Технически университет – София

ПГ по Компютърни Технологии и Системи - Правец

Упражнение - 2

СИСТЕМИ ЗА СИГУРНОСТ

Тема: Моделиране на инцидент в компютърната система и попълване на необходимите документи за неговото отработване

Изготвил:

Доц. д-р Румен Трифонов

1.Въведение

Обработката на инциденти в сферата на компютърната сигурност е важен компонент в ИТ сектора. Кибер атаките не само увеличават своя брой, но и щетите, които причиняват също. Нови типове инциденти свързани със сигурноста се срещат все по често. Превантивни дейности базирани на резултат от оценка на риска могат да намалят броя на инцидентите, но не всички инциденти могат да бъдат избегнати. Възможноста от обработката на инциденти е нужна з бързото откриване на инцидента, минимизиране на загубите и пораженията, намаляване на слабостите, които са открити и възстановяване на IT услуги.

Възможността на обработна на инциденти изисква значително планиране и ресурси. Постоянното следене за атаки е задължително. Установяването на точни процедури за приоритизиране на обработката на инциденти е критичина, както и имплементиране на ефективни методи са събиране, анализиране и рапортиране на данни.

Възможностите за обработка на инциденти трябва да включват следните действия:

А) Създаване на план за обработка на инциденти

Б) Разработване на процедури за изпълняване на обработка на инциденти и съобщаване.

В) Определяне на насоки за комуникация с участници свързани с инцидента.

Г) Избиране на структурата на екип за обработка на инциденти.

Д) Определяне на това какви услуги трябва да предоставя екипа за обработка на инциденти.

Е) Обучение на екипа за обработка на инциденти.

2.Организиране на възможностите за обработка на инциденти

Организиране на ефективна способност за обработка на инцидент (CSIRC) включва няколко основни решения и действия. Едно от първите съображения трябва да бъде да се създаде организационно-специфична дефиниция на термина "инцидент", така че обхвата на понятието е ясен. Организацията трябва да реши какви услуги екипът за отговор на инцидент следва да осигури. Създаване на план, политика и процедури за обработка на инциденти е важна част от създаването на екип, така че обработката на инцидент да се извършва ефективно, ефикасно и последователно, и така, че отборът има правомощия да направи това, което трябва да се направи. Планът, политиката и процедурите следва да отразяват взаимодействието на екипа с други отбори в рамките на организацията, както и с външни страни, като например в областта на правоприлагането, на медиите, както и други организации за обработка на инциденти .

2.1 Събития и инциденти.

Едно събитие е всяка наблюдавана поява в една система или мрежа. Събитията включват потребителско свързване към файл за споделяне на сървъра, получаване на искане за уеб страница, изпращане на електронна поща, както и защитна стена, която блокира опит за връзка. Нежеланите събития са събитията с отрицателен резултат, като например повреждащи система,флууединг на пакети, неразрешено използване на системни привилегии, неоторизиран достъп до чувствителни данни, както и изпълнение на зловреден код, който унищожава данни.

Инцидент е нарушение или непосредствена заплаха от нарушение на политики за компютърна сигурност, политики за приемлива употреба, или стандартни практики за сигурност. Примери на инциденти са са:

 Един нападател дава команда на бот за изпращане на големи обеми от заявки за свързване на уеб сървър, което го кара да се срине.

 Потребителите са подмамени да отворят доклад, изпратен чрез електронна поща, която е всъщност зловреден софтуер

 Един нападател получава чувствителни данни и заплашва, че подробностите ще бъдат пуснати публично, ако организацията не плати определена сума пари.

 А потребителят осигури или разкрива чувствителна информация на други лица чрез peer-to-peer услуги за споделяне на файлове.

2.2 Необходимост от Incident Response

Атаките често компрометират лични и бизнес данни, и това е много важно да се реагира бързо и ефективно, когато се появят нарушения на сигурността. Концепцията за реагиране на инциденти се превърна в широко приета и изпълнена. Една от ползите от които обработката на инциденти е, че тя поддържа отговор на инциденти систематично (т.е., следваща последователна методология за обработка на инциденти), така че са предприети съответните действия. Реагирането при инциденти помага на персонала за свеждане до минимум на загуба или кражба на информация и прекъсване на услугите, причинени от инциденти. Друга полза от реагиране на инциденти е възможността да се използва информация, получена по време на инцидент работа по-добра подготовка за последвали подобни обработки на инциденти и да предложи по добра сигурност на системите и данните. Възможността за обработка на инциденти също помогага за правилното справяне и с правни проблеми, които могат да се породят от инцидента.

2.3 Политика, план и действия при обработка на инциденти

2.3.1 Елементи на политиката на организацията

Политика за обработка на инциденти е силно индивидуализирана към организацията. Въпреки това, повечето политики включват същите основни елементи:

 Отчет за ангажираността на ръководството

 Цел и цели на политиката

 Обхват на политиката (на кого и за какво се отнася това и при какви обстоятелства)

 Дефиниция на инциденти в компютърната сигурност и свързаните с тях условия

 Организационна структура и определяне на роли, отговорности и нива на властта; трябва включва правомощията на екипа за реагиране на инциденти да конфискува или да прекъснете устройства и следи за подозрителни дейности, изискванията за докладване на някои видове инциденти, изискванията и насоки за външни комуникации, споделяне, препредаване и точки на ескалация в процеса на обработка на инцидента.

 приоритизация или рейтинговата тежест на инциденти

 мерки за изпълнение

 Reporting и форми за контакт.

2.3.2 Елементи на плата План Elements

Организациите трябва да имат официален, фокусиран и координиран подход за отговор на инциденти, включително план за обработка на инциденти, които предоставя възможност за имплементиране на целия план за обработка на инциденти. Всяка организация се нуждае от план, който да отговаря на нейните уникални изисквания, които се отнасят до мисия на организацията, размер, структура и функции. Този план трябва да използва необходимите ресурси и подкрепа на управлението. Планът за реагиране на инциденти трябва да включва следните елементи:

 мисия

 стратегии и цели

 Старши подход на мениджмънт

 организационен подход за реагиране на инциденти

 Как екипът на реагиране на инциденти ще комуникира с останалата част от организацията и с другиорганизации

 Условия за измерване на способността за реагиране на инциденти и нейната ефективност

 Как програмата се вписва в цялостната организация.

Мисията на организацията, стратегии и цели за реагиране на инциденти трябва да помогнат при определянето на структурата на своята способност за реагиране инцидент. Структурата на програмата реагиране на инциденти трябва да бъде обсъдено в рамките на плана.

2.3.3 Елементи на процедури

Процедурите трябва да се основават на политиката за реагиране на инциденти и плана. Стандартните оперативни процедури (СОП) са очертаване на конкретните технически процеси, техники, контролните списъци и формуляри, използвани от екипа за обработка на инциденти. СОП трябва да бъдат достатъчно изчерпателни и подробни, за да се гарантира, че следват насоките за обработка на инциденти. Освен това след стандартизирани реакции трябва да се минимизират грешките, по-специално тези, които могат да бъдат предизвикани от стрес при ситуации на обработка инциденти. СОП трябва да бъдат тествани, за да валидира тяхната точност и полезност, а след това да се разпределят всички членове на екипа .

2.3.4 Споделяне на информация с външни страни

Организации често се налага да общуват с външни лица в случай на инцидент. Друг пример е обсъждането на инциденти с други заинтересовани страни, като например Internet доставчици на услуги (ISP), продавач на уязвим софтуер, или други екипи за реагиране при инцидент.

Организациите могат също така активно да обменят съответната информация, която е индикатор за подобряване на откриване и анализ на инциденти. Екипът на реагиране на инциденти трябва да обсъди споделяне на информация с офиси на организацията на обществените дела, правен отдел и управление. Преди инцидент се случи да създават политики и процедури по отношение на обмена на информация. В противен случай, чувствителна информация по отношение на инциденти, може да бъде предоставена на неупълномощени лица, което потенциално

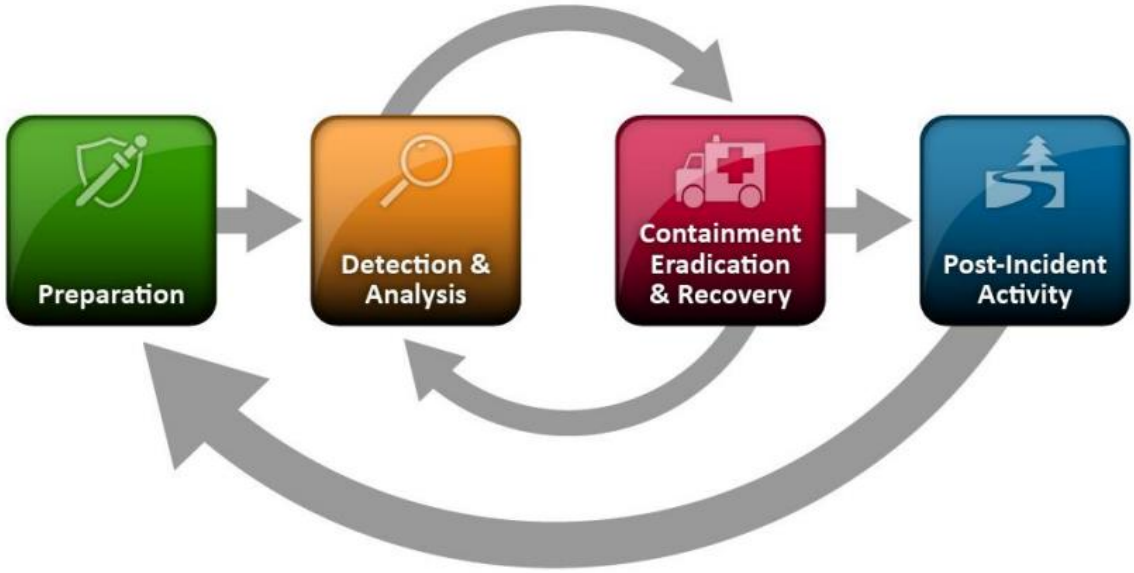
води до допълнително разрушаване и финансови загуби. Екипът трябва да документира всички контакти и комуникации с външни лица за отговорност и доказателствени цели.

Фигурата показва комуникация с външни институции

3. Обработка на инцидент

Процесът на реагиране на инциденти има няколко фази. Началната фаза включва създаване и обучение на екип за обработка на инцидент, отговор, и придобиване на необходимите инструменти и ресурси. По време на приготвянето организацията също така се опитва да ограничи броя на инциденти, които ще се появят чрез избиране и прилагане на набор от контроли въз основа на резултатите от оценките на риска. Въпреки това, остатъчен риск неизбежно ще се запази след провеждане на. При откриване на пробиви в сигурността е необходимо да се предупреди организацията. В съответствие със сериозността на инцидента, организацията може да се смекчи въздействието на инцидента, като го

задържаи и в крайна сметка се възстановяви от неги. По време на тази фаза, дейност често цикли обратно към откриване и анализ-например, за да се види дали допълнителните домакини са заразени със злонамерен софтуер докато трае премахването инцидент със зловреден софтуер. Ако след инцидента системата работи адекватно, организацията издава доклад, който описва причината и цената на инцидента и стъпките, които организацията трябва да предприеме, за да се предотврати бъдещи инциденти.



Жизнен цикъл на обработка на инцидент

3.1. Предотвратяване на Инциденти

Поддържане на броя на инцидентите разумно нискък е много важно за да се защитят бизнес процесите на организацията. Ако контролите за сигурност не са достатъчни, може да се появят по-големи обеми на инциденти. Това може да доведе до бавни и непълни отговори, които трансформират до по-голямо отрицателно влияние върху бизнеса (например, по-големи щети, по-дълги периоди на обслужване и липсата на данни).

Преглед на някои от основните препоръчителни практики за осигуряване на мрежи, системи и приложения:

 Оценка на риска. Периодични оценки на риска на системи и приложения трябва да определят какви рискове са породени от комбинации от заплахи и заплахи. Всеки риск трябва да бъде приоритет, а рискове могат да бъдат смекчени, прехвърлят, или да се приемат, докато се постигне разумно цялостно ниво на риск.

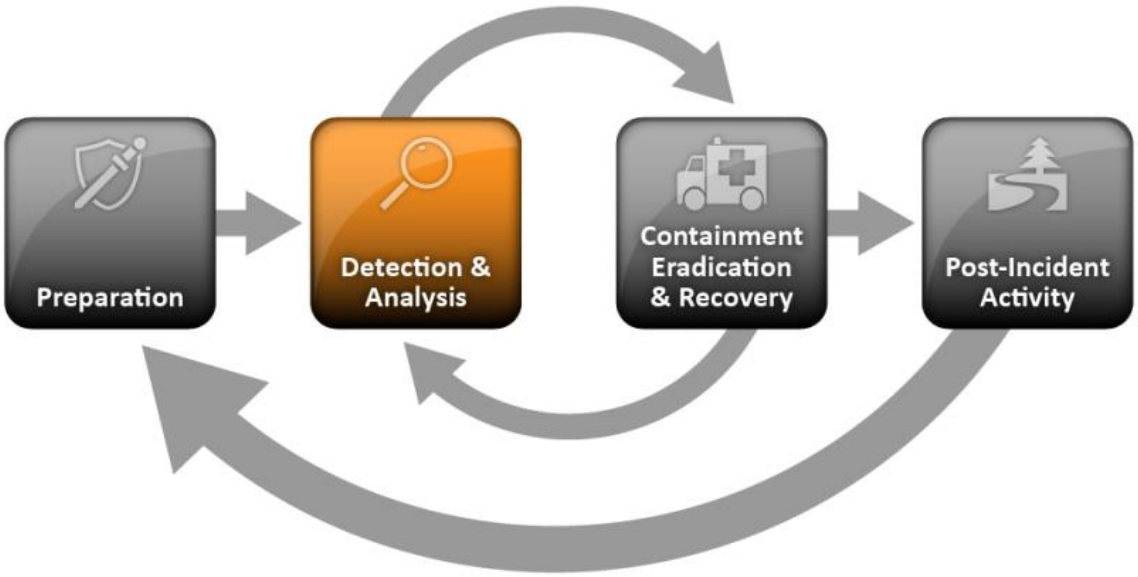
 Network Security. Периметъра на мрежата трябва да бъде конфигуриран да се забранят всички дейности, които не са изрично разрешени. Това включва осигуряване на всички точки на свързване, като виртуални частни мрежи(VPNs) и специални връзки с други организации.

 Malware превенция. Софтуер за откриване и спиране на злонамерен софтуер трябва да бъде разположен на територията на организацията. Malware защита трябва да бъде разположена на нивото на хост (например, сървър и работни станциионерационни системи), нивото на сървър за приложения (например, имейл сървър, уеб пълномощниците), както и прилагането на ниво клиент (например, клиенти за електронна поща, мигновени съобщения клиенти)

 User Информираност и обучение. Потребителите трябва да бъдат информирани за политики и процедури по отношение на подходящо използване на мрежи, системи и приложения.

IT персонал трябва да бъде обучен, така че те да могат да запазят своите мрежи, системи и приложения в съответствие със стандартите за сигурност на организацията.

3.2 Откриване и анализ



3.2.1 Видове атаки

Инциденти могат да се появят по безброй начини, така че е технически невъзможно да се развива стъпка по стъпка инструкции за работа на всеки инцидент. Организациите трябва да се приготвят обикновено да се справят с всеки инцидент, но трябва да се съсредоточат върху това да са готови да се справят с инциденти, които използват общи случай за атака. Различни видове инциденти имат различни стратегии за реагиране.

 Външен / Removable Media: зловредният код се разпространява върху система от заразено USB флаш устройство.

 Брутфорс: Една атака, която използва методи с груба сила, за да разрушава, или унищожи системи, мрежи или услуги (напр. DDoS, предназначени да ограничат или откажат достъп до дадена услуга или приложение;

 Web: An атака изпълнена от един уеб сайт или уеб-базирано приложение, например, крос-сайт скриптове цели да открадне пароли или пренасочване към сайт, който използва уязвимост в браузъра и инсталира зловреден софтуер.

 Email: чрез имейл съобщение или прикачен файл-например, използват код, преоблечен като приложен документ или линк към зловреден сайт в тялото на имейл съобщение.

 Impersonation: An атака, включваща подмяна на нещо доброкачествено с нещо злонамерено - всички атаки включват представяне под чужда самоличност.

 Неправилната употреба

 загуба или кражба на оборудване: загуба или кражба на изчислително устройството или носители , използвани от

организация, като например лаптоп, смартфон, или сертификати(електронен подпис).

 Други: Една атака, която не се вписва в нито една от останалите категории.

3.2.2Анализ

Откриване и анализ на инциденти ще бъде лесно, ако всеки прекурсор или показател са гарантирани и точни; За съжаление, не винаги случаят е такъв. Намирането на реални инциденти, които са се случили от всички показатели, може да се окаже трудна задача.

Извършване на първоначалния анализ и валидиране е предизвикателство. По-долу са препоръки за анализ инцидент :

 профил мрежи и системи. Профилирането е измерване на характеристиките на очакваната активност, така че промени в него може да бъде по-лесно идентифицирани. Примери за профилиране се изпълняват цялостна файлова проверка на сървърите за да се да извлече контролна сума за критични файлове и мониторинг на ползване мрежови трафик за определяне на средните и пикови нива на ползване в различни дни и часове.

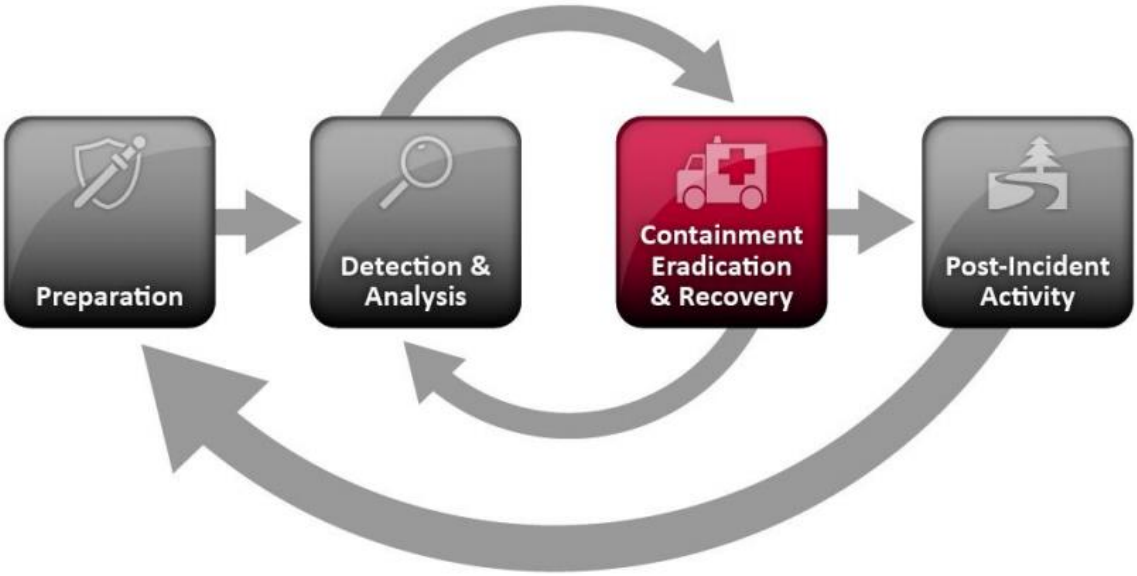
 Разберете нормално поведение на системата . Членовете на екипа за реагиране на инциденти трябва да разучат мрежите, системите,

и приложенията, за да разберат какво нормалното им поведение е така, че необичайно поведение може да бъде разпознато по-лесно.

Анализаторът трябва да бъде в състояние да забележите тенденции и промени с течение на времето.

 Извършване на Корелация на събитие. Доказателство на инцидент може да бъде заловен в няколко трупи, че всеки съдържа различни видове регистър на данни и защитната стена може да има източник на IP адрес, който се използва.

3.3. Задържане, премахване и възстановяване



3.3.1 Избор на Стратегия за задържане

Задържането е важно преди инцидент и предотвратява използването ресурси или увеличаване на вредите. Повечето инциденти изискват ограничаване, така че е важен фактор в началото на процеса на обработка на всеки инцидент.

Задържането осигурява време за разработването на съобразена стратегия за действие. Една съществена част от ограничаването е вземането на решения (напр. изключване на системата, изключване го от мрежата, деактивиране на определени функции). Такива решения са много по-

лесни да се направят, ако има предварително определени стратегии и процедури за поместване на инцидента. Организациите трябва да определят приемливи рискове при справянето с инциденти и развиват съответно стратегии.

Критерии за определяне на подходяща стратегия включват:

 Potential повреда и кражба на ресурси

 Необходимост от запазване на доказателства

 наличността на услуги (например, мрежова свързаност, услуги, предоставяни на външни лица)

 време и ресурси, необходими за изпълнение на стратегията

 ефективността на стратегията (например, частично ограничаване, пълно ограничаване)

3.3.2 Ликвидиране и възстановяване

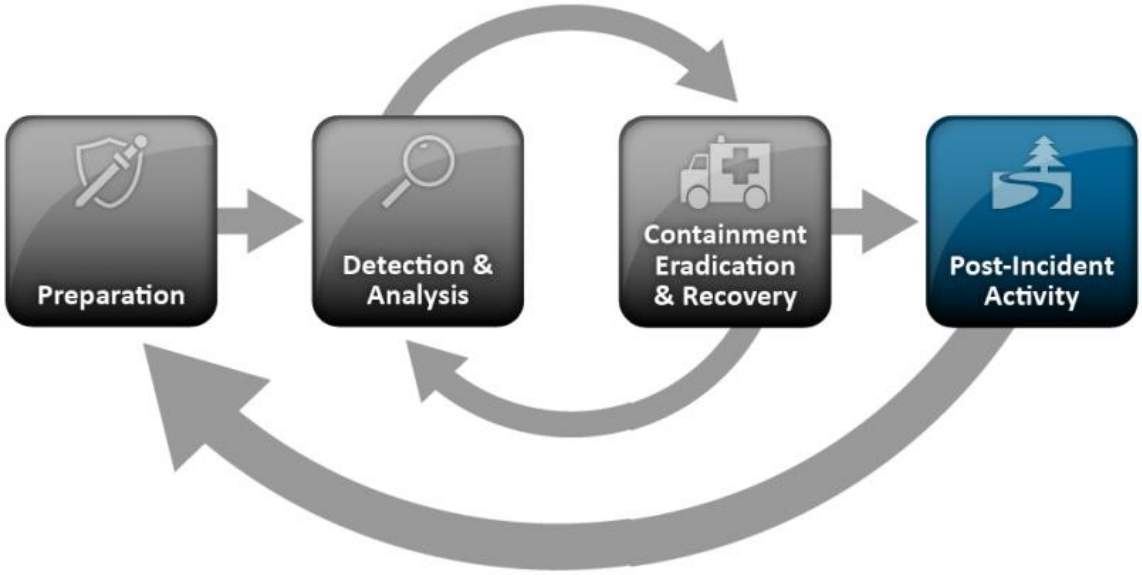
След като инцидента е овладян, изкореняване може да бъде необходимо да се премахнат съставки на:

инцидент, като например изтриване на зловреден софтуер и блокирането на нарушените потребителски акаунти, както и идентифициране и смекчаване на всички уязвимости, които са били експлоатирани. По време на ликвидиране, че е важно да се идентифицират всички засегнати

източници в рамките на организацията. За някои инциденти, изкореняване или не е необходимо или се извършва по време на възстановяването.

В процес възстановяване, администратори възстановят системите за нормална експлоатация, потвърждават, че системите функциониратнормално, и (ако е приложимо) рехабилитирани уязвимости за предотвратяване на подобни инциденти. Recovery може да включва такива действия, като възстановяване системи от чисти копия, възстановяване системи от нулата, заменяйки компрометирана файлове с чисти версии, инсталиране на кръпки, смяна на паролите, както и затягане на сигурността на мрежата.

3.4. След инцидентна активност



Един от най-важните части на реагиране на инциденти е също и най-често пропусната: изучаването и подобрението. Всеки отбор реагиране на инциденти следва да се развива, за да отрази новите заплахи, подобрена технология, и поуки.

Въпроси, които да се даде отговор включват:

 Точно какво се е случило, и по кое време?

 Колко добре персонала и управлението се справя с инцидента? Бяха ли документирани следващи процедури? Бяха ли достатъчно?

 Каква информация е необходима по-рано?

 Имало някакви стъпки или действия, предприети, които биха могли да потиснат възстановяването?

 Какво коригиращи действия могат да сепредприемат за да се предотвратят подобни инциденти в бъдеще?

 Какво са необходими допълнителни инструменти или средства за откриване, анализ и намаляване на бъдещи инциденти?

Използване Събрани данни от инцидента

С течение на времето, на събраните данни за инциденти трябва да бъдат полезни в няколко възможности. Данните, по-специално, общ брой часове на участие и разходите, могат да бъдат използвани, за да оправдае допълнително финансиране от отговора на инцидент екип. Едно проучване на характеристиките на инцидента може да посочи системни слабости и заплахи за сигурността, както и като промени в тенденциите за инциденти. Тези данни могат да бъдат пуснати обратно в процеса на оценка на риска, в крайна сметка, водещ до избора и прилагането на допълнителни мерки за контрол. Друго добро използване на данните е измерване на успеха на екипа за реагиране на инциденти. Ако данни з за инцидент се събират и съхраняват правилно, трябва да осигурят няколко мерки на успеха (или поне на дейностите) на екипа за реагиране на инциденти.

4. Задачи за изпълнение

1) Моделирайте инцидент във вашата компютърна система.

2) Направете стъпка „Предотвратяване на Инциденти“ от Жизнен цикъл на обработка на инцидент.

3) Направете стъпка „Откриване и анализ“ от Жизнен цикъл на обработка на инцидент.

4) Направете стъпка „Задържане, премахване и възстановяване“ от Жизнен цикъл на обработка на инцидент.

5) Направете стъпка „След инцидентна активност“ от Жизнен цикъл на обработка на инцидент.