ИДЕНТИФИКАЦИЈА И ВРЕДНУВАЊЕ НА КРИТИЧНИТЕ РЕСУРСИ И ПРОЦЕНА НА ВЛИЈАНИЕТО

1. Примери за идентификација на ресурси

За да спроведе вреднување на критичните ресурси, организацијата прво треба да ги идентификува своите критични ресурси. Може да се разликуваат два вида ресурси:

- Примарни ресурси:
  - работни процеси и активности и
  - информации
- Ресурси за поддршка (на коишто се потпираат основните елементи) од сите видови:
  - хардвер;
  - софтвер;
  - мрежа;
  - персонал;
  - место и
  - структура на организацијата

1.1. Идентификација на примарните ресурси

Оваа активност се состои во идентификување на основните ресурси, односно процесите, активностите и информациите. Оваа идентификација се врши од страна на мешана работна група којашто вклучува раководители, експерти за информатички системи и корисници на КИС (комуникациско-информатички системи).

Примарните ресурси се обично основните клучни процеси и информации при реализација на дејноста на организацијата. Други примарни ресурси, како што се процеси на работа во организацијата може исто да се земат предвид, што ќе биде посоодветно за подготвување политика за информатичка безбедност или на план за работен континуитет.

Примарните ресурси можат да бидат од два типа:

1. Работни процеси (или потпроцеси) и активности:

- процеси чија загуба или деградација го оневозможуваат извршувањето на работата;

- процеси што, ако се изменет, во голема мера може да влијаат на исполнувањето на работните задачи;
- Процеси што се неопходни за организацијата да биде во согласност со договорни, правни или регулаторни барања.

2. Информации:

- витални информации за остварување на мисијата на организацијата;
- лични информации, како што се дефинирани во согласност со националните закони за приватност;
- стратегиски информации потребни за постигнување на целите утврдени со стратегиските определби;
- информации со висока цена на чинење чиешто собирање, чување, обработка и пренос бара долго време и /или вклучува високи трошоци за стекнување.

1.2. Листа и опис на ресурсите за поддршка

Опсегот се состои од ресурси што треба да бидат идентификувани и опишани. Овие ресурси имаат ранливости што може да се искористат од закани што имаат цел да им нанесат штета на основните ресурси (процеси и информации). Тие може да бидат од различни видови.

ХАРДВЕР

Хардверот се состои од сите физички елементи за поддршка на процесите.

Опрема за обработка на податоци (активна)

Автоматска опрема за обработка на информации, вклучувајќи ги и деловите потребни за да работат самостојно.

Преносliва опрема

Преносна компјутерска опрема.

Примери: лап-топ компјутер, персонална дигитална поддршка (ПДП).

Фиксна опрема

Компјутерска опрема што се користи во просториите на организацијата.

Примери: сервер, микрокомпјутер којшто се користи како работна станица.

Периферни уреди за обработка

Опрема што е поврзана со компјутер преку комуникациска порта (сериски, паралелен линк, итн.) за внесување, пренесување или трансмисија на податоци.

Примери: печатач, преносен диск.

Носител на податоци (пасивен)

Ова се медиуми за чување на податоци или операции.

Електронски медиум

Информатички медиум што може да биде поврзан со компјутер или компјутерска мрежа за чување податоци. И покрај нивните компактни димензии овие медиуми може да содржат големи количини на податоци. Тие можат да се користат со стандардна компјутерска опрема.

Примери: флопи диск, CD-ROM, back-up касета, преносен хард диск, мемориски клуч, лента.

Други медиуми

Статични, неелектронски медиуми што содржат податоци.

Примери: хартија, слајд, документација, факс.

СОФТВЕР

Софтверот се состои од сите програми што придонесуваат за работа на склопот за обработка на податоци.

Оперативен систем

Ова ги вклучува сите програми на компјутерот што ја сочинуваат оперативната база од која работат сите други програми (сервиси или апликации). Тоа го вклучува јадрото и основни функции или услуги. Во зависност од составот, оперативниот систем може да биде монолитен или составен од микро јадра и пакет на системски услуги. Главните елементи на оперативниот систем се сите услуги за управување со опремата (процесор, меморија, диск и мрежни интерфејси), задача или услуги за управување процеси и услуги за управување кориснички права.

Сервисирање, одржување или администрирање софтвер

Софтверот се карактеризира со тоа што ги надополнува услугите на оперативниот систем и не е директно во служба на корисниците или апликациите (иако тоа обично е од суштинско значење, па дури и неопходно за генералната работа на информатичкиот систем).

Софтверски пакет или стандарден софтвер

Стандарден софтвер или софтверски пакет се целосно опремени производи со медиум, отстапување за користење и одржување. Тие обезбедуваат услуги за корисници и апликации, но не се персонализирани или специфични како што се бизнис-апликациите.

Примери: софтвер за управување со база на податоци, софтвер за електронски пораки, софтвер за датотеки, веб-сервер софтвер итн.

МРЕЖА

Типот на мрежа се состои од сите телекомуникациски уреди што се користат за интерконекција на неколку физички оддалечени компјутери или елементи на информатичкиот систем.

Медиум и поддршка

Комуникациските и телекомуникациските медиуми или опрема главно се карактеризираат со физичките и со техничките карактеристики на опремата (точка-до-точка, емитување) и со протоколите за комуникација (врска или мрежа ниво 2 и 3 на OSI – open system interconnection моделот со 7 нивоа).

Примери: јавна телефонска мрежа (PSTN), Ethernet, GigabitEthernet, асиметрична дигитална претплатничка линија (ADSL), спецификации за безжичен протокол (на пример WiFi 802.11), Bluetooth, FireWire.

Пасивно или активно реле

Овој поттип ги опфаќа сите уреди што не се логички прекини на комуникациите (ИС визија), но се посредници или реле уреди. Релеите се карактеризираат со протоколи за комуникација на поддржаната мрежа. Како додаток на основните релеи, тие често вклучуваат и рутирање и/или функции и услуги за филтрирање користејќи комуникациски прекинувачи и рутери со филтри. Тие често може да бидат администрирани од далечина и обично се способни за генерирање записи.

Примери: премостувач, рутер, хаб, свич, автоматска размена.

Интерфејс за комуникација

Интерфејсите за комуникација на единиците за обработка се поврзани со единиците на процесирање но се базираат врз протоколите за поддршка и медиумите, врз какво било инсталирано филтрирање, записи или функции за предупредување и од можноста и потребата за далечинско управување.

Примери: General Packet Radio Service (GPRS), Ethernet адаптер.

ПЕРСОНАЛ

Типот на персонал се состои од сите групи на луѓе што се вклучени во информатичкиот систем.

Носител на одлуки

Носителите на одлуки се сопствениците на основните ресурси (информации и функции) како и раководителите на организацијата или на одреден проект.

Примери: топ-менаџери, проект-лидер.

Корисници

Корисниците се персоналот што ракува со чувствителни елементи во контекст на нивната активност, за што има посебна одговорност. Персоналот може да има специјални права за пристап до информатичкиот систем за извршување на секојдневните задачи.

Примери: управување со човечки ресурси, финансиски менаџмент, менаџер на ризик.

Оперативен персонал/персонал за одржување

Тоа се лицата задолжени за функционирање и одржување на информатичкиот систем. Тие имаат специјални права за пристап до информатичкиот систем за извршување на нивните секојдневни задачи.

Примери: систем-администратор, администратор на податоци, back-up оператор, Help Desk оператор, оператор за инсталирање апликации, безбедносни офицери.

Програмери

Програмерите се задолжени за развој на апликации на организацијата. Тие имаат пристап до дел од информатичкиот систем со право на пристап на високо ниво, но не учествуваат во продуцирањето податоци.

Примери: програмери за бизнис-апликации.

МЕСТОПОЛОЖБА (SITE)

Местоположбата се состои од сите места каде што се вршат активности или делумен број активности како и од физичките средства потребни за извршување на работата.

Локација

Надворешна средина

Ова се однесува на сите локации во кои организациските средства за безбедност не може да се применат.

Примери: домовите на персоналот, просториите на друга организација, средината надвор од работниот простор (урбано подрачје, опасна област).

Простории

Ова место е ограничено со периметарот на организацијата што е во директен контакт со надворешноста. Ова може да биде физичка заштитна граница добиена преку создавање физички бариери или средства за надзор околу зградите.

Примери: установа, згради.

Зона

Зоната се формира од физичката заштитна граница што формира прегради во рамките на просториите на организацијата. Тоа се постигнува преку создавање физички бариери околу инфраструктурата на организацијата каде што се обработуваат информации.

Примери: канцеларии, зони со контролиран пристап, безбедносна зона.

Основни услуги

Сите услуги што се потребни за опремата на организацијата да функционира.

Комуникација

Телекомуникациски услуги и опрема обезбедени од страна на операторот.

Примери: телефонска линија, PABX- Private Automatic Branch Exchange, внатрешни телефонски мрежи.

Комунални услуги

Услуги и средства (извори и инсталација) потребни за обезбедување електрична енергија, до опремата од информатичка технологија и периферните уреди.

Примери: низок напон за напојување, инвертор, електрични кола.

Снабдување со вода.

Отстранување на отпадот.

Услуги и средства (опрема, контрола) за ладење и прочистување на воздухот.

Примери: разладни цевки за вода, климатизери.

ОРГАНИЗАЦИЈА

Типот на организацијата ја опишува организациската рамка којашто се состои од сите структури на персоналот на коишто им е доделена одредена задача и од процедурите за менаџирање со овие процедури.

Авторитети

Тоа се тела од кои односната организација ја црпи својата надлежност (авторитет).

Примери: административно тело, седиште на организацијата.

Структура на организацијата

Се состои од различни гранки на организацијата, вклучувајќи ги нејзините вкрстени функционални активности, коишто се контролирани од страна на менаџментот.

Примери: управување со човечки ресурси, ИТ менаџмент, управување со набавките, управување со деловна единица, градење на безбедносни услуги, противпожарна служба, ревизија.

Организација на проектот или системот

Се однесува на устроеноста на организацијата за специфичен проект или услуга.

Примери: нов проект за развој на апликации, проект за миграција на информатичкиот систем.

Подизведувачи / добавувачи / производители

Тоа се организации коишто ѝ обезбедуваат на организацијата некоја услуга или ресурси и се обврзани на тоа со договор.

Примери: компанија за управување со објектите, надворешна (outsourcing) компанија, консултантски компании.

2. Вреднување на ресурсите

Следниот чекор по идентификација на ресурсите е да се одреди скалата за процена којашто треба да се користи и критериумите за определување на позиција на таа скала за секој ресурс, врз основа на спроведено вреднување. Поради разновидноста на ресурсите што се наоѓаат во повеќето организации, веројатно е дека некои ресурси коишто имаат позната парична вредност ќе бидат вреднувани во локалната валута, додека другите што имаат повеќе квалитативна вредност може да им се додели вредност што ќе се движи, на пример, од „многу ниско“ до „многу високо“. Одлуката да се користи квантитативна скала наспроти квалитативната скала е одлука на самата организација, но таа одлука треба да биде релевантна во однос на ресурсите што се вреднуваат. И двата видови вреднување би можеле да се користат за истиот ресурс.

Типични термини што се користат за квалитативна процена на ресурсите вклучуваат зборови како што се: занемарливо, многу ниско, ниско, средно, високо, многу високо и критично. Изборот и опсегот на терминте соодветни за организацијата во голема мера зависи од безбедносните потреби на организацијата, големината и други специфични фактори на организацијата.

Критериуми

Критериумите што се користат како основа за доделување на вредност на секој ресурс треба да бидат напишани со јасни и недвосмислени термини. Ова често е еден од најтешките аспекти на вреднувањето на ресурсите, бидејќи вредностите на некои ресурси можеби ќе треба да бидат субјективно определени, а најверојатно различни поединци ќе го вршат определувањето. Можните критериуми што ќе се користат за утврдување на вредноста на ресурсот го вклучуваат: основниот трошок, трошокот за негова замена или повторно создавање или пак неговата вредност може да биде апстрактна, на пример, вредноста на угледот на организацијата.

Друга основа за вреднување на ресурсите се трошоците настанати поради загубата на доверливост, интегритет и достапност како резултат на инцидент. Неотповикливоста, одговорноста, автентичноста и веродостојноста треба исто така да се земат во предвид.

Во текот на вреднувањето, може да се случи на многу ресурси да им бидат назначени неколку вредности. На пример: бизнис-планот може да се вреднува врз основа на трудот вложен за да се развие планот, би можел да се вреднува во однос на трудот за внесување на податоците, а може да се вреднува и врз основа на неговата вредност за конкурентот. Секоја од доделените вредности најверојатно значително ќе се разликува. Доделената вредност може да биде максимумот од сите можни вредности или може да биде збир на некои или на сите можни вредности. Во финалната анализа, треба внимателно да се утврди која вредност или кои вредности ќе му се доделат на ресурсот, бидејќи конечната вредност влегува во

одредувањето на другите ресурси што треба да бидат искористени за заштита на односниот ресурс.

Сведување до заедничка основа

Сите вреднувања на средствата треба да се сведат на заедничка основа. Ова може да се направи со помош на критериуми, како оние што следат. Критериумите што може да се користат за да се проценат можните последици од губењето на доверливоста, интегритетот, достапноста, одговорноста, автентичноста или доверливоста на ресурсите се:

- повреда на закон и /или пропис
- оштетување на бизнис-перформансите
- губење на добрата волја /негативен ефект врз угледот
- нарушувања поврзани со лични информации
- загрозување на личната безбедност
- спротивни ефекти од спроведувањето на законот
- нарушување на доверливоста
- нарушување на јавниот ред и мир
- финансиска загуба
- нарушување на деловните активности
- загрозување на безбедноста на средината

Друг пристап за процена на последиците може да биде:

- прекин на услуга
  - неможност да се обезбедат услуги
- губење на довербата на клиентите
  - губење на кредибилитетот во внатрешниот информатички систем
  - штета на угледот
- нарушување на внатрешното работење
  - нарушување внатре во самата организација
  - дополнителни внатрешни трошоци
- нарушување на работата на трети страни:
  -нарушување кај трети страни кои соработуваат со организацијата
  - различни видови на повреди
- повреда на закони /прописи:
  - неспособност да се исполнат законските обврски
- прекршување на договорот:
  - неспособност да се исполнат договорните обврски
- опасност за безбедноста на персоналот/корисникот:

-опасност за вработените и /или корисниците на организацијата

- напад врз приватниот живот на корисниците
- финансиски загуби
- финансиски трошоци за итни случаи или поправки:
  - за персонал,
  - за опрема,
  - за проучувања, извештаи на експерти
- губење стока /фондови /средства
- губење клиенти, губење добавувачи
- судски постапки и казни
- губење конкурентска предност
- губење на технолошкото/ техничко водство
- губење на ефективноста /довербата
- губење на техничката репутација
- слабеење на преговарачкиот капацитет
- индустриски кризи (штрајкови)
- владина криза
- разрешување
- материјална штета

Овие критериуми се примери што треба да се земат предвид при вреднување на ресурсите. Притоа, организацијата треба да избере критериуми релевантни за нејзиниот делокруг на работа и безбедносни потреби. Тоа значи дека некои од критериумите наведени погоре можеби не се применливи, додека други ќе треба да се додадат на листата.

Скала

По утврдувањето на критериумите што треба да се земат предвид, организацијата треба да се согласи за скалата за процена што ќе се користи на ниво на цела организација. Првиот чекор е да се одлучи за бројот на нивоа коишто ќе се користат. Не постојат правила во однос на бројот на нивоа. Повеќе нивоа обезбедуваат поголемо ниво на разграничување, но понекогаш и премногу тесна диференцијација го отежнува конзистентното доделување задачи во организацијата. Нормално, секој број на нивоа помеѓу 3 (на пример, ниско, средно и високо) и 10 може да се користи сè додека тоа е во согласност со пристапот што го користи организацијата за сиот процес за проценка на ризикот.

Една организација може да ги дефинира своите граници за вредност на средствата, како „ниско ниво“, „средно“ или „високо“. Овие ограничувања треба се користат според избраните критериуми (на пример, за можни финансиски загуби тие треба да бидат дадени во парични вредности, но за фактори како што е загрозување на личната безбедност, паричното вреднување може да биде

комплексно и да не биде соодветно за сите организации). Всушност, останува на организацијата да одлучи што ќе се смета за „ниска“ или за „висока“ последица. Последица што би можела да биде катастрофална за мала организација може да биде ниска или дури и занемарлива за многу голема организација.

Меѓузависности (влијанија)

Колку повеќе релевантни и бројни се процесите коишто се поврзани со ресурсот, толку е поголема вредноста на тој ресурс. Меѓусебното влијание на ресурсите на работните процеси и другите ресурси треба, исто така, да се идентификува бидејќи тоа би можело да влијае на вредноста на ресурсите. На пример, доверливоста на податоците треба да се чува во текот на сиот нивен животен циклус, во сите фази, вклучувајќи складирање и обработка. Со други зборови, безбедносните потреби за складирањето на податоците и програмите за обработка треба да бидат директно поврзани со вредноста што ја претставува доверливоста на податоците што се чуваат и обработуваат. Исто така, ако бизнис-процесот се потпира на интегритетот на одредени податоци што се продуцирани од страна на програма, влезните податоци на оваа програма треба да бидат со соодветна веродостојност. Покрај тоа, интегритетот на информациите ќе зависи од хардверот и софтверот што се користат за нивно складирање и обработка. Исто така, хардверот ќе зависи од снабдувањето со електрична енергија и можеби од климатизацијата. Оттука информациите за меѓузависностите ќе помогнат во идентификување на заканите и особено ранливостите. Исто така, тие ќе помогнат да се определи вистинската вредност на ресурсите (врз основа на односите на зависност), притоа укажувајќи на соодветно ниво на заштита.

Вредноста на ресурсите од коишто зависат други ресурси може да биде изменета на следниов начин:

- Ако вредноста на зависните ресурси (на пример податоци) е пониска или еднаква на вредноста на ресурсот што се разгледува (на пример софтвер), неговата вредност останува иста.
- Ако вредноста на зависниот ресурс (на пример податоци) е поголема, тогаш вредноста на односниот ресурс (на пример софтвер) треба да се зголеми во зависност од:
  - степенот на зависност;
  - вредностите на другите ресурси.

Една организација може да има некои ресурси коишто се достапни во поголем број, како што се копии на софтверски програми или еден ист тип на компјутерот се користи во повеќето канцеларии. Важно е овој факт да се разгледа кога се прави вреднување на ресурсите. Од една страна, овие ресурси се занемаруваат лесно, па затоа треба да се води грижа сите да се идентификуваат; од друга страна, тие може да се искористат за да се намалат проблемите сврзани со достапноста.

Излез (резултат)

Конечниот резултат на овој чекор е листа на ресурси и нивните вредности во однос на разоткривање (зачувување на доверливоста), модификација (зачувување на интегритетот, автентичноста и одговорноста), недостапност и уништување (запазување на достапност и веродостојност) и трошоците за замена.

3. Процена на влијанието

Инцидент во информатичката безбедност може да влијае на повеќе од еден ресурс или само на дел од ресурсот. Влијанието е поврзано со степенот на реализација на инцидентот. Како последица на тоа, постои значајна разлика помеѓу вредноста на ресурсот и влијанието што е резултат на инцидентот. Влијанието се разгледува како постоење на непосреден (оперативен) ефект или ефект во иднина што вклучува финансиски и пазарни последици.

Непосредното (оперативно) влијание е или директно или индиректно.

Директно:

а) финансиската вредност за замена на изгубено (дел од) ресурс;

б) трошоците за набавка, конфигурација и инсталација на ново ресурс или на резерва;

в) трошоците за откажаните активности поради инцидентот сè додека не се обноват услугите кои ги обезбедува ресурсот(ите);

г) резултати од влијанието при нарушување на безбедноста на информациите.

Индиректно:

а) трошоци за исползување на можноста (финансиски средства што биле потребни за замена или поправка на ресурсите би биле искористени за друга цел);

б) трошоци за прекинати активности;

в) потенцијална злоупотреба на информациите добиени преку безбедносно нарушување;

г) повреда на статутарни или регулаторни обврски;

д) повреда на етичките кодекси на однесување.