и компетенции, предлагани от такива CSIRT, използвани инструменти и механизми за обмен на информация, както и предизвикателства, пред които са изправени.

За повече информация:

https://www.enisa.europa.eu/news/enisa-news/driving-the-global-ecosystem-of-incident-response-capabilities-new-studies-now-available

Нови насоки за телеком- и 5G сигурността

ENISA издава нови насоки в подкрепа на европейските органи за телекомуникационна сигурност при изпълнението на изискванията за сигурност на Европейския кодекс за електронни съобщения (EECC) и инструментариума на ЕС 5G. Насоките и свързаното с тях допълнение 5G подчертават значението на общия подход към телекомуникационната сигурност за цифровия единен пазар.

10 декември 2020 г.

Днес Агенцията на Европейския съюз за киберсигурност (ENISA) публикува насоки за осигуряване на общ подход за осигуряване на електронни комуникационни мрежи и услуги. Публикацията е актуализация на Техническите насоки за мерки за сигурност на ENISA от 2014 г. съгласно член 13а от Рамковата директива на ЕС за далекосъобщенията. Той предоставя необвързващи технически насоки на органите за телекомуникационна сигурност относно надзора на сигурността, изискван от членове 40 и 41 от ЕИОК. Член 40 от ЕИОК съдържа подробни изисквания за сигурност за доставчиците на електронни комуникации, а член 41 предоставя правомощия на компетентните органи по отношение на прилагането на тези изисквания.

Изпълнителният директор на Агенцията за киберсигурност на ЕС Юхан Лепасаар обяви: „С наближаването на транспонирането на Европейския кодекс за електронни съобщения Агенцията на ЕС за киберсигурност публикува нови насоки за националните органи за телекомуникационна сигурност, които имат за цел да постигнат общо високо ниво на комуникационна сигурност за телекомуникациите доставчици и мрежови оператори в ЕС. “

По-конкретно, Насоките за мерки за сигурност съгласно доклада на ЕИОК съдържа 29 цели на високо ниво на сигурност, изброени в осем области на сигурността (управление и управление на риска; сигурност на човешките ресурси; сигурност на системи и съоръжения; управление на операциите; управление на инциденти; управление на непрекъснатостта на бизнеса; мониторинг, одит и тестване; осъзнаване на заплахата). Докладът също така предоставя подробни мерки за сигурност, организирани в три нива. Всяка мярка за сигурност включва примери за доказателства, които да помогнат да се прецени дали мерките са въведени.

Приложението за 5G предоставя на националните власти ръководство за осигуряване сигурността на техните 5G мрежи и услуги. Публикацията предлага допълнителна стъпка към насоката, като предоставя на властите 70 предложени проверки за 5G при прилагане на мярка или при проверка на доказателствата на насоката. Приложението се фокусира върху киберсигурността на 5G мрежите на ниво политика, произтичащо от инструментариума на ЕС 5G, и включва допълнителна информация и справки на техническо ниво за нови технологии.

Насоките и добавката за 5G бяха изготвени в тясно сътрудничество с експертната група на ECASEC на националните органи за телекомуникационна сигурност и в съответствие с работния поток за 5G киберсигурност в рамките на Групата за сътрудничество за МИС.

Европейският кодекс за електронна комуникация (EECC) замества съществуващата рамкова директива на ЕС за далекосъобщенията и внася значителни промени в надзора върху сигурността на електронните съобщителни услуги. EECC изисква от държавите-членки на ЕС да прилагат новите правила до 21 декември 2020 г. Създадена през 2010 г., Експертната група на ECASEC (предишната експертна група по член 13а) се състои от повече от 50 експерти от националните органи за телекомуникационна сигурност от 31 ЕС, ЕАСТ и ЕС страни кандидатки, които контролират сигурността на телекомуникационните мрежи и услуги. Експертната група изготвя технически насоки за европейските власти относно прилагането на правилата на ЕС за телекомуникационна сигурност и публикува обобщен доклад за големите инциденти в областта на телекомуникационната сигурност всяка година.

За повече информация:

https://www.enisa.europa.eu/news/enisa-news/new-guidelines-for-telecom-and-5g-security