CERT (Computer Emergency Readiness Team)
CSIRT (Computer Security Incident Response Team)

Радослав Йошинов

Computer Security Incident Response Team (CSIRT)

Екипът за реагиране при инциденти по компютърна сигурност (CSIRT, наречен "see-sirt") е организация, която получава доклади за нарушения на сигурността, извършва анализи на отчетите и отговаря на изпращачите. CSIRT може да бъде установена група или ad hoc екип.

Инцидентите, свързани със сигурността на компютърите, включват действително или подозирано нарушение или акт на умишлено причиняване на уязвимост или пробив.

Типичните инциденти включват внедряването на вируси или червеи в мрежа, атаки от тип DoS (отказ от услуга), неразрешено изменение на софтуер или хардуер и кражба на самоличност на лица или институции.

Хакерството като цяло може да се счита за инцидент, свързан със сигурността, освен ако извършителите са преднамерено наети за конкретната цел за тестване на компютър или мрежа за уязвимости.

Видове CSIRT

Освен да реагират на инциденти, CSIRT могат да предоставят проактивни услуги, като например обучение за защита на крайните потребители.

Има различни видове CSIRTS.

Вътрешен CSIRT е екип в рамките на дадена организация, като правителство, корпорация, университет или изследователска мрежа.

Националните CSIRT (един вид вътрешен CSIRT) контролират обработката на инциденти за съответната страна.

Обикновено вътрешните CSIRTS се събират периодично през цялата година за проактивни задачи, както и при необходимост, в случай на нарушение на сигурността.

Външните (спрямо организацията) CSIRT предоставят платени услуги

Алтернативни наименования на CSIRT

- CIRC (Computer Incident Response Capability),
- CIRT (Computer Incident Response Team),
- IRC (Incident Response Center or Incident Response Capability),
- IRT (Incident Response Team),
- SERT (Security Emergency Response Team)
- SIRT (Security Incident Response Team).

Вътрешните CSIRT често използват едно от тези наименования заедно с идентификатор

Роли на членовете от екипа на CSIRT

- Ръководител или ръководител на екип.
- Помощни мениджъри, ръководители или ръководители на групи.
- Гореща линия, бюро за помощ или персонал за подбор.
- Манипулатори на инциденти.
- Манипулатори за уязвимости.
- Аналитичен персонал.
- Специалисти по софтуерни платформи.
- Обучител.
- Технологичен наблюдател.

Конституиране на CSIRT

Времето за реакция--- представлява критично съображение при изграждането, поддръжката и разгръщането на ефективен CSIRT.

Бързият, точно насочен и ефективен отговор може да сведе до минимум цялостното увреждане на финансите, хардуера и софтуера, причинени от конкретен инцидент.

Друго важно съображение включва способността на CSIRT да открие извършителите на инцидент, така че виновните лица да могат да бъдат открити и ефективно преследвани.

Третото съображение включва "втвърдяване" на софтуера и инфраструктурата, за да се сведе до минимум броят на инцидентите, които се случват във времето

CERT (Computer Emergency Readiness Team)

CERT (който е "екипът за компютърна готовност за реагиране при извънредни ситуации") е създаден от Агенцията за съвременни изследвания на отбраната (DARPA) през ноември 1988 г., след като интернет беше атакуван по време на инцидента с червеи.

Днес CERT се съсредоточава върху нарушения на сигурността и инциденти при отказ на услуга, алармирайки за инциденти, предоставяйки насоки при разглеждане на случаите на атаки и за предотвратяване на инциденти.

CERT също провежда кампания за обществена осведоменост и се занимава с изследвания, насочени към подобряване на системите за сигурност.

CERT е установен в университета Карнеги-Мелън в Питсбърг