ПОДХОД ЗА СЪЗДАВАНЕ НА ЦДКСКС СТЪПКА ПО СТЪПКА

Документ за справка WP2006/5.1 (CERT-D1/D2)

Съдържание

1 Управленско резюме

Представеният документ описва процеса на създаване на Център за действие при кризисни ситуации в компютърната сигурност (ЦДКСКС) във всички свързани с това аспекти като бизнес управление, управление на процеса както и от техническа гледна точка. Документът реализира две от целите, описани в Работната програма на Европейската агенция за мрежова и информационна сигурност (ЕАМИС) за 2006 г., глава 5.1:

- Този документ: *Доклад в писмен вид относно подход за създаване стъпка по стъпка на група за действие в екстремни компютърни ситуации (CERT) или подобни структури, като включва примери* .(**CERT-D1**)
- Глава 12 и външни файлове: *Извадка от пътна карта под формата на подробен списък, който позволява лесното прилагане на практика на пътната карта.* (**CERT-D2**)

2 Правна забележка

Трябва да се вземе под внимание, че публикацията представя вижданията и интерпретациите на авторите и редакторите, освен ако не е заявено друго. Публикацията не следва да се приема като действие на Европейската агенция за мрежова и информационна сигурност или на органите на ЕАМИС, освен ако не се приеме съгласно Регламент (ЕО) № 460/2004 относно ЕАМИС. Настоящата публикация по определение не представя най-модерните тенденции и вероятно ще трябва да бъде актуализирана през определен период от време.

Източници от трети страни се цитират в зависимост от случая. ЕАМИС не носи отговорност за съдържанието на външни източници, включително и външни интернет сайтове, цитирани в настоящата публикация.

Настоящата публикация има единствено образователни и информативни цели. Нито ЕАМИС, нито лице, което действа от нейно име, носи отговорност за евентуално използване на информацията, която се съдържа в тази публикация.

3 Благодарности

ЕАМИС би искала да благодари на всички институции и лица, които дадоха своя принос за изготвянето на настоящия документ. Специални благодарности на:

- Henk Bronk, който в ролята си на консултант изготви първата версия на документа;
- координационния център на CERT и по-специално на екипа за развитие на ЦДКСКС, който допринесе с изключително полезен материал и примерни материали за курс в приложението;
- GovCERT.NL за предоставянето на *CERT-in-a-box*;
- екипа на TRANSITS, който допринесе с примерни материали за курс в приложението;
- колегите от сектор „Политики по сигурността“ към техническия отдел, които съдействаха с глава 6.6;
- безбройните сътрудници, които рецензираха документа.

4 Въведение

Комуникационните мрежи и информационните системи се превърнаха в основен фактор за икономическото и социално развитие. Изчислителните и мрежови системи се превръщат в повсеместни услуги подобно на електричеството и водоснабдяването.

Следователно сигурността на комуникационните мрежи и информационните системи, и по-специално тяхната достъпност, все повече притесняват обществото. Причината за това е рискът от заплахи за ключови информационни системи, дължащи се на сложността на системата, повреди, грешки и атаки над физическата инфраструктура, която доставя услуги, критични за благосъстоянието на гражданите на ЕС.

На 10 март 2004 г. бе създадена Европейската агенция за мрежова и информационна сигурност (ЕАМИС)[1]. Целта ѝ бе да осигури висока и ефективна степен на мрежова и информационна сигурност в рамките на Общността и да развие култура на мрежова и информационна сигурност в полза на гражданите, потребителите, предприятията и организациите на публичния сектор в рамките на Европейския съюз, като по този начин допринесе за гладкото функциониране на вътрешния пазар.

От няколко години насам редица общности по сигурността в Европа като CERT/ЦДКСКС, екипи срещу злоупотреби и WARP си сътрудничат за целите на по-сигурен Интернет. ЕАМИС възнамерява да подкрепи тези общности в техните усилия за предоставяне на информация относно мерки за осигуряване на подходящо ниво на качество на обслужването. Освен това ЕАМИС има намерение да увеличи капацитета си за консултиране на държавите-членки на ЕС и органите на ЕС по въпроси, свързани с обхващането на специфични групи от потребители на ИТ с подходящи услуги по сигурността. Следователно, като се основава на констатациите на временната работна група за сътрудничество и подпомагане на CERT, основана през 2005 г., новата работна група ще се занимае с въпроси,

[1] Регламент (ЕО) № 460/2004 на Европейския парламент и на Съвета от 10 март 2004 година относно създаване на Европейската агенция за мрежова и информационна сигурност. „Агенция на Европейската общност“ е орган, създаден от ЕС за изпълнението на специфична техническа, научна или управленска задача в рамките на „общностната сфера“ („първия стълб“) на ЕС.

свързани с предоставянето на адекватни услуги по сигурността („услуги CERT“) на специфични (категории или групи) потребители.

ЕАМИС подкрепя създаването на нови ЦДКСКС, като публикува настоящия доклад на ЕАМИС „Подход за създаването стъпка по стъпка на Център за действие при кризисни ситуации в компютърната сигурност с допълнителен списък за проверка“, който ще Ви помогне да създадете собствен център.

Целева група

Основните целеви групи на настоящия доклад са правителствени и други институции, взели решение да създадат Център за действие при кризисни ситуации в компютърната сигурност с цел да защитят собствената си ИТ инфраструктура или тази на заинтересовани страни.

Начин на използване на настоящия документ

Настоящият документ ще представи информация за това какво представлява ЦДКСКС, какви услуги предлага той и какви са необходимите стъпки за създаването му. Това би трябвало да даде на читателя добър и прагматичен поглед върху подхода, структурата и съдържанието за това как да се създаде ЦДКСКС.

Глава 4 „*Въведение“*
Въведение в настоящия доклад

Глава 5 „*Цялостна стратегия за планиране и създаване на ЦДКСКС“*
Първият раздел представя описание на това какво представлява ЦДКСКС. Също така ще представи информация за различните среди, в които може да работят ЦДКСКС и услугите, които те може да предлагат.

Глава 6 *„Разработване на бизнес план“*
Тази глава описва подхода на бизнес управление при процеса на основаване.

Глава 7 *„Популяризиране на бизнес плана*“
Тази глава третира въпроси, засягащи бизнес казуса и финансирането.

Глава 8 „*Примерни оперативни и технически процедури“*
Тази глава описва процедурата по събиране на информация и представянето ѝ в бюлетин по сигурността. Главата също представя описание на работния поток при справяне с кризисни ситуации.

Глава 9 *„Обучение в ЦДКСКС“*
Тази глава дава резюме на предлаганото обучение за ЦДКСКС. В приложението с цел илюстрация са представени примерни материали за курс.

Глава 10 *„Упражнения: изготвяне на бюлетин по сигурността“*
Тази глава съдържа упражнение как да се изпълнява една от основните (или централни) услуги на ЦДКСКС: издаването на бюлетин по сигурността (или препоръки).

Глава 12 *„Описание на плана на проекта“*
Тази глава насочва към допълнителния план на проекта (списък за проверка), представен с настоящото ръководство. Планът трябва да бъде лесен за ползване инструмент за прилагането на ръководството.

Конвенции, използвани в настоящия документ

За да даде насоки на читателя, всяка глава започва с резюме на предприетите преди нея стъпки в процеса на създаване на ЦДКСКС. Тези резюмета са оградени в таблица както следва:

Досега сме предприели първата стъпка

Всяка глава завършва с практически пример на обсъдените стъпки. В настоящия документ „Примерният ЦДКСКС“ е малък независим ЦДКСКС за средно предприятие или институция. В приложението може да се намери резюме.

Примерен ЦДКСКС

5 Цялостна стратегия за планиране и създаване на ЦДКСКС

За успешно начало на процеса по създаване на ЦДКСКС е важна ясната визия за възможните услуги, които екипът може да предлага на клиентите си, които в „света на ЦДКСКС“ са известни като „конституенти“. Следователно е необходимо да има разбиране за нуждите на конституентите, за да се предоставят подходящи услуги в подходящи срокове и качество.

Какво представлява ЦДКСКС?

ЦДКСКС означава Център за действие при кризисни ситуации в компютърната сигурност. Терминът ЦДКСКС се използва най-вече в Европа вместо защитения термин CERT, регистриран в САЩ от CERT Coordination Center (CERT/CC).
Съществуват редица съкращения, използвани за същия вид центрове:

- CERT или CERT/CC (Computer Emergency Response Team / Coordination Center)
- ЦДКСКС (Център за действие при кризисни ситуации в компютърната сигурност)
- IRT (Incident Response Team)
- CIRT (Computer Incident Response Team)
- SERT (Security Emergency Response Team)

Първият голям пробив на червей в глобалната ИТ инфраструктура възникна в края на 80-те години на 20 век. Червеят бе известен под името Morris[2] и се разпространи бързо, като успя да зарази голям брой информационни системи по целия свят.

Тази кризисна ситуация подейства като сигнал за събуждане: изведнъж много хора осъзнаха голямата необходимост от сътрудничество и координация между системните администратори и ИТ мениджърите с цел справяне със случаи като този. Тъй като времето представляваше критичен фактор, трябваше да се установи по-организиран и структуриран подход към справянето с кризисни ситуации в областта на ИТ сигурността. Така, няколко дни след „кризисна ситуацияа Morris“, Агенцията за проекти за напреднали изследвания в областта на отбраната (DARPA) създаде първия ЦДКСКС: CERT Coordination Center (CERT/CC[3]), разположен в университета „Карнеги Мелън“ в Питсбърг (Пенсилвания).

Скоро след това този модел бе възприет в Европа и през 1992 г. холандският академичен интернет доставчик SURFnet пусна първия ЦДКСКС в Европа, под името SURFnet-CERT[4]. Последваха го много центрове и понастоящем в

[2] Повече информация за червея Morris: http://en.wikipedia.org/wiki/Morris_worm

[3] CERT-CC, http://www.cert.org

[4] SURFnet-CERT: http://cert.surfnet.nl/

Регистъра на ЕАМИС за дейностите в областта на CERT в Европа[5] се изброяват повече от 100 известни центрове, намиращи се в Европа.

През годините CERT увеличиха капацитета си от обикновени групи за действие до доставчици на цялостни услуги по сигурността, включително и превантивни услуги като сигнали, бюлетини по сигурността, услуги по управление на обучението и сигурността. Терминът CERT скоро бе счетен за неадекватен. В резултат на това в края на 90-те години на 20 век бе въведен новият термин ЦДКСКС. В момента и двата термина (CERT и ЦДКСКС) се използват като синоними, като ЦДКСКС е по-прецизният.

5..1 Терминът „конституенти“

Отсега нататък добилият гражданственост (в средите на ЦДКСКС) термин „конституенти” ще бъде използван по отношение на клиентската база на ЦДКСКС. Отделният клиент ще бъде наричан „конституент“, а група от клиенти - „конституенти“.

5..2 Определения за ЦДКСКС

ЦДКСКС е екип от експерти по сигурността в областта на ИТ, чиято основна дейност е да реагира при кризисни ситуации в компютърната сигурност. Той предоставя необходимите услуги за справянето с тях и подпомага конституентите при възстановяване от пробиви.

За смекчаване на рисковете и намаляване на броя на необходмите действия, повечето ЦДКСКС предлагат на своите конституенти както превантивни така и образователни услуги. Издават бюлетини за уязвимости в използвания софтуер и хардуер и също така уведомяват потребителите за експлойти и вируси, които се възползват от тези недостатъци. По този начин конституентите могат бързо да поправят и актуализират системите си. Вижте в глава 5.2 „Възможни услуги” пълния списък с възможни услуги.

5..3 Предимствата от съществуването на ЦДКСКС

Ползването на специализиран екип по ИТ сигурността помага на организацията да смекчи и предотврати кризисни ситуации и помага за защитата на ценни активи.

Други възможни предимства са:

- централизирана координация по въпросите на ИТ сигурността в рамките на организацията (контактно звено);
- централизирано и специализирано действие при и в отговор на ИТ кризисни ситуации;
- налична експертиза за поддръжка и подпомагане на потребителите за бързо възстановяване от кризисни ситуации в сферата на сигурността;
- справяне с правни въпроси и запазване на доказателствен материал в случай на съдебен процес;

[5] Регистъра на ЕАМИС http://www.enisa.europa.eu/cert_inventory/

- проследяване на събития в областта на сигурността;
- стимулиране на сътрудничеството в областта на ИТ сигурността в рамките на групата конституенти (повишаване на информираността).

Примерен ЦДКСКС (стъпка 0)
Разбрахме същността на ЦДКСКС: Примерният ЦДКСКС ще трябва да обслужва средна по големина институция с брой на служителите до 200 души. Институцията има собствен отдел по ИТ и два допълнителни клона в същата страна. ИТ играят ключова роля за компанията, тъй като се използват за вътрешна комуникация, мрежа от данни и е-бизнес 24x7. Институцията има собствена мрежа и разполага с резервна интернет връзка чрез два различни интернет доставчика.

5..4 Описание на различните видове среда за ЦДКСКС

Досега сме предприели първата стъпка

1. Разбрахме какво представлява ЦДКСКС и какви предимства може да донесе.

>>В следващата стъпка се дава отговор на въпроса: „В кой сектор ще бъдат предлагани услугите на ЦДКСКС?“

При основаването на ЦДКСКС (точно както при всеки друг бизнес) е много важно бързо да се разработи ясна визия за това кои са конституентите и за какъв тип среда ще бъдат предлагани услугите на ЦДКСКС. В момента се отличават следните „сектори”:

- ЦДКСКС за академичния сектор
- Комерсиален ЦДКСКС
- ЦДКСКС за сектора на ЗИОВ / ЗИОВИ
- ЦДКСКС за правителствения сектор
- Вътрешен ЦДКСКС
- ЦДКСКС за военната област
- Национален ЦДКСКС
- ЦДКСКС за сектора на малките и средни предприятия (МСП)
- ЦДКСКС за дистрибутори

ЦДКСКС за академичния сектор
Фокус
ЦДКСКС за академичния сектор предлага ЦДКСКС услуги на академични и учебни заведения като университети или изследователски центрове в интернет средата на района на учебното заведение.

Конституенти
Типичните конституенти на този тип ЦДКСКС са университетските служители и студенти.

Комерсиален ЦДКСКС
Фокус
Комерсиалният ЦДКСКС предлага комерсиални ЦДКСКС услуги на своите конституенти. В случая с интернет доставчици ЦДКСКС най-вече предоставят услуги срещу злоупотреби на крайни потребители (Dial-in, ADSL) и ЦДКСКС услугите на техните професионални клиенти.

Конституенти
Комерсиалните ЦДКСКС предлагат услугите си на конституенти, които плащат за тях.

ЦДКСКС за сектора на Защита на информация от особена важност (ЗИОВ) и/или Защита на информация от особена важност и инфраструктура (ЗИОВИ)

Фокус

Дейността на ЦДКСКС в този сектор обхваща основно защитата на информация от особена важност и/или защитата на информация от особена важност и инфраструктурата. В повечето случаи този специализиран ЦДКСКС работи в тясно сътрудничество с правителствен орган по защита на информация от особена важност и инфраструктура. Включва всички критични ИТ сектори в страната и защитава гражданите на държавата.

Конституенти

Правителството, фирми в областта на критичните ИТ инфраструктури, граждани

ЦДКСКС в правителствения сектор

Фокус

Правителственият ЦДКСКС предлага услуги на правителствени ведомства, а в някои страни и на граждани.

Конституенти

Правителството и свързани с правителството ведомства; в някои страни предупредителни услуги се предоставят и на граждани (например в Белгия, Унгария, Нидерландия, Обединеното кралство или Германия).

Вътрешен ЦДКСКС

Фокус

Вътрешният ЦДКСКС предоставя услуги единствено на организацията, в рамките на която съществува и описва повече функциите отколкото сектора. Така например, много телекомуникационни организации и банки имат собствени вътрешни ЦДКСКС. Обикновено те не поддържат уебсайт за широката общественост.

Конституенти

Вътрешни служители и ИТ отдел на организацията майка.

ЦДКСКС във военния сектор

Фокус

В този сектор ЦДКСКС предоставя услуги на военни организации с отговорности за необходима за отбранителни цели ИТ инфраструктура.

Конституенти

Служители на военни институции или тясно свързани органи, например Министерство на отбраната

Национален ЦДКСКС

Фокус

ЦДКСКС с национален фокус, считан за контактно звено по сигурността на страната. В някои случаи правителственият ЦДКСКС също действа в качеството си на контактно звено (като UNIRAS във Обединеното кралство).

Конституенти

Обикновено този вид ЦДКСКС няма преки конституенти, като националният ЦДКСКС играе само роля на посредник за цялата страна.

ЦДКСКС за сектора на малките и средни предприятия (МСП)
Фокус
ЦДКСКС със собствена организация, която предоставя услуги на собствения си бизнес клон или на подобни потребителски групи.
Конституенти
Конституентите на тези ЦДКСКС може да бъдат МСП и техните служители или специализирани заинтересовани групи като асоциация на градовете и общините в дадена държава.

ЦДКСКС за дистрибутори
Фокус
ЦДКСКС за дистрибутори се фокусира върху поддръжката на продукти, специфични за дистрибуторския сектор. Обикновено има за цел да разработва и предлага решения, които да отстранят уязвимостите и да смекчат потенциалните негативни ефекти от пропуските.
Конституенти
Собственици на продукти.

Както бе описано в горния параграф относно националните ЦДКСКС, възможно е един екип да обслужва повече от един сектор. Това, например, оказва влияние върху анализа на групата конституенти и нейните нужди.

Примерен ЦДКСКС (стъпка 1)
Начална фаза В началната си фаза новият ЦДКСКС е планиран като вътрешен ЦДКСКС, който предоставя услуги на компанията майка, местния ИТ отдел и служители. Също така поддържа и координира работата по ИТ сигурността, свързана с кризисни ситуации, между различните клонове.

Възможни услуги, които може да предлага ЦДКСКС

Досега сме предприели първите две стъпки

1. Разбрахме какво представлява ЦДКСКС и какви предимства може да донесе.
2. В кой сектор новият център ще предлага услугите си?

>> В следващата стъпка следва да се даде отговор на въпроса *какви услуги да се предлагат на конституенти.*

Съществуват множество услуги, които може да предлага ЦДКСКС, но досега нито един ЦДКСКС не предоставя всички. Така че изборът на подходящ комплект от услуги е ключово решение. По-долу ще намерите кратък преглед на всички известени услуги на ЦДКСКС, както са определени в публикувания от CERT/CC[6]. „Наръчник за ЦДКСКС“.

[6] Наръчник за ЦДКСКС на CERT/CC http://www.cert.org/archive/pdf/csirt-handbook.pdf

Реактивни услуги	**Проактивни услуги**	**Справяне с артифакти**
• **Сигнали и предупреждения** • **Справяне с иициденти** • **Анализ на кризисни ситуации** • **Поддръжка при действие при кризисни ситуации** • **Координация на действие при кризисни ситуации** • Действие на място при кризисни ситуации • Справяне с уязвимост • Анализ на уязвимост • Действие при уязвимост • Координация на действие при уязвимост	• **Съобщения** • Наблюдение на технологиите • Одити и оценки на сигурността • Конфигурация и поддръжка на сигурността • Разработване на инструменти по сигурността • Услуги по откриване на пробиви • Разпространяване на информация, свързана със сигурността	• *Анализ на артифакти* • *Действие при артифакти* • *Координация на действия при артифакти* ***Управление на качеството на сигурността*** • *Анализ на риска* • *Непрекъснатост на бизнес процеса и възстановяване от бедствия* • *Консултации по сигурността* • *Повишаване на информираността* • *Образование/ обучение* • *Оценка или сертификация на продукт*

Фиг.1 Услуги на ЦДКСКС, изброени от CERT/CC[7]

Централните услуги (отбелязани с по-тъмен шрифт): прави се разлика между реактивни и проактивни услуги. Проактивните услуги целят да предотвратят кризисни ситуации чрез повишаване на информираността и обучението, докато реактивните имат за задача да се справят с кризисни ситуации и да смекчат произтичащите от тях вреди.

Справянето с артифакти обхваща анализа на всякакви файлове или предмети, открити в дадена система, които може да са замесени в зловредни действия, като останки от вируси, червеи, скриптове, троянски коне и др. Включва и обработката и разпространението на произтичащата от това информация към дистрибутори и други заинтересовани страни с цел да се предотврати по-нататъшното разпространяване на малуер и да се намалят рисковете.

Услугите по управление на качеството на сигурността са услуги с по-дългосрочни цели и включват консултации и образователни мерки.

Вижте приложението за подробно обяснение на услугите на ЦДКСКС.

Изборът на точните услуги за вашите конституенти е важна стъпка и ще бъде допълнително спомената в глава *6.1. „Определяне на финансовия модел.“*

Повечето ЦДКСКС започват с разпространяването на „Сигнали и предупреждения“, правят „Съобщения“ и предлагат „Справяне с кризисни

[7] Услуги на CSIRT, изброени от CERT/CC: http://www.cert.org/csirts/services.html

ситуации“ на конституентите си. Обикновено тези централни услуги осигуряват добър профил и привличат вниманието на конституентите и главно се считат за истинската „добавена стойност“.

Една от добрите практики е стартирането на малка група с „пилотни“ конституенти, предоставяне на централни услуги за пилотен период от време и впоследствие търсенето на обратна връзка.
Заинтересованите пилотни потребители обикновено предоставят конструктивна обратна връзка и помагат за развитието на специално пригодени услуги.

Примерен ЦДКСКС (стъпка 2)
Избор на точните услуги В началната фаза се взе решението новият ЦДКСКС да се фокусира основно върху предоставянето на някои централни услуги за служителите. Взе се решение, че след пилотната фаза може да се разгледа разширяването на портфолиото с услуги и прибавянето на някои „Услуги по управление на сигурността“. Това решение ще бъде взето въз основа на обратната връзка от пилотните конституенти и в тясно сътрудничество с отдела по контрол на качеството.

Анализ на конституентите и мисия на центъра

Досега сме предприели три стъпки:

1. Разбрахме какво представлява ЦДКСКС и какви предимства може да донесе.
2. В кой сектор новият център ще предлага услугите си?
3. Какъв вид услуги може да предложи ЦДКСКС на конституентите си.

>> При следващата стъпка следва да се даде отговор на въпроса *какъв тип подход да бъде избран за основаването на ЦДКСКС?*

Следващата стъпка е по-задълбочен поглед върху конституентите, като основната цел е да се изберат правилните комуникационни канали:

- определяне на комуникационния подход към конституентите;
- определяне на мисията на центъра;
- изготвяне на реалистичен план за реализация на проекта;
- определяне на услугите на ЦДКСКС;
- определяне на организационната структура;
- определяне на политиката по информационна сигурност;
- набиране на подходящи служители;
- използване на офиса на ЦДКСКС;
- търсене на сътрудничество с други ЦДКСКС и възможни национални инициативи.

Тези стъпки ще бъдат подробно описани в следващите параграфи и може да се използват като материал за бизнес плана и плана за проекта.

5..1 Комуникационен подход към конституентите

Както бе заявено по-горе, много важно е да се познават нуждите на конституентите както и собствената комуникационна стратегия, която включва и комуникационните канали, най-подходящи за предоставяне на информация към тях.

В теория на управлението са известни няколко възможни подхода към този проблем, като се анализира целевата група. В този документ описваме два от тях: анализите SWOT и PEST.

SWOT анализ
SWOT анализът е инструмент за стратегическо планиране, използван е за оценяване на силните страни (S), слабите страни (W), възможностите (O) и заплахите (T), залегнали в проект или бизнес начинание или в каквато и да е друга ситуация, която изисква взимането на решение. Техниката е заслуга на Албърт Хъмфри, ръководител на изследователски проект към Станфордския университет през 60-те и 70-те години на 20 век, който използва данни от списъка с компании Fortune 500[8].

Силни страни	**Слаби страни**
Възможности	**Заплахи**

Фиг. 2 SWOT анализ

[8] SWOT анализ в Уикипедия: http://en.wikipedia.org/wiki/SWOT_analysis

PEST анализ

Анализът PEST е друг важен и широко използван инструмент за анализ на конституенти с цел запознаване с политическите (P), икономически (E), социокултурни (S) и технологически (T) обстоятелства на средата, в която оперира ЦДКСКС. Той ще помогне да се определи дали планирането все още отговаря на средата и би могло да помогне, за да се избегнат действия, предприети поради погрешни предположения.

Политически	**Икономически**
• Екологични/ природозащитни въпроси • Действащо законодателство на вътрешния пазар • Бъдещо законодателство • Европейско/ международно законодателство • Регулаторни органи и процеси • Правителствени политики • Мандат и смяна на правителството • Политики в областта на търговията • Финансиране, грантове и инициативи • Лобиране на вътрешния пазар/ групи за натиск • Международни групи за натиск	• Вътрешна икономическа ситуация • Вътрешни икономически тенденции • Външни икономики и тенденции • Общи данъчни въпроси • Данъчни въпроси, специфични за продукта/ услугите • Сезонност/ климатични въпроси • Цикличност на пазара и търговията • Специфични за сектора фактори • Пазарни пътища и тенденции в дистрибуцията • Направления клиент/ краен потребител • Лихвен процент и валутен курс
Социални	**Технологически**
• Тенденции в начина на живот • Демография • Нагласи и мнения на потребителите • Виждания на медиите • Промени в закона, които влияят върху социалните фактори • Марка, компания, технологическа визия • Потребителски модел • Мода и ролеви модели • Основни събития и влияния • Потребителски достъп и тенденции • Етнически/ религиозни фактори • Реклама и публичност	• Конкурентно развитие на технологиите • Финансиране на изследванията • Свързани/ помощни технологии • Заместващи технологии/ решения • Степен на развитие на технологиите • Степен на развитие на производството и капацитета • Информация и комуникации • Потребителски механизми/ технологии • Законодателство в областта на технологиите • Иновационен потенциал • Достъп до технологии, лицензиране, патенти • Въпроси, свързани с интелектуалната собственост

Фиг. 3 Модел за PEST анализ

Подробно описание на PEST анализ може да се намери в Уикипедия[9].

И двата инструмента дават изчерпателен и структуриран преглед относно нуждите на конституентите. Резултатите ще допълнят бизнес предложението и с това ще помогнат да се получи финансиране за създаването на ЦДКСКС.

[9] PEST анализ в Уикипедия: http://en.wikipedia.org/wiki/PEST_analysis

Комуникационни канали
Важна тема, която трябва да се включи в анализа, се отнася до възможните методи за комуникация и разпространение на информация („Как да общуваме с конституентите?“)

При възможност може да се помисли за редовни лични посещения на конституентите. Доказан факт е, че общуването на живо улеснява сътрудничеството. Ако и двете страни желаят да работят заедно, тези срещи ще доведат до по-открита връзка.

Обикновено ЦДКСКС работят с комплект от комуникационни канали. Долупосочените са доказали практическата си полза и заслужават внимание:

- обществено достъпен уебсайт;
- затворен сектор за членове в рамките на уебсайта;
- уеб формуляри за докладване за кризисни ситуации;
- мейлинг листи;
- индивидуална електронна поща;
- телефон / факс;
- SMS;
- „старомодни“ писма на хартия;
- месечни или годишни доклади

Освен електронна поща, уеб формуляри, телефон или факс за улесняване на справянето с кризисни ситуации (за да получават доклади за кризисни ситуации от конституенти, да координират с други центрове или да предоставят обратна връзка и поддръжка на жертвата) много ЦДКСКС публикуват свои бюлетини по сигурността на уебсайт, достъпен за обществеността и чрез мейлинг листи,

! Ако е възможно, информацията трябва да се разпространява по сигурен начин. Например, електронната поща може да е с електронен подпис PGP, а деликатните данни за кризисни ситуации може винаги да се изпращат кодирани.

За повече информация вижте глава *8.5 „Наличен инструментариум за ЦДКСКС.“* Вижте също глава *2.3 от RFC2350*[10].

Примерен ЦДКСКС (стъпка 3а)
Изготвяне на анализ на конституентите и подходящите комуникационни канали Сесия с брейнсторминг с някои ключови лица от ръководството и конституентите дадоха достатъчно материал за SWOT анализ. Той доведе до заключението, че е налице нужда от централни услуги: • сигнали и предупреждения;

[10] http://www.ietf.org/rfc/rfc2350.txt

• справяне с кризисни ситуации (анализ, поддръжка на действия и координация на действия); • съобщения.
Трябва да се осигури добре организираното разпространение на информацията, която да достигне до най-голямата възможна част от конституентите. В тази връзка се взе решение сигналите, предупрежденията и съобщенията във форма на бюлетини по сигурността да се публикуват на специално предназначен за целта уебсайт и да се разпространяват чрез мейлинг листа.Електронната поща, телефонът и факсът улесняват ЦДКСКС при получаването на доклади за кризисни ситуации. За следващата стъпка е предвиден единен уеб формуляр. Вижте по-долу за примерен SWOT анализ.

Силни страни • В компанията има известна степен на запознатост. • Харесват плана и имат желание за сътрудничество • Подкрепа и финансиране от управителния съвет	**Слаби страни** • Липсва комуникация между различните отдели и клонове. • Липсва координация при кризисни ситуации в ИТ • Множество „малки отдели“
Възможности • Огромен поток от неструктурирана информация за уязвимостта • Силна нужда от координация • Намаляване на загубите, причинени от кризисни ситуации • Много отворени въпроси в областта на ИТ сигурността • Обучение на служители в областта на ИТ сигурността	**Заплахи** • Липса на достатъчно налични средства • Липса на достатъчно подходящи служители • Високи очаквания • Култура

Фиг.4 Примерен SWOT анализ

5..2 Мисия на центъра

След анализа на нуждите и желанията на конституентите по отношение на услугите на ЦДКСКС следващата стъпка следва да бъде изготвяне на мисия на центъра.

Мисията описва основната функция на организацията в обществото по отношение на продуктите и услугите, които предлага на конституентите си. Това позволява ясното представяне на съществуването и работата на новия ЦДКСКС.

Добра практика е текстът на мисията да е компактен, но не прекалено сбит, защото той обикновено остава непроменен в продължение на няколко години.

Тук са представени някои примери за текст на мисия на действащи ЦДКСКС:

„<наименование на ЦДКСКС> осигурява информация и съдействие на своите <конституенти (определете Вашите конституенти)> при прилагането на проактивни мерки за намаляване на рисковете от кризисни ситуации в компютърната сигурност както и при действие при подобни кризисни ситуации, когато те възникнат.“

„Предлага поддръжка на <конституентите> по предотвратяване и действие при кризисни ситуации, свързани с ИТ сигурността.“[11]

Мисията е много важна и необходима начална стъпка. Моля, вижте глава *2.1* от *RFC2350*[12] за по-подробно описание на това каква информация би трябвало да публикува ЦДКСКС.

Примерен ЦДКСКС (стъпка 3б)
Мениджърите на примерния ЦДКСКС са заявили следната мисия: *„Примерният ЦДКСКС осигурява информация и съдействие на служителите на своята компания майка с цел намаляване на рисковете от кризисни ситуации в областта на компютърната сигурност както и за действие при подобни кризисни ситуации, когато те възникнат.“* С това примерният ЦДКСКС ясно заявява, че е вътрешен ЦДКСКС и основната му дейност е да се справя с въпроси, свързани с ИТ сигурността.

[11] мисия на Govcert.nl: http://www.govcert.nl

[12] http://www.ietf.org/rfc/rfc2350.txt

6 Разработване на бизнес план

Досега сме предприели следните стъпки:

1. Разбрахме какво представлява ЦДКСКС и какви предимства може да донесе.
2. В кой сектор новият център ще предлага услугите си?
3. Какъв вид услуги може да предложи ЦДКСКС на конституентите си.
4. Анализ на средата и на конституентите.
5. Определяне на мисията на центъра

>> Следващата стъпка е да се определи бизнес планът.

Резултатът от анализа Ви осигурява добър преглед на нуждите и (предполагаемите) слаби страни на конституентите, така че се приема като изходен за следващата стъпка.

Определяне на финансовия модел

След анализа бяха избрани няколко централни услуги, с които да се започне. Следващата стъпка е да се обмисли финансовия модел: какви параметри на предлагане на услугата са както подходящи, така и рентабилни.

В един идеален свят финансирането би било адаптирано според нуждите на конституентите, но в реалността портфолиото с услуги, които могат да се предложат, трябва да бъде адаптирано към определен бюджет. Така че е по-реалистично да се започне с планиране на финансовите въпроси.

6..1 Модел на разходите

Двата основни фактора, които влияят върху разходите, са определянето на работното време за обслужване на клиенти и броя (и качеството) на служителите, които следва да бъдат наети. Необходимо ли е да се осигурява действие при кризисни ситуации и техническа поддръжка 24x7, или тези услуги могат да се предлагат в традиционното работно време?

В зависимост от желаната наличност и оборудването в офиса (има ли възможност за работа от вкъщи?), може да е полезно да се работи със списък от дежурства на повикване или списък с разпределени дежурства.

Един от възможните сценарии е предоставянето на проактивни услуги и действие в традиционното работно време. Извън работното време ще бъдат предлагани единствено ограничени услуги от дежурен служител на повикване, като например единствено в случай на значителни бедствия и кризисни ситуации.

Друга възможност е да се търси международно сътрудничество с други центрове на ЦДКСКС. Вече съществуват примери за работа в сътрудничество „като се следва слънцето“. Например сътрудничеството между европейските и

американските центрове се оказва полезно и осигурява добър начин за споделяне на капацитет. Например ЦДКСКС Sun Microsystems, който има множество офиси в различни часови зони по света (но всички са членове на екипа на един и същ ЦДКСКС) осъществява услуги 24x7 чрез непрекъснати смени сред центровете по света. Това намалява разходите, защото екипите винаги работят само в традиционно работно време и също така предлагат услуги на „спящата част“ от света.

Особено добра практика е подробно да се анализира необходимостта от услуги 24x7 сред конституентите. Няма голям смисъл в изпращането на сигнали и предупреждения през нощта, когато получателят ще ги прочете едва на сутринта. Съществува тънка граница между „да имаш нужда от услуга“ и „да искаш услуга“, но специално работните часове водят до голяма разлика в броя на служителите и необходимото оборудване и по този начин оказват голямо въздействие върху модела на разходите.

6..2 Модел на приходите

Когато разходите са известни, следващата добра стъпка е да се обмислят моделите за приходи: как могат да се финансират планираните услуги. Тук са предложени за оценка няколко възможни сценария:

Използване на съществуващи ресурси
Винаги е от полза да се оценят вече наличните ресурси в други части на компанията. Има ли вече наети подходящи служители (например в действащия ИТ отдел) с необходимия опит и експертни познания? Вероятно с ръководството би могло да се уреди този персонал да бъде изпратен в ЦДКСКС за началната фаза или при необходимост да осигурява поддръжка на ЦДКСКС.

Такса за членство
Друга възможност е да продавате Вашите услуги на конституенти чрез годишна/ тримесечна такса за членство. Допълнителните услуги могат да се заплащат на база използването им, като например консултантски услуги или одити на сигурността.

Друг възможен сценарий: услугите за (вътрешни) конституенти се предоставят безплатно, но услугите за външни клиенти трябва да се заплащат. Друга идея е да се публикуват бюлетини по сигурността и информационни бюлетини на обществено достъпните уебсайтове и да има сектор „Само за членове“ със специална, по-подробна или специално изготвена информация.

Доказано на практика е, че „абонаментът за услуга на ЦДКСКС“ има ограничено значение за осигуряването на достатъчно финансиране, особено в началната фаза. Например, има фиксирани основни разходи за екипа и оборудването, които трябва да се платят предварително. Финансирането на тези разходи чрез продажба на услуги на ЦДКСКС е трудно и изисква много подробен финансов анализ, за да се открие „критичната точка“.

Субсидии
Друга възможност, която заслужава внимание, е да кандидатствате за субсидия за проект, отпусната от правителството или правителствен орган, тъй като днес в много държави има средства за проекти за ИТ сигурност. Вероятно добро начало е да се свържете с Министерство на вътрешните работи.

Разбира се, е възможно и комбинация между различните модели.

Определяне на организационната структура

Подходящата организационна структура на ЦДКСКС зависи до голяма степен от съществуващата структура на организацията и конституентите. Също така зависи от наличието на квалифицирани експерти, които да бъдат наети за постоянно или временно.

Типичният ЦДКСКС определя следните роли в рамките на екипа:

Обща
- Генерален мениджър

Служители
- Офис мениджър
- Счетоводител
- Консултант по комуникации
- Юрист

Оперативен технически екип
- Ръководител на техническия екип
- Технически сътрудници ЦДКСКС, които предоставят услугите
- Изследователи

Външни консултанти
- Наемани при нужда

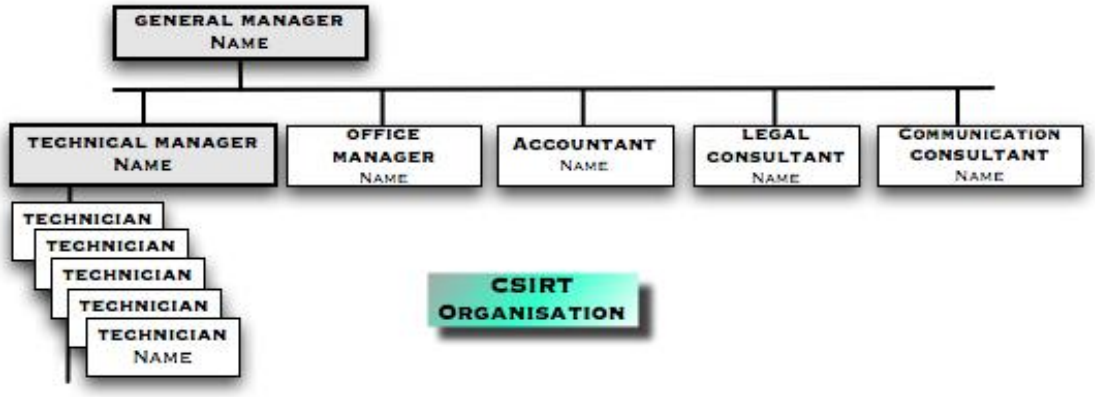
Много полезно е в екипа да има юрист, особено по време на началната фаза на ЦДКСКС. Това ще увеличи разходите, но в крайна сметка ще спести време и правни проблеми.

В зависимост от разнообразието от специалности сред конституентите и също така, когато ЦДКСКС е със силно медийно присъствие, се оказва много полезно в екипа да има и специалист по комуникации. Тези експерти могат да се съсредоточат върху обясняването на сложни технически въпроси чрез по-разбираеми за конституентите или медийните партньори послания. Експертът по комуникации също така ще осигури обратната връзка между конституентите и техническите експерти, така че той/тя може да действа като „преводач“ или „медиатор“ между тези две групи.

Следват няколко примери на организационни модели, използвани от действащи ЦДКСКС.

6..1 Независим бизнес модел

ЦДКСКС е основан и действа като независима организация със собствено ръководство и служители.

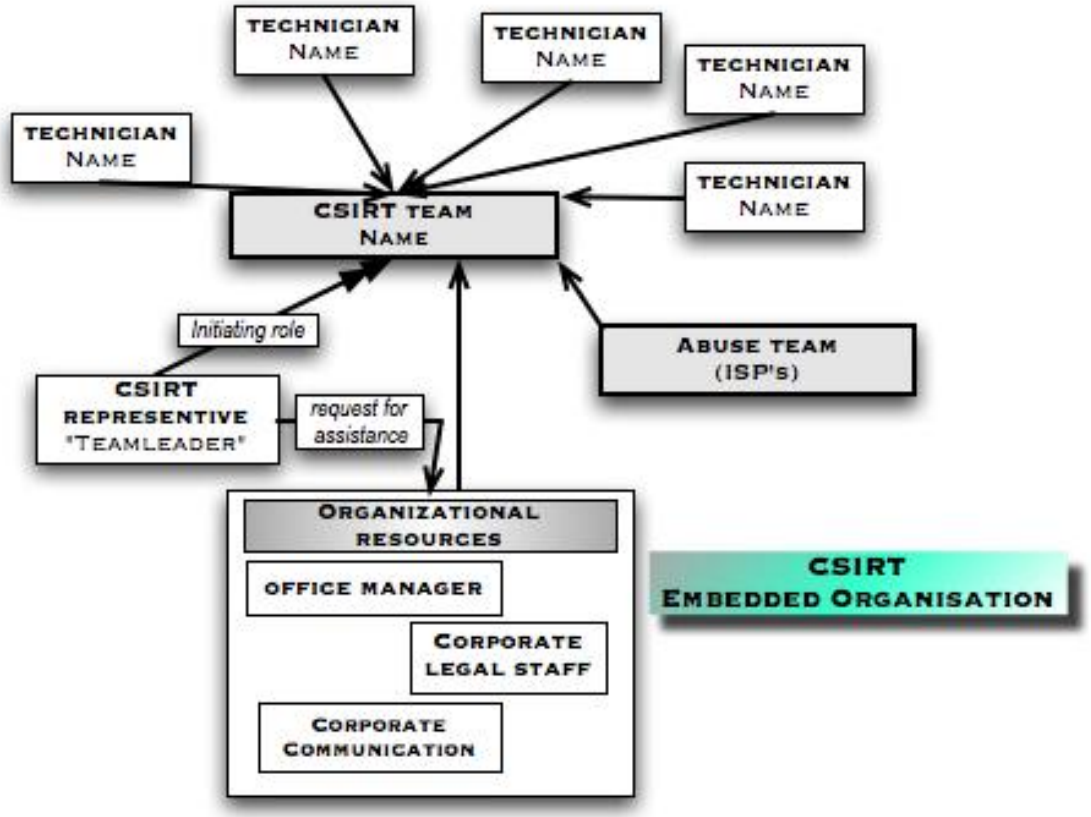


Фиг. 5 Независим бизнес модел

6..2 Внедрен модел

Този модел може да се използва, ако ЦДКСКС е създаден в рамките на съществуваща организация, като, например, се използва съществуващ ИТ отдел. ЦДКСКС се оглавява от ръководител на екипа и той/тя отговаря за дейностите на ЦДКСКС. Ръководителят на екипа събира необходимите технически сътрудници при справянето с кризисни ситуации или работа по дейностите на ЦДКСКС. Той или тя може да поиска съдействие за специализирана поддръжка в рамките на съществуваща организация.

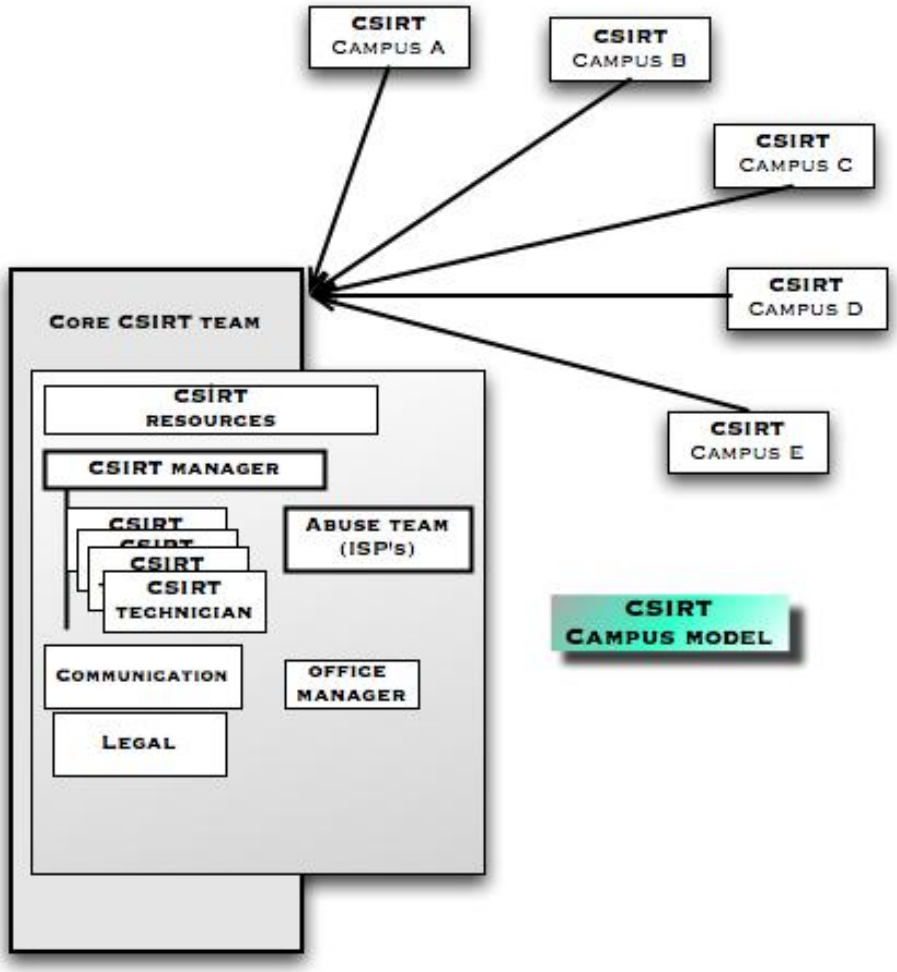
Този модел също може да се адаптира за специфични ситуации, когато те възникнат. В този случай екипът има фиксиран брой служители или отреден еквивалент на пълна заетост (ЕПЗ). Поддръжката срещу злоупотреби за интернет доставчик, например, със сигурност е работа на пълен работен ден за един или (в много случаи) повече от един служител ЕПЗ.



Фиг. 6 Внедрен организационен модел

6..3 Университетски модел

Университетският модел, както предполага името му, е адаптиран най-вече към академичните и научноизследователските ЦДКСКС. Много академични и научноизследователски организации се състоят от различни университети и университетски блокове с различни местонахождения, разпръснати из район или дори из цялата страна (както е в случая с националните изследователски мрежи). Обикновено тези организации са независими една от друга и често поддържат собствен ЦДКСКС. Тези ЦДКСКС обикновено са организирани под шапката на „майка“ или централен ЦДКСКС. Централният ЦДКСКС координира и е единственото контактно звено с външния свят. В много случаи централният ЦДКСКС също предлага централни ЦДКСКС услуги, както и разпространява информация за кризисни ситуации към съответния университетски ЦДКСКС.
Някои ЦДКСКС разпространяват своите централни ЦДКСКС услуги чрез другите университетски ЦДКСКС, като в резултат се постигат намалени режийни разходи за централния ЦДКСКС.



Фиг. 7 Университетски модел

6..4 Доброволен модел

Този организационен модел описва група от хора (специалисти), които се събират, за да предлагат взаимни съвети и подкрепа (и на други) на доброволна основа. Тази общност не е строго организирана и до голяма степен зависи от мотивацията на участниците.
Този модел, например, бе приет от общността WARP[13].

Набиране на подходящи служители

След като се взе решение за услугите и степента на поддръжка, която ще се предлага, и след избирането на организационния модел, следващата стъпка е да се намерят подходящият брой квалифицирани служители за работата.

Почти невъзможно е да се представят точни цифри за броя на необходимите технически сътрудници от тази гледна точка, но следните ключови стойности са се доказали като добър подход:

- за да се предлагат две централни услуги като разпространяването на бюлетин по сигурността, както и справянето с кризисни ситуации - минимум **4** ЕПЗ;

- за пълно обслужване ЦДКСКС в традиционно работно време и поддръжка на системи - минимум от **6 до 8** ЕПЗ

- за пълна заетост със смени 24x7 (2 смени извън традиционното работно време) - минимум от около **12** ЕПЗ.

Тези цифри включват и резерви за случаи на болест, неработни дни и др. Необходимо е и да се направи справка с местните колективни трудови договори. Ако хората работят извън традиционното работно време, това би трябвало да доведе до заплащането на допълнителни суми.

[13] Инициативата WARP http://www.enisa.europa.eu/cert_inventory/pages/04_02_02.htm#12

Следва кратък преглед на ключовите компетенции на техническите експерти за един ЦДКСКС

Компоненти от трудовата характеристика на общите технически служители:

Лични умения

- Гъвкав, креативен дух и умение за работа в екип
- Силни аналитични умения
- Способност за обясняване на сложни технически въпроси на прост език
- Добро чувство за поверителност и работа по процедурния ред
- Добри организаторски умения
- Издръжливост при стрес
- Силни комуникативни умения и умения за писане
- Непредубеденост и желание за учене

Технически умения

- Широки познания в областта на интернет технологиите и протоколите
- Познания за системите Linux и Unix (в зависимост от оборудването на конституентите)
- Познания за системите Windows (в зависимост от оборудването на конституентите)
- Познания за оборудването на мрежова инфраструктура (рутер, контролери, DNS, Proxy, пощенски сървър и др.)
- Познания за интернет приложения (SMTP, HTTP(и), протокол за трансфер на файлове (FTP), telnet, SSH и др.)
- Познания за заплахите за сигурността (атака за отказ на услуга, фишинг, Defacing, „подслушване“ и др.)
- Познания за оценка на риска и практическо реализиране

Допълнителни умения

- Желание за работа на смени 24x7 или за дежурства на повикване (в зависимост от модела на обслужване)
- Максимално разстояние за пътуване (в случай на спешен случай в офиса, максимално време за пътуване)
- Степен на образование
- Опит в работата в сферата на ИТ сигурността

Примерен ЦДКСКС (стъпка 4)
Определяне на бизнес план **Финансов модел** Поради факта, че компанията развива е-бизнес 24x7 и има ИТ отдел 24x7, се взе решение за предлагане на пълно обслужване в рамките на традиционното работно време и дежурства на повикване извън работното време. Услугите ще бъдат предоставяни безплатно за конституентите, но възможността за предлагане на услуги на външни клиенти ще бъде преценена по време на пилотната фаза за оценка. **Модел за приходи**

По време на началната и пилотна фаза ЦДКСКС ще бъде финансиран чрез компанията майка. По време на пилотната фаза за оценка ще бъде обсъден въпросът за допълнително финансиране, включително и възможността да се продават услуги на външни клиенти.

Организационен модел

Организацията майка е малка компания, така че бе избран внедреният модел.

В работно време персонал от трима души ще осигурява централни услуги (разпространение на бюлетини по сигурността и справяне/координация при кризисни ситуации).

ИТ отделът на компанията вече е наел хора с подходящи умения. Сключва се споразумение с отдела, така че при необходимост новият ЦДКСКС може да поиска помощ на временна основа. Също така може да се използва втората линия от техните технически сътрудници на повикване.

Ще има централен екип на ЦДКСКС с четири члена на пълна заетост и пет допълнителни членове на екипа на ЦДКСКС. Един от тях също е на разположение с плаващи смени.

Служители

Ръководителят на екипа на ЦДКСКС има опит в сигурността и в 1-ва и 2-ра степен на поддръжка и е работил в областта на управление на устойчивостта при кризи. Другите трима членове на екипа са специалисти по сигурността. Членовете на екипа на ЦДКСКС на непълен работен ден от ИТ отдела са специалисти по своята част от инфраструктурата на компанията.

Използване и оборудване на офиса

Оборудването и използването на офис пространството и физическата сигурност са доста обширни теми и следователно не може да се представи изчерпателно описание в настоящия документ. Тази глава има за цел да направи кратък преглед на темата.

Повече информация за физическата сигурност може да се намери на:
http://en.wikipedia.org/wiki/Physical_security
http://www.sans.org/reading_room/whitepapers/physcial/
http://www.infosyssec.net/infosyssec/physfac1.htm

„Укрепване на сградата“

Тъй като ЦДКСКС често борави с много деликатна информация, добра практика е да се позволи на екипа да поеме контрол върху физическата сигурност на офиса. Това до голяма степен ще зависи от съществуващите удобства и инфраструктура и действащата политика по информационна сигурност на компанията майка.

Правителствата, например, работят със схеми за класификация и са много стриктни по отношение на начина на работа с поверителна информация. Проучете въпроса за месните правила и политики във Вашата компания или институция.

Обикновено новият ЦДКСКС зависи от съдействието на компанията майка, за да се запознае с местните правила, политики и други правни въпроси.

Изчерпателното описание на цялото оборудване и мерки за сигурност, от които ще има нужда, са извън обхвата на настоящия документ. Въпреки това по-долу ще намерите списък с основните изисквания към Вашия ЦДКСКС:

Общи правила за сградата
- Използвайте устройство за достъп.
- Поне офисът на ЦДКСКС трябва да е достъпен единствено за служителите на ЦДКСКС.
- Наблюдавайте офисите и входовете с камери.
- Архивирайте поверителната информация в заключени шкафове или сейф.
- Използвайте сигурни ИТ системи.

Общи правила за ИТ оборудване
- Използвайте оборудване, което служителите могат да поддържат.
- Укрепете всички системи.
- Обновявайте и актуализирайте всички системи преди да ги свържете към интернет.
- Използвайте софтуер за сигурност (защитни стени, многократни антивирусни скенери, програми против шпионски софтуер и др.).

Поддържане на комуникационните канали
- Уебсайт, достъпен за широката общественост.
- Затворен сектор за членове на уебсайта.
- Уеб формуляри за докладване на кризисни ситуации.
- Електронна поща (PGP / GPG / S/MIME поддръжка).
- Софтуер за мейлинг листа.
- Обявете специален телефонен номер на разположение на конституентите:
  - телефон
  - факс
  - SMS

Система(и) за проследяване на данни
- База данни с контакти с подробности за членове на центъра, на други центрове и др.
- Инструменти за управлението на отношенията с клиенти.
- Тикет система за справяне с кризисни ситуации.

Използвайте „корпоративния стил“ от самото начало за
- Оформлението на стандартни електронни писма и на бюлетина по сигурността.
- „Старомодните“ писма на хартия.
- Месечни или годишни доклади.
- Формуляр за съобщаване за кризисни ситуации.

Други въпроси
- Предвидете независима система за комуникации в случай на атаки.
- Предвидете резерви при интернет връзките.

За повече информация относно специфичния инструментариум на ЦДКСКС вижте глава *8.5 „Наличен инструментариум за ЦДКСКС“.*

Разработване на политика в областта на информационната сигурност

В зависимост от вида ЦДКСКС, ще следвате пригодена политика по информационната сигурност. Освен да описва желаното състояние на оперативните и административни процеси и процедури, тази политика трябва да е съгласувана със законодателството и стандартите, по-специално по отношение на материалната отговорност на ЦДКСКС. Обикновено ЦДКСКС е обвързан с националните закони и нормативни актове, които често се прилагат в контекста на европейското законодателство (обикновено директиви) и други международни споразумения. Стандартите не винаги са с пряк задължителен характер, но може да се нареждат или препоръчват от закони и нормативни актове.
По-долу е представен кратък списък с възможни закони и политики.

Национални
- Различни закони относно информационните технологии, телекомуникациите и медиите
- Закони за защита на данните и правото на неприкосновеност на личния живот
- Закони и нормативни актове за съхранение на данни
- Законодателство за финанси, счетоводство и корпоративно управление
- Етични кодекси за корпоративно управление и управление на ИТ

Европейски
- Директива относно електронните подписи (1999/93/ЕИО)
- Директивите относно личните данни (1995/46/ЕО) и правото на неприкосновеност на личния живот в сектора на електронните комуникации (2002/58/ЕО)
- Директиви относно електронните съобщителни мрежи и услуги (2002/19/ЕО – 2002/22/ЕО)
- Директиви относно корпоративно право (например 8-ма директива по корпоративно право)

Международни
- Споразумението Базел II (специално по отношение на управление на операционен риск)
- Конвенция за киберпрестъпленията на Съвета на Европа
- Конвенция за защита на правата на човека на Съвета на Европа (член 8 относно правото на зачитане на личния живот)
- Международни счетоводни стандарти (МСС, те до известна степен определят контрола в областта на ИТ).

Стандарти
- Британски стандарт BS 7799 (информационна сигурност)
- Международни стандарти ISO2700x (системи за управление на информационната сигурност)
- Германски IT-Grundschutzbuch, Френски EBIOS и други национални версии

За да определите дали Вашият ЦДКСКС действа съгласно националното и международно законодателство, моля консултирайте се с юрист.
Най-основните въпроси, на които трябва да се даде отговор при Вашата политика за боравене с информация са:

- Как се „маркира“ или „класифицира“ входящата информация?
- Как се работи с информацията, и по-специално по отношение на ограничения достъп?
- Какви съображения са приети за разкриването на информация, по-специално ако информация, свързана с кризисна ситуация е предадена на други центрове или звена?
- Има ли правни съображения, които да се вземат предвид по отношение на работата с информация?
- Следвате ли определена политика относно използването на криптография за защита на ограничения достъп и интегритета в архиви и/или при съобщаването на данни, особено по електронна поща?
- Тази политика включва ли условия за правни граници като криптосистема с ключ в трета страна или налагане на разшифроване в случай на съдебни процеси?

Примерен ЦДКСКС (стъпка 5)

Оборудване и местонахождение на офиса

Поради факта, че компанията майка вече разполага с ефективна физическа сигурност, новият ЦДКСКС е добре подсигурен в този аспект.
Осигурява се така наречената „военна стая“, за да се улесни координацията в случай на извънредна ситуация. Закупува се сейф за кодирани материали и деликатни документи. Открива се отделна телефонна линия, която включва и централа за улесняване на горещата линия през работното време и дежурствата „на повикване“ със същия телефонен номер на мобилен телефон извън традиционното работно време.

Също могат да се използват съществуващото оборудване и корпоративен уебсайт за обявяване на информация, свързана с ЦДКСКС. Инсталира се и се поддържа мейлинг листа с ограничен сектор за комуникация между членовете на центъра и с другите центрове. Цялата информация за контакти със служители се съхранява в база данни, като в сейфа се пази разпечатано копие.

Регулиране

Поради факта, че ЦДКСКС е внедрен в компания със съществуваща политика по информационната сигурност, съответните политики за ЦДКСКС са установени с помощта на юрист от компанията.

Търсене на сътрудничество между ЦДКСКС и възможни национални инициативи

Съществуването на други инициативи за ЦДКСКС и голямата необходимост от сътрудничество между тях вече няколко пъти бе спомената в този документ. Добра практика е да се свържете с други ЦДКСКС колкото се може по-скоро, за да поддържате необходимата връзка със средите на ЦДКСКС. Обикновено другите ЦДКСКС са готови да помогнат на новосъздадени центрове да започнат работа.

„Регистърът на дейности на CERT в Европа“[14] на ЕАМИС е много добро начало за търсене на други ЦДКСКС в страната или на национални дейности за сътрудничество в областта на ЦДКСКС.
За да получите подкрепа за намиране на подходящ източник на информация за ЦДКСКС, свържете се с експертите на ЕАМИС по въпросите на ЦДКСКС: CERT-Relations@enisa.europa.eu

[14] Регистър на ЕАМИС: http://www.enisa.europa.eu/cert_inventory

Следва преглед на дейностите на общността на ЦДКСКС. Моля направете справка с *Регистъра* за по-изчерпателно описание и по-задълбочена информация.

Европейска инициатива за ЦДКСКС

Работна група по ЦДКСКС (TF-CSIRT[15])

Работната група по ЦДКСКС подпомага съвместната работа между центровете за действие при кризисни ситуации в компютърната сигурност (ЦДКСКС) в Европа. Основните цели на тази работна група са да осигури форум за обмен на опит и знания, да установи пилотни услуги за европейската общност на ЦДКСКС и да помогне за създаването на нови ЦДКСКС.

Основните цели на работната група са:

- да осигури форум за обмен на опит и знание;
- да установи пилотни услуги за европейската общност на ЦДКСКС;
- да поощри общи стандарти и процедури за действие при кризисни ситуации в сигурността;
- да помогне при създаването на нови ЦДКСКС и при обучението на служители на ЦДКСКС;
- дейностите на РГ-ЦДКСКС са съсредоточени върху Европа и съседните държави съгласно техническото задание, одобрено от Технически комитет TERENA на 15 септември 2004 г.

Глобална инициатива за ЦДКСКС

FIRST[16]

FIRST е първата организация и признат глобален лидер в действията при кризисни ситуации. Членството във FIRST позволява на екипите за действие при кризисни ситуации да реагират по-ефективно при кризисни ситуации за сигурността – реактивни, както и проактивни мерки.

FIRST събира различни центрове за действие при кризисни ситуации в компютърната сигурност от правителствени, търговски и образователни организации. FIRST има за цел да насърчи сътрудничеството и координацията при предотвратяването на кризисни ситуации, да стимулира бързото реагиране на кризисни ситуации и да поощри обмена на информация сред отделните членове на общността.

Освен мрежата на доверието, която изгражда в глобалната общност за действие при кризисни ситуации, FIRST също така предлага услуги с добавена стойност.

Примерен ЦДКСКС (стъпка 6)
Търсене на сътрудничество
Като се използва регистъра на ЕАМИС, бързо бяха открити и бе установен контакт с някои ЦДКСКС в същата страна. Бе уредено посещение на място в един от тях за

[15] TF-CSIRT: http://www.enisa.europa.eu/cert_inventory/pages/04_01_02.htm#06

[16] FIRST: http://www.enisa.europa.eu/cert_inventory/pages/05_02.htm

новопостъпилия ръководител на екипа. Той се запозна с националните дейности в областта на ЦДКСКС и присъства на срещата.
Тази среща беше повече от полезна за събирането на примери за работещи методи и подкрепа от няколко други центъра.

7 Популяризиране на бизнес плана

Досега сме предприели следните стъпки:

1. Разбрахме какво представлява ЦДКСКС и какви ползи може да осигури.
2. В кой сектор новият център ще предлага услугите си?
3. Какви видове услуги ЦДКСКС може да предлага на конституентите си.
4. Анализ на средата и на конституентите.
5. Определяне на мисията на центъра.
6. Разработване на бизнес план.
   а. Определяне на финансовия модел.
   б. Определяне на организационната структура.
   в. Начало на набирането на персонал.
   г. Използване и оборудване на офиса.
   д. Разработване на политика по информационната сигурност
   е. Търсене на партньори за сътрудничество.

>>Следващата стъпка е гореспоменатото да се включи в плана на проекта и да се започне работа!

Добро начало за определянето на Вашия проект е създаването на бизнес казус. Този бизнес казус ще се използва за основа на плана на проекта, също така при кандидатстване за подкрепа от мениджмънта и за получаване на бюджет или други ресурси.

Оказа се, че постоянното докладване пред ръководството е от полза, за да се поддържа високо ниво на информираност по проблемите на ИТ сигурността и постоянна подкрепа за собствения ЦДКСКС.

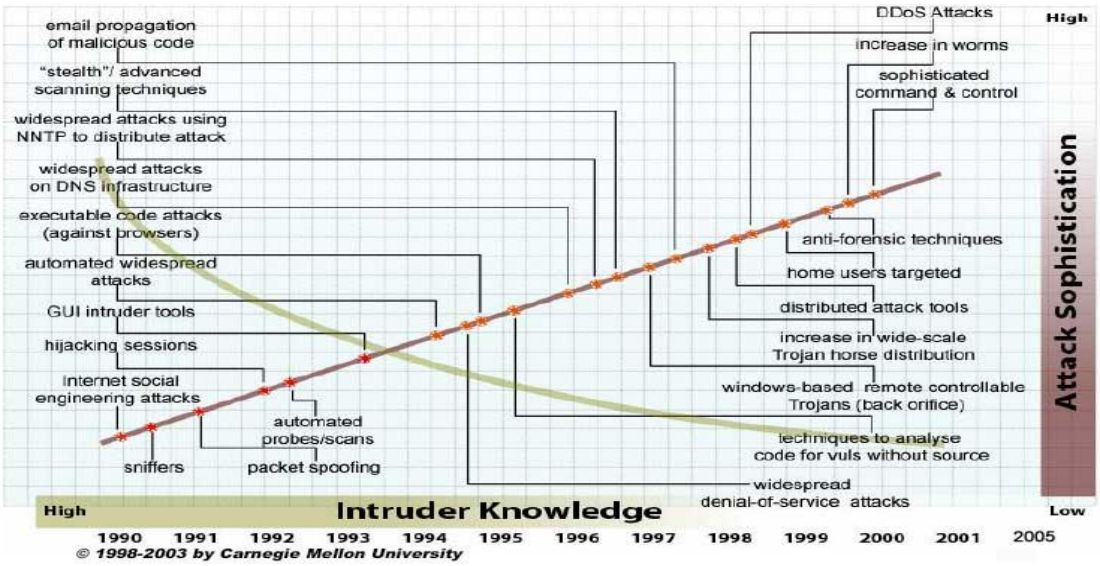
Създаването на бизнес казус започва с анализ на проблемите и възможностите, като се използва модел за анализ, описан в глава *5.3 „Анализ на конституентите“,* и се търсят тесни контакти с потенциални конституенти.

Както вече бе описано, има много въпроси за обмисляне при стартирането на ЦДКСКС. Най-добре е да се пригоди гореспоменатият материал към нуждите на ЦДКСКС по време на развитието му.

При докладване пред ръководството добра практика е собственият казус да се представя с колкото се може по-актуализирани данни, като се ползват наскоро публикувани статии във вестници или Интернет и се обяснява защо услугите на ЦДКСКС и вътрешната координация при кризисни ситуации е изключително важна за сигурността на бизнес активите. Също така е необходимо да се разясни защо

единствено постоянната подкрепа на дейностите по ИТ сигурността води до стабилен бизнес, особено за компания или институция, която зависи от ИТ.

(В една знаменита фраза Брус Шнайер стига до същността на въпроса: *„Сигурността не е продукт, а процес“*[17]*!)*
Следната графика, осигурена от CERT/CC, е известен инструмент за илюстриране на проблеми в сигурността:



Фиг. 8 Познанията на нападателя в сравнение със сложността на атаката (източник CERT-CC[18]*)*

Тя илюстрира тенденциите в ИТ сигурността, и по-специално намаляването на необходимите умения за извършване на значително по-усложнени атаки.

Друга точка, която трябва да се спомене, е постоянното свиване на пролуката от време между излизането на актуализиран за уязвимости софтуер и началото на атаки срещу него.

Софтуерна кръпка -> Експлойт		**Ниво на разпространение**	
Nimda:	11 месец	Code red:	дни
Slammer:	6 месец	Nimda:	часове
Nachi:	5 месец	Slammer:	минути
Blaster:	3 седмици		
Witty:	1 ден (!)		

Събраната информация за кризисни ситуации, потенциални подобрения и направени поуки е подходяща за представяне.

[17] Брус Шнайер: http://www.schneier.com/

[18] http://www.cert.org/archive/pdf/info-sec-ip.pdf

Описание на бизнес планове и механизми за управление

Презентацията пред мениджърите, която включва и популяризирането единствено на ЦДКСКС, не представлява бизнес казус, но ако се направи по подходящ начин, в повечето случаи ще доведе до подкрепа от мениджърите за ЦДКСКС. От друга страна бизнес казусът не трябва да бъде разглеждан просто като упражнение по управление, а трябва също така да се използва за комуникация с екипа и конституентите. Терминът бизнес казус може да звучи малко комерсиално и далеч от ежедневната практика на ЦДКСКС, но осигурява добър фокус и насоки при създаването на ЦДКСКС.

Отговорите на следните въпроси могат да се използват за изготвянето на добър бизнес казус (дадените примери са хипотетични и се използват единствено за илюстрация. „Реалните“ отговори в голяма степен зависят от „реалните“ обстоятелства.)

- Какъв е проблемът?
- Какво бихте искали да постигнете с Вашите конституенти?
- Какво ще се случи, ако не предприемете нищо?
- Какво ще се случи, ако предприемате действия?
- Колко ще струва?
- Какво ще се спечели?
- Кога ще започне и кога ще приключи?

Какъв е проблемът?
В повечето случаи идеята да се създаде ЦДКСКС възниква, когато ИТ сигурността е жизненоважна част от централния бизнес на компания или институция и когато ИТ сигурността се превърне в риск за бизнеса, което прави работата по сигурността нормална бизнес операция.

Повечето компании или институции имат отдел за редовна поддръжка или техническа помощ, но в много случаи кризисните ситуации в сигурността не се третират в достатъчна степен и не по структуриран начин, както би следвало да бъде. В много случаи работата по кризисната ситуация в сигурността изисква специални умения и внимание. Прилагането на по-структуриран подход също е благотворно и ще намали бизнес рисковете и щетите за компанията.

В много случай проблемът е, че липсва координация и съществуващите познания не се използват да справяне с кризисни ситуации, което би предотвратило появата им в бъдеще и би предотвратило възможни финансови загуби и/или вреди за репутацията на институцията.

Какво целите да постигнете с конституентите си?
Както бе обяснено по-рано Вашият ЦДКСКС ще обслужва конституентите си и ще им помага при разрешаването на кризисни ситуации и проблеми за ИТ сигурността. Повишаването на степента на познания за ИТ сигурността и постигането на култура на информираност за сигурността са допълнителни цели.

Тази култура води до проактивни и предпазни мерки от самото начало и следователно до намаляване на оперативните разходи.

В много случаи въвеждането на тази култура на сътрудничество и съдействие в компания или институция стимулира ефективността като цяло.

Какво ще се случи, ако не предприемете нищо?

Един неструктуриран начин на работа по ИТ сигурността може да доведе до по-големи щети, не само за репутацията на институцията. Финансови загуби и правни последствия могат да са сред другите резултати.

Какво ще се случи, ако се предприеме действие?

Повишава се информираността относно възникването на проблеми със сигурността. Това помага за тяхното по-ефективно решаване и предотвратява бъдещи загуби.

Колко ще струва?

В зависимост от организационния модел, ще струва заплатите на членовете на екипа на ЦДКСКС и организацията, оборудването, инструментариума и софтуерните лицензи.

Какво ще се спечели?

В зависимост от бизнеса и загубите в миналото, ще се спечели повече прозрачност в процедурите и практиките по сигурността, следователно защита на съществени бизнес авоари.

Какви са сроковете?

Вижте *глава 12. „Описание на плана на проекта“* за описанието на примерен план на проекта.

Примери за съществуващи бизнес казуси и подходи

Съществуват няколко примери за бизнес казуси в областта на ЦДКСКС, които заслужават внимание:

- http://www.cert.org/csirts/AFI_case-study.html
  Създаване на ЦДКСКС за финансова институция: Анализ на казус.
  Целта на този документ е да се споделят поуките на финансова институция (наричана в документа AFI), тъй като е разработен и реализиран план за справяне с проблеми на сигурността както и Център за действие при кризисни ситуации в компютърната сигурност (ЦДКСКС)

- http://www.terena.nl/activities/tf-csirt/meeting9/jaroszewski-assistance-csirt.pdf
  Резюме на бизнес казус на CERT POLSKA (презентация в PDF формат).

- http://www.auscert.org.au/render.html?it=2252
  Създаването на екип за действие при кризисни ситуации (ЕДКС) през 90-те години на 20 век може да бъде трудна задача. Много от тези, които създават ЕДКС нямат опит в тази област. Този документ разглежда възможната роля на ЕДКС в общността и въпросите, с които трябва да се решат по време на създаването както и след началото на операциите. Може да е от полза за

действащите ЕДКС, тъй като може да повиши тяхната информираност по въпроси, които преди не са били третирани.

- http://www.sans.org/reading_room/whitepapers/casestudies/1628.php
  Анализ на казус в областта на информационната сигурност, укрепване на предприятие от Roger Benton

  Този практикум е анализ на казус на миграцията на застрахователна компания към система за сигурност, обхващаща цялото предприятие. Целта на практикума е да предложи направление, което да се следва при създаването или миграцията към система по сигурността. Първоначално примитивна онлайн система по сигурността е била единственият механизъм за контрол на достъпа до корпоративни данни. Имало е голяма степен на незащитеност – липсвал е контрол на интегритета извън онлайн средата. Всеки с основни умения по програмиране е могъл да добави, промени и/или изтрие данни за производствените процеси.

- http://www.esecurityplanet.com/trends/article.php/10751_688803
  Стратегия по електронна сигурност на Marriott: сътрудничество между бизнеса и ИТ

  Опитът на Chris Zoladz от Marriott International Inc - сигурността на е-бизнеса е процес, а не проект. Това е посланието на Zoladz, отправено на последната конференция и изложение по електронна сигурност в Бостън, спонсорирана от Intermedia Group. Като вицепрезидент по информационната сигурност на Marriott, Zoladz докладва чрез правния отдел, въпреки че не е юрист. Неговата функция е да идентифицира къде се съхранява най-ценната бизнес информация на Marriot и как тя се движи в рамките и извън компанията. В Marriott отделна отговорност, дефинирана за техническата инфраструктура на сигурността, се носи от архитекта по ИТ сигурността.

Примерен ЦДКСКС (стъпка 7)
Популяризиране на бизнес плана Бе взето решение да се съберат факти и цифри за историята на компанията. Това е повече от полезно за статистически преглед на ситуацията с ИТ сигурността. Събирането трябва да продължи и когато ЦДКСКС вече е създаден и работи, за да се актуализира статистиката. Свързахме се с други национални ЦДКСКС и имаше допитване до тях за техните бизнес казуси. Те осигуриха подкрепа за събирането на презентации с информация относно последните събития в областта на кризисните ситуации за ИТ сигурността и относно разходите за кризисните ситуации. В представения случай на примерен ЦДКСКС не съществува належаща нужда да се убедят мениджърите в значимостта на ИТ сферата и затова не бе трудно да се даде зелена светлина за първата стъпка. Бяха изготвени бизнес казус и план на проекта, включващи оценка на разходите по създаване и разходите за операции.

8 Примери за оперативни и технически процедури (работни потоци)

Досега сме предприели следните стъпки:

1. Разбрахме какво представлява ЦДКСКС и какви ползи може да осигури.
2. В кой сектор новият център ще предлага услугите си?
3. Какви видове услуги ЦДКСКС може да предлага на конституентите си.
4. Анализ на средата и на конституентите.
5. Определяне на мисията на центъра.
6. Разработване на бизнес план.
   а. Определяне на финансовия модел.
   б. Определяне на организационната структура.
   в. Начало на набирането на персонал.
   г. Използване и оборудване на офиса.
   д. Разработване на политика по информационната сигурност
   е. Търсене на партньори за сътрудничество.
7. Популяризиране на бизнес план.
   а. Получаване одобрение за бизнес казус.
   б. Включване на всичко в план за проекта.

>> Следващата стъпка е: въвеждане в действие на ЦДКСКС

Доброто определяне на работните потоци на място ще подобри качеството и необходимото време за кризисна ситуация или случай на уязвимост.

Както бе описано в показаните таблици, примерният ЦДКСКС ще предлага основните централни ЦДКСКС услуги.

- Сигнали и предупреждения
- Справяне с кризисни ситуации
- Съобщения

Тази глава предлага примери за работни потоци, които описват ключовите дейности на ЦДКСКС. Тази глава съдържа също така сведения относно събирането на информация от различни източници, като се проверява нейната приложимост и автентичност и се преразпределя към конституентите. И най-накрая тази глава съдържа примери за най-основните процедури и специфичен инструментариум на ЦДКСКС.

Оценка на инсталационната база на конституентите

Първата стъпка е да се направи обзор на ИТ системите, инсталирани при Вашите конституенти. По този начин ЦДКСКС може да оцени приложимостта на получената информация и да я филтрира преди преразпределянето, така че конституентите да не са затрупани с информация, която е по същество ненужна за тях.

Добра практика е да се започне просто, например с използването на документ в Excel като следния:

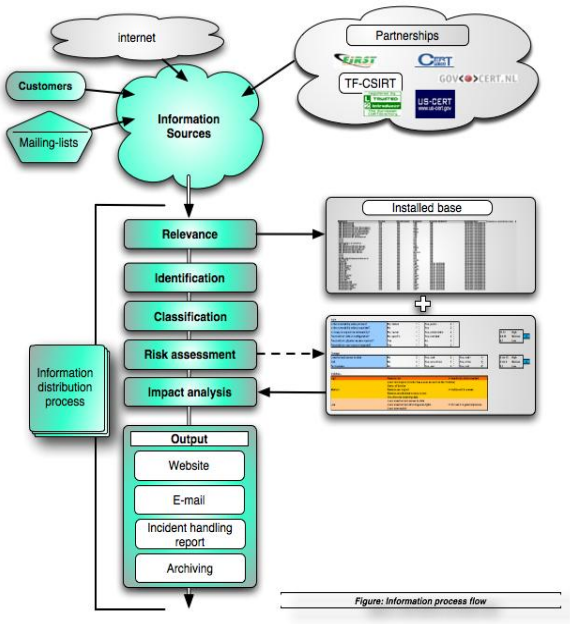
Категория	Приложение	Софтуерен продукт	Версия	OS	Версия OS	Конституент
Компютър	Office	Excel	x-x-x	Microsoft	XP-prof	A
Компютър	Браузър	IE	x-x-	Microsoft	XP-prof	A
Мрежа	Рутер	CISCO	x-x-x	CISCO	x-x-x-	B
Сървър	Сървър	Linux	x-x-x	L-distro	x-x-x	B
Услуги	Уеб сървър	Apache		Unix	x-x-x	B

Когато филтърът функционира в Excel, е много лесно да изберете подходящия софтуер и да видите кой конституент какъв вид софтуер използва.

Генериране на сигнали, предупреждения и съобщения

Генерирането на сигнали, предупреждения и съобщения следва едни и същи работни потоци:

- Събиране на информация
- Оценка на информацията относно приложимост и източник
- Оценка на риска въз основа на събраната информация
- Разпространение на информацията



Фиг. 9 Поток на информационния процес

В следващите параграфи този работен поток ще бъде описан с повече подробности.

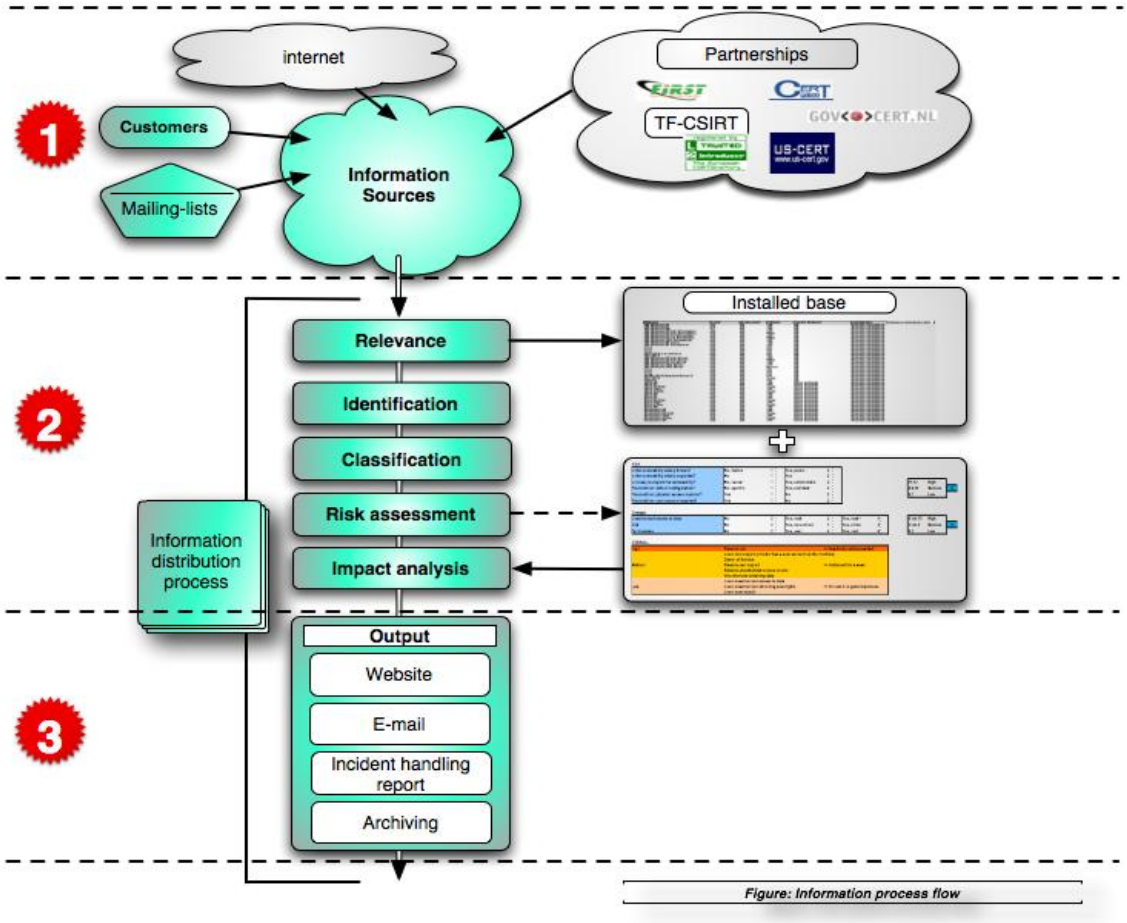


Figure: Information process flow

Стъпка 1: Събиране на информация относно уязвимостта.

Обикновено има два основни типа информационни източници, които допринасят с входяща информация за услугите.

- Информация относно уязвимостта на (Вашите) ИТ системи
- Доклади за кризисни ситуации

В зависимост от вида на бизнеса и ИТ инфраструктурата съществуват много обществено достъпни източници и такива с ограничен достъп с информация за уязвимостта:

- Обществени и затворени мейлинг листи
- Информация за уязвимостта на продукта от дистрибутора
- Уебсайтове
- Информация в Интернет (Google, др…)
- Публично-частни партньорства, които осигурят информация за уязвимостта (FIRST, TF-CSIRT, CERT-CC, US-CERT….)

Цялата тази информация допринася за степента на запознатост със специфичните уязвимости в ИТ системите.

Както бе вече заявено, съществуват много добри и лесно достъпни източници на информация за сигурността, налични в интернет. Временната работна група на ЕАМИС „CERT услуги“ за 2006 г. изготви по-изчерпателен списък за периода на писане, който се предполага, че представя ситуацията в края на 2006 г. [19].

Стъпка 2: Оценка на информацията и оценка на риска

Тази стъпка ще доведе до анализ на въздействието на специфична уязвимост върху ИТ инфраструктурата на конституентите.

Идентификация
Входящата информация за уязвимостта винаги трябва да бъде идентифицирана от нейния източник и трябва да се определи дали източникът е меродавен преди да се даде каквато и да е информация на конституентите. В противен случай хората може да получат фалшив сигнал, което да доведе до ненужно объркване на бизнес процесите и в крайна сметка да навреди на репутацията на ЦДКСКС.

[19] Временна работна група „Услуги CERT“:
http://www.enisa.europa.eu/pages/ENISA_Working_group_CERT_SERVICES.htm

Следната процедура илюстрира идентифицирането на автентичността на послание:

Процедура за начин на идентифициране на автентичността на послание и неговия източник

Общ списък за проверка

1. Източникът известен ли е и регистриран ли е като такъв?
2. Информацията идва ли по редовен канал?
3. Съдържа ли „странна“ информация, която изглежда погрешна?
4. Следвайте интуицията си, ако имате съмнение за информация, не действайте, а проверете отново!

Източници от електронната поща

1. Адресът на източника познат ли е на организацията и включен ли е в списъка с източници?
2. PGP подписът правилен ли е?
3. Когато се съмнявате, проверявайте пълната заглавна част на посланието.
4. Когато се съмнявате, използвайте „nslookup“ или „dig“, за да проверите домейна на подателите[20].

Източници от WWW

1. Проверете сертификатите на браузъра, когато се свързвате със сигурен уебсайт (https ://).
2. Проверете източника по отношение на съдържание и валидност (технически).
3. Когато се съмнявате, не следвайте линкове и не сваляйте никакъв софтуер.
4. Когато се съмнявате, използвайте „lookup“ и „dig“ относно домейна и направете „traceroute“.

Телефон

1. Слушайте внимателно за името.
2. Разпознавате ли гласа?
3. Когато се съмнявате, искайте номер на телефона и поискайте да се обадите обратно на събеседника.

Фиг. 10. Пример за процедура по идентифициране на информация.

Приложимост

Изготвеният по-рано преглед на инсталирания хардуер и софтуер може да се използва за филтриране на входящата информация за уязвимости по отношение на нейната приложимост с цел да се намери отговор на въпросите: „ Конституентите използват ли този софтуер?“; „Информацията приложима ли е за тях?“

Класификация

Част от получената информация може да се класифицира или маркира като поверителна (например входящите доклади за кризисни ситуации от други центрове). С цялата информация трябва да се работи в съответствие с искането

[20] Инструменти за проверка на идентичността в CHIHT:
http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

на подателя и собствената Ви политика по информационна сигурност. Добро основно правило е *„Не разпространявайте информация, ако не е ясно, че трябва да се разпространи; когато се съмнявате, попитайте подателя за разрешение да я разпространите.“*

Оценка на риска и анализ на въздействието
Има няколко метода за определяне на риска и въздействието на (потенциална) уязвимост.

Рискът е дефиниран като потенциална възможност уязвимостта да бъде използвана. Има няколко важни фактора (измежду други):

- Уязвимостта добре позната ли е?
- Уязвимостта широкоразпространена ли е?
- Лесно ли е да се използва уязвимостта?
- Възможно ли е да се използва уязвимостта от разстояние?

Всички тези въпроси дават ясна представа за сериозността на уязвимостта.
Много лесен начин на калкулиране на риска е следната формула:

Въздействие = Риск X потенциална Вреда

Потенциалната вреда може да се изразява в

- Неоторизиран достъп до данни
- Отказ на услуга (DOS)
- Получаване или удължаване на разрешения

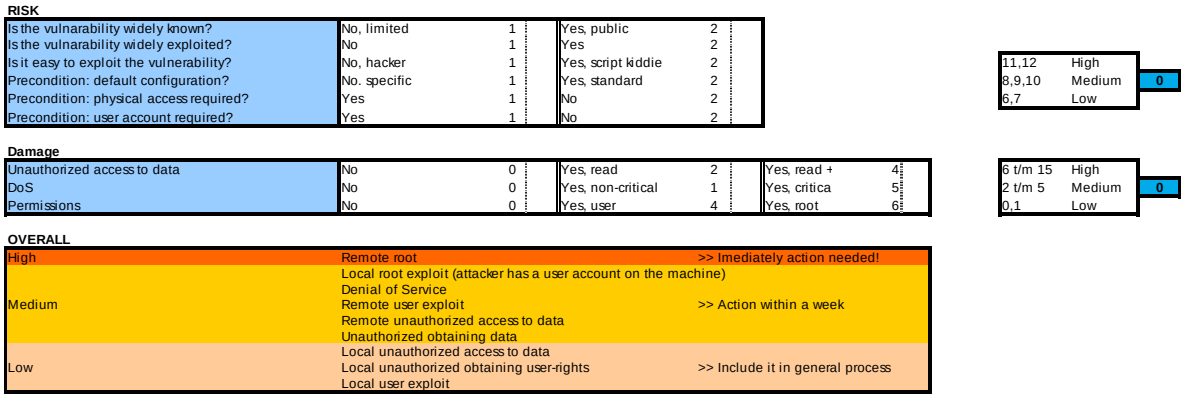
(За по-подробни схеми за класификация, моля вижте края на тази глава).

С отговорите на тези въпроси, може да се добави цялостна класация към бюлетина по сигурността, като се дава информация за потенциалния риск и вреда. Често се използват прости термини като НИСКА, СРЕДНА и ВИСОКА степен.

Други, по-подробни схеми за оценка на риска са:

Схема за класиране на GOVCERT.NL[21]

Холандският правителствен ЦДКСКС GOVCERT.NL изготви матрица за оценка на риска, която бе разработена в началната фаза на Govcert.nl и все още се актуализира според последните тенденции.



Фиг. 11 Схема за класиране на GOVCERT.NL

Описание на формата на общия бюлетин по сигурността на EISPP[22]

Европейската програма за подпомагане на информационната сигурност (EISPP) е проект, съфинансиран от Европейската комисия по Петата рамкова програма. Проектът EISPP цели да развие европейска мрежа не само за обмен на знания по сигурността, а и за определяне на съдържанието и начините за разпространяване на информация по сигурността към МСП. Като предоставя на европейските МСП необходимите услуги за ИТ сигурността, те ще бъдат поощрени да развият доверието и използването на електронната търговия, което ще доведе до повече и по-добри възможности за нов бизнес. EISPP е пионер във визията на Европейската комисия за сформиране на европейска мрежа на експертни познания в рамките на Европейския съюз.

Форматът на бюлетин по сигурността на DAF (Deutsches Advisory Format)[23]

DAF е инициатива на немския CERT-Verbund и е централен компонент на инфраструктура за изготвяне и обмен на бюлетини по сигурността от различни центрове. DAF е специално разработен за нуждите на немските ЦДКСКС;

[21] Матрица на уязвимостта: http://www.govcert.nl/download.html?f=33

[22] EISPP: http://www.enisa.europa.eu/cert_inventory/pages/04_03.htm#03

[23] DAF: http://www.enisa.europa.eu/cert_inventory/pages/04_03.htm#02

стандартът е разработен и поддържан от CERT-Bund, DFN-CERT, PRESECURE и Siemens-CERT.

Стъпка 3: Разпространение на информацията

ЦДКСКС може да избира между различни методи на разпространение в зависимост от желанията на конституентите и Вашата комуникационна стратегия.

- Уебсайт
- Електронна поща
- Доклади
- Архиви и изследвания

Бюлетините по сигурността, които се разпространяват от ЦДКСКС, винаги трябва да следват една и съща структура. Това ще повиши тяхната яснота и читателят бързо ще намира цялата приложима информация.

Бюлетинът трябва да съдържа поне следната информация:

Заглавие на бюлетина ……
Номер за справка …… **Засегнати системи** **-** …… **-** …… **Свързана OS + версия** …… **Риск** (Висока-Средна-Ниска степен) …… **Въздействие/потенциална вреда** (Висока-Средна-Ниска степен) …… **Външен идентификатор:** (Често срещани възможности за уязвимост и излагане на риск, Идентификатор на бюлетин по уязвимостта) ……
Преглед на уязвимостта …… **Въздействие** …… **Решение** …… **Описание (подробности)** …… **Приложение** ……

Фиг. 12 Примерна схема на бюлетин по сигурността

Вижте глава *10. „Упражнения“* за пълен пример за бюлетин по сигурността.

Справяне с кризисни ситуации

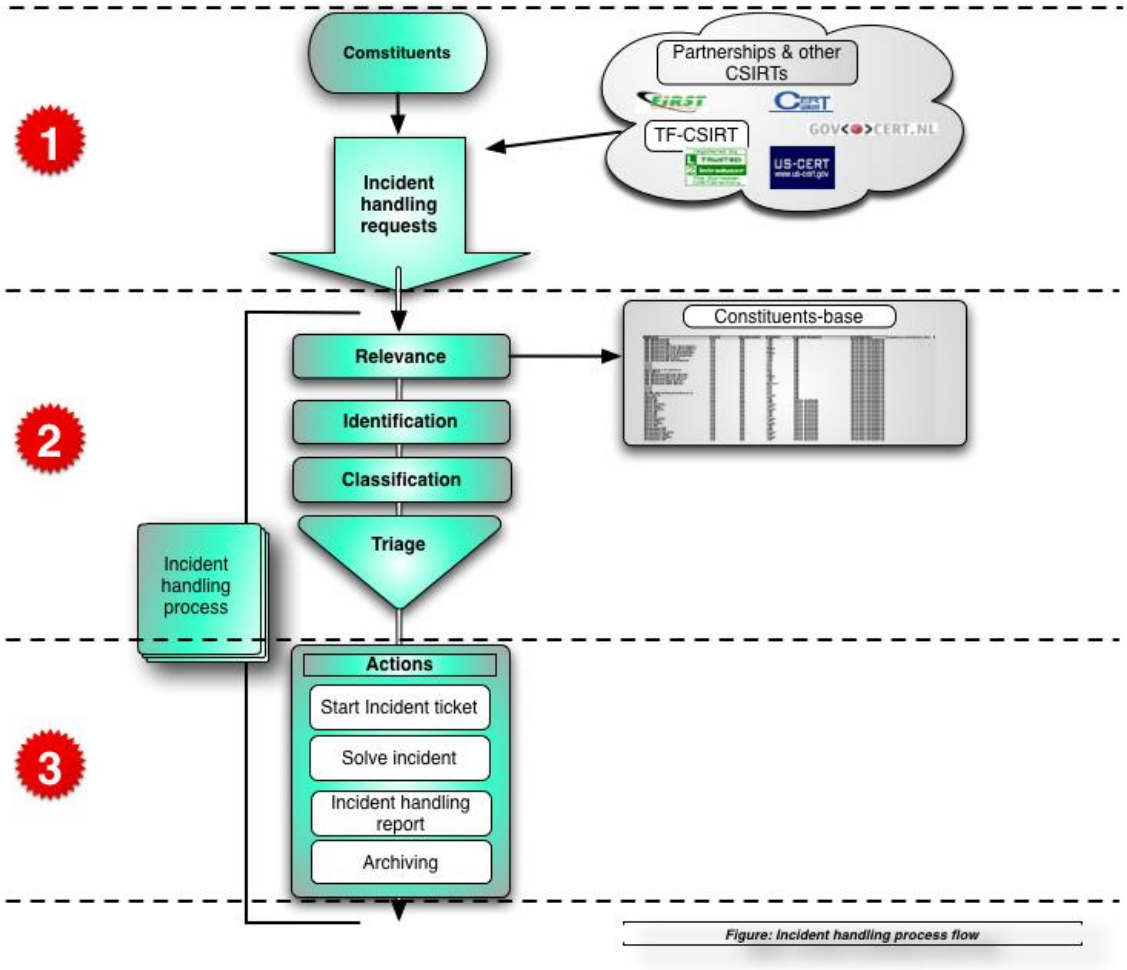
Както бе споменато в увода към настоящата глава, процесът на работа с информация по време на справяне с кризисна ситуация много прилича на този по време на съставянето на сигнали, предупреждения и съобщения. Но частта по събирането на информация обикновено е различна, тъй като нормалният начин за получаване на информация, свързана с кризисни ситуации е или чрез получаване на доклади за кризисни ситуации от конституенти или от други центрове, или чрез получаване на обратна връзка от засегнатите страни по време на процеса на справяне с кризисни ситуации. Обикновено информацията тече (кодирана) по електронна поща; понякога се налага ползването на телефон или факс.

При получаване на информация по телефона добра практика е да се запише всеки отделен детайл веднага или чрез ползването на инструмент за справяне/докладване на кризисни ситуации, или чрез изготвянето на резюме. Необходимо е веднага (преди края на разговора) да се издаде номер на кризисната ситуация (ако досега не съществува такъв за тази кризисна ситуация) и да се уведоми докладчика по телефона (или по електронна поща с изпратено след това резюме) за справка при по-нататъшна комуникация.

Останалата част от тази глава описва основния процес по справяне с кризисни ситуации. Много задълбочен анализ за пълния процес на управление на кризисни ситуации и всички включени работни потоци и под-потоци е достъпен в документацията на CERT/CC „*Определяне на процесите за управление на кризисни ситуации за ЦДКСКС“.* [24].

[24] „Определяне на процесите за управление на кризисни ситуации“: http://www.cert.org/archive/pdf/04tr015.pdf

По същество справянето с кризисни ситуации следва следния работен поток:



Фиг. 13 Поток на процеса по справяне с кризисни ситуации

Стъпка 1: Получаване на доклади за кризисни ситуации

Както бе вече споменато, докладите за кризисни ситуации стигат до ЦДКСКС по няколко канала, най-вече електронна поща, но също така и по телефон или факс.

Както вече бе споменато, добра практика е да се записват всички детайли във фиксиран формат по време на получаване на доклада за кризисната ситуация. По този начин се гарантира, че не е изпусната съществена информация. Следва примерна схема:

ФОРМУЛЯР ЗА ДОКЛАДВАНЕ НА КРИЗИСНИ СИТУАЦИИ

Моля попълнете този формуляр и го изпратете по факс или имейл на: …….
*Редовете, маркирани с * са задължителни.*

Име и организация
1. Име*:
2. Наименование на организацията*:
3. Тип сектор:
4. Държава*:
5. Град:
6. Електронен адрес*:
7. Телефонен номер*:
8. Други:

Засегнат(и) хост(ове)
9. Брой на хостовете:
10. Име на хоста и IP*:
11. Функция на хоста*:
12. Часова зона:
13. Хардуер:
14. Операционна система:
15. Засегнат софтуер:
16. Засегнати файлове:
17. Сигурност:
18. Име на хоста & IP:
19. Протокол/ порт:

Кризисна ситуация
20. Номер за справка ref #:
21. Вид кризисна ситуация:
22. Кризисната ситуация възникна:
23. Това е действаща кризисна ситуация: ДА НЕ
24. Време и начин на откриването ѝ:
25. Известни уязвимости:
26. Подозрителни файлове:
27. Контрамерки:
28. Подробно описание*:

Фиг. 14. Съдържание на доклада за кризисни ситуации

Стъпка 2: Оценка на кризисната ситуация

По време на тази стъпка се проверява автентичността и уместността на докладваната кризисна ситуация и тя се класифицира.

Идентификация
За да се предотвратят всякакви ненужни действия, добър навик е да се проверява дали източникът е надежден и дали е един от Вашите конституенти или конституент на колега от ЦДКСКС. Прилагат се правила, подобни на описаните в глава *8.2 „Генериране на сигнали“.*

Уместност
При тази стъпка проверявате дали искането за справяне с кризисна ситуация произхожда от конституенти на ЦДКСКС и дали докладваната ситуация засяга ИТ системи на конституентите. Ако никое от горните не е налице, докладът се препраща на правилния ЦДКСКС[25].

Класификация
При тази стъпка се подготвя триажът чрез класификация на сериозността на кризисната ситуация. Извън обхвата на този документ е да навлиза в подробности за класификация на кризисните ситуации. Добро начало е да се използва схемата за класификация на случаи за ЦДКСКС (пример за предприятие ЦДКСКС).

Incident Categories
All incidents managed by the CSIRT should be classified into one of the categories listed in the table below.

Incident Category	Sensitivity*	Description
Denial of service	S3	• DOS or DDOS attack.
Forensics	S1	• Any forensic work to be done by CSIRT.
Compromised Information	S1	• Attempted or successful destruction, corruption, or disclosure of sensitive corporate information or Intellectual Property.
Compromised Asset	S1, S2	• Compromised host (root account, Trojan, rootkit), network device, application, user account. This includes malware-infected hosts where an attacker is actively controlling the host.
Unlawful activity	S1	• Theft / Fraud / Human Safety / Child Porn. Computer-related incidents of a criminal nature, likely involving law enforcement, Global Investigations, or Loss Prevention.
Internal Hacking	S1, S2, S3	• Reconnaissance or Suspicious activity originating from inside the Company corporate network, excluding malware.
External Hacking	S1, S2, S3	• Reconnaissance or Suspicious Activity originating from outside the Company corporate network (partner network, Internet), excluding malware.
Malware	S3	• A virus or worm typically affecting multiple corporate devices. This does not include compromised hosts that are being actively controlled by an attacker via a backdoor or Trojan. (See Compromised Asset)
Email	S3	• Spoofed email, SPAM, and other email security-related events.
Consulting	S1, S2, S3	• Security consulting unrelated to any confirmed incident.
Policy Violations	S1, S2, S3	• Sharing offensive material, sharing/possession of copyright material. • Deliberate violation of Infosec policy. • Inappropriate use of corporate asset such as computer, network, or application. • Unauthorized escalation of privileges or deliberate attempt to subvert access controls.
* - Sensitivity will vary depending on circumstances. Guidelines are provided.		

Фиг. 15 Схема за класификация на кризисни ситуации (източник: FIRST)[26]

[25] Инструменти за проверка на идентичност в CHIHT:
http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

[26] Класификация на казуси ЦДКСКС: http://www.first.org/resources/guides/csirt_case_classification.html

Триаж
Триажът е система, използвана от медицински персонал и служителите на спешно отделение за разпределяне на ограничени медицински ресурси, когато броят на ранените, които имат нужда от помощ, надвишава наличните ресурси за осигуряване на помощ, така че да се лекуват възможно най-големия брой пациенти.[27].

CERT/CC предлага следното описание:

Триажът е съществен елемент от всеки капацитет за управление на кризисни ситуации, особено при установените ЦДКСКС. Триажът е част от критичния път на разбирането какво се докладва по време на организацията. Служи за механизъм, чрез който цялата информация се влива в едно контактно звено, което позволява поглед на предприятието върху актуалната дейност и цялостно съотношение на всички докладвани данни. Триажът позволява първоначалната оценка на входящ доклад и го нарежда за по-нататъшна обработка. Също така осигурява място за започване на първоначалната документация и вписване на данни на доклад или искане, ако все още не е започнало в процеса на разкриване.

Функцията на триаж дава моментна снимка на сегашното положение на цялата докладвана дейност – кои доклади са отворени или затворени, кои действия са висящи и колко от всеки тип доклади са получени. Този процес може да помогне за идентифициране на потенциални проблеми по сигурността и да се подреди работата по приоритет. Събраната по време на триажа информация може също така да се използва за създаване на тенденции и статистика на уязвимостта и кризисните ситуации за по-високопоставените мениджъри.[28].

Триаж би трябва да се извършва само от най-опитните членове на екипа, защото изисква задълбочено познаване на потенциалното въздействие на кризисни ситуации върху специфични части на конституентите и способност да се вземе решение кой да бъде подходящият член на екипа, който да работи по тази кризисна ситуация.

[27] Триаж в Уикипедия: http://en.wikipedia.org/wiki/Triage

[28] Определяне на процесите по управление на кризисни ситуации: http://www.cert.org/archive/pdf/04tr015.pdf

Стъпка 3: Действия

Обикновено сортираните кризисни ситуации се нареждат на опашка в системата за справяне с кризисни ситуации, използвана от един или повече специалисти по справяне с кризисни ситуации, които по същество следват следните стъпки.

Първоначален тикет на кризисната ситуация
Тикет-номерът на кризисната ситуация може вече да е изведен в предишна стъпка (например при получаването на доклада за кризисната ситуация по телефона). Ако не е, първата стъпка е да се създаде такъв номер, който ще бъде използван при всяка следваща комуникация относно тази кризисна ситуация.

Жизнен цикъл на кризисната ситуация
Справянето с кризисната ситуация не следва редица стъпки, които в крайна сметка да доведат до решение, а по-скоро следва кръг от стъпки, които се прилагат многократно до крайното разрешаване на кризисната ситуация и всички засегнати страни разполагат с цялата необходима информация. Този кръг, наричан също „Жизнен цикъл на кризисната ситуация“, съдържа процесите

Анализ	Анализират се всички подробности на докладваната кризисна ситуация.
Получаване на информация за контакти	За да може по-нататък да докладва информация, свързана с кризисната ситуация на всички засегнати страни, като други ЦДКСКС, жертви и може би собствениците на системите, с които е злоупотребено за целите на атаката.
Предоставяне на техническа помощ:	Помощ на жертвите за бързо възстановяване от следствията на кризисната ситуация и събиране на повече информация относно атаката.
Координация	Информиране на други засегнати страни като ЦДКСКС, отговарящ за ИТ системата, използвана за атака или други жертви.

Тази структура се нарича „жизнен цикъл“, защото всяка стъпка води до друга, а последната, координационна част, може също да води до нов анализ и цикълът да започне отново. Процесът завършва, когато всички засегнати страни са получили и докладвали цялата необходима информация.

Моля разгледайте наръчника на CERT/CC за ЦДКСКС за по-подробно описание на жизнения цикъл на кризисната ситуация[29].

Доклад за справяне с кризисна ситуация

[29] Наръчник за ЦДКСКС: http://www.cert.org/archive/pdf/csirt-handbook.pdf

Бъдете готови да отговаряте на въпросите на мениджърите относно кризисната ситуация като изготвите доклад. Друга добра практика е да се напише документ (само за вътрешно ползване) относно „извлечените поуки с цел обучение на служителите и предотвратяване на грешки в бъдещите процеси по справяне с кризисни ситуации".

Архивиране
Разгледайте правилата за архивиране, описани по-рано в глава *6.6 „Разработване на политика в областта на информационната сигурност".*

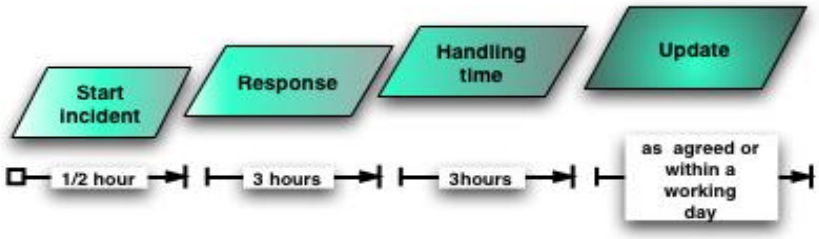
Моля разгледайте приложение раздел *A.1 „За повече информация"* за изчерпателни напътствия относно управлението на кризисни ситуации и жизнения цикъл на кризисната ситуация.

Примерен график за действие

Определянето на сроковете за действие често се пренебрегва, но трябва да бъде част от всяко добре изготвено споразумение за нивото на обслужване между ЦДКСКС и неговите конституенти. Своевременното предоставяне на обратна връзка на конституентите по време на справянето с кризисната ситуация е съществено за собствените отговорности на конституентите както и за репутацията на центъра.

Сроковете за действие трябва да са ясно съобщени на конституентите, за да се избегнат погрешни очаквания. Следният съвсем базов график може да се ползва изходна точка за по-подробно споразумение с конституентите на ЦДКСКС относно нивото на обслужване.

Това е пример за практически график за действие от момента на приемане на искането за помощ.



Фиг. 16. Примерен график за действие

Също добра практика е да се инструктират конституентите за техните собствени срокове за действие, по-специално, кога да се свържат с ЦДКСКС при спешен случай. В много случаи е по-добре да се свържат на ранен етап с техните ЦДКСКС и е добре те да бъдат поощрявани да постъпват така при съмнение.

Наличен инструментариум на ЦДКСКС

Тази глава предлага някои указания за общи инструменти, използвани от ЦДКСКС. Тя дава само примери, повече насоки могат да се намерят в *Clearinghouse of Incident Handling Tools*[30] (CHIHT).

Софтуер за кодиране на имейли и съобщения

- GNUPG http://www.gnupg.org/
  GnuPG е пълното и свободно реализиране на стандарта OpenPGP, определен от RFC2440, от проект на GNU. GnuPG Ви позволява да кодирате и подписвате Вашите данни и комуникация.

- PGP http://www.pgp.com/
  Комерсиална версия

Инструмент за справяне с кризисни ситуации

Управляване на кризисни ситуации и техните последици, като проследявате действията.

- RTIR http://www.bestpractical.com/rtir/
  RTIR е свободна система с отворен код за справяне с кризисни ситуации, замислена като се вземат предвид нуждите на центровете CERT и на други центрове за действие при кризисни ситуации.

Инструменти на управление на взаимоотношенията с клиенти (CRM)

Когато имате много различни конституенти и трябва да проследявате всички уговорени срещи и подробности, от полза може да е база данни за управление на взаимоотношенията с клиенти. Съществуват много различни варианти; ето някои примери:

- SugarCRM http://www.sugarcrm.com/crm/

- Sugarforce (свободна версия с отворен код) http://www.sugarforge.org/

Проверка на информация

- Website watcher http://www.aignes.com/index.htm
  Тази програма наблюдава уебсайтове за актуализации и промени.

- Watch that page http://www.watchthatpage.com/
  Тази услуга изпраща информация по имейл (безплатно както и срещу заплащане) относно промени в уебсайтове.

[30] CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

Намиране на информация за контакти

Намирането на правилните контакти за докладване на кризисни ситуации не е лесна задача. Име няколко източника на информация, които могат да се използват:

- RIPE[31]
- IRT-object[32]
- TI[33]

Освен това CHIHT изброява някои инструменти за намиране на информация за контакти[34].

Примерен ЦДКСКС (стъпка 8)
Установяването на потоци на процеса и оперативни и технически процедури Примерният ЦДКСКС се съсредоточава върху централните ЦДКСКС услуги. • Сигнали и предупреждения • Съобщения • Справяне с кризисни ситуации Центърът разработва процедури, които работят добре и са лесно разбираеми от всеки член на екипа. Примерният ЦДКСКС наема и юрист, за да работи по въпроси в областта на правната отговорност и политиката по информационната сигурност. Центърът въведе някои полезни инструменти и намери полезна информация по оперативните въпроси от дискусии с други ЦДКСКС. Бе направен шаблон за бюлетини по сигурността и за доклади за кризисни ситуации. Центърът използва RTIR за справяне с кризисни ситуации.

[31] RIPE whois: http://www.ripe.net/whois

[32] IRT-object in the RIPE database: http://www.enisa.europa.eu/cert_inventory/pages/04_02_01.htm#08

[33] Trusted Introducer: http://www.enisa.europa.eu/cert_inventory/pages/04_01_03.htm#07

[34] Инструменти за проверка на идентичност в CHIHT:
http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

9 Обучение в ЦДКСКС

Досега сме предприели следните стъпки:

1. Разбрахме какво представлява ЦДКСКС и какви ползи може да осигури.
2. В кой сектор новият център ще предлага услугите си?
3. Какви видове услуги ЦДКСКС може да предлага на конституентите си.
4. Анализ на средата и на конституентите.
5. Определяне на мисията на центъра.
6. Разработване на бизнес план.
   а. Определяне на финансовия модел.
   б. Определяне на организационната структура.
   в. Начало на набирането на персонал.
   г. Използване и оборудване на офиса.
   д. Разработване на политика по информационната сигурност
   е. Търсене на партньори за сътрудничество.
7. Популяризиране на бизнес план.
   а. Получаване одобрение за бизнес казус.
   б. Включване на всичко в план за проекта.
8. Пускане в действие на ЦДКСКС.
   а. Създаване на работни потоци
   б. Реализиране на инструментариума на ЦДКСКС.

>> Следващата стъпка е: обучение на персонала

Тази глава представя двата основни източника на специализирано обучение за ЦДКСКС: курсове към TRANSITS и CERT/CC.

TRANSITS

TRANSITS е европейски проект за подпомагане на създаването на Центрове за действие при кризисни ситуации в компютърната сигурност (ЦДКСКС) и укрепването на съществуващите ЦДКСКС, като се реши проблема с недостига на квалифициран персонал за ЦДКСКС. Към тази цел води предлагането на специализирани курсове за обучение на персонала на (новосъздадено) ЦДКСКС по организационни, оперативни, технически и правни въпроси, засегнати в предлагането на ЦДКСКС услуги.

По-конкретно TRANSITS е:

- разработил, актуализирал и редовно ревизирал материалите за курса по модулно обучение;
- организирал семинари за обучение, на които са раздадени материалите за курса;
- създал условия за участие на служители на (нови) ЦДКСКС на тези семинари за обучение със специален акцент върху участието от новоприсъединилите се държави-членки на ЕС;

- разпространил материалите за курса за обучение и осигурил ползването на резултатите[35].

ЕАМИС улеснява и подкрепя курсовете на TRANSITS. Ако искате да научите как да кандидатствате за курсове, при какви изисквания и разходи, моля свържете се с експертите на ЕАМИС по ЦДКСКС:
CERT-Relations@enisa.europa.eu
В приложението на настоящия документ ще откриете примерни материали за курс!

CERT/CC

Сложността на компютърните и мрежови инфраструктури и предизвикателството за администрирането им усложняват правилното управление на мрежовата сигурност. Мрежовите и системни администратори не разполагат с достатъчно хора и практики по сигурността, за да се защитят срещу атаки и да намалят вредите. В резултат на това се наблюдава нарастващ брой кризисни ситуации за компютърната сигурност.
При възникването на кризисни ситуации за компютърната сигурност, организациите трябва да реагират бързо и ефективно. Колкото по-бързо организацията разпознае, анализира и реагира на кризисна ситуация, толкова по-добре може да ограничат вредите и да се намалят разходите за възстановяване. Създаването на център за действие при кризисни ситуации в компютърната сигурност (ЦДКСКС) е отличен начин за осигуряване на тази способност за бързо действие както и за подпомагане на предотвратяването на бъдещи кризисни ситуации.

CERT-CC предлага курсове за мениджъри и технически персонал в области като: създаване и управление на центрове за действие при кризисни ситуации в компютърната сигурност (ЦДКСКС), реакция и анализ на кризисни ситуации за сигурността и подобряване на мрежовата сигурност. Освен ако не е отбелязано друго, всички курсове се провеждат в Питсбърг, Пенсилвания. Наши служители също така водят курсове по сигурността в Университета „Карнеги Мелън“.

Налични курсове на CERT/CC[36], предназначени за ЦДКСКС

Създаване на Център за действие при кризисни ситуации с компютърната сигурност (ЦДКСКС)
Управление на Център за действие при кризисни ситуации с компютърната сигурност (ЦДКСКС)
Основи на справянето с кризисни ситуации
Напреднал курс за справяне с кризисни ситуации за техническия персонал

В приложението на настоящия документ ще откриете примерни материали за курс!

Примерен ЦДКСКС (стъпка 9)
Обучение на служителите

[35] TRANSITS: http://www.enisa.europa.eu/cert_inventory/pages/04_02_02.htm#11

[36] Курсове на CERT/CC: http://www.sei.cmu.edu/products/courses

Примерният ЦДКСКС реши да изпрати целия технически персонал на следващите организирани курсове на TRANSITS. Отделно ръководителят на екипа посещава курса „Управление на ЦДКСКС“ на CERT/CC.

10 Упражнения: изготвяне на бюлетин по сигурността

Досега сме предприели следните стъпки:

1. Разбрахме какво представлява ЦДКСКС и какви ползи може да осигури.
2. В кой сектор новият център ще предлага услугите си?
3. Какви видове услуги ЦДКСКС може да предлага на конституентите си.
4. Анализ на средата и на конституентите.
5. Определяне на мисията на центъра.
6. Разработване на бизнес план.
   а. Определяне на финансовия модел.
   б. Определяне на организационната структура.
   в. Начало на набирането на персонал.
   г. Използване и оборудване на офиса.
   д. Разработване на политика по информационната сигурност
   е. Търсене на партньори за сътрудничество.
7. Популяризиране на бизнес план.
   а. Получаване одобрение за бизнес казус.
   б. Включване на всичко в план за проекта.
8. Пускане в действие на ЦДКСКС.
   а. Създаване на работни потоци
   б. Реализиране на инструментариума на ЦДКСКС.
9. Обучение на служителите

>> Следващата стъпка е упражнение и подготовка за истинската работа!

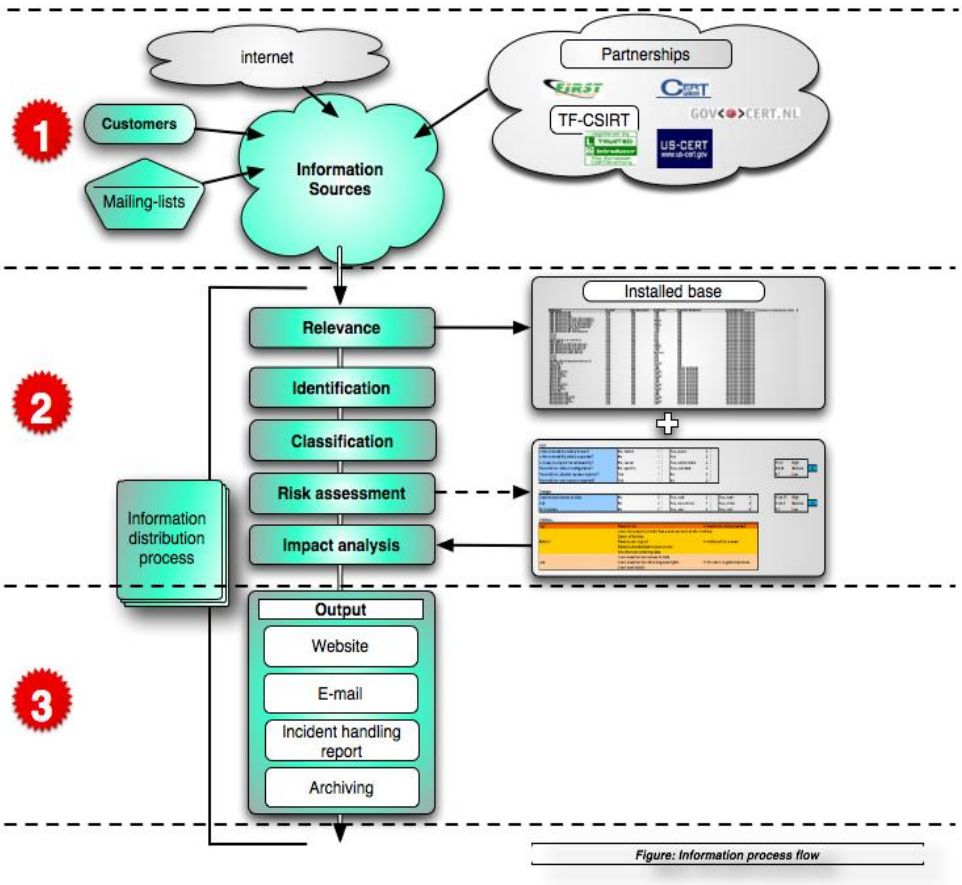
За илюстрация тази глава описва примерно упражнение за всекидневна задача на ЦДКСКС: създаване на бюлетин по сигурността.

Началото бе дадено от следния бюлетин по сигурността, разпространен от Microsoft:

Идентификатор на бюлетина	**Бюлетин по сигурността на Microsoft MS06-042**
Заглавие на бюлетина	**Кумулативна актуализация на защитата за Internet Explorer (918899)**
Изпълнително резюме	Тази актуализация решава някои уязвимости в Internet Explorer, които могат да позволят отдалеченото изпълнение на код.
Оценка на максималната сериозност	Критична
Въздействие на уязвимостта	Отдалечено изпълнение на код
Атакуван	**Windows, Internet Explorer.** За повече информация вижте раздел

софтуер	„Засегнат софтуер и папки за сваляне.“

Този бюлетин на дистрибутора се отнася до наскоро открита уязвимост в Internet Explorer. Дистрибуторът публикува множество корекции на този софтуер за множество версии на Microsoft Windows.
След получаване на информацията за уязвимостта чрез мейлинг листа примерният ЦДКСКС започва с описания в глава *8.2 „Генериране на сигнали, предупреждения и съобщения“* работен поток.



1 Стъпка 1: Събиране на информация за уязвимостта.

Първата стъпка е да се прегледа уебсайта на дистрибутора. Там примерният ЦДКСКС проверява автентичността на информацията и събира повече подробности относно уязвимостта и засегнатите ИТ системи.

Стъпка 2: Оценка на информацията и оценка на риска

Идентификация
Информацията вече е проверена чрез повторна проверка на информацията за уязвимостта, получена по имейл с текста на уебсайта на дистрибутора.

Приложимост
Примерният ЦДКСКС сверява списъка със засегнати системи, открит на уебсайта, със списъка на използваните от конституентите системи. Открива, че поне един от конституентите използва Internet Explorer, така че информацията за уязвимостта е приложима.

Категория	Приложение	Софтуерен продукт	Версия	OS	OS Версия	Конституент
Компютър	Браузър	IE	x-x-	Microsoft	XP-prof	A

Класификация
Информацията е публична, следователно може да се използва и препраща.

Оценка на риска и анализ на въздействието
Отговорите на въпросите показват, че рискът и въздействието са от *висока степен* (оценени от Microsoft като *критични*).

РИСК

Уязвимостта добре известна ли е?	да
Уязвимостта широко разпространена ли е?	да
Лесно ли е да се използва уязвимостта?	да
Може ли отдалечено да се използва уязвимостта?	да

ВРЕДИ
Възможното въздействие включва отдалечен достъп и потенциално отдалечено изпълнение на код. Тази уязвимост съдържа множество въпроси, които правят риска от вреда *висок.*

Стъпка 3: Разпространение

Примерният ЦДКСКС е вътрешен ЦДКСКС. Разполага с електронна поща, телефон и вътрешен уебсайт като комуникационни канали. ЦДКСКС изготвя този бюлетин въз основа на шаблона от глава *8.2 Генериране на сигнали, предупреждения и съобщения.*

Заглавие на бюлетина
Множество уязвимости, открити в Internet Explorer

Номер за справка
082006-1
Засегнати системи
- Всички компютърни системи, които ползват Microsoft

Свързана OS + версия
- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1
- Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with SP1 for Itanium-based Systems
- Microsoft Windows Server 2003 x64 Edition

Риск (Ниска-Средна-Висока степен)
ВИСОКА
Въздействие/потенциална вреда (Ниска-Средна-Висока степен)
ВИСОКА
Външен идентификатор: (Често срещани възможности за уязвимост и излагане на риск, Идентификатор на бюлетин по уязвимостта)
MS-06-42

Преглед на уязвимостта
Microsoft откри няколко критични уязвимости в Internet Explorer, които могат да доведат до отдалечено изпълнение на код.

Въздействие
Атакуващият може да поеме пълен контрол върху системата, като инсталира програми, добавя потребители и наблюдава, променя или заличава данни. Смекчаващ фактор е, че гореспоменатото може да се случи само, ако потребителят е регистриран с права на администратор. Потребители, регистрирани в по-ограничени права, могат да бъдат засегнати в по-малка степен.

Решение
Незабавно актуализирайте Вашия IE

Описание (подробности)
За повече информация вижте ms06-042.mspx

Приложение
За повече информация вижте ms06-042.mspx

Този резултат вече е готов за разпространение. Тъй като бюлетинът е критичен, препоръчително е също да се обадите на конституентите, когато е възможно.

Примерен ЦДКСКС (стъпка 10)
Упражнение През първите седмици на действие примерният ЦДКСКС използва няколко фиктивни случая (получени като примери от други ЦДКСКС), които бяха използвани за упражнение. Освен това изготви няколко бюлетини по сигурността въз основа на реална информация за уязвимост, разпространена от дистрибутори на хардуер и софтуер, които пригоди и настрои според нуждите на конституентите.

11 Заключение

Тук ръководството свършва. Документът, който е на разположение, има за цел да даде много кратък преглед на различните процеси, необходими за създаване на ЦДКСКС. Не претендира да е изчерпателен нито пък навлиза в много специфични подробности. Моля разгледайте раздел *A.1 „За повече информация“* в приложението за публикации по темата, които си струва да бъдат прочетени.

Последващи важни стъпки за примерния ЦДКСКС сега са:

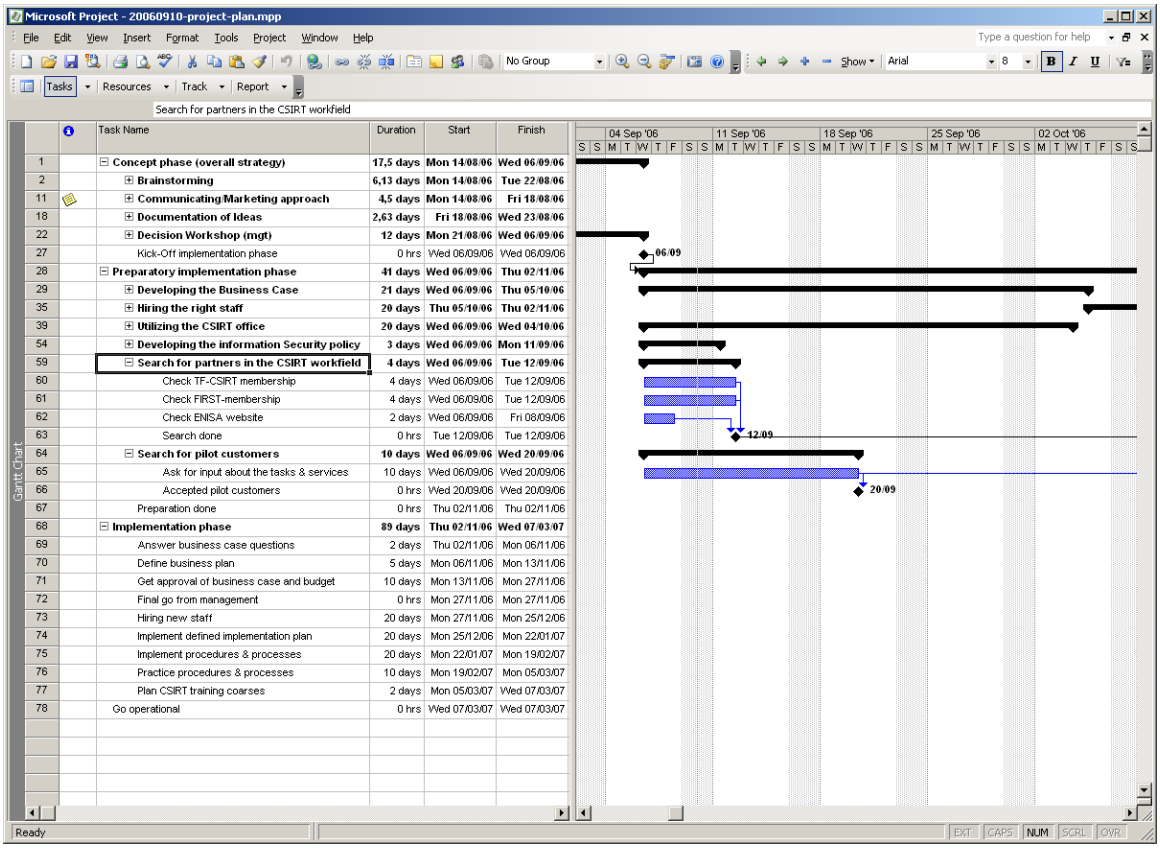
- да получи обратна връзка от конституентите, за да приспособи предлаганите услуги;
- да установи практиката си в ежедневната работа;
- да направи упражнение за извънредни ситуации;
- да поддържа тясна връзка с различни ЦДКСКС общности с цел да допринесе за тяхната доброволна работа в бъдеще.

12 Описание на плана на проекта

ЗАБЕЛЕЖКА: Планът на проекта е първата оценка на необходимата продължителност. В зависимост от наличните ресурси реалното времетраене на проекта може да варира.

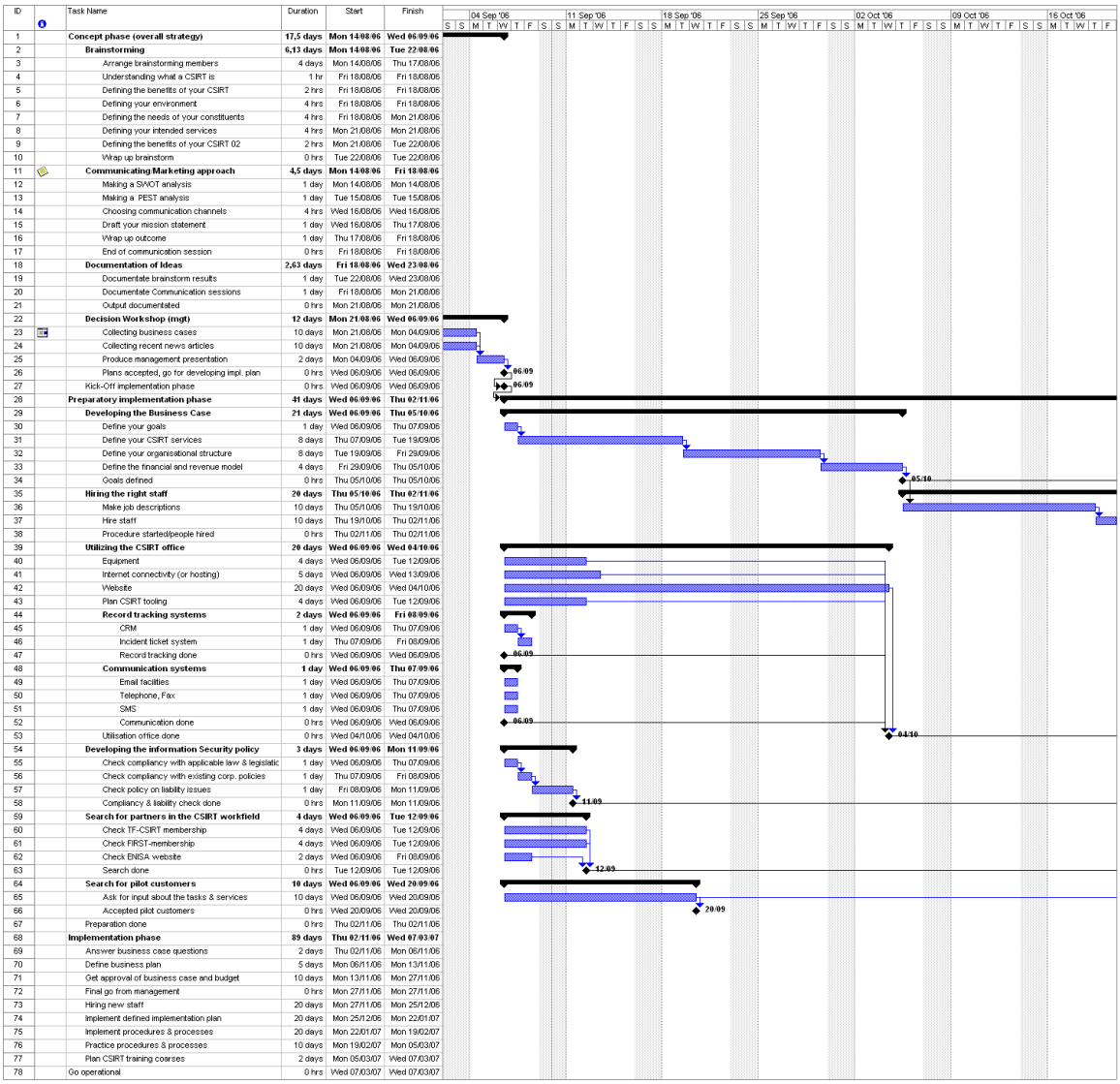
Планът на проекта е достъпен в различни формати на CD и на сайта на ЕАМИС. Напълно покрива всички процеси, описани в този документ.

Основният формат ще бъде Microsoft Project, така че да може да бъде пряко използван в този инструмент за управление на проект.



	Task Name	Duration	Start	Finish
1	Concept phase (overall strategy)	17,5 days	Mon 14/08/06	Wed 06/09/06
2	Brainstorming	6,13 days	Mon 14/08/06	Tue 22/08/06
11	Communicating/Marketing approach	4,5 days	Mon 14/08/06	Fri 18/08/06
18	Documentation of Ideas	2,63 days	Fri 18/08/06	Wed 23/08/06
22	Decision Workshop (mgt)	12 days	Mon 21/08/06	Wed 06/09/06
27	Kick-Off implementation phase	0 hrs	Wed 06/09/06	Wed 06/09/06
28	Preparatory implementation phase	41 days	Wed 06/09/06	Thu 02/11/06
29	Developing the Business Case	21 days	Wed 06/09/06	Thu 05/10/06
35	Hiring the right staff	20 days	Thu 05/10/06	Thu 02/11/06
39	Utilizing the CSIRT office	20 days	Wed 06/09/06	Wed 04/10/06
54	Developing the information Security policy	3 days	Wed 06/09/06	Mon 11/09/06
59	Search for partners in the CSIRT workfield	4 days	Wed 06/09/06	Tue 12/09/06
60	Check TF-CSIRT membership	4 days	Wed 06/09/06	Tue 12/09/06
61	Check FIRST-membership	4 days	Wed 06/09/06	Tue 12/09/06
62	Check ENISA website	2 days	Wed 06/09/06	Fri 08/09/06
63	Search done	0 hrs	Tue 12/09/06	Tue 12/09/06
64	Search for pilot customers	10 days	Wed 06/09/06	Wed 20/09/06
65	Ask for input about the tasks & services	10 days	Wed 06/09/06	Wed 20/09/06
66	Accepted pilot customers	0 hrs	Wed 20/09/06	Wed 20/09/06
67	Preparation done	0 hrs	Thu 02/11/06	Thu 02/11/06
68	Implementation phase	89 days	Thu 02/11/06	Wed 07/03/07
69	Answer business case questions	2 days	Thu 02/11/06	Mon 06/11/06
70	Define business plan	5 days	Mon 06/11/06	Mon 13/11/06
71	Get approval of business case and budget	10 days	Mon 13/11/06	Mon 27/11/06
72	Final go from management	0 hrs	Mon 27/11/06	Mon 27/11/06
73	Hiring new staff	20 days	Mon 27/11/06	Mon 25/12/06
74	Implement defined implementation plan	20 days	Mon 25/12/06	Mon 22/01/07
75	Implement procedures & processes	20 days	Mon 22/01/07	Mon 19/02/07
76	Practice procedures & processes	10 days	Mon 19/02/07	Mon 05/03/07
77	Plan CSIRT training coarses	2 days	Mon 05/03/07	Wed 07/03/07
78	Go operational	0 hrs	Wed 07/03/07	Wed 07/03/07

Фиг. 17 План на проекта



ID	Task Name	Duration	Start	Finish
1	**Concept phase (overall strategy)**	**17,5 days**	**Mon 14/08/06**	**Wed 06/09/06**
2	**Brainstorming**	**6,13 days**	**Mon 14/08/06**	**Tue 22/08/06**
3	Arrange brainstorming members	4 days	Mon 14/08/06	Thu 17/08/06
4	Understanding what a CSIRT is	1 hr	Fri 18/08/06	Fri 18/08/06
5	Defining the benefits of your CSIRT	2 hrs	Fri 18/08/06	Fri 18/08/06
6	Defining your environment	4 hrs	Fri 18/08/06	Fri 18/08/06
7	Defining the needs of your constituents	4 hrs	Fri 18/08/06	Mon 21/08/06
8	Defining your intended services	4 hrs	Mon 21/08/06	Mon 21/08/06
9	Defining the benefits of your CSIRT 02	2 hrs	Mon 21/08/06	Tue 22/08/06
10	Wrap up brainstorm	0 hrs	Tue 22/08/06	Tue 22/08/06
11	**Communicating/Marketing approach**	**4,5 days**	**Mon 14/08/06**	**Fri 18/08/06**
12	Making a SWOT analysis	1 day	Mon 14/08/06	Mon 14/08/06
13	Making a PEST analysis	1 day	Tue 15/08/06	Tue 15/08/06
14	Choosing communication channels	4 hrs	Wed 16/08/06	Wed 16/08/06
15	Draft your mission statement	1 day	Wed 16/08/06	Thu 17/08/06
16	Wrap up outcome	1 day	Thu 17/08/06	Fri 18/08/06
17	End of communication session	0 hrs	Fri 18/08/06	Fri 18/08/06
18	**Documentation of Ideas**	**2,63 days**	**Fri 18/08/06**	**Wed 23/08/06**
19	Documentate brainstorm results	1 day	Tue 22/08/06	Wed 23/08/06
20	Documentate Communication sessions	1 day	Fri 18/08/06	Mon 21/08/06
21	Output documentated	0 hrs	Mon 21/08/06	Mon 21/08/06
22	**Decision Workshop (mgt)**	**12 days**	**Mon 21/08/06**	**Wed 06/09/06**
23	Collecting business cases	10 days	Mon 21/08/06	Mon 04/09/06
24	Collecting recent news articles	10 days	Mon 21/08/06	Mon 04/09/06
25	Produce management presentation	2 days	Mon 04/09/06	Wed 06/09/06
26	Plans accepted, go for developing impl. plan	0 hrs	Wed 06/09/06	Wed 06/09/06
27	Kick-Off implementation phase	0 hrs	Wed 06/09/06	Wed 06/09/06
28	**Preparatory implementation phase**	**41 days**	**Wed 06/09/06**	**Thu 02/11/06**
29	**Developing the Business Case**	**21 days**	**Wed 06/09/06**	**Thu 05/10/06**
30	Define your goals	1 day	Wed 06/09/06	Thu 07/09/06
31	Define your CSIRT services	8 days	Thu 07/09/06	Tue 19/09/06
32	Define your organisational structure	8 days	Tue 19/09/06	Fri 29/09/06
33	Define the financial and revenue model	4 days	Fri 29/09/06	Thu 05/10/06
34	Goals defined	0 hrs	Thu 05/10/06	Thu 05/10/06
35	**Hiring the right staff**	**20 days**	**Thu 05/10/06**	**Thu 02/11/06**
36	Make job descriptions	10 days	Thu 05/10/06	Thu 19/10/06
37	Hire staff	10 days	Thu 19/10/06	Thu 02/11/06
38	Procedure started/people hired	0 hrs	Thu 02/11/06	Thu 02/11/06
39	**Utilizing the CSIRT office**	**20 days**	**Wed 06/09/06**	**Wed 04/10/06**
40	Equipment	4 days	Wed 06/09/06	Tue 12/09/06
41	Internet connectivity (or hosting)	5 days	Wed 06/09/06	Wed 13/09/06
42	Website	20 days	Wed 06/09/06	Wed 04/10/06
43	Plan CSIRT tooling	4 days	Wed 06/09/06	Tue 12/09/06
44	**Record tracking systems**	**2 days**	**Wed 06/09/06**	**Fri 08/09/06**
45	CRM	1 day	Wed 06/09/06	Thu 07/09/06
46	Incident ticket system	1 day	Thu 07/09/06	Fri 08/09/06
47	Record tracking done	0 hrs	Wed 06/09/06	Wed 06/09/06
48	**Communication systems**	**1 day**	**Wed 06/09/06**	**Thu 07/09/06**
49	Email facilities	1 day	Wed 06/09/06	Thu 07/09/06
50	Telephone, Fax	1 day	Wed 06/09/06	Thu 07/09/06
51	SMS	1 day	Wed 06/09/06	Thu 07/09/06
52	Communication done	0 hrs	Wed 06/09/06	Wed 06/09/06
53	Utilisation office done	0 hrs	Wed 04/10/06	Wed 04/10/06
54	**Developing the information Security policy**	**3 days**	**Wed 06/09/06**	**Mon 11/09/06**
55	Check compliancy with applicable law & legislatic	1 day	Wed 06/09/06	Thu 07/09/06
56	Check compliancy with existing corp. policies	1 day	Thu 07/09/06	Fri 08/09/06
57	Check policy on liability issues	1 day	Fri 08/09/06	Mon 11/09/06
58	Compliancy & liability check done	0 hrs	Mon 11/09/06	Mon 11/09/06
59	**Search for partners in the CSIRT workfield**	**4 days**	**Wed 06/09/06**	**Tue 12/09/06**
60	Check TF-CSIRT membership	4 days	Wed 06/09/06	Tue 12/09/06
61	Check FIRST-membership	4 days	Wed 06/09/06	Tue 12/09/06
62	Check ENISA website	2 days	Wed 06/09/06	Fri 08/09/06
63	Search done	0 hrs	Tue 12/09/06	Tue 12/09/06
64	**Search for pilot customers**	**10 days**	**Wed 06/09/06**	**Wed 20/09/06**
65	Ask for input about the tasks & services	10 days	Wed 06/09/06	Wed 20/09/06
66	Accepted pilot customers	0 hrs	Wed 20/09/06	Wed 20/09/06
67	Preparation done	0 hrs	Thu 02/11/06	Thu 02/11/06
68	**Implementation phase**	**89 days**	**Thu 02/11/06**	**Wed 07/03/07**
69	Answer business case questions	2 days	Thu 02/11/06	Mon 06/11/06
70	Define business plan	5 days	Mon 06/11/06	Mon 13/11/06
71	Get approval of business case and budget	10 days	Mon 13/11/06	Mon 27/11/06
72	Final go from management	0 hrs	Mon 27/11/06	Mon 27/11/06
73	Hiring new staff	20 days	Mon 27/11/06	Mon 25/12/06
74	Implement defined implementation plan	20 days	Mon 25/12/06	Mon 22/01/07
75	Implement procedures & processes	20 days	Mon 22/01/07	Mon 19/02/07
76	Practice procedures & processes	10 days	Mon 19/02/07	Mon 05/03/07
77	Plan CSIRT training coarses	2 days	Mon 05/03/07	Wed 07/03/07
78	Go operational	0 hrs	Wed 07/03/07	Wed 07/03/07

Фиг. 18 Планът на проекта с всички задачи и част от графика на Gant

Планът на проекта също е достъпен във формати CVS и XML. Искане за по-нататъшно ползване може да се изпрати на експертите на ЕАМИС по ЦДКСКС: CERT-Relations@enisa.europa.eu

ПРИЛОЖЕНИЕ

A.1 За повече информация

Handbook for CSIRTs (CERT/CC)
Много изчерпателна публикация за справки на всички теми, свързани с работата на ЦДКСКС.
Източник: http://www.cert.org/archive/pdf/csirt-handbook.pdf

Defining Incident Management Processes for CSIRTs: A Work in Progress
Задълбочен анализ на управлението на кризисни ситуации
Източник: http://www.cert.org/archive/pdf/04tr015.pdf

State of the Practice of Computer Security Incident Response Teams (CSIRTs)
Изчерпателен анализ на актуалната ситуация относно картината на ЦДКСКС в световен мащаб, включително и история, статистика и още много.
Източник: http://www.cert.org/archive/pdf/03tr001.pdf

CERT-in-a-box
Изчерпателно описание на поуки, извлечени от създаването на GOVCERT.NL и „De Waarschuwingsdienst“, холандската национална служба за сигнали.
Източник: http://www.govcert.nl/render.html?it=69

RFC 2350: Expectations for Computer Security Incident Response
Източник: http://www.ietf.org/rfc/rfc2350.txt

NIST[37] Computer Security Incident Handling Guide
Източник: http://www.securityunit.com/publications/sp800-61.pdf

ENISA Inventory of CERT activities in Europe
Публикация за справки, която изброява информация относно ЦДКСКС в Европа и техните различни дейности.
Източник: http://www.enisa.europa.eu/cert_inventory

[37] NIST: Национален институт за стандартизация и технологии

A.2 Услуги на ЦДКСКС

Специални благодарности на CERT/CC, които предоставиха този списък

Реактивни услуги	***Проактивни услуги***	***Справяне с артифакти***
• Сигнали и предупреждения • Справяне с кризисни ситуации • Анализ на кризисни ситуации • Действие на място при кризисни ситуации • Поддръжка при действие при кризисни ситуации • Координация на действие при кризисни ситуации • Справяне с уязвимост • Анализ на уязвимост • Действие при уязвимост • Координация на действие при уязвимост	• Съобщения • Наблюдение на технологиите • Одити или оценки на сигурността • Конфигурация и поддръжка на сигурността • Разработване на инструменти за сигурност • Услуги по откриване на пробив • Разпространение на информация, свързана със сигурността	• Анализ на артифакти • Действие при артифакти • Координация на действие при артифакти ***Управление на качеството на сигурността*** • Анализ на риска • Непрекъснатост на бизнес процеса и възстановяване от бедствия • Консултации по сигурността • Повишаване на информираността • Образование/ обучение • Оценка или сертификация на продукт

Фиг. 19 Списък с услуги на ЦДКСКС на CERT/CC

Описание на услугите

Реактивни услуги

Реактивните услуги са предназначени да отговорят на искане за съдействие, доклади за кризисни ситуации от конституенти на ЦДКСКС и каквито и да е заплахи и атаки срещу системи на ЦДКСКС. Може да бъде дадено начало на някои услуги чрез известие от трети страни или наблюдение, мониторинг или чрез система за откриване на пробивите (IDS) и сигнали.

Сигнали и предупреждения

Тази услуга включва разпространяването на информация, която описва атака на нарушител, уязвимост в сигурността, сигнал за пробив, компютърен вирус или измама и осигуряване на всякакво препоръчано краткосрочно действие за справяне с произтичащия проблем. Сигналът, предупреждението или бюлетина по сигурността се изпращат като реакция на актуален проблем за уведомяване на конституентите за дейността и за предлагане на насоки за защита на техните системи или за възстановяване на засегнати системи. Информацията може да

бъде изготвена от ЦДКСКС или може да бъде препратена от дистрибутори, други ЦДКСКС или експерти по сигурността, или други част от конституентите.

Справяне с кризисни ситуации

Справяне с кризисни ситуации включва получаване, обучение и действие при искане и доклади както и анализ на кризисни ситуации и събития. Конкретните действия могат да обхващат:

- предприемане на действия за защита на системи и мрежи, засегнати или заплашени от действие, целящо пробив;
- предлагане на решения и стратегии за смекчаване от приложими бюлетини по сигурността или сигнали;
- търсене на дейности, целящи пробив в други част на мрежата;
- филтриране на мрежовия трафик;
- повторно изграждане на системи;
- поставяне на софтуерни кръпки или поправяне на системите;
- разработване на други стратегии за реакция или заобикаляне на проблема

Тъй като дейностите за справяне с кризисни ситуации се реализират по различни начини от различните видове ЦДКСКС, тази услуга също така се категоризира въз основа на типа извършени дейности и типа предоставено съдействие, както е изложено по-долу.

Анализ на кризисни ситуации

Съществуват много нива на анализ на кризисни ситуации и много подуслуги. По същество анализът на кризисни ситуации е изучаване на наличната информация и помощните доказателства и артифакти, свързани с кризисната ситуация или събитието. Целта на анализа е да се идентифицира обхвата на кризисната ситуация, степента на вреда, причинена от кризисната ситуация и характера на кризисната ситуация и наличните стратегии за реакция или за заобикаляне на проблема. ЦДКСКС може да използва резултатите от анализа на уязвимостта и на артифактите (описани по-долу), за да разбере и предостави най-изчерпателен и актуализиран анализ на случилото се с конкретна система. ЦДКСКС съпоставя дейности при различни кризисни ситуации и определя съотношение, тенденции, модели или подписи на нарушители. Две подуслуги, които могат да се извършват като част от анализа на кризисна ситуация, в зависимост от мисията, целите и процесите на ЦДКСКС са

Събиране на съдебни доказателства

Събиране, запазване, документиране и анализ на доказателства от атакувана компютърна система за определяне на промените в системата и за подпомагане на възстановяването на събития, водещи до пробива. Събирането на информация и доказателства може да бъде извършено, така че да документира доказуемо проследяване на продукцията, което може да се приеме в съда съгласно правилата за доказателствен материал. Задачите, включени в събирането на съдебни доказателства включват (но не се ограничават до) създаването на бит-имидж копие на хард диска на засегнатата система; проверка на промените в системата като нови програми, файлове, услуги и потребители; търсене на действащи процеси и отворени портове; и проверка за програми с троянски коне и

инструменти за създаване на програми. Служителите на ЦДКСКС, които извършват тази дейност трябва да са подготвени при необходимост да действат като вещи лица по съдебно дело.

Проследяване

Проследяване на произхода на нарушителя или идентифицирането на системите, до които има достъп. Тази дейност може да включва проследяване на начина, по който нарушителят е влязъл в засегната система и свързаните мрежи, кои системи са били използвани за получаване на достъп, къде е възникнала атаката, и кои други системи и мрежи са били използвани като част от атаката. Може също да включва и опит за идентифициране на нарушителя. Това може да бъде самостоятелна дейност, но обикновено включва и работа със служители на правоприлагащите органи, доставчиците на интернет или други заинтересовани организации.

Действие на място при кризисни ситуации

ЦДКСКС осигуряван пряко съдействие на място в помощ на конституентите при възстановяване от кризисна ситуация. Самият ЦДКСКС физически анализира засегнатите системи и ръководи поправката и възстановяването на системите, вместо да предлага само поддръжка при действие при кризисни ситуации по телефон или електронна поща (вижте по-долу). Тази услуга включва всички действия, предприети на местно ниво, които са необходими, ако има съмнения или възникне кризисна ситуация. Ако ЦДКСКС не се намира на засегнатото място, членове на екипа ще пътуват до мястото, за да извършат действието. В други случаи местен екип може вече да е на място, като предоставя действие при кризисна ситуация като част от рутинната си работа. Това се прилага особено, ако справянето с кризисни ситуации, вместо на установен ЦДКСКС, се предлага като част от нормалната работа на системни, мрежови администратори и служители по сигурността.

Поддръжка при действие при кризисни ситуации

ЦДКСКС подпомага и напътства жертвите на атаката при възстановяването от кризисната ситуация по телефон, електронна поща, факс или чрез документация. Това може да включва техническа помощ за интерпретирането на събраните данни, предоставяне на информация за контакти или препредаване на насоки за стратегии за смекчаване и възстановяване. Не включва преки действия на място за реакция при кризисни ситуации, както бе описано по-горе. Вместо това ЦДКСКС осигурява напътствия от разстояние, така че самите служители да могат да извършат на място възстановяването.

Координация при действие при кризисна ситуация

ЦДКСКС координира усилията по действието между страните, ангажирани в кризисната ситуация. Обикновено това включва жертвата на атаката, други страни, засегнати от атаката и всички страни, които имат нужда от съдействие за анализ на атаката. Може да включва и страните, които осигуряват ИТ поддръжка на жертвата като интернет доставчици, други ЦДКСКС и системни и мрежови администратори на място. Координацията може да включва събиране на информация за контакти, уведомяване на потенциално засегнати страни (като

жертви или източник на атака), събиране на статистически данни относно броя на замесените и улесняване на обмена и анализа на информация. Част от работата по координация може да включва уведомяване и сътрудничество с юриста, отделите по човешки ресурси или връзки с обществеността на организацията. Също може да включва координация с правоприлагащи органи. Тази услуга не обхваща пряки действия на място при кризисна ситуация.

Справяне с уязвимост

Справянето с уязвимост включва получаване на информация и на доклади относно уязвимости в хардуера и софтуера, анализ на характера, механиката и последствията от уязвимостите и разработване на стратегии за действие за откриване и поправяне на уязвимости. Тъй като дейностите за справяне с уязвимости се реализират по различни начини от различни типове ЦДКСКС, тази услуга също се категоризира въз основа на типа извършени дейности и типа осигурено съдействие, както следва:

Анализ на уязвимостта

ЦДКСКС извършва технически анализ и изучава уязвимостите в хардуера или софтуера. Това включва проверка на предполагаеми уязвимости и технически преглед на уязвимостта на хардуера и софтуера, за да се установи къде се намира и как може да се използва. Анализът може да включва и проверка на кода на източника, като се използва дебъгер, за да се установи къде възниква уязвимостта или да се направи опит за възпроизвеждане на проблема на пробна система.

Действие при уязвимост

Тази услуга включва определянето на подходящи действия за смекчаването или поправяне на уязвимостта. Това може да включва разработването или търсенето на софтуерни кръпки, корекции или начин да се заобиколи проблема. Също така включва уведомяване на другите за стратегията за смекчаване, ако е възможно чрез изготвянето и разпространението на бюлетини по сигурността или сигнали. Тази услуга може да включва извършването на действие чрез инсталиране на софтуерни кръпки, корекции или заобикаляне на проблема.

Координация на действия при уязвимост

ЦДКСКС уведомява различни части от предприятието или конституентите относно уязвимостта и споделя информация за това как да се поправи или смекчи уязвимостта. ЦДКСКС проверява успешното прилагане на стратегията за действие при уязвимост. Тази услуга може да включва комуникация с дистрибутори, други ЦДКСКС, технически експерти, членове на конституентите и лица или групи, които първоначално са открили или докладвали за уязвимостта. Действията включват улесняването на анализа на уязвимостта или доклада на уязвимостта; координация на графиците за публикация на съответните документи, софтуерни кръпки или заобикаляне на проблема; и синтезиране на техническия анализ, направен от различни страни. Тази услуга може също да включва поддържането на публичен или частен архив или база данни с информация за уязвимост и съответните стратегии за действие.

Справяне с артифакти

Артифакт е всеки файл или предмет, намерен в система, който участва в сондиране или атака на системи и мрежи или който е използван за неутрализиране на мерки за сигурност. Артифактите могат да включват - но без да са ограничени само до тях - компютърни вируси, троянски коне, червеи, скриптове с експлойт код и инструменти за създаване на програми.
Справянето с артифакти включва получаване на информация и копие на артифактите, които са използвани в атаката на нарушителя, в разузнаване и други неоторизирани или разрушителни действия. Щом бъде получен, артифактът се разучава. Това включва анализ на характера, механиката, версията и ползването на артифактите и разработване (или предлагане) на стратегии за действие по откриването, премахването и защитата срещу тези артифакти. Тъй като дейностите по справяне с артифакти се реализират по различни начини от различните типове ЦДКСКС, тази услуга по-нататък е категоризирана въз основа на типа извършени дейности и типа предоставено съдействие, както следва:

Анализ на артифакти

ЦДКСКС извършва технически преглед и анализ на всеки артифакт, намерен в системата. Направеният анализ може да включва идентифициране на типа файл и структурата на артифакта, сравнение на нов артифакт със съществуващи артифакти или други версии на същия артифакт, за да се открият прилики и разлики или „обратно инженерство“ или код за разглобяване, за да се определи целта и функцията на артифакта.

Действие при артифакти

Тази услуга включва определянето на подходящи действия за откриване и премахване на артифакти от системата, както и действия за предотвратяване на инсталирането на артифакти. Това може да включва и създаването на подписи, които да се добавят към антивирусен софтуер или система за откриване на пробиви (IDS).

Координация при действие при артифакти

Тази услуга включва обмена и синтезирането на резултати от анализ и стратегии за действие във връзка с артифакт с други изследователи, ЦДКСКС, дистрибутори и други експерти по сигурността. Дейностите включват уведомяване на другите и синтез на техническия анализ от различни източници. Дейностите могат също така да включват поддържането на публичен архив или такъв на конституента с известни артифакти, тяхното въздействие и съответни стратегии за действие.

Проактивни услуги

Проактивните услуги са предназначени за подобряване на инфраструктурата и процесите по сигурността на конституентите преди възникването или откриването на кризисна ситуация или събитие. Основните цели са да се избегнат кризисни ситуации и да се намали тяхното въздействие и обхват, когато възникнат.

Съобщения

Това включва - но без да се ограничава само до тях - сигнали за пробиви, предупреждения за уязвимости и бюлетини по сигурността. Подобни съобщения информират конституентите относно нови събития със средносрочно и

дългосрочно въздействие като новооткрити уязвимости или инструменти за пробиви. Съобщенията позволяват на конституентите да защитят системите и мрежите си срещу новооткрити проблеми преди те да бъдат използвани.

Наблюдение на технологиите

ЦДКСКС наблюдава развитието на новите технологии, дейностите на нарушители и свързаните с тях тенденции, за да помогне за идентифицирането на бъдещи заплахи. Разгледаните теми могат да бъдат разширени до включване на правни и законодателни правила, социални и политически заплахи и нововъзникващи технологии. Тази услуга включва четене на мейлинг листи по сигурността, уебсайтове относно сигурността и актуални новини и статии от журнали в областта на науката, технологиите, политиката и правителството за извличане на информация, свързана със сигурността на системите и мрежите на конституента. Може да включва и комуникация с други страни, които са авторитети в тези области, за да се гарантира, че е получена най-добрата и точна информация или интерпретация. Резултатът от тази услуга може да се изразява в някакъв вид съобщение, насоки или препоръки, съсредоточени върху средносрочни или дългосрочни въпроси на сигурността.

Одити и оценки на сигурността

Тази услуга осигурява подробен преглед и анализ на инфраструктурата по сигурността на дадена организация въз основа на изисквания, определени от организацията или от други стандарти, които се прилагат за сектора. Може да включва и преглед на практиките по организационна сигурност. Съществуват много различни типове одит или оценки, които могат да се предоставят, включително и

Преглед на инфраструктурата

Ръчен преглед на конфигурациите на хардуера и софтуера, рутери, защитни стени, сървъри и устройства на компютри, за да се гарантира, че съответстват на политиката на най-добрите практики на организацията или сектора и на стандартни конфигурации

Преглед на най-добрите практики

Интервюиране на служители и системни и мрежови администратори за да се определи дали техните практики по сигурността съответстват на формулираната политика по сигурността на организацията или на някои специфични стандарти за сектора

Сканиране

Използването на скенери за уязвимост или вируси за определяне на уязвимите системи или мрежи.

Тест за пробив

Тестване на сигурността чрез целенасочена атака на системите и мрежите.
Необходимо е получаването на разрешение от високопоставените мениджъри преди да се извършат такива одити или оценки. Възможно е някои от тези подходи да са забранени от политиката на организацията. Предоставянето на тази услуга

може да включва разработването на общ комплект от практики, срещу които се провеждат тестовете или оценките, заедно с развитието на необходимите умения или изисквания за сертификация на персонала, който извършва тестването, оценката, одитите или прегледите. Тази услуга може също да се възложи на външен изпълнител трета страна или на доставчик на услуги в областта на управлението на сигурността с необходимите експертни познания в извършването на одити и оценки.

Конфигурация и поддръжка на инструменти за сигурност, приложения, инфраструктури и услуги

Тази услуга идентифицира и предлага подходящи насоки за сигурно конфигуриране и поддръжка на инструменти, приложения и общи изчислителни инфраструктури, използвани от конституентите на ЦДКСКС и от самия ЦДКСКС. Освен осигуряването на насоки, ЦДКСКС може да извършва актуализации на конфигурация и поддръжка на инструменти за сигурността и услуги като откриване на пробиви (IDS), сканиране на мрежа или мониторинг на системи, филтри, обвивки, защитни стени, виртуални частни мрежи (VPN) или механизми за проверка на автентичността. ЦДКСКС може дори да предостави тези услуги като част от основната си функция. ЦДКСКС може също така да конфигурира и поддържа сървъри, компютри, лаптопи, лични цифрови помощници (PDA устройства) и други безжични устройства според насоките за сигурност. Тази услуга включва предаването на по-високопоставени мениджъри на всички въпроси или проблеми с конфигурации или ползване на инструменти и приложения, които според ЦДКСКС може да направят системата уязвима на атака.

Разработване на инструменти по сигурността

Тази услуга включва разработването на нови инструменти, специфични за конституента, които се изискват или търсят от конституентите или от самия ЦДКСКС. Това може да включва например разработването на софтуерни кръпки за сигурност за приспособен софтуер, използван от конституенти или разпространението на сигурен софтуер, който може да се използва за възстановяване на атакувани хостове. Може също да включва разработването на инструменти или скриптове, които разширяват функционалността на съществуващите инструменти за сигурност, като нова приставка за уязвимост или скенер на мрежа, скриптове, които улесняват използването на технологии за криптиране или автоматични механизми за разпределение на софтуерни кръпки.

Услуги по откриване на пробив

ЦДКСКС, които извършват тази услуга, преглеждат съществуващите регистрации в IDS, анализират и започват действия за всички събития, които отговарят на определения от тях праг, или препращат сигнали според предопределеното споразумение за степента на обслужване или стратегия за делегиране на работа. Откриването на пробив и анализът на свързаните регистрации в сигурността може да бъдат предизвикателство – не само за определяне къде да се разположат сензорите в средата, а и при събирането на големи количества данни и последващия им анализ. В много случаи се изискват специализирани инструменти или експертни познания за синтезирането или интерпретирането на информацията, за да се идентифицират фалшиви сигнали, атаки или мрежови събития и да се реализират стратегии за елиминирането или намаляването на

тези събития. Някои организации избират да възложат тази дейност на външни изпълнители, които имат повече експертни познания в извършването на тези услуги като доставчици на услуги в областта на управлението на сигурността.

Разпространение на информация, свързана с сигурността

Тази услуга предлага на конституентите събраната изчерпателна и лесна за намиране полезна информация, която помага за подобряването на сигурността. Подобна информация може да включва:

- докладване на насоки и информация относно контакти за ЦДКСКС;
- архиви със сигнали, предупреждения и други съобщения;
- документация относно актуални най-добри практики;
- общи насоки за компютърна сигурност;
- политики, процедури и списъци за проверка;
- разработване на софтуерна кръпка и разпространяване на информация;
- връзки с дистрибутори;
- актуалната статистика и тенденции в докладването на кризисни ситуации;
- друга информация, която може да подобри цялостните практики по сигурността.

Тази информация може да бъде развита и публикувана от ЦДКСКС или от друга част от организацията (ИТ, човешки ресурси или връзки с медиите), и може да включва информация от външни ресурси като други ЦДКСКС, дистрибутори и експерти по сигурността.

Услуги по управлението на качеството на сигурността

Услугите, които спадат към тази категория не са уникални за справянето с кризисни ситуации или по-специално за ЦДКСКС. Те са добре известни, установени услуги, предназначени да подобрят цялостната сигурност на организацията. Като използва опита, придобит при предоставянето на реактивни и проактивни услуги, описани по-горе, ЦДКСКС може да предложи уникална гледна точка върху услугите по управление на качеството, която в противен случай може да не е достъпна. Тези услуги целят да включат обратната връзка и извлечени поуки въз основа на придобитите познания чрез действието при кризисни ситуации, уязвимости и атаки. Възможно е интегрирането на подобен опит в установени традиционни услуги (описани по-долу) като част от процес по управление на сигурността да подобри дългосрочните усилия в областта на сигурността в организацията. В зависимост от организационните структури и отговорности ЦДКСКС може да предлага тези услуги или да участва като част от усилията на по-голям организационен екип.
Следните описания обясняват как експертизата на ЦДКСКС може да е от полза за услугите по управление на качеството на сигурността.

Анализ на риска

ЦДКСКС може да осигури добавена стойност на анализа и оценката на риска. Това може да подобри способността на организацията да оценява реални заплахи, да предлага реалистични качествени и количествени оценки на рисковете за информационните активи и да оцени стратегиите за защита и действие. ЦДКСКС, които извършват тази услуга, биха провели или съдействали с дейности за анализ

на риска за информационната сигурност на новите системи и бизнес процесите или оценка на заплахите и атаките срещу активите и системите на конституентите.

Непрекъснатост на бизнес процеса и планиране на възстановяването на щети

Въз основа на минали събития и прогнози за бъдещето за възникването на кризисни за сигурността ситуации или тенденции, все повече кризисни ситуации имат потенциал да се превърнат в сериозни щети за бизнес операциите. Следователно, в процеса на планиране трябва да се разгледат опитът и препоръките на ЦДКСКС за определянето на най-добрия начин за действие при подобни кризисни ситуации, така че да се осигури непрекъснатостта на бизнес операциите. ЦДКСКС, които извършват тази услуга, са ангажирани в непрекъснатостта на бизнес процеса и планирането на възстановяване на щети при събития, свързани със заплахи и атаки срещу компютърната сигурност.

Консултации по сигурността

ЦДКСКС може да бъде използван за предоставяне на съвети и насоки относно най-добрите практики по сигурността за реализиране на бизнес операции на конституентите. ЦДКСКС, които предоставят тази услуга, са ангажирани в подготвянето на препоръки или набелязването на изисквания за покупки, инсталиране или обезопасяване на нови системи, мрежови устройства, софтуерни приложения или бизнес процеси за цялото предприятие. Тази услуга включва предоставянето на насоки и съдействие в развитието на политики по организацията или сигурността на конституентите. Може също така да включва данни или съвети към законодателни или други правителствени органи.

Повишаване на информираността

ЦДКСКС може да идентифицират в кои области конституентите се нуждаят от повече информация и насоки, за да се приспособят по-добре към практиките по сигурността и политиките по организационната сигурност. Повишаването на общата информираност на конституентите относно сигурността не само ще подобри тяхното разбиране по въпросите на сигурността, а и ще им помогне да извършват всекидневните операции по по-сигурен начин. Това може да намали случаите на възникване на успешни атаки и да повиши възможността конституентите да откриват и докладват за атаки, като така се намалява нуждата от възстановяване и се премахват или минимизират загубите.
ЦДКСКС, които извършват тази услуга, търсят възможности за повишаване на информираността относно сигурността чрез разработването на статии, плакати, бюлетини, уебсайтове или други източници на информация, които разясняват най-добрите практики по сигурността и предлагат съвети за взимането на предпазни мерки. Дейностите могат да включват и насрочването на срещи и семинари за запознаване на конституентите с действащи процедури по сигурността и потенциални заплахи за организационните системи.

Образование/ обучение

Тази услуга включва предоставянето на информация на конституенти относно въпроси на компютърната сигурност чрез семинари, ателиета, курсове и консултации. Темите могат да включват насоки за докладване на кризисна

ситуация, подходящи методи за действие, инструменти за действие при кризисна ситуация, методи за предотвратяване на кризисна ситуация и друга информация, необходима за защита, откриване, докладване и действие при кризисни ситуации за компютърната сигурност.

Оценка или сертификация на продукта

При тази услуга ЦДКСКС може да извърши оценка на продукта по отношение на инструменти, приложения или други услуги, за да се осигури сигурността на продуктите и тяхната съвместимост с приемливи за ЦДКСКС или за организационната сигурност практики. Разгледаните инструменти и приложения могат да за с отворен код или комерсиални продукти. Тази услуга може да се предлага като оценка или чрез програма за сертифициране в зависимост от стандартите, които се прилагат от организацията или от ЦДКСКС.

А.3 Примерите

Примерен ЦДКСКС

Стъпка 0- Разбрахме същността на ЦДКСКС:
Примерният ЦДКСКС ще трябва да обслужва средна по големина институция, чийто служители наброяват до 200 души. Институцията има собствен отдел по ИТ и два допълнителни клона в същата страна. ИТ играят ключова роля за компанията, тъй като се използват за вътрешна комуникация, мрежа от данни и е-бизнес 24x7. Институцията има собствена мрежа и разполага с резервна връзка с интернет чрез два различни интернет доставчика.

- -

Стъпка 1 - Начална фаза
В началната си фаза новият ЦДКСКС е планиран като вътрешен ЦДКСКС, който предлага услуги на компанията майка, местния ИТ отдел и служители. Също така поддържа и координира между различните клонове работата по ИТ сигурността, свързана с кризисни ситуации.

- -

Стъпка 2 - Избор на точните услуги
В началната фаза се взе решението новият ЦДКСКС да се фокусира основно върху предоставянето на някои централни услуги за служителите.

Взе се решение след пилотната фаза да се разгледа разширяването на портфолиото с услуги и може да се прибавят някои „Услуги по управление на сигурността". Това решение ще бъде взето въз основа на обратната връзка от пилотните конституенти и в тясно сътрудничество с отдела по осигуряване на качеството.

- -

Стъпка 3 - Изготвяне на анализ на конституентите и подходящите комуникационни канали

Сесия с брейнсторминг с някои ключови лица от ръководството и конституентите дадоха достатъчно материал за SWOT анализ. Той води до заключението, че съществува нужда от централни услуги:

- Сигнали и предупреждения
- Справяне с кризисни ситуации (анализ, поддръжка на действията и координация на действията)
- Съобщения

Трябва да се осигури добре организираното разпространение на информацията, която да достигне до най-голямата възможна част от конституентите. Следователно се взе решение сигналите, предупрежденията и съобщенията във форма на бюлетини по сигурността да се публикуват на предназначен за целта уебсайт и да се разпространяват чрез мейлинг листа. Електронната поща, телефонът и факсът улесняват ЦДКСКС при получаването на доклади за кризисни ситуации. Единен уеб формуляр е предвиден за следващата стъпка.

Стъпка 4 –Мисия на центъра
Мениджърите на примерния ЦДКСКС са заявили следната мисия:
„Примерният ЦДКСКС предоставя информация и съдействие на служителите на своята компания с цел намаляване на рисковете от кризисни ситуации в областта на компютърната сигурност както и за действие при подобни кризисни ситуации, когато те възникнат.“

С това примерният ЦДКСКС ясно заявява, че е вътрешен ЦДКСКС и основната му дейност е да се справя с въпроси, свързани с ИТ сигурността.
- -

Стъпка 5 - Определяне на бизнес план

Финансов модел
Поради факта, че компанията развива е-бизнес 24x7 и има ИТ отдел 24x7, се взе решение за предлагане на пълно обслужване в рамките на традиционното работно време и дежурства на повикване извън работното време. Услугите ще бъдат предоставяни безплатно за конституентите, но възможността за предлагане на услуги на външни клиенти ще бъде оценена по време на пилотната фаза за оценка.

Модел за приходи
По време на началната и пилотна фаза ЦДКСКС ще бъде финансиран чрез компанията майка. По време на пилотната фаза за оценка ще бъде обсъден въпросът за допълнително финансиране, включително и възможността да се продават услуги на външни клиенти.

Организационен модел
Организацията майка е малка компания, така че бе избран внедреният модел.
В работно време персонал от трима души ще осигурява ключови услуги (разпространение на бюлетини по сигурността и справяне/ координация при кризисни ситуации).
ИТ отделът на компанията вече е наел хора с подходящи умения. Сключва се споразумение с отдела, така че при необходимост новият ЦДКСКС може да поиска помощ на временна основа. Също така може да се използва втората линия от техните технически сътрудници на повикване.
Ще има централен екип на ЦДКСКС с четири члена на пълна заетост и пет допълнителни членове на екипа на ЦДКСКС. Един от тях също е на разположение с плаващи смени.

Служители
Ръководителят на екипа на ЦДКСКС има опит в сигурността и в 1-ва и 2-ра степен на поддръжка и е работил в областта на управление на устойчивостта при кризи. Другите трима членове на екипа са специалисти по сигурността. Членовете на екипа на ЦДКСКС на непълен работен ден от ИТ отдела са специалисти по своята част от инфраструктурата на компанията.

Стъпка 5 – Използване на офиса и политика по информационна сигурност
Оборудване и местонахождение на офиса

Поради факта, че компанията майка вече разполага с ефективна физическа сигурност, новият ЦДКСКС е добре подсигурен в този аспект.
Осигурява се така наречената „военна стая“, за да се улесни координацията в случай на извънредна ситуация. Закупува се сейф за кодирани материали и деликатни документи. Открива се отделна телефонна линия, която включва и централа, за улесняване на горещата линия през работно време и дежурства „на повикване“ на мобилен телефон за времето извън традиционното работно време със същия телефонен номер.

Също могат да се използват съществуващото оборудване и корпоративен уебсайт за обявяване на информация, свързана с ЦДКСКС. Инсталира се и се поддържа мейлинг листа с ограничен сектор за комуникация между членовете на екипа и с другите центрове. Цялата информация за контакти със служители се съхранява в база данни, като в сейфа се пази разпечатано копие.

Регулиране
Поради факта, че ЦДКСКС е внедрен в компания със съществуваща политика по информационната сигурност, съответните политики за ЦДКСКС са установени с помощта на юрист от компанията.
- -

Стъпка 7 -Търсене на сътрудничество
Като се използва Регистъра на ЕАМИС, бързо бяха открити и бе установен контакт с някои ЦДКСКС в същата страна. Бе уредено посещение на място в един от тях за новопостъпилия ръководител на екипа. Той се запозна с националните дейности в областта на ЦДКСКС и присъства на срещата.
Тази среща беше повече от полезна за събирането на примери за работещи методи и подкрепа от няколко други екипа.
.- -

Стъпка 8 -Популяризиране на бизнес план

Бе взето решение да се съберат факти и цифри за историята на компанията. Това е повече от полезно за статистически преглед на ситуацията с ИТ сигурността. Събирането трябва да продължи и когато ЦДКСКС вече е създаден и работи, за да се актуализира статистиката.

Свързахме се с други национални ЦДКСКС и имаше допитване до тях за техните бизнес случаи. Те осигуриха подкрепа за събирането на презентации с информация относно актуалното развитие в областта на кризисните ситуации за ИТ сигурността и относно разходите за кризисните ситуации.

В представения случай на примерен ЦДКСКС не съществува належаща нужда да се убедят мениджърите за значимостта на ИТ бизнеса, и затова не бе трудно да се даде зелена светлина за първата стъпка. Бяха изготвени бизнес казус и план на проекта, включващи оценка на разходите по създаване и разходите за операции.
- -

Стъпка 9 - Установяването на потоци на процеса и оперативни и технически процедури

Примерният ЦДКСКС се съсредоточава върху централните услуги ЦДКСКС.

- Сигнали и предупреждения
- Съобщения
- Справяне с кризисни ситуации

Центърът разработва процедури, които работят добре и са лесно разбираеми за всеки член на екипа. ЦДКСКС също наема юрист, за да работи по въпроси в областта на правната отговорност и политиката по информационната сигурност. Екипът прие някои полезни инструменти и намери полезна информация за оперативните въпроси от дискусии с други ЦДКСКС.

Бе направен шаблон за бюлетини по сигурността и за доклади за кризисни ситуации. Центърът използва RTIR за справяне с кризисни ситуации.

- -

Стъпка 10 - Обучение на служителите

Примерният ЦДКСКС реши да изпрати целия технически персонал на следващите достъпни курсове на TRANSITS. Отделно ръководителят на екипа посещава курса „Управление на ЦДКСКС“ на CERT/CC.

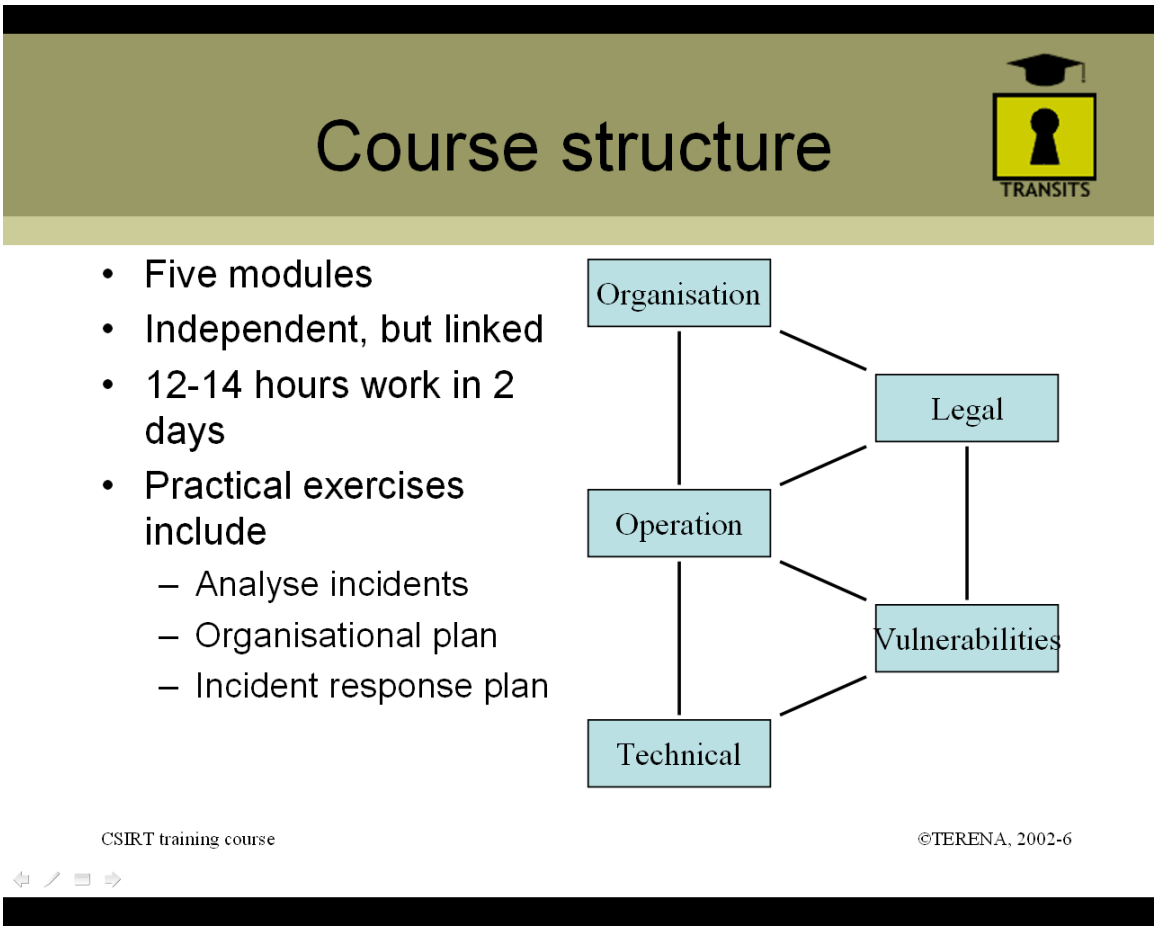
- -

Стъпка 11 - Упражнения

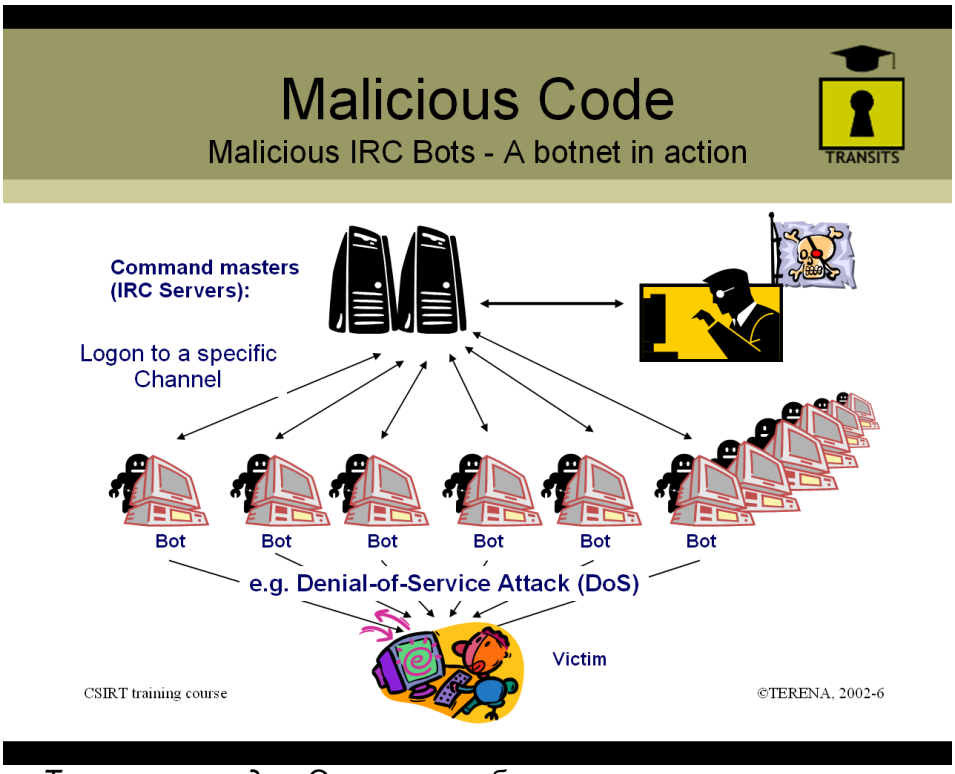
През първите седмици на работа ЦДКСКС използва няколко фиктивни казуса (които получиха като примери от други ЦДКСКС), които бяха използвани за упражнение. Освен това издаде няколко бюлетини по сигурността въз основа на реална информация за уязвимост, разпространена от дистрибутори на хардуер и софтуер, които пригоди и нагласи според нуждите на конституентите.

A.4 Примерни материали от курсове за ЦДКСКС

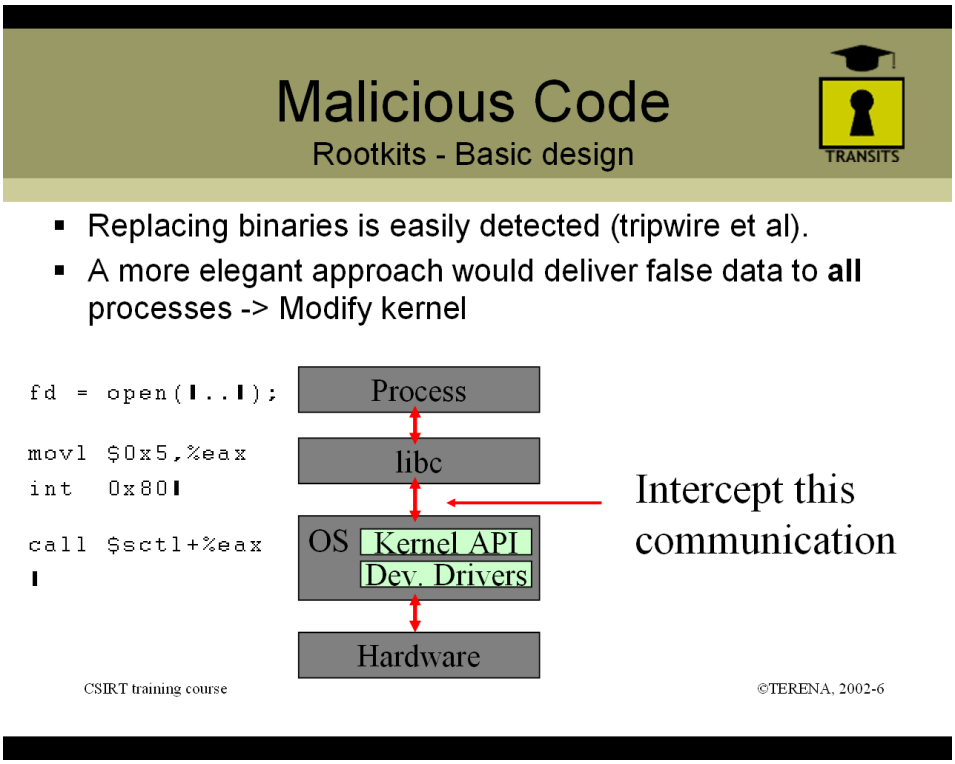
TRANSITS (с любезното разрешение на Terena, http://www.terena.nl)



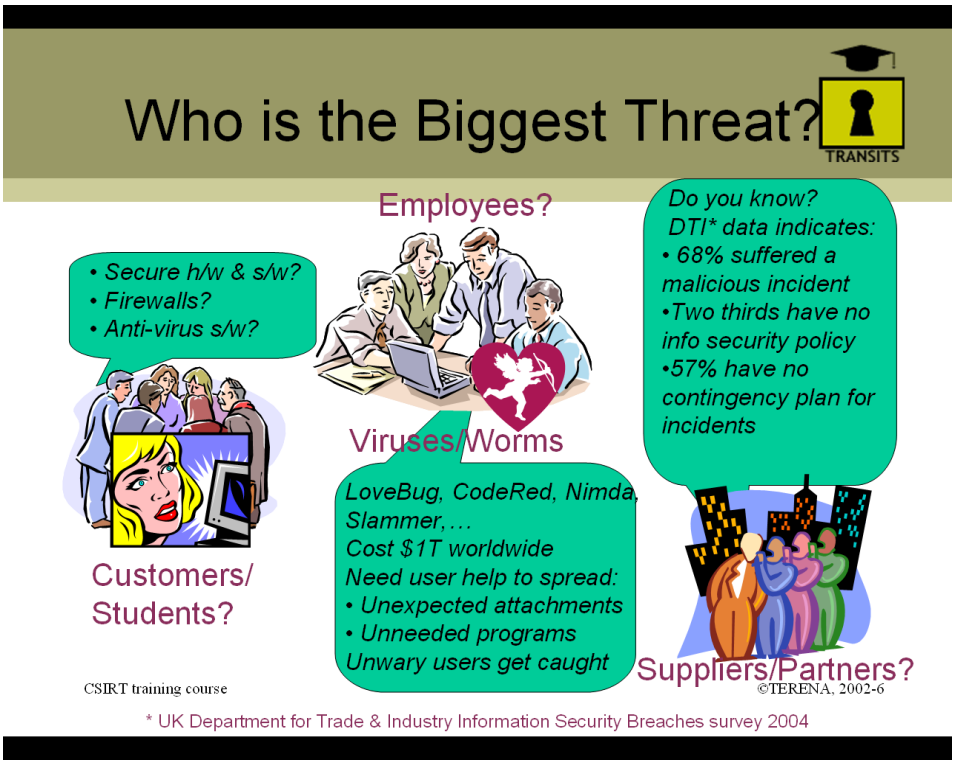
Преглед: Структура на курса



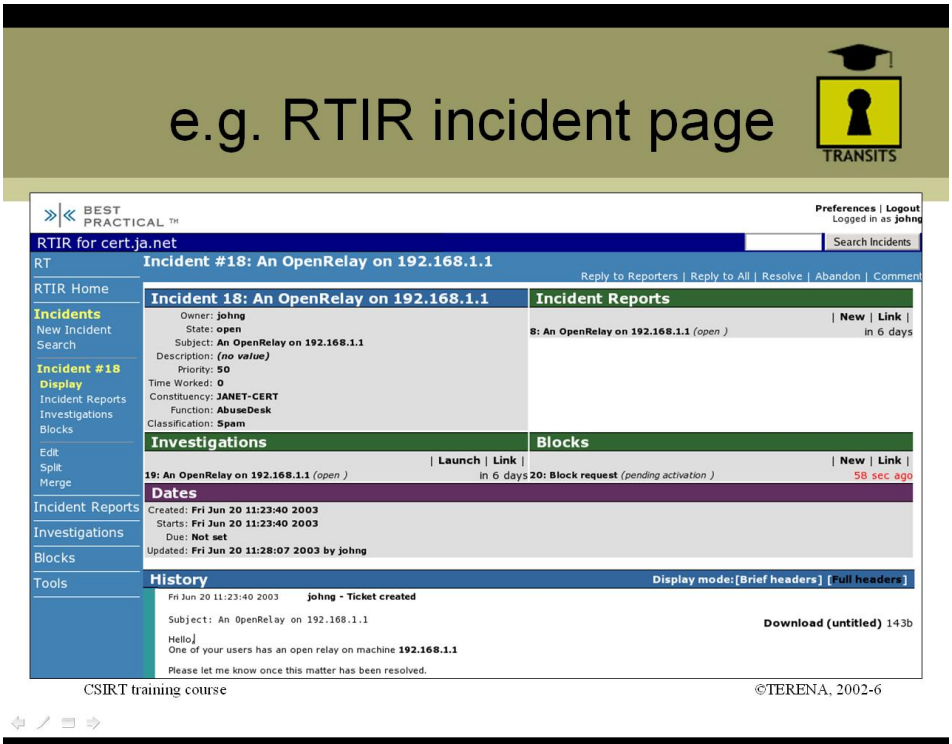
от *Технически модул*: Описание на ботнет



От *Технически модул*: Основен дизайн на руткит



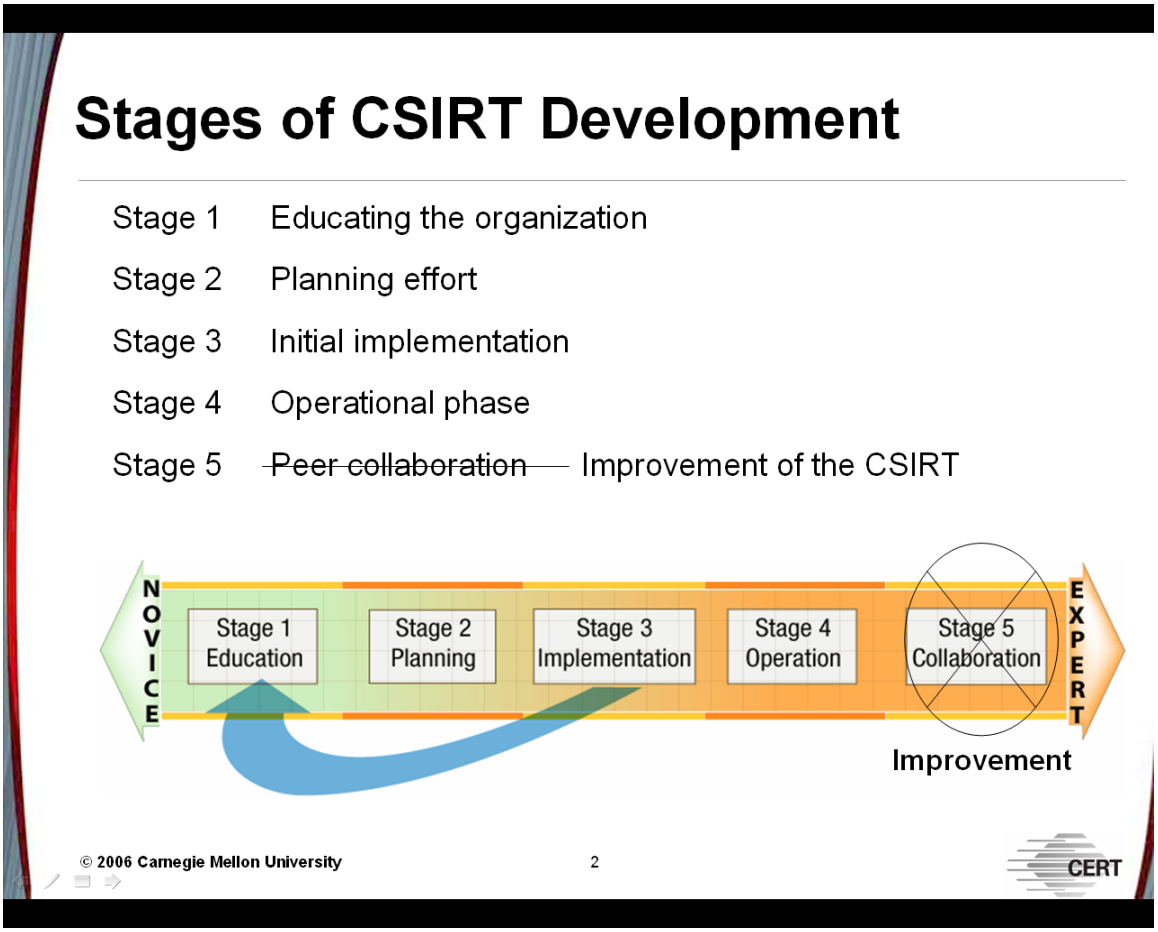
От *Организационен модул*: Вътрешна или външна – къде е по-голямата заплаха?



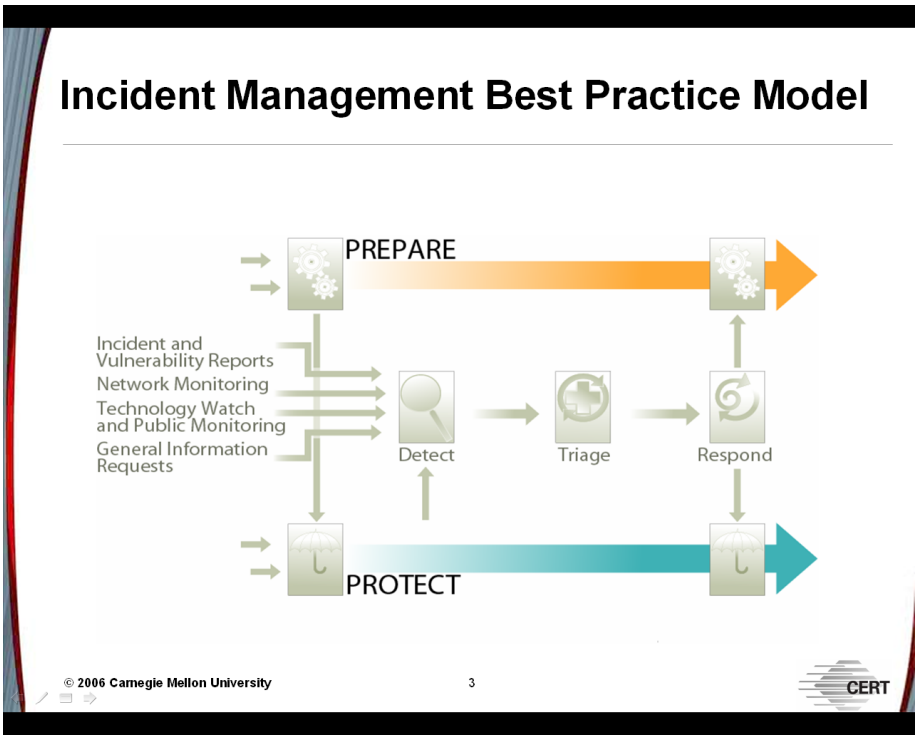
От *Оперативно направление* : Проследяване на искания за действие при кризисни ситуации (RTIR)

„Създаване на ЦДКСКС“ (с любезното разрешение на CERT/CC, http://www.cert.org)

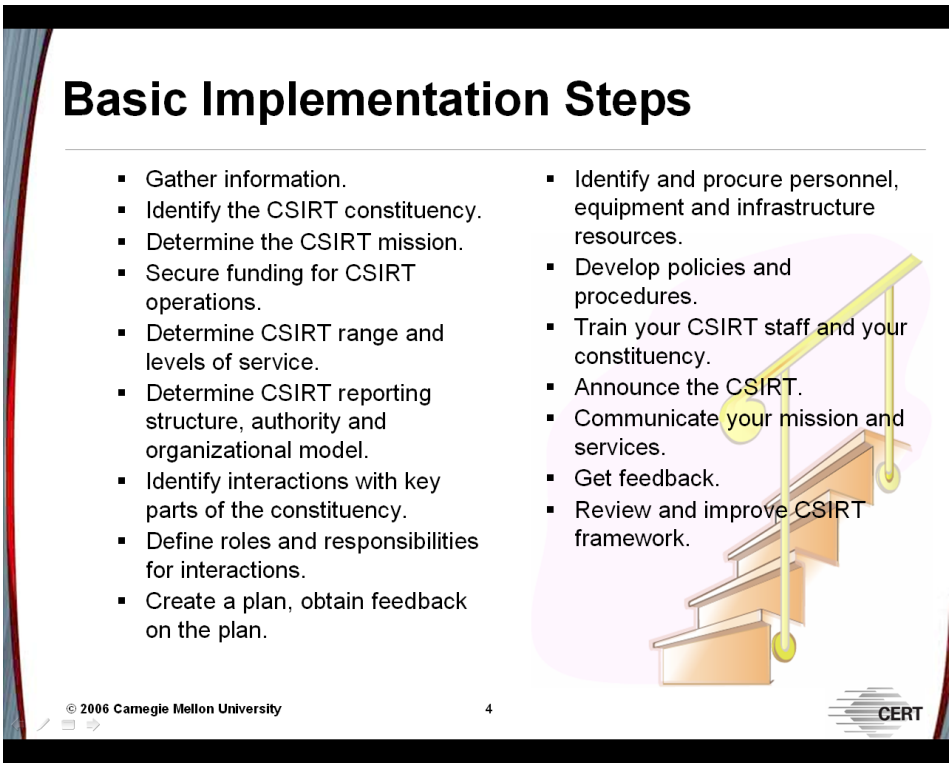
ЕАМИС изразява признателността си към екипа за развитие на ЦДКСКС към Програма CERT за позволението да използваме съдържанието на техните курсове за обучение!



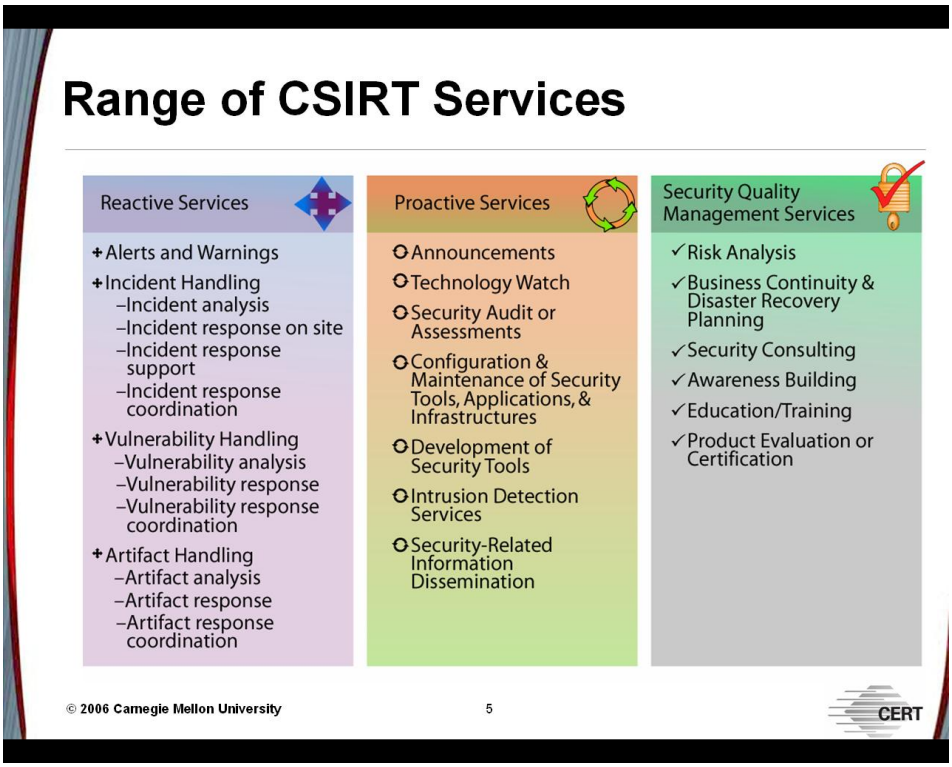
от *CERT/CC Курс за обучение*: етапи от развитието на ЦДКСКС



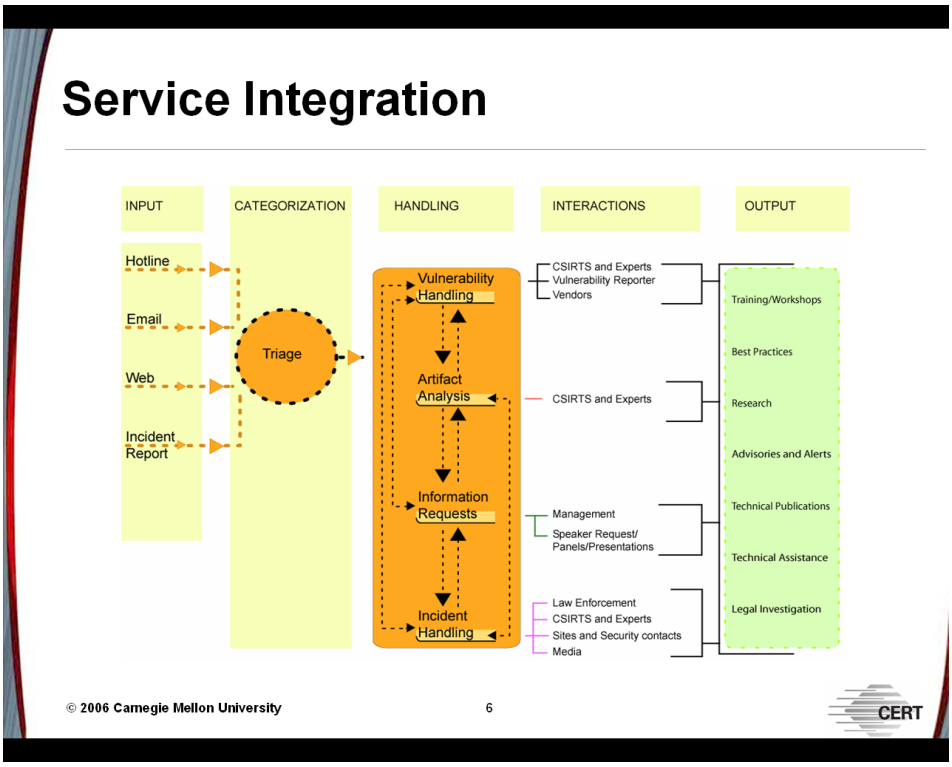
от *CERT/CC Курс за обучение*: Най-добри практики за управление на кризисни ситуации



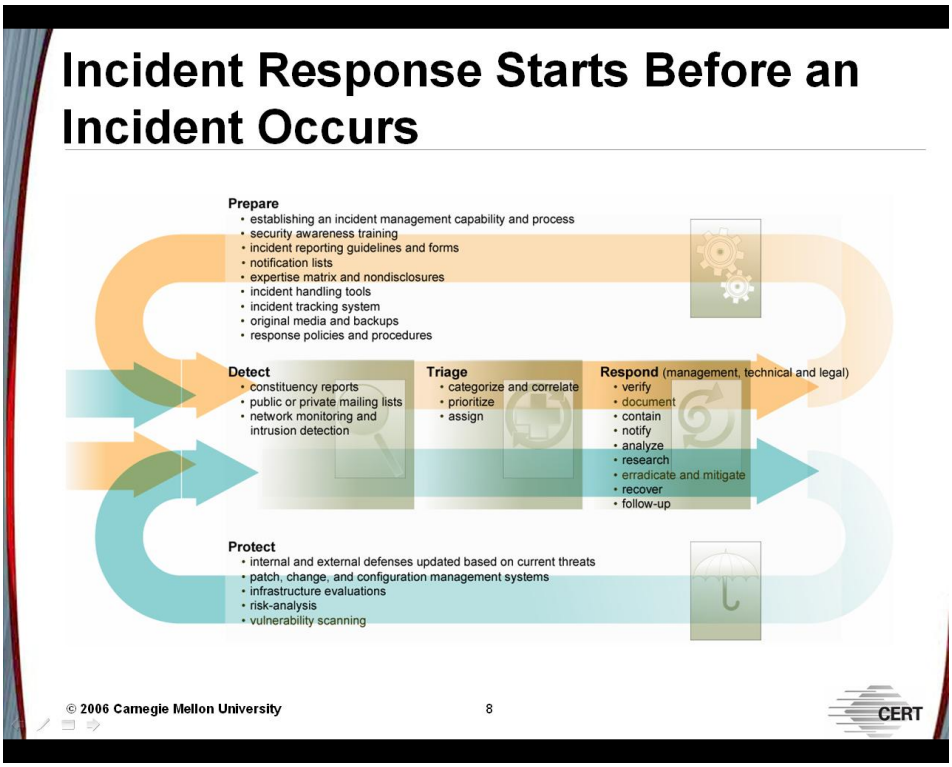
от *CERT/CC Курс за обучение*: Стъпки при създаването на ЦДКСКС



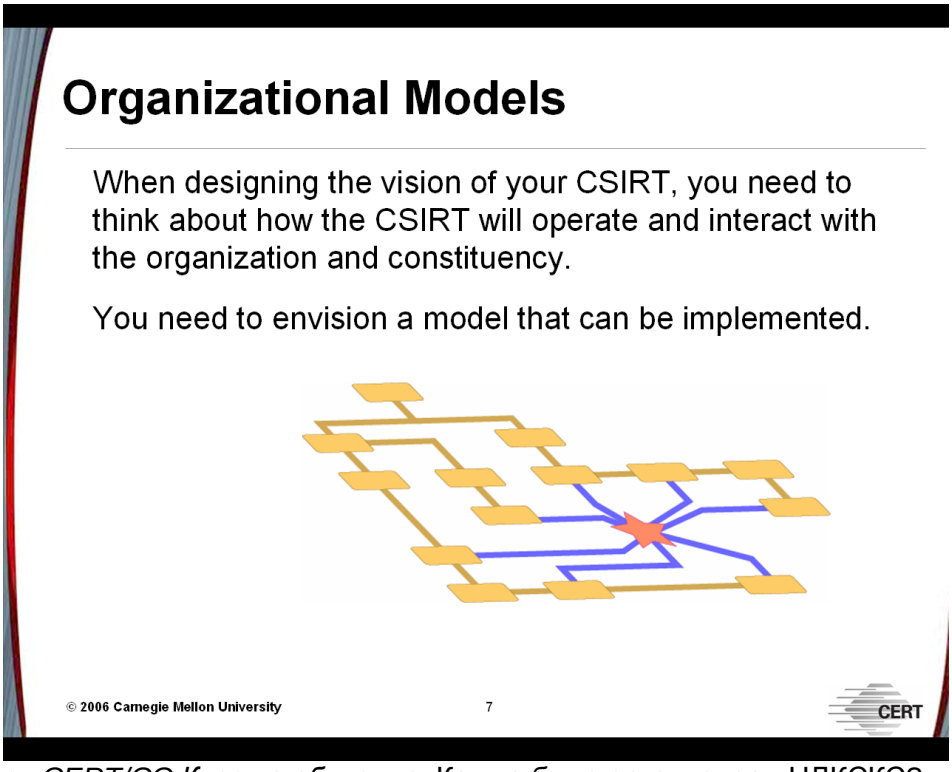
от *CERT/CC Курс за обучение:* Услуги, които може да предлага ЦДКСКС



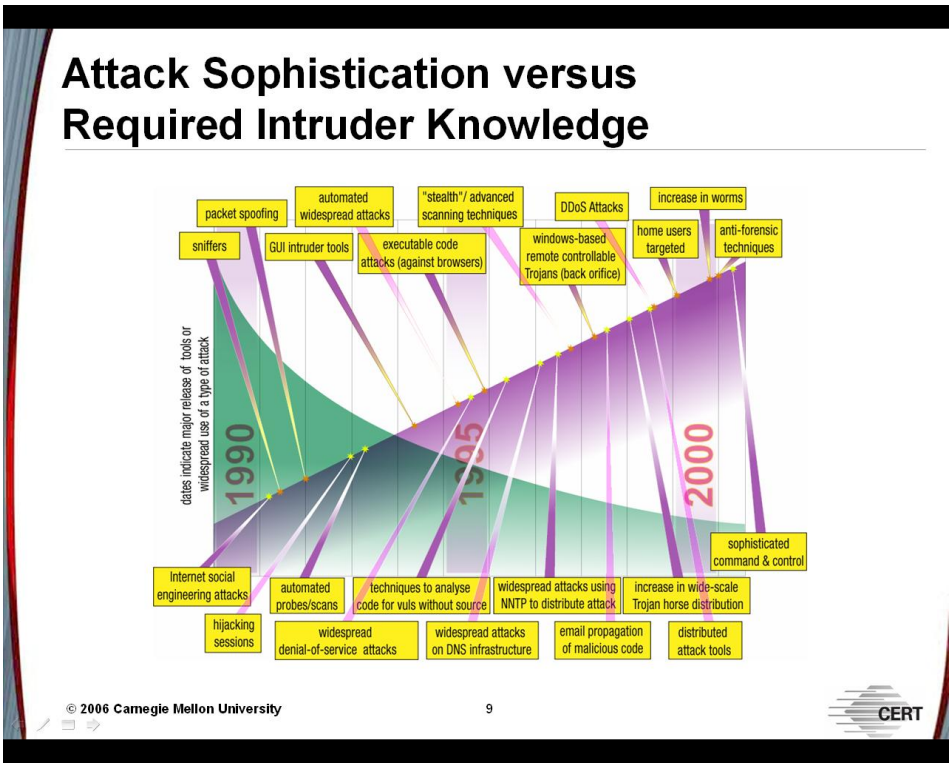
от *CERT/CC Курс на обучение:* Работен поток за управление на кризисни ситуации



от *CERT/CC Курс на обучение:* Действие при кризисни ситуации



от *CERT/CC Курс на обучение:* Как да бъде организиран ЦДКСКС?



от *CERT/CC Курс на обучение:* По-малко познания, повече вреди