Механізми аналізу ризиків захищеності інформаційних систем

Виконав:

студент групи КА-51
Матюх Антон Ігорович

Науковий керівник:

Проф., д.т.н. Мухін В.Є

Актуальність задачі, що розглядається

В нашу еру інформаційних технологій майже кожна компанія має комп’ютери для роботи з даними, а також майже кожна людина постійно працює з персональним комп’ютером, через що кожен рік збільшується кількість інцидентів пов’язаних з інформаційною безпекою, а тому аналіз ризиків захищеності інформаційних систем - важливий аспект в мінімізації потенційних інцидентів пов’язаних з інформаційною безпекою.

Існуючі методи вирішення задачі

Існує дуже велика кількість методик, методів та засобів для аналізу ризиків інформаційних систем. З їх допомогою ризик-менеджери, спеціалісти з інформаційної безпеки а також прості користувачі мають змогу провести ретельний аналіз системи в якій вони працюють і тим самим зрозуміти слабкі сторони системи, які можуть стати потенційними приводами для інцидентів інформаційної безпеки. Коли людина володіє інформацією, щодо вразливих місць у системі вона має можливість виправити їх опираючись на рекомендації програмного засобу і тим самим зменшити ризики загрози для системи, або інакше кажучи зменшити ризики захищеності інформаційної системи.

Існуючі методи вирішення задачі

Найбільш популярними методами аналізу ризиків захищеності інформаційних систем є програмні засоби які на основі вхідних даних детально аналізують ситуацію у компанії та роблять певні рекомендації, які ризик менеджери використовують для зниження ризиків.

Загальне поняття ризику, види та функції ризиків

В цілому ризик можна визначити як поєднання ймовірності та наслідків від того, що певна небажана подія настала.

Ризик завжди передбачає імовірнісний характер результату, найчастіше під словом ризик люди розуміють ймовірність отримати певний небажаний результат, однак ризик також можна розуміти як ймовірність отримати результат, який буде відрізнятися від очікуваного

Загальне поняття ризику, види та функції ризиків

Взагалі, існує два погляди на ризик, які постійно конфліктують у різних галузях. Перша точка зору на ризик основана на наукових та технічних оцінках і називається “теоретичний ризик”, а друга - на людському сприйнятті ризику і має назву “ефективний ризик”.

Загальне поняття ризику, види та функції ризиків

У випадку ефективного ризику існує багато неформальних методів, що використовуються при його оцінці. Формальні методи, що використовуються для виміру найчастіше оцінюють одну з мір ризику, яка називається VaR - Value at Risk. VaR - вартісна міра ризику. Більш глибоким визначенням для VaR є наступна характеристика. Це виражена в грошових одиницях оцінка величини, яка не перевищить очікувані протягом даного періоду часу втрати з заданою вірогідністю.

Загальне поняття ризику, види та функції ризиків

Як приклад ефективного ризику може бути розглялнутий технічний ризик, який описується наступною формулою

$R = P * L,$

де R - ризик, P - ймовірність однієї небажаної події, L - кількість збитків, наприклад кількість втрачених грошей, або кількість жертв у випадку однієї небажаної події.

Ризики у галузі інформаційної безпеки

Відносно до ISACA ризик інформаційної безпеки - ймовірність настання події, яка буде здійснювати негативний вплив на певну організацію та її інформаційні системи.

Відносно до ГОСТ Р ИСО 27005, ризик інформаційної безпеки - ймовірність того, що деяка загроза може використати вразливість активу, або сукупності активів і тим самим завдасть збиток для організації.

Ризики у галузі інформаційної безпеки

Ризик - комплексна величина, яка визначається як функція таких факторів як:

- Загрози інформаційної безпеки.
- Потенційно можливі збитки.
- Вразливість інформаційної системи.
- Контрміри.

Ризики у галузі інформаційної безпеки

Основні аспекти інформаційної безпеки - доступність, цілісність та конфіденційність.

Доступність - можливість доступу суб’єкту за допомогою запита до певних даних у будь-який момент часу, коли система працює.

Цілісність - актуальність і несуперечливість інформації, її захищеність від руйнування та несанкціонованого редагування.

Конфіденційність - захищеність інформації від несанкціонованого доступу на читання.

Моделі аналізу ризиків інформаційної безпеки

Аналіз ризиків інформаційної безпеки не є однозначним процесом, оскільки існує велика кількість різних підходів для аналізу ризиків інформаційної безпеки, а також деяка кількість методологій, серед яких важко обрати найкращу, оскільки кожна з них має свої певні плюси і мінуси.

При оцінюванні ризиків існує дві основні моделі, а саме модель якісної оцінки та модель кількісної оцінки, а також відносно специфічна додаткова модель узагальненого вартісного результату Міори.

Моделі аналізу ризиків інформаційної безпеки

Плюси моделі якісної оцінки:

Немає необхідності кожен раз для кожного активу присвоювати певну грошову вартість.

Підрахунки робляться скоріше і є значно простішими у виконанні.

Немає необхідності визначати частоту появи загрози та точний розмір втрат.

Не потрібно підраховувати відносини ефективності потенціальних мір загрозам.

Моделі аналізу ризиків інформаційної безпеки

Модель кількісної оцінки. Опишемо основні терміни, що використовуються у моделі кількісної оцінки:

Річна частота небажаних подій (Annualized Rate of Occurrence - ARO) - ймовірність того, що збиток з’явиться.

Очікуваний одиничний збиток (Single Loss Expectancy - SLE) - ціна збитку, яка є результатом одної вдалої атаки.

Очікуваний річний збиток (Annualized Loss Expectancy - ALE) - величина, яка дорівнює добутку річної частоти небажаних подій та очікуваного одиничного збитку.

Моделі аналізу ризиків інформаційної безпеки

Формули для підрахунку

ALE = ARO * SLE

SLE підраховується як добуток кількісного значення актива (Asset Value - AV) та фактору взаємодії (Exposure Factor - EF), де фактор взаємодії - розмір збитку, або ж вплив на значення активу, а саме та частину, яку актив втратить в результаті певного інциденту.

SLE = AV * FE

ALE = ARO * AV * FE

Порівняння існуючих продуктів для аналізу ризиків інформаційної безпеки

Перед тим як порівнювати існуючі продукти опишемо загальний процес управління ризиками.

Порівняння існуючих продуктів для аналізу ризиків інформаційної безпеки

Процес управління ризиками складається з наступних логічних етапів:

1) Формування для організації певного рівня ризику, що можна вважати прийнятним.

2) Ідентифікація ризиків, аналіз ризиків та оцінка ризиків.

3) Ранжування ризиків.

4) Ухвалення рішення відносно ризиків і розробка плану реагування на ризики.

5) Прийняте за кожним ризиком рішення повинно бути зафіксовано в плані реагування на ризики.

6) Реалізація заходів з реагування на ризики.

7) Оцінка ефективності реалізованих заходів.

Порівняння існуючих продуктів для аналізу ризиків інформаційної безпеки

Програмні продукти для аналізу ризиків інформаційної безпеки

1) CRAMM

2) ГРИФ

3) RiskWatch

4) Octave

5) MSAT

Переваги обраного програмного продукту (MSAT)

Перевагами даного програмного засобу є наступні можливості:

- Безкоштовна ліцензована версія програмного засобу
- Комплексний підхід до оцінки ризиків інформаційних систем
- Можливість сформувати велику кількість вхідних параметрів, на базі яких будується детальна оцінка ризиків кожного з аспектів
- Легкий інтерфейс, що не потребує великих часових ресурсів для зрозуміння
- Можливість використовувати на реальних бізнес проектах

Результати роботи та аналіз даних

Вхідні дані

Назва компанії	К-сть моніторів	К-сть серверів	К-сть співробітників	Критерій 1	Критерій 2	Критерій 3	...	Критерій 50	Критерій 51
Компанія1	50 - 149	1 - 5	150 - 299	1	0	0		0	1
Компанія2	150 - 290	1 - 5	50 - 149	1	0	0		1	0
Компанія3	0 - 50	0	0 - 10	0	0	0		1	0
Компанія4	0 - 50	1 - 5	10 - 49	1	1	1		0	0
Компанія5	400 - 500	6 - 10	400 - 500	1	0	1		1	1

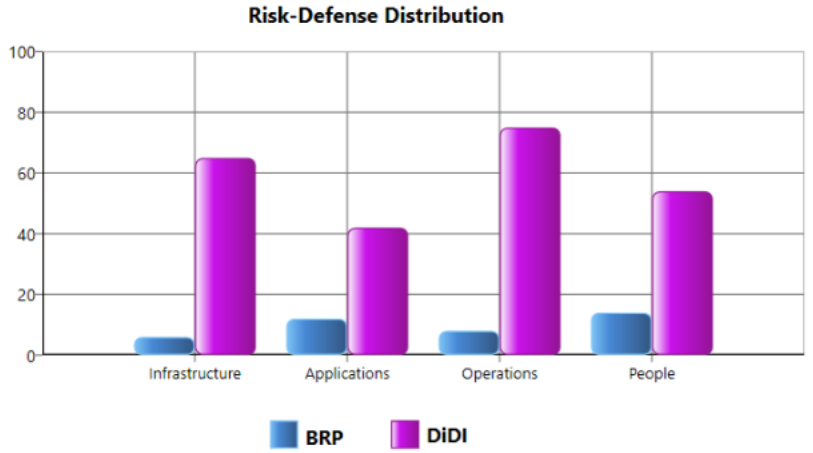
...

Компанія28	300 - 399	6 - 10	300 - 399	0	0	0		1	0
Компанія29	300 - 399	6 - 10	300 - 399	0	0	0		1	0
Компанія30	300 - 399	6 - 10	300 - 399	0	0	0		1	0

Результати роботи та аналіз даних

Результати роботи програмного продукту для конкретного прикладу даних

Business Risk Profile vs. Defense-in-Depth Index Summary Report



Areas of Analysis	Risk-Defense Distribution	Security Maturity
People	●	●
Operations	●	●
Applications	●	●
Infrastructure	●	●

Результати роботи та аналіз даних

Інтегрована оцінка ризику підраховувалася за наступною формулою:

$$R = \sum BRP1*w1$$

Де BRP1, BRP2, BRP3, BRP4 - оцінка ризиків різних аспектів у компанії

w1, w2, w3, w4 - вагові коефіцієнти, що були отримані як експертні оцінки

Результати роботи та аналіз даних

Вихідні дані

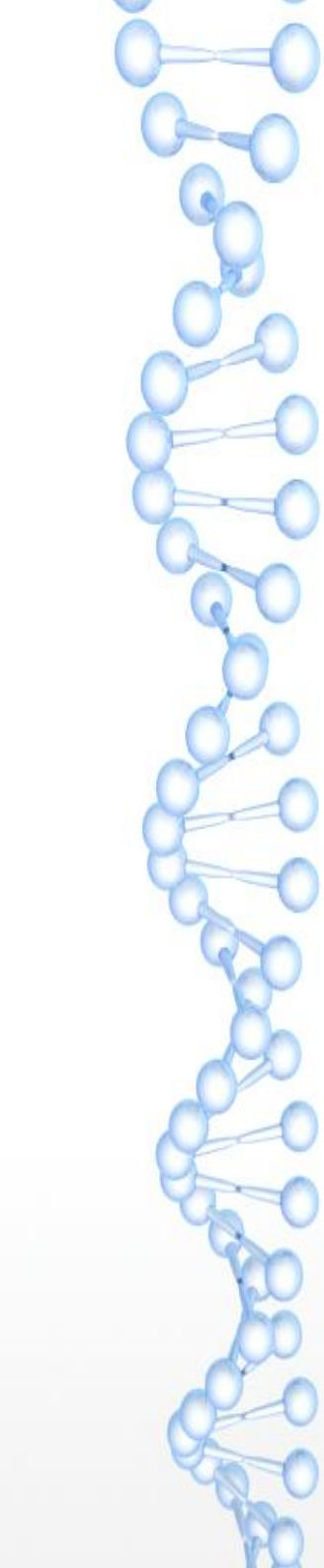
#	Infrastructure security risk	Application security risk	Operations security risk	People security risk	Integrated security risk
Компанія1	0.17	0.27	0.28	0.22	0,2365
Компанія2	0.05	0.125	0.075	0.15	0,11625
Компанія3	0.01	0.03	0.02	0.06	0,0375
Компанія4	0.18	0.1	0.09	0.21	0,1545
Компанія5	0.38	0.39	0.53	0.42	0,4215

...

Компанія28	0,21	0,2	0,21	0,01	0,127
Компанія29	0	0,2	0,21	0,19	0,1675
Компанія30	0,21	0,2	0,21	0,19	0,199

Подальші перспективи

Запропонувати власну методику оцінки ризиків інформаційної безпеки та розробити власний програмний продукт для реалізації цієї методики.



Дякую за увагу!