Адаптивне управління ресурсами захисту інформації

Г. В. Вербовська

В даній роботі розглянуто принципи динамічного (або адаптивного) управління ресурсами захисту інформації, метою якого є досягнення оптимального розміру інвестицій в інформаційну безпеку і оптимального моменту інвестування. Адаптивний підхід передбачає "пристосування" захисту відповідно до дій зловмисника. Прийнято вважати, що успішна реалізація атаки несе за собою тільки негативні наслідки і великі витрати. При визначених параметрах і певних умовах напад можна використовувати на свою користь, визначаючи після атаки найслабші місця захисту і завдяки цьому мати змогу скоригувати його, знаючи степінь вразливості. В роботі приведено приклад, в якому порівнюються результати попереднього розподілу, коли ресурси вносяться після першого нападу. Проаналізовано умови, при яких доцільно застосовувати адаптивне управління, і ситуації, в яких воно дає найкращі результати.

Вступ

Необхідність динамічного управління ресурсами інформаційної безпеки обумовлена двома основними причинами:

- невизначеністю відносно дій суперника, а саме направленістю його зусиль по вилученню інформації і масштабом цих зусиль;
- зміною з часом як внутрішніх, так і зовнішніх умов протистояння, а саме: стану інформаційної системи (вартості інформації і її розподілу між об'єктами),направленості атак суперника, появою нових суперників тощо.

Одним з важливих завдань економічного менеджменту інформаційної безпеки є визначення двох пов'язаних між собою величин: оптимального розміру інвестицій y^0 в інформаційну безпеку і оптимального моменту t^0 інвестування. Існування оптимуму відносно моменту внесення інвестицій можна пояснити наступними міркуваннями. Затримка в інвестуванні в умовах послідовних атак, звичайно, приведе до певних втрат. Проте попередній розподіл ресурсів, коли ще не проявилась націленість суперника, може виявитись неефективним і привести до ще більших втрат. Тому настає момент t^0, який визначається пороговим значенням i^0 кількості втраченої інформації, при настанні якого стає доцільним виділення певної кількості ресурсів захисту y^0 і певного розподілу $\{y_k^0\}$ їх між об'єктами.

Шукані значення y^0 і t^0 можна знайти з умови досягнення максимуму цільової функції, яка визначає прибуток від внесення інвестицій. Ця величина дорівнює вартості захищеної в результаті внесення інвестицій інформації за відрахуванням втрат на її захист.

Постановка задачі

Аналізу поставленої задачі присвячена низка робіт[1-3]. У роботі двох японських вчених розглядається питання оптимальних термінів інвестування. У порядку підрахунку оптимального часу введення інвестицій розглядаються кілька змінних і параметрів [1] :

1. Параметр L - потенційні втрати, пов'язані із загрозою інформаційній системі. $L = \lambda$, де T являється випадковою змінною реалізації загрози, а λ-збитки(в грошовому еквіваленті), обумовлені реалізацією загрози.
2. Параметр ν - вразливість, тобто ймовірність успішної одноразово реалізованої атаки.
3. Загальний очікуваний збиток, пов'язаний із загрозою інформаційній системі - ν L.
4. $S(z, \nu)$ - залишкова вразливість при z - івестованих коштах.

5. Очікувана вигода від інвестицій (позначимо її V), яка є скороченням очікуваного збитку, може бути обчислена як $V = (\nu - S(z,\nu)) \cdot L$, де $(\nu - S(z,\nu))$ є скорочення вразливості інформаційної системи. Очікувана чиста вигода (NPV) може бути обчислена як $NPV = (\nu - S(z,\nu)) \cdot L - z$.

Оптимальний момент інвестування згідно цієї статті визначається саме двома останніми показниками P та NPV. Він залежить від того, наскільки рентабельно буде застосовувати захист на тому чи іншому етапі. При цьому часовий поріг інвестицій залежить також від фактору волатильності σ (представляє степінь невизначеності). При збільшенні степені невизначеності необхідно більше часу на уточнення ситуації, збір більш чіткої і повної інформації про можливі загрози, таким чином і збільшується кількість інвестиційних витрат. За умови наявності досить суттєвої степені невизначеності ефективним буде застосувати адаптивний метод введення інвестицій.

В [2] розглядається антагоністичне протистояння двох сторін у сфері інформаційної безпеки: захисту, який знаходиться у невизначеності щодо дій суперника, і нападу, котрий має певне уявлення про структуру системи захисту і направляє свої зусилля в найслабшу ланку системи безпеки. Розподіл ресурсів захисту на блокування різного типу загроз може вестись як в активному режимі - випереджаючи дії суперника, так і реактивному, з затримкою інвестування, коли захист визначає напрямок розподілу коштів в інформаційну безпеку. Ця модель призначена саме для тієї ситуації, коли захисник не впевнений у можливій цілі нападу, при умові, що відбуваються численні атаки суперника, причому в результаті кожної атаки вилучається незначна кількість активів. Динаміка протистояння проявляється в тому, що захист, зафіксувавши направленість дій суперника, прагне заблокувати їх, а напад змінює напрямок своїх зусиль, відшуковуючи інші слабкі місця в системі захисту.

Модель адаптивного інвестування

Для ілюстрації цієї моделі використаємо цільову функцію, що вводиться в [3], яка визначає кількість втраченої інформації:

$$I = \sum_{k=1}^{l} I_k = \sum_{k=1}^{l} g_k \cdot p_k(x,y) \cdot q_k(x,y) \cdot f_k(x,y) \tag{1}$$

k - номер об'єкта; g_k-кількість інформації на k-му об'єкті; $p_k(x,y)$-імовірність нападу на k-ий об'єкт; $q_k(x,y)$-щільність імовірності виділення ресурсів x при нападі на k-ий об'єкт; $f_k(x,y)$ - частка вилученої інформації з k-го об'єкта.

Залежності $f_k(x,y)$ оберемо у вигляді: $f_k(x,y) = \frac{(x/y)^n}{a_k \cdot (x/y)^n + c_k}$. Ці залежності задовольняють двом необхідним умовам: при $\frac{x}{y} \to 0$ $f_k(x,y) \to 0$; при $\frac{x}{y} \to \infty$ $f_k(x,y) \to 1$. Параметри a,c,n визначають форму залежності для кожного об'єкта.

Для ілюстрації методики розглянемо спрощений варіант: $p_k(x,y) = 1$ і $q_k(x,y) = 1$. Візьмемо $l = 5$ і $g_k = g$ - інформаційна система містить 5 однакових об'єктів. Припустимо, що напад здійснюється на 2 об'єкти. Вартість активів залишається незмінною, оскільки їх втрати можуть бути компенсовані за рахунок прибутку. Тоді в силу однаковості об'єктів:

$$I = \sum_{k=1}^{l} I_k = \sum_{k=1}^{l} g_k \cdot f_k(x,y) = 2g_k \cdot f_k(x,y) \tag{2}$$

Залежність $f_k(x,y)$ оберемо у вигляді: $f_k(x,y) = \frac{x/y}{10(x/y)+4}$. Параметри, що входять в цю залежність, вибрані такими, що при $\frac{x}{y} = 1$ $f_k(x,y) = 0,071$ - це значення вважаємо близьким до реальності. Покладемо $Y = 1$ і $Z = \frac{X}{Y} = 2$. Розглянемо 2 випадки:

1. Попередній розподіл ресурсів захисту. $y_k = y = \frac{Y}{l} = 0,2$; $x_k = x = \frac{X}{2} = 1$; $I = 2g_1 \cdot 0,093 = 0,185g_1$.
2. Адаптивний розподіл - ресурси захисту вносяться після першого нападу і розподіляються так, щоб блокувати подальші атаки на визначені об'єкти нападу. Втрачена інформація складається з двох частин:

- інформація, втрачена під час першого нападу ($x = 1, y = 0$): $I = 2g_1 \cdot 0,1 = 0,2g_1$
- інформація, втрачена під час другого нападу ($x = 1, y = 0,5$): $I = 2g_1 \cdot 0,083 = 0,167g_1$

Інформація, втрачена в результаті двох атак, в першому випадку становить $I = 2 \cdot 0,185g_1 = 0,370g_1$, в другому - $I = 0,367g_1$, (в наших розрахунках ми вважали, що інформація про ступінь вразливості після кожної атаки поповнюється). При подальших атаках, націлених на ті ж об'єкти, перевага другого варіанту розподілу ресурсів збільшується. Зокрема, після трьох спроб нападу маємо:

1. Попередній розподіл ресурсів захисту: $I = 3 \cdot 0,185g_1 = 0,555g_1$
2. Адаптивний розподіл: $I = 0,2g_1 + 0,167g_1 + 0,167g_1 = 0,534g_1$

Нами розглянуто найбільш простий приклад для розуміння принципу моделі. Модель ускладнюються при збільшенні кількості загроз, при цьому за мету ставлять розрахувати оптимальну кількість загроз, на які потрібно направити захист. Крім того, наблизити ситуацію до реальної можливо, врахувавши такий важливий фактор, як рівень невизначеності (σ). При достатній обізнаності щодо загроз захисник може успішно знайти оптимальне співвідношення ресурсів; при зростанні невпевненості за браком інформації він буде вимушений рівномірно розподілити інвестиції між всіма об'єктами, витрачаючи кошти економно з метою пізніше використати отриману інформацію для більш цілеспрямованого захисту - саме в таких випадках підхід найбільш ефективний. При великій невизначеності захисник виграє набагато більше не застосовуючи захист взагалі, а прийнявши на себе втрати від нападу.

Висновки

Приведений приклад дозволяє зробити деякі висновки щодо доцільності використання кожного з двох варіантів розподілу ресурсів - попереднього і адаптивного. Адаптивний розподіл має сенс використовувати при виконанні наступних умов:

1. наявність великої кількості об'єктів;
2. невизначеність відносно націленості атак суперника;
3. достатній рівень природної захищеності об'єктів (невелика початкова вразливість);
4. повторюваність атак.

Адаптивний підхід дає змогу значно скоротити втрати від нападу, або навіть уникнути їх, при цьому більш раціонально використовуючи ресурси фірми.

Список літератури

[1] Tatsumi Ken-ichi, Goto Makoto, Optimal timing of information security investment: A real options approach — WEIS July 21, 2009

[2] Bohme Rainer, Moor Tyler, The iterated weakest link: A model of adaptive security investment. — WEIS, London, 24 June 2009

[3] Левченко Є.Г., Оптимізація розподілу ресурсів між об'єктами захисту інформації. — НТЖ "Захист інформації №1, 2007, с.33-38.

Автори

Ганна Василівна Вербовська — магістр 1-го року навчання, Інститут інформаційно-діагностичних систем, Національний авіаційний університет, Київ, Україна; E-mail: *anna_ verbovskaya@ukr.net*