УДК 519.876.5:004.491.42
DOI: 10.31673/2409-7292.2023.030002

Хавер А. В., Савченко В. А.

МАТЕМАТИЧНА МОДЕЛЬ ЗАХИСТУ ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ ВІД ТРОЯНСЬКИХ ПРОГРАМ

У статті пропонується концептуальна математична модель захисту об'єктів критичної інфраструктури від троянських програм. Модель заснована на теоретико-ігровому підході, де захисник і нападаючий мають суперечливі цілі. При застосуванні моделі проводиться аналіз уразливостей об'єктів критичної інфраструктури, щоб виявити потенційні слабкі місця, якими можуть скористатися троянські програми. Потім формулюється ігрова модель для фіксації стратегічної взаємодії між захисником і нападником. Вводяться оптимальні інвестиції в безпеку для захисника, які збалансовують вартість безпеки та очікувані втрати від успішної атаки. Також, оцінюється ефективність запропонованих стратегій захисту за допомогою методів тестування та оцінювання. Результати дослідження показують, що модель ефективна для захисту об'єктів критичної інфраструктури від троянських програм і може допомогти особам, які приймають рішення, розподілити ресурси безпеки для максимального захисту при мінімізації витрат.

Ключові слова: троянська програма, об'єкти критичної інфраструктури, математична модель, теорія ігор, аналіз уразливостей, оцінка ризиків, стратегії захисту.

Вступ

Об'єкти критичної інфраструктури є важливим компонентом сучасного суспільства, зокрема у сфері надання послуг, таких як енергетика, транспорт і зв'язок. Ці системи все більше залежать від комп'ютерних систем і мереж, що також робить їх уразливими до кіберзагроз, таких як троянські програми. За останні роки у світі сталося кілька резонансних атак на об'єкти критичної інфраструктури, зокрема кібератака на енергомережі України у 2015 році [1]. У зв'язку з цим виникає нагальна потреба у розробці математичної моделі захисту об'єктів критичної інфраструктури від атак троянських програм.

Постановка проблеми

За останні роки у світі відбулося кілька серйозних інцидентів з використанням троянських програм, які мали значний вплив на організації та окремих осіб. Ось кілька прикладів:

NotPetya – це тип троянського програмного забезпечення, яке завдало значної шкоди організаціям у всьому світі в червні 2017 року. Троянські програми було замасковане під оновлення програмного забезпечення та змогло швидко поширюватися мережами, спричиняючи масові збої та шкоду для бізнесу та об'єкти критичної інфраструктури в кількох країнах. За оцінками, атака завдала збитків у мільярди доларів [2].

SolarWinds: у грудні 2020 року було виявлено, що програмне забезпечення SolarWinds, основного постачальника інструментів керування мережею, було скомпрометовано атакою троянського програмного забезпечення. Атака була здійснена спонсорованою державою хакерською групою та дозволила зловмисникам отримати доступ до широкого спектру конфіденційної інформації від кількох відомих організацій, включаючи уряд США та компанії зі списку Fortune 500 [3].

Emotet – це тип троянського програмного забезпечення, який діє з 2014 року і використовувався для здійснення низки кібератак, включаючи крадіжки даних, програми-вимагачі та атаки через ботнети. У січні 2021 року була розпочата скоординована міжнародна операція з ліквідації інфраструктури Emotet, яка, як вважають, завдала збитків на мільйони доларів [4].

Ці приклади підкреслюють значний вплив атаки троянських програм на організації та об'єкти критичної інфраструктури. Вони також підкреслюють важливість впровадження суворих заходів безпеки для захисту від таких атак і швидкого й ефективного реагування на напади. З точки зору досліджень існує велика потреба формулювання математичної моделі захисту об'єкта критичної інфраструктури від троянських програм.

Аналіз джерел

Захист об'єктів критичної інфраструктури від троянських програм є важливим завданням для забезпечення безпеки та надійності цих об'єктів. Щоб розробити математичну модель для цього завдання, важливо переглянути існуючу літературу з цього питання.

Модель загрози. У статті [5] автори запропонували динамічну ігрову модель для аналізу впливу атак троянських програм на об’єкти критичної інфраструктури. Модель враховує поведінку зловмисника та захисника та їх стратегії атаки та захисту об’єктів критичної інфраструктури. У дослідженні [6] автори запропонували теоретико-ігрову модель для визначення оптимальних інвестицій у безпеку захисту критичної інфраструктури. Модель враховує процес прийняття рішення зловмисником і рішення захисника про інвестиції в безпеку.

Архітектура системи. У статті [7] автори пропонують модель залежностей і взаємозалежностей об’єктів критичної інфраструктури. Модель враховує залежності між різними об’єктами інфраструктури та вплив відмови одного об’єкта на інші. У дослідженні [8] автори запропонували модель взаємозалежностей об’єктів критичної інфраструктури. Модель враховує залежності між різними об’єктами інфраструктури та їх уразливість до каскадних збоїв.

Аналіз уразливостей. У статті [9] авторами запропоновано математичну модель для аналізу уразливості об’єктів критичної інфраструктури. Модель враховує уразливі місця різних компонентів і їх взаємозалежність. У дослідженні [10] запропоновано модель для аналізу уразливості мереж критичної інфраструктури. Модель враховує уразливі місця різних компонентів і їх взаємозалежність.

Стратегії захисту. У статті [11] автори запропонували інтегрований підхід до захисту критичної інфраструктури. Підхід передбачає виявлення потенційних загроз, уразливості об’єктів критичної інфраструктури та розробку відповідних стратегій захисту. У дослідженні [12] запропоновано модель впливу кібератак на енергосистему. Модель розглядає уразливі місця різних компонентів та їх взаємозалежності та пропонує відповідні стратегії захисту.

Огляд літератури показує, що для математичного моделювання захисту об’єктів критичної інфраструктури від атак троянських програм запропоновано кілька моделей. Ці моделі враховують поведінку зловмисника та захисника, залежності та взаємозалежності об’єктів критичної інфраструктури, уразливості різних компонентів та розробку відповідних стратегій захисту.

Метою даної статті є розробка комплексної математичної моделі, яка враховує ці фактори, може допомогти в забезпеченні безпеки та надійності об’єктів критичної інфраструктури.

Особливості реалізації та загрози троянських програм

Троянські програми може становити серйозну загрозу об’єктам критичної інфраструктури, тобто системам і активам, необхідним для функціонування суспільства та економіки. Визначимо особливості та загрози троянських програм спеціально для об’єктів критичної інфраструктури:

Особливості:

1. Камуфляж: троянські програми створені для маскування під законне програмне забезпечення, що ускладнює їх виявлення та видалення. Це дозволяє зловмисникам отримати доступ до об’єктів критичної інфраструктури, не будучи виявленими.

2. Стійкість: троянські програми можуть залишатися прихованим і активним протягом тривалого часу, дозволяючи зловмисникам збирати конфіденційну інформацію та здійснювати атаки протягом тривалого часу.

3. Віддалений доступ: після встановлення троянського програмного забезпечення на критично важливий об’єкт інфраструктури зловмисники можуть віддалено контролювати його на відстані, що дозволяє їм здійснювати атаки в будь-який час.

© Хавер, А. В., & Савченко, В. А. (2023). Математична модель захисту об’єкта критичної інфраструктури від троянських програм. Сучасний захист інформації, 3(55), 12–21. https://doi.org/10.31673/2409-7292.2023.030002.

4. Ескалація привілеїв: троянські програми також можуть бути розроблені для використання уразливостей у безпеці об’єкта критичної інфраструктури, дозволяючи зловмисникам підвищити свої привілеї та отримати доступ до конфіденційної інформації чи систем.

Загрози:

1. Крадіжка даних: троянські програми часто використовуються для викрадення конфіденційної інформації з об’єктів критичної інфраструктури, включаючи конфіденційні дані, пов’язані з операціями, фінансами та клієнтами.

2. Порушення роботи системи: троянські програми можуть використовуватися для порушення нормального функціонування об’єкта критичної інфраструктури, завдаючи значної економічної та соціальної шкоди.

3. Диверсія: троянські програми можуть бути використані для здійснення диверсійних атак на критичні об'єкти інфраструктури, що може призвести до значних фізичних пошкоджень або навіть до людських жертв.

4. Програми-вимагачі: троянські програми також можуть бути використані для впровадження програм-вимагачів, які є типом зловмисного програмного забезпечення, яке блокує системи чи дані критичного об’єкта інфраструктури та вимагає викуп в обмін на звільнення системи чи даних.

Ці загрози підкреслюють значні ризики, які троянські програми може становити для об’єктів критичної інфраструктури.

Приклад коду троянської програми

Троянські програми можуть приймати різні форми та бути написаними різними мовами програмування. Ось простий приклад того, як може виглядати троянська програма:

```c
#include <stdio.h>
#include <stdlib.h>

int main()
{
  // Connect to remote server
  char *server_address = "10.0.0.1";
  int server_port = 8080;
  int sockfd = connect_to_server(server_address,
server_port);

  // Execute malicious commands
  execute_malicious_commands(sockfd);

  // Clean up and exit
  close(sockfd);
  return 0;
}
```

```c
void execute_malicious_commands(int sockfd)
{
  // Send commands to the server
  send_command(sockfd, "download
sensitive_data.txt");
  send_command(sockfd, "install keylogger");
  send_command(sockfd, "escalate_privileges");

  // Wait for commands from the server
  while (1) {
    char *command = wait_for_command(sockfd);
    if (strcmp(command, "reboot_system") == 0) {
      reboot_system();
    } else if (strcmp(command, "delete_files") == 0) {
      delete_files();
    }
  }
}
```

У цьому прикладі програма підключається до віддаленого сервера та виконує набір шкідливих команд. Ці команди можуть включати завантаження конфіденційних даних, встановлення кейлоггера або підвищення привілеїв для отримання більшого доступу до системи. Програма також очікує команд від сервера та може виконувати низку додаткових шкідливих дій, таких як видалення файлів або перезавантаження системи.

Важливо зазначити, що справжні троянські програми часто набагато складніші та витонченіші, ніж цей простий приклад. Вони можуть бути розроблені таким чином, щоб уникнути виявлення програмним забезпеченням безпеки та здійснити низку конкретних атак на цільову систему.

Розробка математичної моделі захисту об'єкта критичної інфраструктури від троянських програм.

Для кількісної оцінки впливу троянських програм на об'єкти критичної інфраструктури та вибору доцільних заходів протидії модель повинна охоплювати питання: аналізу уразливостей об'єкта інфраструктури, процесу атаки та оптимальних інвестицій у систему безпеки об'єкта.

Аналіз уразливостей. Рівняння аналізу уразливості використовується для кількісної оцінки ризику атаки троянської програми на об'єкт критичної інфраструктури. Воно враховує уразливі місця компонентів об'єкта та їх взаємозалежність:

$$V(x) = \sum_{i=1}^{n} v_i(x) w_i(x),$$

де $V(x)$ – уразливість об'єкта критичної інфраструктури x,
$v_i(x)$ – уразливість i-го компонента x,
$w_i(x)$ – вага i-го компонента x.

Уразливість кожного компонента $v_i(x)$ є функцією конкретних уразливостей, пов'язаних із цим компонентом. Ці уразливості можуть включати такі речі, як помилки програмного забезпечення, помилки конфігурації та недоліки безпеки. Вага кожного компонента $w_i(x)$ відображає відносну важливість цього компонента для загального функціонування об'єкта критичної інфраструктури. Компонентам, які є більш критичними для функціонування об'єкта, призначаються вищі ваги.

Об'єднуючи уразливості кожного компонента та їх ваги, рівняння аналізу уразливостей забезпечує кількісну міру загального ризику, пов'язаного з атакою троянського програмного забезпечення на об'єкт критичної інфраструктури. Потім цю інформацію можна використовувати для прийняття рішень про те, як найкраще захистити об'єкт і зменшити ризик успішної атаки.

Ігрова модель процесу атаки. Рівняння ігрової моделі використовується для аналізу впливу атак троянських програм на об'єкти критичної інфраструктури. Розглядається поведінка зловмисника та захисника, стратегії атаки та захисту об'єктів критичної інфраструктури. З точки зору захисту рівняння матиме вигляд:

$$\text{Min}\,[E(U)] = \text{Min}\,[\alpha \times P(x, a) - \beta \times (1 - P(x, a))],$$

де $E(U)$ – очікуваний прибуток зловмисника або шкода, заподіяна об'єкту критичної інфраструктури,
α – виграш від успішної атаки,
$P(x, a)$ – ймовірність успіху атаки,
β – втрати від невдалої атаки,
x – об'єкт критичної інфраструктури,
a – дії зловмисника.

Рівняння ігрової моделі враховує поведінку атакуючого та захисника та їх стратегії для нападу та захисту об'єктів критичної інфраструктури. Мета нападника – завдати якомога більшої шкоди, тоді як мета захисника – запобігти або мінімізувати шкоду, спричинену нападом. Очікувана корисність зловмисника $E(U)$ представляє очікувану користь або цінність, яку зловмисник очікує отримати від атаки. Це значення визначається ймовірністю успіху атаки $P(x, a)$ і прибутком або вигодою від успішної атаки α, мінус втрати або вартість невдалої атаки β, помножену на обернену ймовірність успіху $1 - P(x, a)$. Імовірність успіху атаки $P(x, a)$ залежить від заходів безпеки, які застосовуються для захисту об'єкта критичної

© Хавер, А. В., & Савченко, В. А. (2023). Математична модель захисту об'єкта критичної інфраструктури від троянських програм. Сучасний захист інформації, 3(55), 12–21. https://doi.org/10.31673/2409-7292.2023.030002.

інфраструктури, а також від навичок і ресурсів зловмисника. Прибуток від успішної атаки α представляє шкоду, яку зловмисник очікує завдати, якщо атака буде успішною, тоді як втрата від невдалої атаки β, представляє ресурси, які зловмисник витратить, не досягнувши своєї мети.

Аналізуючи рівняння ігрової моделі, можна зрозуміти стратегії зловмисника та захисника та розробити контрзаходи для захисту об'єктів критичної інфраструктури від атак троянських програм.

Оптимальні інвестиції у безпеку об'єкта. Рівняння оптимальних інвестицій у безпеку використовується для визначення оптимального рівня інвестицій у безпеку, які необхідно зробити для захисту об'єкта критичної інфраструктури від атак троянських програм.

Рівняння формулюється наступним чином:

$$\pi = R(S) - C(S) - E(U),$$

де π – прибуток власника об'єкта критичної інфраструктури,

$R(S)$ – дохід, отриманий об'єктом як функція рівня інвестицій у безпеку,

$C(S)$ – вартість інвестицій у безпеку,

$E(U)$ – потенціальні втрати внаслідок успішної атаки.

Прибуток π, являє собою дохід, отриманий об'єктом критичної інфраструктури, мінус витрати на інвестиції в безпеку та потенційні втрати через успішну атаку. Дохід $R(S)$, створений об'єктом, є функцією рівня інвестицій у безпеку S. Вартість інвестицій у безпеку представлена $C(S)$. Потенційний збиток через успішну атаку $E(U)$ є важливим фактором у рівнянні, оскільки він відображає потенційний фінансовий вплив успішної атаки. Потенційні втрати може бути важко оцінити, оскільки вони залежать від ряду факторів, таких як вартість об'єкта критичної інфраструктури, ймовірність атаки та потенційна шкода, яку може завдати атака.

Метою власника об'єкта критичної інфраструктури є максимізація прибутку π. Цього можна досягти шляхом інвестування в заходи безпеки, які зменшують потенційні втрати внаслідок успішної атаки, одночасно мінімізуючи вартість інвестицій у безпеку. Використовуючи рівняння оптимальних інвестицій у безпеку, власник об'єкта критичної інфраструктури може визначити рівень інвестицій у безпеку, який максимізує його прибуток. Це може допомогти прийняти рішення про те, як найкраще розподілити ресурси для заходів безпеки та забезпечити належний захист об'єкта критичної інфраструктури від атак троянських програм.

Ці рівняння є лише кількома прикладами типів рівнянь, які можна використовувати в математичній моделі для захисту об'єктів критичної інфраструктури від атак троянських програм. Використовувані конкретні рівняння залежатимуть від конкретної моделі, що розробляється, і факторів, які враховуються.

Методика реалізації математичної моделі захисту об'єкта критичної інфраструктури від троянських програм.

Модель загрози. Для розробки математичної моделі захисту об'єктів критичної інфраструктури від троянських програм необхідно розуміти характеристики та поведінку троянських програм. Троянські програми – це зловмисне програмне забезпечення, яке виглядає нешкідливим, але після встановлення в системі воно може виконувати низку несанкціонованих дій, зокрема крадіжку даних, пошкодження систем і надання неавторизованого доступу до системи. Для захисту об'єктів критичної інфраструктури від троянських програм важливо визначити типи троянських програм, які можуть бути використані для атаки, і потенційний вплив успішної атаки на об'єкти критичної інфраструктури.

© Хавер, А. В., & Савченко, В. А. (2023). Математична модель захисту об'єкта критичної інфраструктури від троянських програм. Сучасний захист інформації, 3(55), 12–21. https://doi.org/10.31673/2409-7292.2023.030002.

Архітектура системи. Наступним кроком є розробка архітектури системи, яка описує об’єкти критичної інфраструктури та їх взаємозалежності. Це включає визначення компонентів та їхніх функцій, а також каналів зв’язку між ними. Цей крок має вирішальне значення, оскільки він допомагає зрозуміти потенційні уразливості системи та вплив атаки троянських програм на систему. Об’єкти критичної інфраструктури можуть мати різні форми та різні типи системної архітектури залежно від конкретної інфраструктури та її функцій. Проте, можна навести загальний приклад архітектури системи для типового об’єкта критичної інфраструктури, наприклад електростанції (рис. 1):

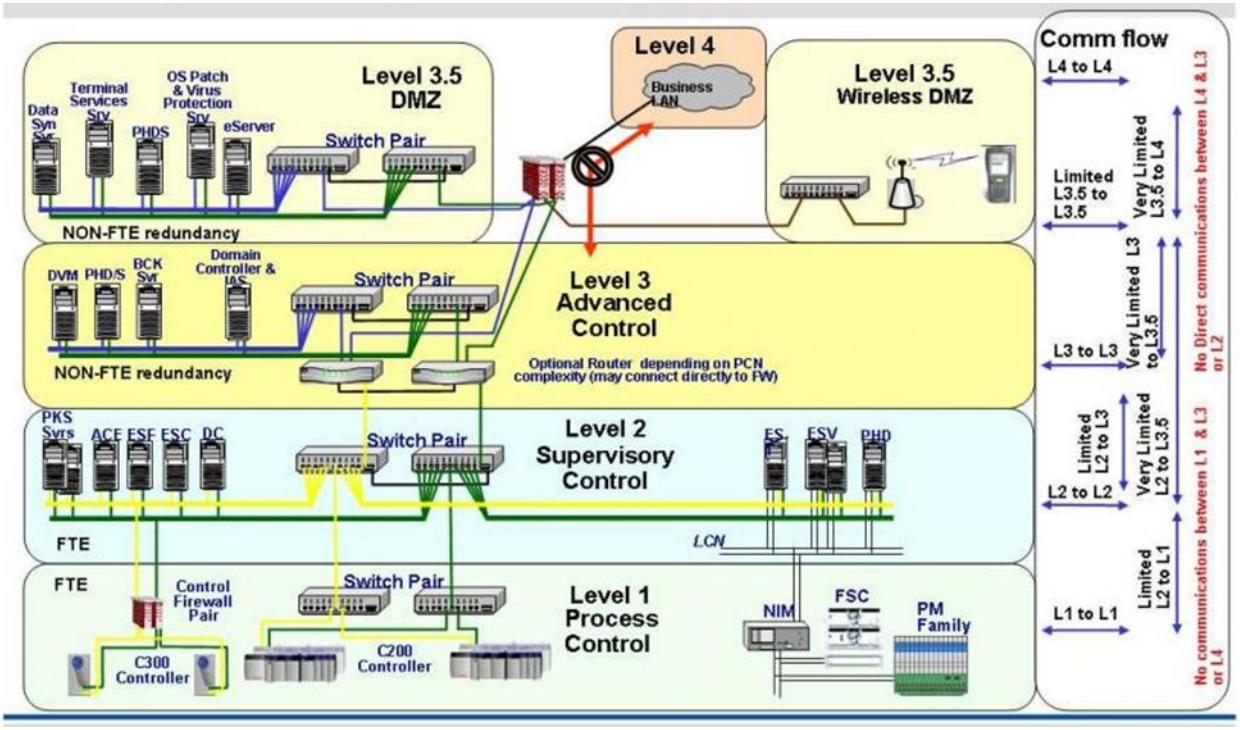

Рис. 1. Архітектура системи безпеки об’єкта критичної інфраструктури [13]

1. Польові пристрої: цей рівень включає різноманітні пристрої, які використовуються для моніторингу та керування різними процесами на електростанції. Приклади можуть включати датчики температури, тиску, а також клапани, насоси та інші механічні компоненти. Ці пристрої зазвичай підключаються до локальної системи керування за допомогою стандартних протоколів зв’язку.

2. Локальна система керування: цей рівень відповідає за керування різними польовими пристроями та забезпечення їх правильної роботи. Він включає в себе програмовані логічні контролери (ПЛК) та інші типи систем керування, які відповідають за реалізацію певних алгоритмів керування та реагування на зміну умов на підприємстві.

3. Система диспетчерського керування та збору даних (SCADA): Цей рівень забезпечує вищий рівень огляду електростанції та відповідає за координацію діяльності локальних систем керування. Він включає в себе програмне забезпечення, яке використовується для моніторингу стану різних систем на підприємстві та внесення коригувань за потреби. Система SCADA зазвичай включає людино-машинний інтерфейс (HMI), який дозволяє операторам переглядати систему та взаємодіяти з нею.

4. Комунікаційна мережа: цей рівень забезпечує інфраструктуру для зв’язку між різними системами електростанції. Він включає як проводові, так і безпроводові канали зв’язку, а також різні мережеві протоколи та заходи безпеки для забезпечення цілісності та конфіденційності даних, що передаються.

5. Внутрішні системи: цей рівень включає різноманітні внутрішні системи, які використовуються для управління та підтримки загальної роботи електростанції. Приклади можуть включати системи управління активами, системи технічного обслуговування та ремонту, а також фінансові та бухгалтерські системи.

Важливо зазначити, що це лише один приклад архітектури системи для об'єкта критичної інфраструктури, і що конкретні деталі архітектури відрізнятимуться залежно від конкретної інфраструктури та її функцій.

Аналіз уразливостей. Після визначення архітектури системи можна виконати аналіз уразливостей, щоб визначити слабкі місця та потенційні вектори атак. Цей аналіз включає оцінку наявних заходів безпеки та оцінку їхньої ефективності для пом'якшення атак троянських програм. Аналіз повинен враховувати потенційні наслідки успішної атаки, такі як збій у наданні послуг, фінансові втрати або навіть людські втрати (таблиця 1).

Таблиця 1

Приклад аналізу уразливостей для об'єкта критичної інфраструктури

Уразливість	**Загроза**	**Ймовірність**	**Вплив**	**Рівень ризику**
Застаріле програмне забезпечення	Зараження шкідливим програмним забезпеченням	Висока	Високий	Високий
Слабка політика паролів	Несанкціонований доступ	Середня	Високий	Високий
Незахищений зв'язок	Перехоплення даних	Середня	Високий	Високий
Відсутність моніторингу системи	Системний компроміс	Висока	Високий	Високий
Неналежний контроль доступу	Внутрішня загроза	Низька	Високий	Середній
Незашифровані конфіденційні дані	Крадіжка даних	Низька	Високий	Середній
Фізична уразливість безпеки	Несанкціонований доступ	Низька	Високий	Середній
Відсутність навчання співробітників	Атаки соціальної інженерії	Середня	Середній	Середній
Відсутність плану аварійного відновлення	Втрата даних або час простою	Низька	Високий	Середній
Відсутність резервування системи	Час простою	Низька	Високий	Середній

У цьому прикладі ми визначили кілька уразливостей у системі, а також пов'язані з ними загрози, ймовірність їх виникнення, потенційний вплив і кінцевий рівень ризику. Рівень ризику визначається комбінацією ймовірності та впливу, причому уразливі місця з високим ступенем ризику – це ті, які мають високу ймовірність виникнення та високий потенційний вплив.

Цей тип аналізу уразливостей може бути корисним інструментом для виявлення потенційних ризиків безпеці та визначення пріоритетів інвестицій у безпеку на основі рівня ризику, який створює кожна уразливість. Розуміючи конкретні уразливості в системі, організації можуть вживати цілеспрямованих заходів для пом'якшення ризиків і захисту об'єктів критичної інфраструктури від кібератак.

Оцінка ризиків. Наступним кроком є проведення оцінки ризику, яка враховує ймовірність і вплив атаки троянських програм на об'єкти критичної інфраструктури. Ця оцінка повинна враховувати потенційні наслідки успішної атаки, такі як збій у роботі послуг, фінансові втрати або навіть втрата життя. Оцінка повинна визначити типи троянських програм, які можуть становити найвищий ризик, і потенційний вплив успішної атаки на об'єкти критичної інфраструктури (таблиця 2).

У цьому прикладі визначено кілька загроз системі, а також пов'язані з ними уразливості, потенційний вплив, ймовірність виникнення, кінцевий рівень ризику та стратегії пом'якшення. Рівень ризику визначається комбінацією ймовірності та впливу, причому загрози високого ризику – це ті, які мають високу ймовірність виникнення та високий потенційний вплив. Цей тип оцінки ризику може бути корисним інструментом для розуміння

© Хавер, А. В., & Савченко, В. А. (2023). Математична модель захисту об'єкта критичної інфраструктури від троянських програм. Сучасний захист інформації, 3(55), 12–21. https://doi.org/10.31673/2409-7292.2023.030002.

загального профілю ризику об’єкта критичної інфраструктури та для визначення конкретних областей, де потрібні інвестиції в безпеку. Розставляючи пріоритети для інвестицій у безпеку на основі рівня ризику, який представляє кожна загроза, організації можуть вживати цілеспрямованих заходів для пом’якшення ризиків і захисту своїх критичних об’єктів інфраструктури від кібератак.

Стратегії захисту. На основі оцінки ризику можна розробити відповідні стратегії захисту для зменшення ризиків атаки троянських програм. Ці стратегії можуть включати впровадження додаткових заходів безпеки, оновлення існуючих протоколів безпеки або розробку нових протоколів для вирішення нових загроз. Стратегії повинні бути розроблені таким чином, щоб мінімізувати ймовірність і вплив атаки троянських програм на об’єкти критичної інфраструктури.

Таблиця 2

Приклад оцінки ризику кібератаки для об’єкта критичної інфраструктури

Загроза	**Уразливість**	**Вплив**	**Ймовірність**	**Рівень ризику**	**Стратегія пом'якшення**
Зараження шкідливим програмним забезпеченням	Застаріле програмне забезпечення	Високий	Висока	Високий	Регулярні оновлення програмного забезпечення та виправлення безпеки
Несанкціонований доступ	Слабка політика паролів	Високий	Середня	Середній	Надійна політика паролів і багатофакторна автентифікація
Перехоплення даних	Незахищений зв'язок	Високий	Середня	Середній	Використання шифрування та безпечних протоколів зв’язку
Системний компроміс	Відсутність моніторингу системи	Високий	Висока	Високий	Впровадити системи моніторингу та виявлення вторгнень
Внутрішня загроза	Неналежний контроль доступу	Високий	Низька	Середній	Сильний контроль доступу та регулярні перевірки доступу користувачів
Крадіжка даних	Незашифровані конфіденційні дані	Високий	Низька	Середній	Шифрування та безпечне зберігання конфіденційних даних
Несанкціонований доступ	Фізична уразливість безпеки	Високий	Низька	Середній	Покращені заходи фізичної безпеки
Атаки соціальної інженерії	Відсутність навчання співробітників	Середній	Середня	Середній	Регулярні тренінги з питань безпеки для співробітників
Втрата даних або час простою	Відсутність плану відновлення	Високий	Низька	Середній	Реалізація планів аварійного відновлення та безперервності бізнесу
Час простою	Відсутність резервування системи	Високий	Низька	Середній	Впровадження резервованих систем і механізмів відновлення після збоїв

Стратегії захисту критично важливих об'єктів інфраструктури від троянських програм, як правило, передбачають поєднання технічних, адміністративних і фізичних засобів контролю. Технічні засоби контролю включають такі механізми безпеки, як брандмауери, системи виявлення вторгнень, антивірусне програмне забезпечення та шифрування даних. Адміністративний контроль передбачає політику, процедури та навчання, які допомагають переконатися, що співробітники обізнані про ризики безпеці та розуміють, як слідувати

© Хавер, А. В., & Савченко, В. А. (2023). Математична модель захисту об’єкта критичної інфраструктури від троянських програм. Сучасний захист інформації, 3(55), 12–21. https://doi.org/10.31673/2409-7292.2023.030002.

найкращим практикам безпеки. Фізичний контроль включає такі заходи, як контроль доступу, моніторинг і спостереження, які допомагають гарантувати, що лише авторизовані особи мають доступ до інфраструктури.

Нижче наведено кілька прикладів стратегій захисту, які можна використовувати для захисту об’єктів критичної інфраструктури від троянських програм:

1. Регулярні оновлення програмного забезпечення та виправлення безпеки: Оновлення програмного забезпечення та операційних систем за допомогою найновіших виправлень безпеки має важливе значення для усунення відомих уразливостей, якими може скористатися троянські програми.

2. Політика надійних паролів і багатофакторна автентифікація. Впровадження політик надійних паролів і багатофакторної автентифікації може допомогти запобігти несанкціонованому доступу до систем і знизити ризик зараження троянськими програмами.

3. Шифрування та безпечні протоколи зв’язку. Використання шифрування та безпечних протоколів зв’язку може допомогти запобігти перехопленню даних і захистити конфіденційну інформацію від викрадення чи зламу.

4. Моніторинг системи та виявлення вторгнень. Впровадження систем моніторингу та виявлення вторгнень може допомогти виявити та реагувати на зараження троянським програмним забезпеченням та інші порушення безпеки в режимі реального часу.

5. Контроль доступу та перевірки доступу користувачів: впровадження надійних засобів контролю доступу та регулярних перевірок доступу користувачів може допомогти запобігти внутрішнім загрозам і несанкціонованому доступу до критичних об’єктів інфраструктури.

6. Шифрування та безпечне зберігання конфіденційних даних. Використання механізмів шифрування та безпечного зберігання може допомогти захистити конфіденційні дані від доступу або викрадення троянським програмним забезпеченням.

7. Покращені заходи фізичної безпеки: впровадження заходів фізичної безпеки, таких як контроль доступу, моніторинг і спостереження, може допомогти запобігти несанкціонованому доступу до об’єктів критичної інфраструктури та зменшити ризик фізичного пошкодження або крадіжки.

8. Регулярні тренінги з питань безпеки для співробітників: Проведення регулярних тренінгів з питань безпеки для співробітників може допомогти переконатися, що вони обізнані про ризики безпеки та розуміють, як слідувати найкращим практикам безпеки.

9. Впровадження планів аварійного відновлення та безперервності бізнесу: розробка та впровадження планів аварійного відновлення та безперервності бізнесу може допомогти забезпечити швидке відновлення об’єктів критичної інфраструктури після кібератак та інших порушень безпеки.

Загалом стратегії захисту критично важливих об’єктів інфраструктури від троянських програм вимагають багаторівневого підходу, який включає поєднання технічних, адміністративних і фізичних засобів контролю. Впроваджуючи низку стратегій захисту, організації можуть допомогти знизити ризики зараження троянським програмним забезпеченням та інших порушень безпеки, а також захистити об’єкти критичної інфраструктури від кібератак.

Тестування та оцінка. Нарешті, стратегії захисту повинні бути протестовані та оцінені, щоб визначити їх ефективність у захисті об’єктів критичної інфраструктури від атак троянських програм. Це тестування повинно проводитися в контрольованому середовищі для забезпечення безпеки та надійності об’єктів критичної інфраструктури. Оцінка має порівняти ефективність різних стратегій захисту та визначити будь-які сфери, які потребують покращення. Тестування передбачає процес перевірки того, що модель поводиться так, як очікувалося, і дає бажані результати. Це можна зробити за допомогою різних засобів, таких як тестування програмного коду, запуск моделювання та аналіз результатів. Процес тестування допомагає виявити будь-які проблеми, помилки чи обмеження в моделі та дозволяє їх

© Хавер, А. В., & Савченко, В. А. (2023). Математична модель захисту об’єкта критичної інфраструктури від троянських програм. Сучасний захист інформації, 3(55), 12–21. https://doi.org/10.31673/2409-7292.2023.030002.

виправити перед впровадженням. Оцінка передбачає процес оцінювання ефективності моделі в реальних сценаріях. Це можна зробити, порівнявши модель із даними та сценаріями реального світу, щоб побачити, наскільки добре вона працює у прогнозуванні та пом'якшенні атак троянських програм. Процес оцінювання допомагає виявити будь-які слабкі сторони чи обмеження в моделі та надає зворотний зв'язок для подальшого вдосконалення.

Щоб забезпечити точність і надійність моделі, необхідно регулярно проводити тестування та оцінювання з урахуванням змін у ландшафті загроз, технологічного прогресу та нових уразливостей. Це допомагає гарантувати, що модель залишається актуальною та ефективною для захисту об'єктів критичної інфраструктури від атак троянських програм.

Загалом, тестування та оцінка є критичними складовими розробки та впровадження математичної моделі захисту об'єктів критичної інфраструктури від троянських програм. Випробовуючи й оцінюючи модель, організації можуть переконатися, що вона ефективна, точна й надійна для зменшення ризиків атак троянських програм і захисту критичних об'єктів інфраструктури.

Висновок

Підсумовуючи дане дослідження, можна констатувати, що захист критичних об'єктів інфраструктури від атак троянських програм вимагає комплексної математичної моделі, яка враховує потенційні загрози, уразливості та ризики, пов'язані з такими атаками. Модель також повинна враховувати ефективність існуючих заходів безпеки та розробку нових стратегій захисту для пом'якшення ризиків успішної атаки. Реалізація даної моделі може допомогти в забезпеченні безпеки та надійності об'єктів критичної інфраструктури, які необхідні для забезпечення ефективного функціонування держави.

Перелік посилань

1. SANS Institute. (2016). Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case. Retrieved from https://www.sans.org/reading-room/whitepapers/incident/analysis-cyber-attack-ukrainian-power-grid-defense-case-37192
2. Cherepanov, A. (2017). Analysis of the June 27, 2017 Petya-like outbreak. Retrieved from https://securelist.com/supply-chain-attack-on-ukraine/81432/
3. FireEye. (2020). Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor. Retrieved from https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
4. Europol. (2021). Emotet: Disrupting one of the most significant botnets in the world. Retrieved from https://www.europol.europa.eu/newsroom/news/emotet-disrupting-one-of-most-significant-botnets-in-world
5. Gao, Y., Chen, Z., & Li, Y. (2015). A dynamic game model for Trojan horse attack on critical infrastructure. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 45(7), 1016-1025.
6. Shu, J., & Ye, Y. (2013). Game-theoretic model for optimal security investment in critical infrastructure protection. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 43(5), 1142-1151.
7. Warren, D. E., Ehlen, M. A., & Black, S. P. (2011). Modeling critical infrastructure dependencies and interdependencies. IEEE Systems Journal, 5(2), 271-281.
8. Dong, Y., Han, Z., & Liu, J. (2013). Modeling and analysis of interdependent critical infrastructures. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 43(6), 1291-1305.
9. Ganjali, A., Marwat, S. S., & Sifalakis, M. (2012). Critical infrastructure protection: A mathematical modeling perspective. Journal of Network and Systems Management, 20(1), 128-144.
10. Chen, Y., Dong, Y., & Han, Z. (2012). Vulnerability analysis of critical infrastructure networks. IEEE Transactions on Power Systems, 27(1), 56-63.
11. Maras, M. H., & von Solms, R. (2014). An integrated approach to critical infrastructure protection. Computers & Security, 46, 80-92.
12. Huffaker, B., Kang, R., Brown, A., Borgeson, S., Hauer, J. F., & others. (2014). Modeling the effects of cyber attacks on a power grid: Emergent failures, interdependencies, and cascading outages. IEEE Transactions on Smart Grid, 5(5), 2197-2206.
13. Cyber Security for Industrial Control Systems. Keeping Worms and Viruses at Bay. Honeywell GmbH. 21.01.2011. https://www.chemanager-online.com/en/news/cyber-security-industrial-control-systems

Надійшла: 12.07.2023 Рецензент: д.т.н., професор Гайдур Г.І.