PACS номери: 00
УДК 004

СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ В УМОВАХ ДИНАМІЧНИХ РИЗИКІВ

О. В. Кіреєнко[1, a], О. Є. Архипов[2]

[1] *Національний технічний університет України «Київський політехнічний інститут»*

Анотація

В роботі представлений опис методів розробки систем захисту інформації та розрахунку ризиків. Описані можливі стратегії поведінки зловмисників і сторони захисту та підходи до прогнозування дій суперника. Запропоновано способи поширення вже існуючих методів для випадку динамічного ризику. Розглянуто теоретичний, економічний та поведінковий підходи розрахунку сценаріїв реалізації загроз.

Ключові слова: вразливість, загроза, динамічний і статичний ризик, атака, формула Гордона-Лоеба, ЗКІ — знецінена конфіденційна інформація.

Вступ

Сьогодні захист інформації є одним з основних напрямків діяльності будь-якої організації. Можливі втрати від розголошення конфіденційної інформації через втрату клієнтів, появу товарів-аналогів у конкурентів, компрометацію системи документообігу та електронної пошти значно перевищують витрати на усунення наслідків стихійних лих, оплату страховки, юридичних та консультаційних послуг. Побудова будь-якої системи захисту починається з оцінки ризиків. Саме тут виникають основні проблеми. В ідеальному випадку фірма має бути необмежена в часі свого існування, тобто єдиною умовою її ліквідації є добровільне бажання директора чи власника. Діяльність фірми має приносити прибуток, але ця умова є необов'язковою, адже можливе фінансування фірми ззовні. В будь-якому випадку необхідно робити прогнози на майбутнє. Неможливо передбачити, які саме способи здійснення атак з'являться у зловмисників у майбутньому, проте можна констатувати факт – нові засоби обов'язково з'являться.

1. ПІДХОДИ ДО РОЗВЯЗКУ ЗАДАЧІ

Теорія ігор використовується для моделювання конфліктів, в тому числі і спроб взломати систему [1].

Відповідно до цієї теорії є 2 гравця(зловмисник і захист), стартова позиція (розстановка «фігур» тобто розподіл коштів між засобами захисту), правила, згідно яких здійснюються ходи (правила, що визначають атаки, вибрані зловмисником), почерговість дій — сторона захисту за один хід або нічого не робить, або модифікує систему. Зловмисник за 1 хід здійснює 1 атомарну дію зі сценарію атаки. Обидві сторони розуміють правила гри, свою мету, наслідки перемоги та поразки. Удача не впливає на результат. Імовірність втрати · загальні втрати = можливі втрати (тобто якщо імовірність не 0 то припускаються, що зловмисник завдасть збитків у розмірі $(100 \cdot P)\%$ від максимально можливих де P — імовірність — величина від 0 до 1). Визначені правила приведуть до закінчення гри, коли можна буде підрахувати результат обох гравців. Гравець, в якого не залишилось ходів — програє автоматично. Зловмисник без коштів не може провести наступну атаку, сторона захисту не здатна відновити контроль над захопленою зловмисником системою та ін. (так як сторона захисту на кожному кроці може пропустити хід, то умовою програшу для сторони захисту буде відмова від продовження гри – повна втрата контролю над системою захисту та повна втрата інформації. Для зловмисника умовою програшу є відсутність ресурсів для проведення наступних атак(якщо ресурси обмежені), неможливість завдати хоча б яких-небудь збитків захисту(коли проведення атаки недоцільне))

Класифікуємо даний конфлікт:

1) Віднесемо його до класу партизанських ігор(коли гравці знаходяться в різних стартових умовах.)
2) Це екстенсивна гра (стратегію можна змінювати протягом гри.)
3) Це гра з ненульовою сумою. В загальному випадку втрати одного гравця не дорівнюють здобутку другого.
4) Це не нульова гра. (перемога не залежить від того, хто здійснить перший хід. Перший

[a] kirealex12@gmail.com

хід завжди здійснює захист, створюючи систему захисту, але це не дає йому жодних переваг/вразливостей перед зловмисником у перспективі.)

5) Ця гра не є позитивною/негативною (не існує 100% шансу перемоги в загальному випадку для жодної із сторін)

1.1 Формула Гордона – Лоеба та її похідна

Похідна від зазначеної формули дозволяє знайти оптимальні витрати на побудову системи захисту [2]. Цю формулу можна використовувати як для ізольованого середовища, де є тільки 1 зловмисник та 1 система, що підлягає захисту, так і для множини систем, що підлягають захисту. Якщо ми хочемо використати її для множини систем, то треба визначити правила їх взаємодії. Правилами може бути передбачено, якою саме інформацією діляться гравці. Наприклад, можна повідомити про факт здійснення атаки, але приховати інформацію про власні втрати від даної атаки. Анти кооперативна гра не має сенсу. Якщо є 2 або більше систем захисту у фірм-конкурентів, то вони просто не спілкуються, так як одне одному не довіряють.

1.2 Теоретичний підхід Б. Журиленко

Тепер розглянемо інший підхід до розрахунку ризиків. Нехай m — кількість спроб взлому. Розраховуємо імовірність взлому не для однієї атаки, а для послідовності атак зловмисника. Нехай нам потрібно створити систему, яка з імовірністю 99% витримає m атак зловмисника. При цьому вважатимемо, що атаки проходять незалежно, не впливають на успіх наступних атак, ризик при цьому залишається статичним [3]. (ситуацію з динамічним ризиком розглянемо пізніше)

Позначимо p — імовірність успіху атаки, q — імовірність провалу. $p + q = 1$

$$1 - (p + q \cdot p + q^2 \cdot p + \ldots + q^{m-1} \cdot p) = 0,99.$$

Так як p виражається через q, то ми маємо рівняння з однією змінною. З нього можна знайти p – максимально допустиму імовірність успіху зловмисника.

Для динамічних ризиків $p = p(x_1, x_2, \ldots, x_n)$. Це функція від n параметрів. Для функцій виконується та сама умова, що і для констант:

$$q(\ldots) = 1 - p(\ldots)$$

Якими б не були наші інвестиції в захист, при безкінечній кількості спроб зловмисник може отримати майже 100% імовірність успіху. Але зловмиснику немає потреби досягати такої імовірності. Вже при 50% математичне очікування успіху — всього 2 спроби. Зловмисник у своїх діях керується бажанням отримати максимальний прибуток при мінімальних витратах. При вищезгаданих 50% на успіх зловмисник здійснить атаку тільки якщо можливий дохід вдвічі перевищить його витрати на проведення атаки. У випадку невдачі він з другої спроби виходить в нуль по витратам.

1.3 Модель КІ-ЗКІ О.Н. Маслова

До цього часу ми розглядали випадок, коли втрачена захистом інформація одразу спричиняла певні збитки для системи. В реальній ситуації все набагато складніше. Конфіденційна Інформація (КІ) може перейти в стан знеціненої конфіденційної інформації (ЗКІ). Перехід із ЗКІ в КІ теж можливий. Існує певний критичний об'єм КІ, що може перейти в ЗКІ. До досягнення цього значення процес є оборотним. Сторона захисту може впливати на КІ, ЗКІ і зловмисника. Вплив на КІ — це власне інвестиції в систему захисту. Вплив на ЗКІ — будь-які дії, що прискорюють старіння цієї інформації. Чим швидше вона стане не актуальною, тим краще. Вплив на зловмисника – повідомлення власної служби безпеки, поліції. Також можна домовитись із зловмисником – заплатити викуп, залякати, знищити і тд. Зловмисник може впливати тільки на КІ та захист. ЗКІ для зловмисника не представляє більше інтересу.

В цій моделі захист допускає, що частина КІ може перейти в стан ЗКІ без шкоди для системи. Захист визначає параметри сигналу тривоги по часу та об'єму.

$$1 - P_R = \exp(-\frac{\tau_k \cdot k_R}{R_0}),$$

де $1 - P_R$ – Імовірність того, що дії зловмисника залишаться непоміченими.
τ_k – час впливу на систему
$R_k = \tau_k \cdot k_R$ – рівень сигналу тривоги
R_0 – визначений нормативами рівень сигналу тривоги.

Аналогічно для об'єму викраденої зловмисником інформації [4].

2. Комплексний підхід до захисту інформації

Політика безпеки повинна визначати строгий порядок дій при зміні ризику. Дії працівників мають бути регламентовані відповідними інструкціями та попередньо відпрацьовані. Необхідно запобігти помилкам, що можуть виникнути в умовах стресу чи паніки.

Політика безпеки та зацікавленість персоналу потребують незначного фінансування, тому більшість фірм використовує саме ці 2 підходи. Варто зазначити, що без технічного захисту інформації ці підходи марні.

При плануванні системи захисту необхідно визначити приблизний об'єм робіт. Кожна фірма потребує індивідуального підходу, але можна виділити деякі параметри, що визначатимуть її початкову вразливість.

Вразливість до зараження системи вірусом залежить від кількості адрес електронної почти (вузлів

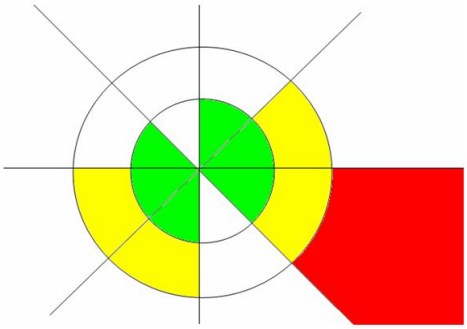

Рис. 1. Рівні сигналу тривоги при застосуванні підходу Маслова.

у системі, що використовують цей сервіс), напрямку діяльності фірми (якщо напрямків декілька то вразливість зростає), структури мережі та її розмірів. Загальна формула має вигляд [5]

$$V = \alpha \cdot \log(Emails) + \beta \cdot SysV + \sum_{i=1}^{n} \gamma_i \cdot Ind_i + \delta \cdot D \cdot P \cdot H - c$$

(це видозмінена формула Танаки-Матсуури. В оригінальній формулі V має відповідати вразливості і не перевищувати 1, а доданки в правій частині менші за 1.

3. РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ

Найкращим підходом до реалізації систем захисту в умовах динамічних ризиків на данний момент я вважаю підхід Маслова. Даний підхід варто застосовувати то систем, на які часто здійснюються атаки. Даний підхід є ефективним як для сторони захисту, так і для зловмисника. Застосовуючи цей підхід, сторона захисту може розробити систему, що буде здатна відновитись з єдиного вцілівшого вузла або з окремого модуля програми. На даний момент такого результати можна досягти шляхом реплікації даних та їх кодування. Зловмисники можуть застосовувати цей підхід при розробці нового шкідливого забезпечення, яке буде практично неможливо знищити. Потрапивши в мережу така програма буде поширюватись доки залишаються вразливі вузли, що можна гарантувати на даний момент, так як серед під'єднаних до мережі компютерів завжди дуже великий % незахищених та неправильно захищених компютерів. На рис 1. представлено діаграму, що пояснює захист системи, реалізованої за підходом Маслова.

Концентричними колами позначено множини дій користувачі. Внутрішне коло (позначено зеленим) — дозволені дії, що не можуть зашкодити системі взагалі. Зовнішнє коло – підозрілі дії, можуть бути здійснені як зловмисником, так і деякими користувачами (помилки користувачів, випадкове нанесення шкоди системі). Вихід за межі цього кола(позначено червоним) означає явно зловмисні дії, що напряму загрожують системі. Такі дії одразу викликають спрацьовування сигналізації за обсягом. На діаграмі також видно порожні сектори — це періоди повної бездіяльності зловмисника (або звичайного користувача). Ця діаграма відповідає визначеному стороною захисту інтервалу часу (в даному випадку 8 одиниць часу. Наприклад, 8 годин або 8 днів) Кожен раз, коли проходить цей інтервал часу, виконується перевірка сигналізації за часом. Порівнюється зафарбована площа та загальна площа зовнішнього кола. Якби на цій діаграмі не було порушення рівня безпеки за обсягом, то можна було б сказати, що зловмисник виконував підозрілі дії протягом половини часу функціонування системи, ще четвертину цього часу зловмисник виконував тільки дозволені дії, і ще четвертину вичікував, щоб зменшити імовірність спрацьовування сигналізації. Такий спосіб організації сигналізації досить зручний. Для кожного користувача можна встановити різні рівні сигналізації. Також можна відслідковувати бездіяльність в системі — якщо користувач взагалі нічого не робить протягом тривалого проміжку часу це означає, що він або байдикує, або щось впливає на систему детектування дій (можливо зловмисник таким способом проводить атаку).

Підхід Маслова часто використовують тоді, коли передбачається захист конфіденційності інформації. Типовим прикладом є викрадення паролів. Зловмисник намагається скопіювати паролі користувачів системи, а сторона захисту намагається зменшити вартість отриманої зловмисником інформації. Для цього можна або змінювати паролі (конфіденційна інформація переходить в стан знеціненої конфіденційної інформації) або змінити/перемістити об'єкти, до яких здійснюється доступ за допомогою цих паролів.

Висновки

В цій роботі розглянуто існуючі підходи до побудови систем захисту в умовах статичних ризиків. Запропоновано способи переходу до динамічних ризиків. Вказано сферу застосувань існуючих методів. Не розглянутими залишилось питання самого процесу модифікації системи між циклами, особливості появи вразливостей під час модифікації. Поведінковий (біхевіористичний) підхід досліджено не повністю, так як в даний момент мені не відомі всі фактори, що стимулюють зловмисника до проведення атаки. Розвитком даної теми буде дослідження застосування даних методів то проектування гнучких систем та відмовостійких мереж.

Література

1. J.H. Conway Winning ways for your mathematical plays

2. L.A. Gordon, M.P. Loeb the economics of information security investment

3. Б.Журиленко, Н.Николаева, Н. Пелих Оптимальне финансовые затраты и основне критерии построения или модернизации комплекса технической защиты информации

4. О.Н. Маслов О моделировании риска принятия решений в области обеспечения информационной безопасности

5. W.Liu, H Tanaka, K. Matsuura An Empirical Analysis of Security Investment in Countermeasures Based on an Enterprise Survey in Japan