

Технологии за управление на рисковете при информационните системи

Наличието на система за управление на рисковете е задължителен елемент от цялата система за осигуряване на информационна сигурност по всяко време от жизнения цикъл. Под управление на информационните рискове (Risk Management for Information Technology Systems) се разбира процесът на идентификация и елемениране или намаляване на рисковете които могат да въздействат върху информационната система.

Основните понятия с които се работи по-нататък в материала са:

Заплаха- *съвкупност от условия и фактори които могат да станат причина за нарушаване на целостта, достъпността и конфиденциалността на информацията.*

Уязвимост- *слабост в системата за защита която прави възможна реализацията на заплахата.*

Отношението на една организация към въпросите на информационната сигурност е критерий за нейната степен на зрялост. При разработения от *Carnegie Mellon University* модел на организация са въведени 5 нива на зрелост, които по правило съответстват на различното разбиране проблемите за информационната сигурност в организациите.

На първото ниво въпроса по принцип не се поставя от ръководството на организацията. Но това не значи че той не се решава от сътрудниците ѝ по тяхна собствена инициатива и то ефективно.

На второ ниво въпроса за осигуряване на информационна сигурност се решава неформално въз основата на постепенно трупаш се опит. **Тук въпросът за ефективността на защитата не се поставя.** По такъв начин с времето се създава списък от актуални за организацията класове от рискове, който постепенно се попълва. **Ако не се случат сериозни инциденти, то ръководството на организацията не счита въпросите на информационната сигурност за приоритетни.** При сериозен инцидент създадената система за сигурност се коригира.

На трето ниво в организацията се счита за целесъобразно в една или друга степен да се спазват международните стандарти които осигуряват базовото ниво на информационна сигурност, като на въпросите на документирането се отделя нужното внимание.

При четвърто ниво за ръководството на организацията са актуални въпросите за измерване и контрол на параметрите описващи режима на информационна сигурност. На това ниво *ръководството съзнателно приема върху себе си отговорността за избор на определени размери на остатъчните рискове (те остават винаги).* Рисковете по правило се оценяват по няколко критерия и те не са само стойности.

Технологията за управление на режима на информационна сигурност остава същата, както и на трето ниво, *но на етапа на анализ на рисковете се прилагат количествени методи, които позволяват да се оценят параметрите на остатъчните рискове и ефективността на различните варианти за противодействие при управление на рисковете.*

На пето ниво се поставят и решават следните варианти на оптимизационни задачи в областта на гарантиране на режима на информационна сигурност:

- а) Избор на подсистема за информационна сигурност, оптимизиран според критерия *цена/ефективност* при зададено ниво на остатъчните рискове;
- б) Избор на подсистема за информационна сигурност при който да се минимизират остатъчните рискове, при зададена цена на подсистемата за сигурност;
- в) Избор на архитектура на подсистема за информационна сигурност с минимална цена за притежание през времето на жизнения ѝ цикъл при определено ниво на остатъчните рискове.

Нива на зрялост на организацията

Ниво 1 - “Анархия”

Признаци:

- сътрудниците сами определят кое е добро и кое лошо;
- разходите и качеството не се прогнозира;
- няма формализирани планове;
- няма контрол върху промените;
- висшето ръководство няма представа за реалното състояние на нещата.

Ниво 2- “Фолклор”

Признаци:

- доловена е определена повторимост на организационните процеси;
- опитът на организацията е представен като “предания от корпоративната митология”;
- знанията се натрупват като личен опит на сътрудниците и се губят при напускането им;

Ниво 3- “Стандарти”

Признаци:

- корпоративната митология е документирана;
- процесите са повторяеми и не зависят от личните качества на изпълнителите;
- не се събира информация за процесите измерващи ефективността;
- наличието на формализирано описание на процесите не означава че те работят;
- организацията започва да адаптира опита си към спецификата на бизнеса;
- прави се анализ на знанията и уменията на сътрудниците с цел да се определи нужното ниво на компетентност;

Характеристики на организацията в областта на информационната

сигурност

Политиката в областта на информационната сигурност (ИС) не е формализирана, ръководството не се занимава с тези въпроси. С осигуряване на ИС, сътрудниците могат да се занимават по своя инициатива в съответствие със своите разбирания за задачите. Работоспособността на ИС зависи от професионалните и морални качества на сътрудниците.

На ниво ръководство има някакво разбиране на задачите отнасящи се до ИС. Съществуват стихийно създадени процедури за осигуряване на ИС, но тяхната пълнота и ефективност не се анализират. Процедурите не са документирани и напълно зависят от личностите на въвлечените в тях сътрудници. Ръководството не поставя задачи по формализацията на процедурите за защита на информацията.

Ръководството разбира задачите в областта на ИС.

В организацията има документация (по-вероятно непълна) относно политиката на ИС.

Ръководството е заинтересовано от използването на стандарти в областта на ИС, има документация за тях. Осъзната е необходимостта от управление режима на ИС през всички фази от жизнения цикъл на информационната технология.

- разработва се стратегия за развитие на компетентността;

Ниво 4- “Измеряемо”

Признаци :

- измеряеми
- стандартизирани

Има пълен комплект от документи които се отнасят до осигуряване на режима на ИС и те са оформени в съответствие с някакъв стандарт.

Инструкциите се спазват, документите служат като ръководство за работа на длъжностните лица.

Редовно се извършва вътрешен и външен одит в областта на ИС.

Ръководството отделя нужното внимание на въпросите на ИС и има адекватна представа за съществуващите нива на заплахи, уязвимости и потенциални загуби в случай на възможни инциденти.

Ниво 5- “Оптимизируемо”

Признаци:

- фокусиране върху повторяе-

моста и измерване на ефективността и оптимизацията;

- фиксиране цялата информация за функциониране на процесите

Ръководството е заинтересовано от количествена оценка на съществуващите рискове и е готово да поеме отговорност за

избора на определени нива остатъчни рискове, да поставя оптимизационни задачи за изграждане на система за защита на информацията.

Подходи за управление на рискове

Организациите прилагат варианти на система за управление на рисковете, започвайки от третото ниво на зрелост. Националните институти по стандартите в индустриално развитите страни и организациите специализирали се в комплексно решаване на въпросите на информационната сигурност имат близки концепции за управление на информационните рискове, за пример ще разгледаме прилагания в САЩ стандарт **NIST 800-30**.

Управление на рисковете

Системата за управление на информационните рискове трябва да минимизира възможните негативни последици свързани с използването на информационната технология и да осигурят възможност за изпълнение на основните бизнес цели на организацията. Тази система трябва да бъде интегрирана в системата за управление на жизнения цикъл на информационната система.

Фаза от жизнения цикъл на информационната система (ИС)

1. Предпроектна фаза на ИС (концепция за дадена ИС: определяне на целите, задачите и документирането им).
2. Проектиране на ИС

3. Изграждане на ИС: доставка на елементи, монтаж, настройка

Съответствие на фазата с управлението на риска

Откриване на основните класове рискове за дадена ИС, произлизащи от целите и задачите на концепцията за осигуряване. Откриване на специфичните рискове за дадена ИС, произлизащи от особеностите на архитектурата на ИС.

Преди започване функционирането на ИС, трябва да се идентифицират и вземат под

и конфигуриране.

внимание всички класове рискове.

4. Функциониране на ИС

Да се прави периодична преценка на рисковете, породена от промяна на външните условия и в конфигурацията на ИС.

5. Функционирането на ИС се прекратява- информационните и изчислителни ресурси повече не се използват по предназначение.

Спазване на изискванията за информационна сигурност по отношение на извежданите от работа информационни ресурси.

Идентифициране на рисковете

При всяка методика трябва да се идентифицират рисковете и техните компоненти- заплахите и уязвимостите. Основното изискване към един списък от рискове е неговата пълнота. На базовото ниво на безопасност (трето ниво на зрелост на организацията) е достатъчно да се използва подходящ за конкретния случай стандартен списък на класове рискове.

Оценка на рисковете

Може да се отделят следните три аспекта: а) скали и критерии, по които може да се измерва риска; б) оценка на вероятността за събитието; в) измерване на рисковете.

Скали и критерии по които се измерва риска

Скалите са преки (естествени) или косвени (производни). Пример за преки скали са скалите за измерване на физически величини, напр. секунда за измерване на време.

В много случаи преки скали няма и се налага да се използват или преки скали за други свойства, свързани с интересуващите ни, или да се определят нови скали. Например скалата за измерване на субективното свойство "Ценност на информационния ресурс". Тя може да се измерва в производни скали като *стойност за възстановяване на ресурса и време за възстановяване на ресурса*. Друг вариант е да се определи скала за получаване на експертна оценка, където: а) Малоценен информационен ресурс, от който не зависят критични задачи и той може да бъде възстановен с неголеми разходи на време и средства; б) Ресурс със средна ценност, от който зависят редица важни задачи, но в случай на загубата му той може да бъде възстановен за време по-кратко от критически допустимото и стойността на възстановяването му е висока; в) Ценен ресурс, от който зависят критически важни задачи, в случай на загуба, времето за възстановяването му превишава критически допустимото или стойността на възстановяване е прекалено висока.

От споменатото дотук може да се направи извода че, **за измерване на рисковете няма естествена скала.**

Рисковете могат да се оценяват по *обективни или субективни критерии*. При методиките за анализ на риска *се използват субективни критерии, измервани в качествени скали* защото, *оценката трябва да отразява субективната гледна точка на собственика на информационни ресурси и трябва да се отчитат не само техническите, но и организационните, психологическите и други аспекти.*

Обективни и субективни вероятности

За думата “вероятност” има две тълкувания които се означават със словосъчетанията “обективна вероятност” и “субективна вероятност”. **Под обективна (физическа) вероятност се разбира относителната честота за поява на дадено събитие в общия обем от наблюдения, или отношението на броя благоприятни изходи към общия им брой.** Обективната вероятност се появява при анализ на резултатите от голям брой наблюдения станали в миналото.

Под субективна вероятност се разбира мярата на увереност на даден човек, или група от хора, че дадено събитие ще се случи. Най-често субективната вероятност представлява вероятностна мера получена по експертен начин.

За получаване на оценки за субективна вероятност има три етапа:

а) Подготвителен; б) Получаване на оценки; в) Анализ на получените оценки.

Първи етап. Формира се обекта на изследване- множеството от събития, извършва се предварителен анализ на свойствата на това множество (установява се зависимостта или независимостта на събитията, дискретността или непрекъснатостта на случайната величина пораждаща даденото множество от събития). На основата на този анализ се избира един от подходящите методи за получаване на субективна вероятност. На този етап се извършва и подготовката на експертите, запознаването им с метода и проверка на разбиранията им за поставената задача.

Втория етап включва използването на метода избран на първия етап. Резултат от него е набор от числа който отразява субективния възглед на групата от експерти, за вероятността от едно или друго събитие. Това обаче далеч не може да се смята като окончателно получено разпределение защото може да бъде противоречиво.

Третия етап е изследване на резултатите от допитването. Ако вероятностите получени от експертите не се съгласуват с аксиомите за вероятности, то за това се обръща внимание на експертите и се прави уточняване на отговорите с цел съответствието им с аксиомите.

Измерване на рисковете с оценка по два фактора

Има много подходи за измерване на рисковете но най разпространени са – *оценка по два фактора и оценка по три фактора.* Поради относителната му простота ще се спрем само на първия от тях.

В най-простия случай се използва оценката на два фактора: *вероятност за случване на произшествие и тежест от възможните му последици.* Приема се че риска е толкова по-голям, колкото по-голяма е вероятността за случване на произшествие и тежестта от възможните му последици. Смисълът се показва с формулата:

РИСК= Вероятност за случване на произшествие * Цена на загубите

Ако променливите са количествени величини то тогава риска е оценка на математическите очаквания за загуби. Но ако променливите са качествени величини то тогава операцията умножение не е определена.

Ще разгледаме варианта с качествените величини, който е по-често срещаният в практиката. В началото се определят скалите.

1. Субективната скала за вероятността от събития включва: **А-** Събитието практически никога не се случва; **В-** Събитието се случва рядко; **С-** Вероятността от случване на събитието през разглеждания интервал от време е около 0,5; **Д-** По вероятно е събитието да се случи; **Е-** Събитието почти сигурно ще се случи.

2. Субективна скала за сериозността на произшествията:

N (Negligible)- Въздействието може да се пренебрегне.

Mi (Minor)- Незначително произшествие, последствията са лесно отстраними, разходите за ликвидиране на последиците не са големи.

Mo (Moderate)- Произшествие с умерени последици, ликвидирането им не е свързано с големи разходи, не са засегнати критически важните задачи.

S (Serious)- Произшествие със сериозни последици, ликвидирането им е свързано с големи разходи, въздействието върху информационните технологии е съществено, влияе върху изпълнението на критически важни задачи.

C (Critical)- Произшествието води до невъзможност за решаване на критически важни задачи.

За оценка на рисковете има скала с три значения: Нисък, Среден и Висок риск.

Рискът за определено събитие, зависещ от два фактора може се определи така:

| | Negligible | Minor | Moderate | Serious | Critical |
|----------|-------------------|--------------|-----------------|----------------|-----------------|
| A | Нисък риск | Нисък риск | Нисък риск | Среден риск | Среден риск |
| B | Нисък риск | Нисък риск | Среден риск | Среден риск | Висок риск |
| C | Нисък риск | Среден риск | Среден риск | Среден риск | Висок риск |
| D | Среден риск | Среден риск | Среден риск | Среден риск | Висок риск |
| E | Среден риск | Висок риск | Висок риск | Висок риск | Висок риск |

При разработката или използването на методики за оценка на риска е нужно да се отчитат следните особености: а) Значенията на скалите да са словесно ясно определени и да се разбират еднозначно от всички участници в процедурата по експертна оценка. б) Да се изготви необходимата обосновка за избраната таблица.

Методики за оценка на заплахите и уязвимостите

Използваните методики се основават на: а) Експертни оценки; б) Статистически данни; в) Съобразяване с факторите влияещи на нивата на заплахата и уязвимост. Начин за разработване на подобни методики е набирането на статистически данни за станали произшествия, анализ и класификация на причините за тях, откриване на факторите от които те зависят. На база тази информация може да се оценят заплахите и уязвимостите и при други информационни системи. Практическата сложност при реализацията на този подход е че, трябва да бъде събран обширен материал за произшествията в дадената област. Ако информационната система е голяма (има много елементи и е разположена на голяма територия и/или има дълга история), то този подход е приложим. Ако системата е сравнително по-малка и използва най-новите технологии (за които все още няма достоверна статистика), преценките за заплахите и уязвимостите може да са невалидни.

Съществуват програмни продукти реализиращи различни методики за анализ на риска и те могат да се използват като инструмент на аналитика на проектния риск. **Но универсален метод няма и при всеки случай е нужно да се избира подходящия продукт и той да се настройва според спецификата на изследвания обект.** Поради тази причина все още книжните методики си остават най- разпространени.