УДК 004.056
DOI: 10.31673/2409-7292.2021.035565

Кукшин Д.В.

МЕТОДИ ОЦІНЮВАННЯ СТАНУ ЗАХИЩЕНОСТІ ПІДПРИЄМСТВ ВІД ЗАГРОЗ КІБЕРБЕЗПЕЦІ

Розглянуто дев'ять методів оцінювання стану захищеності підприємств: метод оцінки вразливостей, метод оцінки мережі, метод оцінки виявлення вірусів, метод оцінки аутентифікації, метод оцінки тестом на проникнення, метод оцінки загроз від соціальної інженерії, метод оцінки апаратних загроз, метод оцінки політик та контрзаходів та метод оцінки природних загроз.

Ключові слова: оцінка, інформаційна безпека, загроза, соціальна інженерія, кібербезпека, кібератака.

Вступ

Оцінка інформаційної безпеки дуже важлива для організацій, щоб створити якісну систему захисту від кіберзагроз. Така оцінка має враховувати цілі забезпечення інформаційної безпеки на підприємстві щодо забезпечення цілісності, доступності та конфіденційності інформаційних активів. Удосконалення, поліпшення результатів оцінки можливо за умови знання станів характеристик і параметрів використовуваних захисних заходів, процесів менеджменту, усвідомлення понять інформаційної безпеки і розуміння ступеня їх відповідності необхідним результатами. Результати оцінки інформаційної безпеки організації можна отримати за допомогою моделі оцінки безпеки на підставі свідчень оцінки, критеріїв оцінки і з урахуванням контексту оцінки.

Оцінка інформаційної захищеності підприємства має декілька методів реалізації. Зазвичай оцінка вразливості розглядається як єдиний метод оцінки кібербезпеки, тоді як існує ряд інших методів, які є не менш важливими. На сьогоднішній день існує дев'ять методів проведення оцінки захисту інформації [1]:

1. Метод оцінки вразливості.

Оцінка вразливості - це вивчення потенційних вразливостей, які можуть бути використані при атаці на систему чи мережу. Зловмисник може використовувати різні вразливості системи, такі як: виявлення застарілих версій програмного забезпечення, виявлення відкритих портів в операційних системах та програмах, що працюють у мережі. Все, що може бути використане для виявлення слабких місць системи у мережах, додатках та комунікаційних пристроях. Однак сканери вразливості також використовують заздалегідь визначені бази даних для виявлення та потенційного зменшення недоліків. Сканування вразливостей також використовують зловмисники, які шукають системні вразливості для входу в мережу. Сканери вразливостей допомагають IT-персоналу на сучасному підприємстві виявляти слабкі місця в мережі, такі як відкриті порти, якими можуть користуватися користувачі, які не мають офіційного дозволу чи схвалення, та програми, в яких відсутні останні оновлення системи безпеки. Це допомагає переконатися, що мережа захищена і ніхто не зможе порушити політику безпеки.

Робота сканера вразливостей така ж, як і у інших антивірусів, які використовують бази даних, де зберігається опис різних типів вразливостей. Сканер вразливості збирає всю цю інформацію з мережі, а потім перевіряє порти мережевої системи, виявляючи будь-які порушення паролів та визначаючи відсутність оновлень безпеки. Що робить сканер вразливості відмінного від інших, так це те, що він не тільки ідентифікує вразливість, але й пропонує поради щодо відновлення вразливості.

Провідні сканери вразливостей надають користувачам інформацію про: слабкі місця в їх середовищі; аналіз ступенів ризику від кожної вразливості; рекомендації щодо зменшення вразливості.

2. Метод оцінки мережі.

Оцінка мережі – це другий метод оцінки та вимірювання кібербезпеки. Він може включати аналіз мережевих пристроїв, щоб виявити, які пристрої старі, не оновлені та не

підтримуються. Це також може включати оцінку продуктивності мережі, перевірку архітектури, огляд безпеки (конфігурація, точки доступу, помилки, вразливості). Термін оцінки мережі також може бути використаний для визначення того, які мережеві пристрої працюють. Також включає оцінку програм, персональних комп'ютерів, серверів та операційних систем.

Оцінку мереж можна розділити на три групи:

1. Оцінка мережевої інфраструктури.
2. Оцінка продуктивності та доступності мережі.
3. Оцінка безпеки мережі.

3. Метод оцінки виявлення вірусів.

Виявлення вірусів - це третій метод оцінки та вимірювання кібербезпеки, виявлення вірусів передбачає використання програмного забезпечення для виявлення вірусів, шпигунських програм, хробаків, троянських коней, руткітів, кейлогерів або будь-якого інструменту, який працює для розкриття інформації стороннім особам або шкоди для систем. Оскільки сучасні підприємства все більше займаються IP-мережами, і більшість транзакцій стали мережевими, отже, стали мішенню для кібератак. Тож для сучасних підприємств необхідно звертати увагу на вірусні детектори та періодично оновлювати.

Виявлення вірусів можна розділити на дві групи залежно від способу встановлення: мережевий детектор та детектор на основі кінцевих точок. Обидва вони мають переваги та недоліки.

Існує багато методів, доступних і використовуваних для виявлення вірусів, таких як методи, що базуються на сигнатурі атаки та методи, що базуються на евристиці.

Метод, що базується на сигнатурі атак сьогодні є найбільш використовуваними методами виявлення вірусів як в хост-детекторах, так і в мережевих детекторах. Сигнатура атаки - це заздалегідь визначений шаблон байтів, які зберігаються в базі даних для розрізнення шкідливого коду від позитивного. Бази даних сигнатур розробляються та створюються в лабораторіях шляхом аналізу зразків зловмисного програмного забезпечення. Детектори на основі методу аналізу сигнатур швидкі, прості та ефективні проти багатьох вірусів. Одним з недоліків цього методу є те, що вони завжди вимагають оновленої бази даних сигнатур, бо нові віруси, якщо їх не додати до бази, не будуть виявлені.

Метод, заснований на евристиці має ще інші назви, такі як виявлення на основі поведінки або аномалії; ці методи спостерігають та зосереджуються на діях, що виконуються програмним забезпеченням під час роботи, щоб виявити, чи є це зловмисне програмне забезпечення чи ні. Даний метод складається з двох етапів: етапу навчання, де детектор спостерігає та аналізує поведінку шкідливої і перевіреної програми. Друга стадія - це фаза тесту, детектор класифікує програму на шкідливу або перевірену на основі дій, що виконуються програмою. Перевага детекторів, побудованих на евристичному методі, - це здатність виявляти шкідливі програми, які не можуть виявити детектори, які побудовані на методі, що базується на сигнатурах. Недоліки детекторів, які побудовані на евристичному методі, - це те, що вони потребують часу, щоб провести сканування [1].

4. Метод оцінки аутентифікації.

Аутентифікація - це ідентифікація користувача на основі набору характеристик, таких як щось, що належить користувачеві, чи те, що він знає, або щось, що його відрізняє. Процес аутентифікації також складається з набору методів, які визначаються на основі необхідного рівня захисту. Оцінка аутентифікації також є дуже важливим методом вимірювання та оцінки методів кібербезпеки для сучасних підприємств, оскільки це один із найбільш використовуваних методів.

Процес аутентифікації можна розділити на три типи: 1) доказ знань; 2) доказ володіння; 3) доказ характеристик.

Доказ знань: стосується чогось, що знає користувач. Це може бути будь-яка аутентифікація, що складається з інформації, яку користувач знає. Наприклад, PIN-код

«персональний ідентифікаційний номер», ім’я користувача та пароль або секретне запитання.

Доказ володіння: стосується того, що є у користувача. Це може бути будь-яка аутентифікація на основі того, що є у користувача. Наприклад, мобільний телефон, смарт-картки, номери жетонів, посвідчення особи, посвідчення водія.

Доказ характеристик: відноситься до чогось, що є характерним для користувача. Це може бути будь-яка аутентифікація, що складається з фізіологічної або поведінкової інформації, що відрізняє користувача. Наприклад, відбиткі пальців, зчитування геометрії рук, довжина та вага, розпізнавання обличчя, розпізнавання сітківки ока, аналіз ДНК, розпізнавання голосу та шаблони підписів.

5. Метод оцінки тестом на проникнення

Являє собою змодельовану фактичну кібератаку на цільові системи для перевірки ефективності та стабільності систем перед реальними кібератаками та для виявлення вразливостей, якими можуть скористатися зловмисники. З метою вимірювання та оцінки ефективності кібербезпеки на підприємстві процес перевірки системи на проникнення можна класифікувати на п'ять типів:

1. Тест на проникнення в мережу.
2. Тестування на проникнення веб-додатків.
3. Тест на проникнення в бездротову мережу.
4. Тест на проникнення через соціальну інженерію.
5. Тест на проникнення зі сторони клієнта.

Та три методи проведення тесту на основі інформації, яку дозволено використовувати для тесту під час узгодження процесу тестування:

1. Тестування чорної скриньки.
2. Тестування білої скриньки.
3. Тестування сірої скриньки.

Незалежно від типу процесу тесту на проникнення, він складається з шести етапів: починаючи з планування та підготовки і закінчуючи підготовкою звіту про результати.

Тест на проникнення можна класифікувати на п’ять типів залежно від області тесту:

1. Тест на проникнення в мережу. Цей тип тесту є загальним та основним, і має на меті виявити прогалини та виявити вразливості в інфраструктурі мереж.

2. Тестування на проникнення веб-додатків. Перед проведенням цього тесту потрібно перевірити кінцеві точки всіх веб-додатків, з якими користувач може регулярно взаємодіяти. Через це на підготовку тесту потрібно ретельне планування та час. Крім того, із збільшенням загроз від веб-додатків способи їх перевірки постійно змінюються.

3. Тест на проникнення в бездротову мережу. Цей тест призначений для аналізу бездротових пристроїв, розміщених на балансі підприємства, це ноутбуки, планшети, смартфони, пристрої IOT. Тест на проникнення повинен розглянути протоколи, які використовувались для налаштування бездротового зв'язку. Це допоможе виявити слабкі місця, перевірити точки доступу, виявити точки, які порушують права доступу.

4. Тест на проникнення через соціальну інженерію. Цей вид тесту вважається важливим і підпадає під категорію оцінки фізичної безпеки. Цей вид тестування призначений для експертизи працівників підприємства. Він імітує атаки соціальної інженерії. Однак його можна розділити на дві під категорії: віддалене тестування - воно має на меті змусити працівника викрасти конфіденційну інформацію (виконавець тесту може здійснити таку атаку за допомогою фішингового електронного листа); фізичні тести - вимагають безпосереднього спілкування з працівником для отримання конфіденційної інформації (може включати шантаж, залякування, переконання та інші методи).

5. Тест проникнення зі сторони клієнта. Цей тест спрямований на виявлення загроз безпеці на локальних робочих станціях користувачів. Це можуть бути недоліки та помилки в програмних додатках, що працюють на робочій станції користувача, які можуть легко

використати хакери. Тестування проходять такі програми, як веб-браузери (Chrome, Firefox, Safari, IE, Opera), Putty, Sniffers, клієнти Git, MS PowerPoint, Photoshop, Adobe Flash Player, медіаплеєри, сторонні програми та програмне забезпечення з відкритим кодом.

Тест на проникнення може бути виконаний за допомогою одного з цих методів на основі факторів, які визначаються на основі природи тесту на проникнення, таких як

1. Визначення об’єкту тесту на проникнення.
2. Місце тесту на проникнення.
3. Виконавець тесту на проникнення.
4. Тест на попереднє проникнення.

6. Метод оцінки загроз від соціальної інженерії

Соціальна інженерія - це термін, що використовується для широкого кола зловмисних дій, що здійснюються завдяки взаємодії людей. Він використовує психологічні маніпуляції, щоб змусити працівників робити помилки в системі безпеки або видати конфіденційну інформацію. Атаки соціальної інженерії відбуваються в один або кілька кроків. Зловмисник спочатку розслідує передбачувану жертву, щоб зібрати необхідну довідкову інформацію, таку як потенційні точки входу та слабкі протоколи безпеки, необхідні для продовження нападу. Потім зловмисник рухається, щоб завоювати довіру жертви та забезпечити стимули для подальших дій, які порушують практику безпеки, наприклад, розкриття конфіденційної інформації або надання доступу до важливих ресурсів.

Особливо небезпечним робить соціальну інженерію те, що вона спирається на людські помилки, а не на вразливості програмного забезпечення та операційних систем. Помилки працівників менш передбачувані, що ускладнює їх виявлення та перешкоджання, ніж вторгнення на основі шкідливого програмного забезпечення. Атаки соціальної інженерії мають різні форми і можуть бути здійснені в будь-якому місці, де задіяна взаємодія людини. Нижче наведено п’ять найпоширеніших форм нападів на цифрову соціальну інженерію.

Приманка. Як випливає з назви, напади на приманки використовують фальшиву обіцянку, щоб викликати жадібність або цікавість жертви. Вони заманюють працівників у пастку, яка викрадає їх особисту інформацію або заносить до системи шкідливе програмне забезпечення.

Найбільш ганебна форма приманки використовує фізичні носії для розповсюдження шкідливого програмного забезпечення. Наприклад, зловмисники залишають приманку - як правило, заражені шкідливим програмним забезпеченням флешки - у помітних місцях, де потенційні жертви їх неодмінно бачать (наприклад, ванні кімнати, ліфти, стоянка цільової компанії). Жертви підбирають приманку з цікавості та вставляють її в робочий комп'ютер, в результаті чого в системі автоматично встановлюється шкідливе програмне забезпечення.

Шахрайство з приманками не обов'язково повинно здійснюватися у фізичному світі. Інтернет-форми приманки складаються з привабливих оголошень, які ведуть на шкідливі веб-сайти або спонукають працівників завантажувати заражену шкідливим програмним забезпеченням програму.

Залякування. Залякувальне програмне забезпечення передбачає бомбардування жертв фальшивими тривогами та вигаданими погрозами. Працівники вважають, що їх система заражена шкідливим програмним забезпеченням, що спонукає їх встановити програмне забезпечення, яке не має реальної вигоди (крім винного) або є самим шкідливим програмним забезпеченням. Залякувальне програмне забезпечення також називають програмним забезпеченням для обману, програмним забезпеченням сканера та шахрайством. Поширеним прикладом такого програмного забезпечення є спливаючі банери, що з’являються у вашому браузері під час веб-пошуку, відображаючи такий текст, як «Ваш комп’ютер може бути заражений шкідливими програмами-шпигунами». Він пропонує або встановити інструмент (часто заражений зловмисним програмним забезпеченням), або направить на шкідливий сайт, де комп’ютер заразиться. Залякувальне програмне забезпечення також

розповсюджується за допомогою електронної пошти, що містить неправдиві попередження або пропонує користувачам купувати нікчемні або шкідливі послуги.

Попереднє тестування. Тут зловмисник отримує інформацію через серію хитро сформованої брехні. Шахрайство часто ініціюється зловмисником, роблячи вигляд, що йому потрібна конфіденційна інформація від жертви, щоб виконати важливе завдання. Зазвичай зловмисник починає з встановлення довіри до своєї жертви, видаючи себе за колег, працівників поліції, банківських та податкових служб або інших осіб, які мають право знати повноваження. Претендент задає запитання, які нібито необхідні для підтвердження особи жертви, за допомогою яких вони збирають важливі особисті дані. За допомогою цієї афери збираються всілякі відповідні відомості та записи, такі як номери соціального страхування, особисті адреси та номери телефонів, телефонні записи, дати відпусток персоналу, банківські записи та навіть інформація про безпеку.

Фішинг. Як один з найпопулярніших видів атак соціальної інженерії, фішинг-шахрайство - це кампанії електронною поштою та текстовими повідомленнями, спрямовані на те, щоб створити у жертв відчуття терміновості, цікавості чи страху. Потім він підказує їм видавати конфіденційну інформацію, натискати посилання на шкідливі веб-сайти або відкривати вкладення, що містять шкідливе програмне забезпечення. Прикладом є електронний лист, надісланий працівникам організації, який попереджає їх про порушення політики, що вимагає негайних дій з їх боку, таких як необхідна зміна пароля. Він включає посилання на нелегітимний веб-сайт - майже ідентичний на вигляд законній версії, що спонукає нічого не підозрюючого працівника ввести свої поточні дані та новий пароль. Після подання форми інформація надсилається зловмиснику.

З огляду на те, що однакові або майже ідентичні повідомлення надсилаються всім користувачам у фішинг-кампаніях, їх виявлення та блокування набагато простіше для поштових серверів, що мають доступ до платформ спільного використання загроз.

Ціленапрямлена фішингова атака. Це більш цілеспрямована версія фішингового шахрайства, за допомогою якого зловмисник вибирає конкретних осіб або підприємства. Потім вони пристосовують свої повідомлення на основі характеристик, посади та контактів, що належать їх жертвам, щоб зробити їх атаку менш помітною. Ціленапрямлена фішингова атака вимагає набагато більше зусиль від імені винного і може зайняти тижні та місяці.

Сценарій такої фітингової атаки може включати зловмисника, який, видаючи себе за IT-консультанта організації, надсилає електронне повідомлення одному або кільком працівникам. Він сформульований і підписаний точно так, як це робить консультант, тим самим обманюючи одержувачів, вважаючи, що це справжнє повідомлення. Повідомлення пропонує одержувачам змінити пароль і надає їм посилання, яке перенаправляє їх на шкідливу сторінку, де зловмисник тепер фіксує їх облікові дані [5].

7. Метод оцінки апаратних загроз

Загрози апаратного забезпечення - це будь-яке порушення даних, що виникає внаслідок потенційного ризику фізичного доступу до апаратного забезпечення інформаційних технологій, наприклад неналежне використання апаратного забезпечення користувачами, крадіжка або кібератаки.

Загрози апаратного забезпечення може бути розділена на два види:

1. Загроза для користувача. Ця загроза включає ризики, спричинені працівником апаратного забезпечення. Наприклад, неправильне використання, яке призводить до проникнення зловмисників у мережу та порушення даних, або використання зовнішніх пристроїв зберігання даних, таких як жорсткі диски, CD, DVD або флеш-накопичувачі, що призводить до зараження вірусами, що, в свою чергу, призводить до порушення даних, а також використання неоригінальних деталей, які можуть заздалегідь бути зараженими вірусами або негативно вплинути на роботу пристрою.

2. Загроза доступу. Така загроза відображає ризики, спричинені несанкціонованим доступом до IT-обладнання. Це може призвести до викрадення апаратного забезпечення або

злому через повторну експлуатацію пароля за допомогою інструментів для скидання пароля або розповсюдження троянського вірусу на апаратному забезпеченні, що призводить до порушення даних[1].

8. Метод оцінки політик та контрзаходів

Політика інформаційної безпеки та контрзаходи - це закон і конституція, що регулює всі технічні дії на підприємствах, написані та узгоджені IT департаментом, керівництвом та юристами. Це можуть бути паролі, контроль доступу співробітників, фізичний контроль доступу, мережева безпека, управління мобільними пристроями, безпека серверів, практики управління ризиками, безпека даних, резервне копіювання та відновлення даних, план відновлення після аварій, журнали та моніторинг подій. Сучасні підприємства повинні розробляти політику інформаційної безпеки та контрзаходи, що відповідають їх бізнес-цілям, політика інформаційної безпеки та оцінка контрзаходів проводяться в основному для оцінки відповідності обов'язковим стандартам інформаційно-технічної безпеки.

У наші дні, з постійними змінами у бізнесі та технологіях, ресурси компаній, як маленькі, так і великі, є ціллю багатьох хакерів. Тому політика безпеки та контрзаходи вважаються методами запобігання, якими має керуватися більшість компаній, які використовують технології. Вони допомагають їм захищатись від можливих порушень або допомагають відновити мережу та інформацію у разі порушення. Політика безпеки необхідна і важлива для будь-якої організації, оскільки вона визначає, що робити, якщо користувачі зловживають мережевими активами, або відбувається кібератака в мережі або збій мережі через стихійне лихо.

9. Метод оцінки природних загроз

Природні загрози, які можуть загрожувати безпеці та конфіденційності інформації або пристроїв, такі як повені, землетруси або грози. Ці природні загрози можуть призвести до пожеж, високих температур і навіть уражень електричним струмом, спричиняючи потенційні фізичні збитки та втрату даних. Природні загрози розглядаються як ненавмисні та непередбачувані загрози. Однак вони мають дуже значний вплив на безпеку інформації. Тому їх слід враховувати під час оцінки інформаційної безпеки та під час підготовки політики безпеки та контрзаходів.

Висновок

Отже, існує багато різних видів оцінювання безпеки підприємства від сучасних загроз кібербезпеці. Вони всі створенні для оперативного встановлення відповідних заходів для забезпечення інформаційної безпеки. Так керівники можуть бути впевненими у захищеності своїх активів. Але потрібно проводити оцінки на постійній основі, адже технології постійно розвиваються. Проведення систематичних оцінок інформаційної безпеки допоможе вчасно оновлювати системи на підприємствах та розраховувати бюджет на поточний рік з урахуванням витрат на інформаційну безпеку.

Перелік посилань

1. Said F. Aboelfotoh, Noha A. Hikal. A Review of Cyber-security Measuring and Assessment Methods for Modern Enterprises. International journal on informatics visualization. 2019. №2. С. 157-176 URL: https://www.researchgate.net/publication/335105910_A_Review_of_Cybersecurity_Measuring_and_Assessment_Methods_for_Modern_Enteprises

2. Risk Based Security Assessments [Електронний ресурс] – Режим доступу:https://www.standardfusion.com/blog/risk-based-security-assessments/

3. What to know about Vulnerability Scanners and Scanning Tools [Електронний ресурс] – Режим доступу: https://web-pre-prod.balbix.net/insights/what-to-know-about-vulnerability-scanning-and-tools/

4. Social Engineering [Електронний ресурс] – Режим доступу: https://www.imperva.com/learn/application-security/social-engineering-attack/

Надійшла: 16.07.2021 Рецензент: д.т.н., доцент Ахрамович В.М.