1 БЕЗПЕКА БЕЗДРОТОВИХ МЕРЕЖ ТА ЇЇ ЗАБЕЗПЕЧЕННЯ

1.1 Технологія Wi-Fi та її особливості

У науковій та технічній літературі існує безліч статей про функцій Wi-Fi, які полегшують створення бездротової мережі. Технологія Wi-Fi є версією Ethernet без дротів у вигляді бездротової локальної мережі. Технологія Wi-Fi може використовуватися для підключення двох або більше двох пристроїв для різних цілей, наприклад, для обміну даними. Немає потреби у використанні дротів для підключення до Інтернету або для побудови мережі.

Wi-Fi – це нова характеристика мереж, в якій з'явилася нова функція. Передача даних здійснюється за допомогою радіохвиль. Завдяки технології Wi-Fi, користувач може легко отримати доступ до Інтернету, щоб ділитися ним по всьому світу. Тепер створення комп'ютерної мережі в будь-якому бізнесі не складає труднощів, наприклад, у компаніях, кафе, бібліотеках, кампусах, готелях, коледжах, університетах, приватних інститутах.

Wi-Fi створює нові можливості для підключення будь-якого пристрою. Є багато утиліт, ініційованих Wi-Fi.

Wi-Fi пропонує технологію Fortress для забезпечення дозволу бездротового зв'язку, що стримує посилення. Переваг Wi-Fi кілька. Він підтримує групу для створення мережі між однотипними мережами перетворення даних. Wi-Fi дозволяє легко підключати різні пристрої до комп'ютера, такі як ігрові пристрої, MP3-плеєр, радіо.

Технології Wi-Fi властива функція безпечного підключення до мережі Інтернет. Система безпеки технології Wi-Fi робить її надійнішою, а її інструменти захищають дані. Конфігурація пристроїв дуже проста, оскільки вона має безпеку

мережі, вбудовану систему і стандартні пристрої. Гнучкі методи аутентифікації спрощують транспортування та процедуру введення ключів. Технологія Wi-Fi сама по собі досить розумна, щоб забезпечити безпеку ПК, але також пропонує простий спосіб мережевої установки [1].

Самі протоколи бездротової передачі даних Wi-Fi були винайдені NCR Corporation / AT&T у Нідерландах у 1991 році. Використовуючи цю технологію, можна обмінюватися інформацією між двома чи більше пристроями. Wi-Fi був розроблений для мобільних обчислювальних пристроїв, таких як ноутбуки, але в даний час він широко використовується для мобільних додатків та побутової електроніки, такої як телевізори, цифрові камери, пилососи, система «Розумний дім». Wi-Fi – це один із видів бездротової технології. Зазвичай це називається бездротовою локальною мережею (локальна мережа). Технологія Wi-Fi дозволяє локальним мережам працювати без кабелів та дротів. Це популярний вибір для домашніх та ділових мереж. Бездротовий адаптер комп’ютера передає дані в радіосигнал і транспортує до антени для користувачів.

Wi-Fi – це високошвидкісне інтернет-з’єднання та підключення до мережі без використання будь-яких кабелів або дротів. У бездротовій мережі використовуються три основні елементи: радіосигнали, антена та маршрутизатор. Радіохвилі - це ключі, які уможливлюють створення мереж Wi-Fi.

Wi-Fi дозволяє людині отримати доступ до мережі у будь-якому місці фактично наданої області.

Як тільки комп’ютер отримує сигнали в діапазоні від 30 до 45 метрів маршрутизатора, він негайно підключає пристрій. Дальність дії Wi-Fi залежить від навколишнього середовища, у приміщенні чи на вулиці. Карти Wi-Fi будуть зчитувати сигнали та створювати інтернет-з’єднання між користувачем та мережею. Швидкість пристрою, що використовує з’єднання Wi-Fi, збільшується при наближенні комп’ютера до основного джерела, а швидкість зменшується по мірі видалення комп’ютера. На рис. 1.1 зображене з’єднання WI-FI.

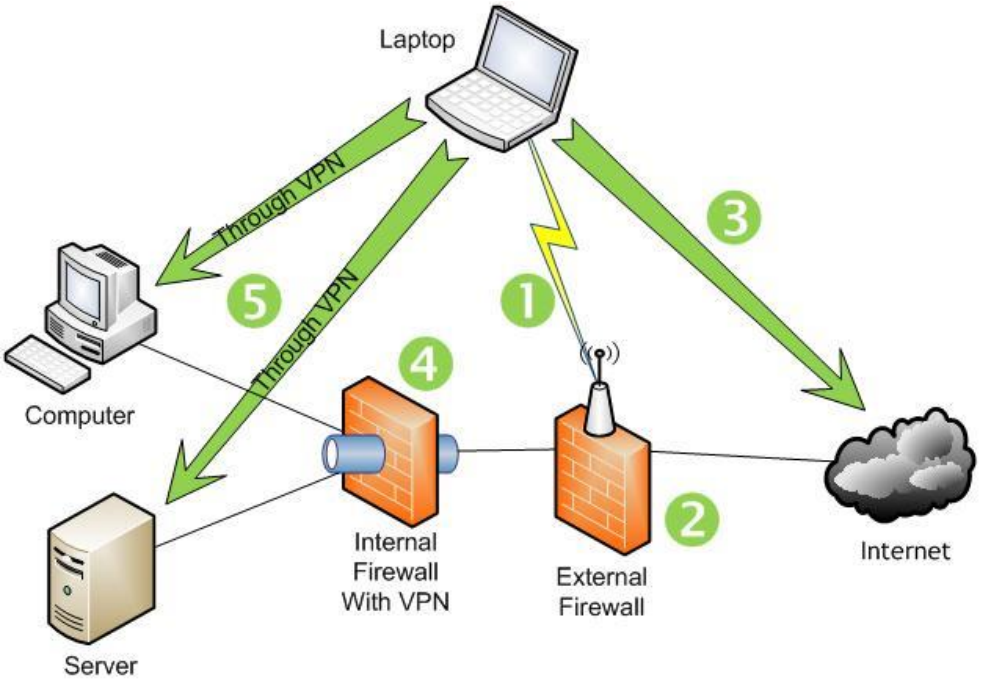

Рисунок 1.1 – З’єднання WI-FI

Нові ноутбуки і мобільні телефони мають вбудовані карти Wi-Fi. Якщо це безкоштовний тип підключення до мережі, користувачеві буде запропоновано ввести логін і пароль. Підключення до мережі Wi-Fi створює гарячі точки у містах. Гарячі точки – це точка підключення до мережі Wi-Fi.

Безпека – важливий елемент у технології Wi-Fi. Використовуючи бездротове з’єднання, необхідно звертати увагу на захист особистих даних. Можна легко підключитися до незахищених бездротових маршрутизаторів. Проблема в тому, що будь-хто підключений до бездротового маршрутизатора, який використовує користувач, може використовувати як його дані, так і займатися діяльністю, яка в Україні заборонена законодавчо, наприклад, нелегально завантажувати фільми та музику з піратських сайтів, порушуючи законодавство про авторське право.

Як зазначає М. Ільман, кожна бездротова мережа складається з хоча б однієї точки доступу, в більшості випадків, у якості точки доступу використовується мережевий маршрутизатор. Мережеві маршрутизатори поділяються – як за ціною, так і за областю використання. Таким чином, для великих корпоративних мереж,

та маленьких корпоративних мереж використовується більш дороге, та складне обладнання, а для маленьких офісів та домашнього використання – призначені маршрутизатори, з істотно нижчою ціною та більш простими налаштуваннями. Якщо подивитися на статистику продаж маршрутизаторів, то можна зробити висновок, що 85% користувачів мають дома свою мережу Wi-Fi. В той самий час 90% Wi-Fi мереж – домашні, або стоять у не великих офісах і лише 10% належать корпоративним мережам [2].

Усі маршрутизатори мають веб-сторінку, на якій можна підключитися до налаштування безпеки Wi-Fi. Для цього необхідно увімкнути WEP, ввести пароль та запам’ятати його. Наступного разу, коли ноутбук підключиться, маршрутизатор Wi-Fi попросить ввести пароль для підключення.

Бездротовий маршрутизатор – це один із видів обладнання, який зазвичай використовується в домашніх умовах. Це серце бездротової мережі. Цей пристрій здебільшого використовується провайдерами інтернет-послуг для підключення свого інтернет-кабелю. Іноді його також називають пристроєм WLAN.

Найпоширеніший метод бездротового підключення користувачів до Інтернету – це настільний Wi-Fi роутер. Ці маршрутизатори мають невеликі розміри і виглядають як коробки з антеною. Цей пристрій транслює сигнал на робочому місці або вдома. Коли користувач знаходиться далеко від базового Wi-Fi-роутера, сигнал буде слабким. Тому на робочому місці влаштовується кілька бездротових маршрутизаторів, наприклад, повторювачів сигналу. Розширювач діапазону Wi-Fi розташований у масиві, щоб збільшити чи розширити зону покриття Інтернету.

Крім того, у кожному смартфоні є мобільна точка доступу. Після увімкнення точки доступу в мобільному телефоні оператор мобільного зв’язку може спільно використовувати бездротову мережу через інші пристрої, щоб дозволити доступ до Інтернету. Зручна точка доступу Wi-Fi – це мобільна точка доступу, яка досягається через оператора мобільного телефону.

Різні пристрої, такі як ноутбуки, iPod, можуть бути підключені бездротовою мережею до пристрою, який підключається до Інтернету. Як і у випадку зі смартфоном, щомісячна вартість мобільної точки доступу залежить від використання обраного тарифного плану. Цей вид точок доступу більш узгоджений для забезпечення доступу до Інтернету шляхом пошуку стаціонарних точок доступу Wi-Fi.

В даний час це чотири основні типи технологій WI-FI:

- Wi-Fi - 802.11a – одна з бездротових технологій, визначає формат і структуру радіосигналів, що надсилаються мережними маршрутизаторами та антенами WI-FI;

- Wi-Fi - 802.11b – підтримує пропускну здатність 11 Мбіт/с. Сигнал у нерегульованому частотному діапазоні близько 2,4 ГГц. Це низька частота в порівнянні з Wi-Fi - 802.11a, що означає, що вона працює на більшій відстані. Це перешкоди для бездротових телефонів та іншої техніки. Дальність сигналу підходить при використанні побутової техніки;

- Wi-Fi - 802.11g – у 2002 і 2003 роках ця технологія підтримувала нові продукти. Це був швидкий доступ та максимальна швидкість на той час;

- Wi-Fi - 802.11n – це новітня технологія WI-FI. Вона була розроблена для покращення стандарту 802.11g. Об’єм смуги пропускання, що підтримується за рахунок використання декількох бездротових сигналів та антен замість однієї. Вона підтримує смугу пропускання 100 Мбіт/с та підвищену інтенсивність сигналу [3];

- Wi-Fi - 802.11ac – запущений в кінці 2014 року. Покращення пропускної здатності мережі над 802.11a і 802.11g, 75 метрів з формуванням променя і швидкість 1 Гбіт/с. Багатокористувацька технологія кількох входів і кількох виходів (MIMO) [4].

До елементів Wi-Fi належать:

1) бездротова точка доступу. Точка бездротового доступу використовується, щоб дозволити бездротовим пристроям підключатися до бездротової мережі.

Бездротова мережа спростить роботу з новими пристроями, перевівши їх в оперативний режим і забезпечивши хорошу підтримку для мобільних користувачів. Функція бездротової точки доступу в мережі аналогічна функції підсилювача домашньої стереосистеми. Точка доступу використовує смугу пропускання для розширення, щоб кілька пристроїв могли переміщатися через мережу на великій відстані. Однак точка бездротового доступу надає дуже корисні дані про пристрої в мережі для безпеки, а також використовується в практичних цілях;

2) картки Wi-Fi. Ці карти дозволяють передавати бездротовий сигнал, а також інформацію про реле, яке може бути внутрішнім або зовнішнім. Карти Wi-Fi також відомі як адаптери.

Брандмауери захищають такі мережі, як антивірусне програмне забезпечення, від непроханих користувачів та забезпечують безпеку інформації.

До обмежень Wi-Fi відносяться:

- обмежений діапазон;

- перешкоди з інших пристроїв, таких як мікрохвильові печі, телефони;

- висока потужність;

- ризики безпеки даних.

До переваг технології Wi-Fi відносять:

- бездротовий ноутбук можна переносити з одного місця до іншого і при цьому бути в мережі Інтернет;

- пристрої мережного зв’язку Wi-Fi без дротів можуть знизити вартість мережі;

- налаштування Wi-Fi простіше, ніж процес прокладання кабелю;

- можливість підключення до Інтернету через точки доступу.

До недолів технології Wi-Fi можна віднести:

- Wi-Fi генерує випромінювання, яке може завдати шкоди здоров’ю людини;

- необхідність відключення з’єднання Wi-Fi щоразу, коли не використовується сервер;

- існують деякі обмеження на передачі даних.

Отже, технологія Wi-Fi – це простий та економічний спосіб підключення до Інтернету без використання дротів [3].

З технічного боку стандарт IEEE 802.11 визначає протоколи, які забезпечують зв’язок із поточними бездротовими пристроями з підтримкою Wi-Fi, включаючи бездротові маршрутизатори та точки бездротового доступу. Точки бездротового доступу підтримують різні стандарти IEEE, про які йшлося вище. Кожен стандарт – це виправлення, яке було ратифіковано з часом. Стандарти працюють на різних частотах, забезпечують різну смугу пропускання та підтримують різну кількість каналів.

Точка доступу бере смугу пропускання, що надходить від маршрутизатора, і розтягує її, щоб багато пристроїв могли виходити в мережу на віддалених відстанях. Але точка бездротового доступу робить більше, ніж просто розширює Wi-Fi.

Найбільш поширений тип бездротової мережної системи – централізоване розгортання, що традиційно розгортається там, де будівлі та мережі знаходяться в безпосередній близькості. Таке розгортання консолідує бездротову мережу, спрощуючи оновлення та забезпечуючи розширені бездротові функції. Контролери базуються на підприємстві та встановлюються централізовано.

Конвергентне розгортання поєднує провідні та бездротові мережі на одному мережному пристрої – комутаторі доступу – і виконує подвійну роль комутатора та бездротового контролера.

Хмарне розгортання: система, яка використовує хмару для керування мережевими пристроями, розгорнутими локально у різних місцях [5].

4G LTE домашній Інтернет. Якщо користувач знаходиться у сільській місцевості, де можливості доступу до Інтернету обмежені, варто подумати про домашній Інтернет 4G LTE. Він пропонує високошвидкісний інтернет-сервіс, що

доставляється через вишки стільникового зв’язку та мобільні мережі із середньою швидкістю завантаження близько 25 Мбіт/с, зазвичай з меншою затримкою та більшим обсягом даних, ніж можна отримати через супутник. Переваги – найкраща швидкість та надійність залежно від оператора зв’язку. Деякі недоліки домашнього Інтернету 4G LTE можуть включати обмежену доступність та вартість обслуговування та налаштування.

Домашній Інтернет 5G. У міру того, як домашній Інтернет 5G (фіксований бездротовий доступ) стає все більш доступним, він може стати однією з найкращих та найекономічніших інтернет-послуг. Використовуючи новий спектр потужних радіочастот у бездротовій мережі, він пропонує більшу ємність, ніж 4G, значно більшу швидкість (до 1 гігабайта) і меншу затримку, ніж у більшості людей вдома. Оскільки базові станції 5G бездротового зв’язку зазвичай розташовані в межах 10 миль від будинків, надійність обслуговування часто буває чудовою. Єдиний реальний недолік домашнього Інтернету 5G зараз полягає в тому, що доступність його вкрай обмежена, але все це скоро зміниться.

Виходить, що мережа Wi-Fi – це просто підключення до Інтернету, яке використовується декількома пристроями в будинку чи офісі через бездротовий маршрутизатор. Маршрутизатор підключається безпосередньо до інтернет-модему та діє як концентратор для трансляції інтернет-сигналу на всі пристрої з підтримкою Wi-Fi. Це дає можливість залишатися на зв’язку з Інтернетом, поки користувач перебуває в зоні дії домашньої мережі. Термін був створений маркетинговою фірмою, тому що індустрія бездротового зв’язку шукала зручну для користувача назву для позначення не такої зручної для користувача технології IEEE 802.11.

Оскільки пристрої з мережі Wi-Fi «спілкуються» по радіохвилях, пристрої та особиста інформація користувачів можуть стати вразливими для хакерів, кібератак та інших загроз. Це особливо актуально, коли користувач підключається до публічної мережі Wi-Fi у таких місцях, як кафе чи аеропорт. По можливості

краще підключатися до бездротової мережі, захищеної паролем, або до особистої точки доступу [6].

Існують статистичні дані, згідно з якими станом на 2019 рік щороку по всьому світу постачається понад 3,05 мільярда пристроїв із підтримкою Wi-Fi.

Смуги хвиль Wi-Fi мають відносно високе поглинання і найкраще підходять для використання в прямій видимості. Багато поширених перешкод, таких як стіни, стовпи, побутова техніка, можуть значно зменшити радіус дії, але це також допомагає звести до мінімуму перешкоди між різними мережами в переповненому середовищі [7].

1.2 Загрози безпеки по каналу Wi-Fi

Основною проблемою безпеки бездротової мережі є її спрощений доступ до мережі в порівнянні з традиційними дротовими мережами, такими як Ethernet. З дротовою мережею необхідно або отримати доступ до будівлі (фізичне підключення до внутрішньої мережі), або пробити зовнішній брандмауер [8]. Щоб отримати доступ до Wi-Fi, потрібно просто перебувати в зоні дії мережі Wi-Fi. Більшість бізнес-мереж захищають конфіденційні дані та системи, намагаючись заборонити зовнішній доступ. Увімкнення бездротового підключення знижує безпеку, якщо мережа використовує недостатнє шифрування або його відсутність [9].

Зловмисник, який отримав доступ до маршрутизатора мережі Wi-Fi, може ініціювати атаку DNS-спуфінгу проти будь-якого іншого користувача мережі, підробивши відповідь до того, як запитуваний DNS-сервер зможе відповісти [10].

Старіший стандарт бездротового шифрування, Wired Equivalent Privacy (WEP), легко зламаний, навіть якщо його правильно налаштувати. Шифрування Wi-Fi Protected Access (WPA і WPA2), яке стало доступним в пристроях у 2003

році, було спрямоване на вирішення цієї проблеми. Зазвичай точки доступу Wi-Fi за замовчуванням працюють у режимі без шифрування (відкритий). Початківці користувачі отримують перевагу від пристрою з нульовою конфігурацією, який працює «з коробки», але цей параметр за замовчуванням не забезпечує бездротової безпеки, забезпечуючи відкритий бездротовий доступ до локальної мережі. Щоб увімкнути безпеку, користувач повинен налаштувати пристрій, як правило, за допомогою програмного графічного інтерфейсу користувача (GUI). У незашифрованих мережах Wi-Fi підключені пристрої можуть відстежувати та записувати дані (включаючи особисту інформацію). Такі мережі можна захистити лише за допомогою інших засобів захисту, таких як VPN або безпечний протокол передачі гіпертексту через захист транспортного рівня (HTTPS) [11].

Оскільки постійно кількість пристроїв, підключених по каналу Wi-Fi зростає, важливо реалізувати стратегію безпеки, щоб мінімізувати їхній потенціал для експлуатації. Пристрої, підключені до Інтернету, можуть використовуватись зловмисниками для збирання особистої інформації, крадіжки особистих даних, компрометації фінансових даних та мовчазного прослуховування або спостереження за користувачами. Прийняття деяких заходів безпеки під час налаштування та використання пристроїв може допомогти запобігти подібним діям [12].

До трьох найпоширеніших загроз безпеці WLAN відносяться:

1) атаки типу «відмова в обслуговуванні» – зловмисник наповнює мережу повідомленнями, що впливають на доступність мережевих ресурсів;

2) спуфінг та захоплення сеансу – коли зловмисник отримує доступ до мережевих даних та ресурсів, приймаючи особу дійсного користувача;

3) підслуховування – коли неавторизовані треті сторони перехоплюють дані, що передаються захищеною мережею [13].

Поєднання зловмисника з мережею користувача. Якщо не захистити бездротову мережу, будь-хто, хто має бездротовий комп’ютер у межах досяжності точки доступу, зможе використовувати з’єднання. Типовий діапазон

внутрішнього сигналу точки доступу становить 45-90 метрів. На відкритому повітрі цей діапазон може досягати 305 метрів. Отже, якщо житловий район щільно заселений, або якщо користувач живе у квартирі, відсутність захисту бездротової мережі може відкрити інтернет-з'єднання для багатьох користувачів. Ці користувачі можуть займатися незаконною діяльністю, відстежувати та перехоплювати веб-трафік або викрадати особисті файли.

Вардрайвінг – це особливий вид з'єднання. Радіус дії точки бездротового доступу може зробити підключення до Інтернету доступним за межами будинку, навіть на вулиці. Досвідчені користувачі комп'ютерів знають про це, і деякі з них їздять містами і районами з комп'ютером з бездротовим підключенням – іноді з потужною антеною – у пошуках бездротових мереж. Ця практика відома як «вардрайвінг».

В подвійній атаці зловмисник збирає інформацію про точку доступу до загальнодоступної мережі, а потім налаштовує свою систему, щоб видати себе за неї. Зловмисник використовує сильніший широкомовний сигнал, ніж той, що генерується основною точкою доступу; потім користувачі, що нічого не підозрюють, підключаються, використовуючи сильніший сигнал. Оскільки жертва підключається до Інтернету через зловмисника, зловмисник може легко використовувати спеціалізовані інструменти для читання будь-яких даних, які жертва відправляє через Інтернет. Ці дані можуть включати номери кредитних карток, комбінації імені користувача та пароля та іншу особисту інформацію. Перед використанням завжди підтверджуйте ім'я та пароль загальнодоступної точки доступу Wi-Fi. Це гарантує підключення до надійної точки доступу.

Багато точок громадського доступу не захищені, і трафік, що передається ними, не зашифрований. Це може призвести до бездротового сніфінгу і поставити під загрозу конфіденційні повідомлення або транзакції. Оскільки з'єднання передається «у відкритому вигляді», зловмисники можуть використовувати інструменти сніфінгу для отримання конфіденційної інформації, такої як паролі

чи номери кредитних карток. Необхідно переконуватися, що всі точки доступу, які підключаються, використовують шифрування не нижче WPA2.

Незахищена загальнодоступна бездротова мережа в поєднанні з незахищеним обміном файлами може дозволити зловмиснику отримати несанкціонований доступ до будь-яких каталогів та файлів, які користувач ненавмисно зробив доступними для спільного використання. Необхідно впевнитися, що при підключенні пристроїв до загальнодоступних мереж заборонене спільне використання файлів та папок. Дозволити спільне використання можна лише у визнаних домашніх мережах і лише тоді, коли це необхідно для обміну елементами. Якщо це не потрібно, спільний доступ до файлів вимикається. Це допоможе запобігти доступу невідомого зловмисника до файлів пристрою.

У громадських місцях зловмисники можуть просто зазирнути через плече, поки користувач друкує. Просто спостерігаючи за користувачем, вони можуть вкрасти конфіденційну чи особисту інформацію. Захисні плівки, які заважають серфінгістам побачити екран пристрою, можна використовувати у протидії даним методикам [12].

Згідно з дослідженням, проведеним Kaspersky Security Network, майже чверть загальнодоступних точок доступу Wi-Fi у світі не використовують жодного шифрування. З метою безпеки даних дуже важливо забезпечити шифрування мережі Wi-Fi, до якої підключається користувач. Проте низка інших ризиків може призвести до проблем, навіть якщо точка доступу використовує шифрування.

Більшість користувачів, які працюють із загальнодоступним Wi-Fi, мають на своїх пристроях багато важливої і, можливо, конфіденційної інформації, яка може завдати серйозної шкоди, якщо хакер оволодіє нею. На жаль, більшість користувачів загальнодоступного Wi-Fi швидше за все не усвідомлюють загрози, з якими вони стикаються.

Якщо користувач хоче залишатися в безпеці під час використання загальнодоступної мережі Wi-Fi, необхідно знати, які потенційні загрози можуть нашкодити.

Підсумовуючи вищезазначене, окреслимо 7 основних загроз безпеки по каналу Wi-Fi:

1. Крадіжка особистої інформації. Одна з найсерйозніших і найпоширеніших загроз. Особиста інформація буває різних форм: облікові дані для входу, фінансова інформація, особисті дані, фотографії.

Якщо хакер отримає доступ до комп'ютера або інших особистих пристроїв через зламане загальнодоступне з'єднання Wi-Fi, він може отримати повну свободу дій з усім, що зберігається.

2. Кібератаки на бізнес. Бізнесмени, які перебувають у дорозі протягом дня, можуть підключитися до загальнодоступного Wi-Fi, щоб перевірити електронну пошту, завантажити файли, переглянути інформацію про клієнтів та виконати різні інші завдання, для яких потрібне підключення до мережі.

Більшість підприємств вживають заходи безпеки, щоб знизити ризик підключення через Wi-Fi, але якщо необхідно увійти до будь-якого інструменту безпеки, щоб отримати доступ до мережі компанії, використання загальнодоступного підключення, як і раніше, пов'язане з ризиком.

Наприклад, користувач ніколи не знає, що може відстежувати провайдер Wi-Fi. Багато загальнодоступних з'єднань безкоштовні, але це не означає, що вони не потребують додаткових витрат. Провайдер Wi-Fi може відстежувати все, що користувач робить з підключенням Wi-Fi, і продавати дані рекламодавцям.

3. Атаки «зловмисник посередині». Атака «зловмисник посередині» відбувається, коли хтось видає себе за законну загальнодоступну службу Wi-Fi, щоб обманом змусити здійснити підключення. Хакери – «люди посередині», можуть мати доступ до всієї інформації для входу, паролів та іншого, що робить користувач при підключенні до Wi-Fi.

4. Незашифровані з’єднання. Коли користувач підключається до веб-сайту, який підтримує шифрування, дані, які передаються туди та назад, шифруються за допомогою безпечного ключа. Якщо хтось перехопить ці дані без ключа, він не зможе їх прочитати – дані будуть виглядати як комп’ютерний код, що не читається.

Однак не всі веб-сайти пропонують шифрування. Про це можна судити за префіксом HTTP, вказаним перед доменним ім’ям. Якщо воно починається з HTTPS, це зашифрований сайт. Якщо веб-адреса містить лише HTTP, вона не зашифрована.

Коли користувачі підключені до загальнодоступної мережі Wi-Fi, будь-хто в межах досяжності комп’ютера може перехопити все, що відправляється або отримується. Якщо користувач підключений до незашифрованого веб-сайту, він повністю читається.

5. Аналіз пакетів / підслуховування. Будь-хто, хто підключений до тієї ж мережі Wi-Fi, що і користувач, може підслуховувати те, що відправляється та отримується, за допомогою інструмента, який називають аналізатором пакетів або сніффером пакетів. Ці інструменти надають можливість переглядати все, що передається через мережу Wi-Fi, якщо воно не зашифроване.

Аналізатори пакетів дозволяють мережевим адміністраторам усувати проблеми з підключенням та інші проблеми з продуктивністю бездротових мереж. З іншого боку, вони також дозволяють хакерам перехоплювати інформацію інших користувачів і красти щось цінне.

6. Розповсюдження шкідливого ПЗ. Ще одна загроза, яка може виникнути при використанні загальнодоступного Wi-Fi, – це використання шкідливого ПЗ на пристрої. Шкідливе ПЗ існує у багатьох формах: віруси, черв’яки, троянські коні, програми-вимагачі, рекламне ПЗ.

Якщо хтось із того ж загальнодоступного Wi-Fi, має погані наміри, він може впровадити шкідливе програмне забезпечення на ПК, якщо він не захищений

належним чином. Підозрюваний провайдер Wi-Fi може використовувати точку доступу, щоб заразити комп’ютер однією або декількома з цих загроз.

Це може бути так само просто, як використання мережі Wi-Fi для розміщення реклами на кожному відвідуваному веб-сайті. На веб-сайті реклама не розміщується, але служба Wi-Fi може накладати її поверх інших веб-сайтів.

У цьому випадку реклама зазвичай зникає після відключення від Wi-Fi та повернення до домашнього чи офісного підключення. У більш серйозних випадках вони можуть встановити шкідливе програмне забезпечення на особисті пристрої, яке зберігатиметься при всіх підключеннях.

7. Зламування сеансу. Захоплення сеансу – ще одна загроза безпеці загальнодоступного Wi-Fi. У цьому випадку зловмисник перехоплює інформацію про комп’ютер та його підключення до веб-сайтів або інших служб. Отримавши цю інформацію, зловмисник може налаштувати свій комп’ютер відповідно до ПК користувача та перехопити з’єднання [14].

1.3 Забезпечення безпеки по каналу Wi-Fi

Якщо потрібно використовувати загальнодоступний Wi-Fi, користувач можете зробити кілька речей, щоб захистити себе від цих загроз. Деякі з них ефективніші, ніж інші, але слід пам’ятати, що хакери зазвичай прагнуть шляху найменшого опору.

По-перше, якщо потрібно підключитися до загальнодоступної мережі Wi-Fi без будь-яких заходів захисту, користувачу необхідно переконатися, що він не ділиться чимось особистим і не входить на будь-які конфіденційні веб-сайти. Також, доречно звести до мінімуму перегляди, не перевіряти електронну пошту та одразу ж відключитися від загальнодоступної мережі Wi-Fi, як тільки користувач знайде потрібну інформацію.

Служба віртуальної приватної мережі або VPN шифрує все, що користувач надсилає та отримує через мережу Wi-Fi.

За допомогою VPN користувач підключається до VPN-сервера через зашифроване з'єднання і все, що він робить, маршрутизується через цей сервер. Будь-хто, хто спробує підслухати чи перехопити цю інформацію, все одно не зможе її прочитати.

Також, доречно використати двофакторну автентифікацію. Багато веб-сайтів, які мають справу з конфіденційною інформацією, використовують функцію безпеки, яка називається двофакторною автентифікацією (2FA). Це додатковий метод аутентифікації, який працює разом із вашим паролем.

Він використовує або спеціальну програму на смартфоні, наприклад Google Authenticator, або текстові повідомлення, щоб відправити унікальний код після введення імені користувача та пароля. Якщо хакеру вдасться вкрасти інформацію для входу, він все одно не зможе увійти до системи без цього коду 2FA.

Найбезпечніший спосіб уникнути загроз безпеці загальнодоступних мереж Wi-Fi – це впершу чергу уникати їх. Замість підключення до загальнодоступної мережі Wi-Fi рекомендується використовувати з'єднання для передачі даних через стільникову мережу.

Наведені вище методи надають приватне з'днання, яке набагато безпечніше, ніж використання загальнодоступного [14].

До того ж, щоб мінімізувати ризики для бездротової мережі змінюють стандартні паролі. Більшість мережних пристроїв, включаючи точки бездротового доступу, попередньо налаштовані з паролями адміністратора за умовчанням для спрощення налаштування. Ці паролі за умовчанням легко доступні для отримання в Інтернеті, тому вони забезпечують лише мінімальний захист. Зміна стандартних паролів ускладнює доступ зловмисників до пристрою.

Крім того, можна дозволити доступ до мережі лише авторизованим користувачам. Кожна частина обладнання, підключена до мережі, має адресу керування доступом до середовища (MAC). Користувач має змогу обмежити

доступ до своєї мережі, відфільтрувавши ці MAC-адреси. Також можна використовувати «гостьовий» обліковий запис, який широко використовується на багатьох бездротових маршрутизаторах. Ця функція дозволяє надавати гостям бездротовий доступ окремим бездротовим каналом з окремим паролем, зберігаючи при цьому конфіденційність основних облікових даних.

Шифрування бездротових даних запобігає їх перегляду будь-ким, хто може отримати доступ до мережі. Для забезпечення цього захисту є кілька протоколів шифрування. Захищений доступ Wi-Fi (WPA), WPA2 та WPA3 шифрують інформацію, що передається між бездротовими маршрутизаторами та бездротовими пристроями. WPA3 в даний час є найнадійнішим шифруванням. WPA і WPA2, як і раніше, доступні; однак рекомендується використовувати обладнання, яке спеціально підтримує WPA3, оскільки використання інших протоколів може залишити мережу відкритою для експлуатації.

Щоб запобігти доступу сторонніх до мережі, уникають розголошення SSID. Усі маршрутизатори Wi-Fi дозволяють користувачам захищати SSID свого пристрою, що ускладнює зловмисникам пошук мережі. Якщо залишити це значення за умовчанням, встановлене виробником, потенційний зловмисник зможе визначити тип маршрутизатора і, можливо, скористатися будь-якими відомими вразливостями.

Користувачеві необхідно розглянути можливість встановлення брандмауера безпосередньо на бездротових пристроях (брандмауер на основі хоста), а також у домашній мережі (брандмауер на основі маршрутизатора або модему). Зловмисники, які можуть безпосередньо підключитися до бездротової мережі, можуть обійти мережевий брандмауер – брандмауер на основі хоста додасть рівень захисту до даних на ПК.

Також, для забезпечення безпеки по бездротовому з’єднанні, потрібно підтримувати антивірусне програмне забезпечення. Багато антивірусних програм мають додаткові функції, які виявляють та захищають від шпигунського ПЗ.

Необхідно з обережністю використовувати спільний доступ до файлів. Якщо в цьому немає необхідності, слід вимкнути файли між пристроями.

Важливо регулярно оновлювати програмне забезпечення точки доступу. Виробник точки бездротового доступу буде періодично випускати оновлення та виправлення для програмного забезпечення та прошивки пристрою [12].

Сучасні бездротові системи потребують іншого набору функцій, ніж раніше. У зв'язку з підвищеним попитом на бездротову і дротову інфраструктуру необхідно включити балансування навантаження з високою пропускною здатністю. Це означає, що при перевантаженні однієї точки доступу система активно перемикатиме користувачів з однієї точки доступу на іншу залежно від доступної ємності.

Зростання популярності нових бездротових пристроїв лише збільшуватиметься. Мережа повинна мати можливість починати з малого, якщо необхідно, але розширюватися з точки зору покриття та пропускної спроможності в міру необхідності – без необхідності капітального ремонту чи будівництва нової мережі.

Побудова «герметичної» мережі не зводиться лише до одного компоненту.

Однак основою цієї системи є мережевий брандмауер, який забезпечує створення правильного балансу між продуктивністю та безпекою, антивірусний захист, фільтрування спаму, глибоку перевірку пакетів (DPI), фільтрування додатків [15].

Наприклад, віддалений доступ до елементів керування маршрутизатора дозволяє змінювати налаштування через Інтернет. WPS дозволяє натиснути кнопку на маршрутизаторі, щоб підключити пристрій до Інтернету, а не вводити пароль мережі. Нарешті, UPnP дозволяє пристроям знаходити один одного в мережі. Ці функції можуть спростити, наприклад, додавання пристроїв до мережі або дозволити гостям використовувати Wi-Fi, але вони можуть зробити мережу менш захищеною [16].

2 МОЖЛИВІ ВРАЗЛИВОСТІ ТОЧОК ДОСТУПУ ПО КАНАЛУ WI-FI

2.1 Витік даних по бездротовій мережі

Незахищений Wi-Fi може призвести до витоку даних. Wi-Fi – відмінне середовище, що дозволяє користувачам отримувати доступ до мереж як гостьових користувачів або користувачів BYOD зі своїх власних пристроїв. Однак нездатність належним чином захистити цю мережу може порушити захист користувачів. А коли захист порушено, дані будуть скомпрометовані, що може призвести до так званого витоку даних.

Розглянемо три способи, якими незахищений Wi-Fi може призвести до несанкціонованого витоку конфіденційних даних.

1. Відсутність рольового контролю доступу.

Керування доступом на основі ролей (RBAC) для тих, хто не обізнаний – це метод управління доступом користувачів до об’єктів мережної файлової системи. Існують програми, як Ruckus Cloudpath, які пропонують керування доступом на основі ролей для IT-фахівців. Багато витоків даних відбуваються через ненавмисне розкриття інформації, а не через навмисних кіберзлочинців. Це означає, що ненавмисний гість або співробітник можуть помилково отримати доступ до конфіденційних даних, тому що вони просто не були налаштовані в мережі доступу на основі ролей.

Стратегія безпечного доступу вимагає, щоб користувачам було надано доступ лише до ресурсів, які вважаються відповідними або важливими для їхньої «ролі». Заснований на політиці контроль є наріжним каменем таких стратегій.

2. Невиконання перевірки стану безпеки.

Багато IT-фахівців погодяться, що програми BYOD підвищують продуктивність співробітників і що відвідувачі очікують, що їх пристрої легко

підключатимуться до мережі. IT-команди не мають можливості контролювати ці пристрої, тому вони не мають можливості гарантувати, що на них встановлені останні оновлення або встановлений антивірус. Нездатність виконати попередню перевірку стану безпеки до підключення та гостьових пристроїв також є областю ризику. Шкідливе програмне забезпечення вважається основною причиною витоку даних (шкідливе програмне забезпечення призначене для порушення, пошкодження або отримання несанкціонованого доступу).

Політика запобігання розповсюдженню шкідливого програмного забезпечення у мережі полягає в тому, щоб на мережевих пристроях було встановлено засіб захисту від шкідливого програмного забезпечення та не дозволяти використання пристроїв BYOD у мережі без встановленого програмного забезпечення для захисту від зловмисного програмного забезпечення. Якщо співробітники можуть підключити свій ноутбук до мережі без встановленого та оновленого антивірусного програмного забезпечення, це пролом у безпеці.

3. Незашифрований мережевий трафік.

Незашифровані мережеві дані, що передаються Wi-Fi, можна переглянути. Інструменти, що забезпечують таку атаку, легко доступні.

Багато веб-сайтів, до яких здійснюється доступ, обслуговуються через https, але часто не всі ресурси сторінки зашифровані. Так само мобільні програми можуть однаково або не можуть шифрувати свій трафік даних, особливо якщо використовуваний додаток не дуже добре адаптований [17].

2.2 Класифікація атак на каналі Wi-Fi

В індустрії бездротового зв’язку важко стримувати атаки на бездротові мережі та їх потенційні наслідки. Всі типи бездротових мереж уразливі для наступних атак та їх класифікацій:

1. Атаки контролю доступу, які намагаються проникнути в мережу за допомогою бездротових або обхідних заходів контролю доступу до WLAN:

- War Driving – виявлення бездротових локальних мереж шляхом прослуховування сигналів маяків;

- несанкціоновані точки доступу – встановлення незахищеної точки доступу всередині брандмауера;

- спеціальні асоціації – підключення безпосередньо до незахищеної станції;

- підміна MAC-адреси – переналаштування MAC-адреси зловмисника, щоб він видавав себе за авторизовану точку доступу або станцію;

- RADIUS Cracking – відновлення секрету RADIUS за допомогою грубої сили.

2. Атаки на конфіденційність, які намагаються перехопити особисту інформацію, що надсилається через бездротові асоціації:

- підслуховування – перехоплення та декодування незахищеного трафіку додатків;

- зламування WEP-ключа – захоплення даних для відновлення ключа WEP з використанням пасивних або активних методів;

- Evil Twin AP – видає себе за авторизовану точку доступу, передаючи SSID бездротової локальної мережі, щоб заманити користувачів;

- AP Phishing – запуск дублюючого порталу або веб-сервера на злісному двійнику AP для «фішингу» для входу користувачів та номерів кредитних карток;

- людина посередині – використання традиційних інструментів атаки типу людина посередині.

3. Атаки на цілісність, які відправляють підроблені кадри управління, керування або даних бездротової мережі, щоб ввести одержувача в оману або полегшити інший тип атаки:

- Frame Injection – ін'єкція Wi-Fi кадрів;

- відтворення даних – захоплення кадрів для подальшого відтворення;

- EAP Replay – захоплення протоколів автентифікації, що розширюються, для подальшого відтворення;

- RADIUS Replay – захоплення повідомлень RADIUS Access-Accept або Reject для подальшого відтворення.

4. Атаки аутентифікації, які можуть використовуватися зловмисниками для крадіжки справжніх ідентифікаторів та облікових даних користувачів для доступу до приватних мереж та служб:

- підбір загального ключа – спроба автентифікації із загальним ключем із ключами WEP, ключами за умовчанням виробника або зламаними ключами WEP;

- злом PSK – відновлення WPA / WPA2 PSK із захоплених ключових кадрів рукостискання за допомогою інструмента атаки за словником;

- крадіжка входу – захоплення облікових даних користувача з протоколів додатків з відкритим текстом;

- злом входу в домен – відновлення облікових даних користувача шляхом зламування хешів паролів NetBIOS;

- зламування входу до системи VPN – відновлення облікових даних користувача шляхом проведення атак грубої сили на протоколи аутентифікації VPN.

5. Атаки доступності, які перешкоджають доставці бездротових послуг законним користувачам, або відмовляючи їм у доступі до ресурсів WLAN, або завдаючи шкоди цим ресурсам:

- AP Theft – фізичне видалення AP з громадського простору;

- DoS Квінсленд – використання CSMA / CA;

- Beacon Flood – створення тисяч підроблених маяків, які ускладнюють станціям пошук законної точки доступу [18].

Багато з найпоширеніших атак на бездротові мережі мають кон'юнктурний характер. Хакери Wi-Fi шукають бездротові мережі, які легко атакувати.

Хакери більш ніж щасливі скористатися слабким контролем безпеки, щоб отримати доступ до конфіденційної інформації та поширювати зловмисне програмне забезпечення. Навіщо витрачати час на атаки на добре захищені мережі Wi-Fi, коли їх багато з недостатнім захистом чи без нього?

Погано захищені мережі Wi-Fi також стають мішенню для більш витончених кіберзлочинців та організованих злочинних груп, які прагнуть закріпитись у мережі. Атаки можуть бути надзвичайно прибутковими. Доступ до корпоративної мережі може дозволити встановити програми-вимагачі, і якщо шкідливе програмне забезпечення може бути встановлене в POS-системах, номери кредитних / дебетових карт десятків або сотень тисяч клієнтів можуть бути вкрадені.

Дослідження, проведене «Лабораторією Касперського» у 2016 році, показало, що понад чверть загальнодоступних точок доступу Wi-Fi, встановлених у торгових центрах, небезпечні та не мають навіть елементарних заходів безпеки. Чверть не шифрувала трафік взагалі, тоді як дослідження, проведене Skycure, показало, що п'ять із 10 найбільш завантажених торгових центрів США мали небезпечні мережі Wi-Fi.

В одному торговому центрі в Лас-Вегасі було виявлено 14 небезпечних точок доступу Wi-Fi. Хакери можуть використовувати аналізатори пакетів для перехоплення трафіку у незашифрованих мережах Wi-Fi. Відстеження пакетів – одна з найпоширеніших атак на бездротові мережі.

Ці поширені атаки на бездротові мережі легко виконуються на старих маршрутизаторах, наприклад, які використовують шифрування WEP. WPA пропонує кращу безпеку, WPA2 ще краще, або, в ідеалі, слід використовувати новий протокол шифрування WPA3, якщо він підтримується точкою доступу.

Атаки на бездротові мережі мають не лише теоретичний характер. Нижче наведено деякі приклади поширених атак на бездротові мережі, які призвели до встановлення шкідливого ПЗ або крадіжки конфіденційної інформації. Ці останні атаки на безпеку бездротової мережі можна було б легко запобігти, якби було реалізовано відповідні заходи безпеки.

Одним із яскравих прикладів того, наскільки легко хакеру може бути захоплення мережі Wi-Fi, є Тель-Авів. Тель-Авів пропонує загальноміську безкоштовну мережу Wi-Fi, яка включає базові заходи безпеки для забезпечення безпеки користувачів в мережі. Однак це виявилося не так надійно, як думала міська влада.

Дорогою додому мешканець Тель-Авіва Аміхай Нейдерман зауважив, що з’явилася нова точка доступу Wi-Fi. Точка доступу FREE_TLV була надана містом і Нейдерман вирішив перевірити її заходи безпеки. Після визначення IP-адреси, через яку клієнти Wi-Fi виходили в Інтернет, він відключився, просканував маршрутизатор і виявив, що веб-інтерфейс входу в систему був запущений через порт HTTPS 443.

Хоча він не виявив серйозних уразливостей, після ретельного аналізу він виявив вразливість переповнення буфера, яку він успішно використав, щоб отримати повний контроль над маршрутизатором. Таким чином, якби він був такий схильний, він міг би перехопити трафік від десятків тисяч користувачів.

Можливо, це не одна з найпоширеніших атак на мережі Wi-Fi, проте примітна зростанням використання пристроїв IoT. Можливості Інтернету речей включені у всі види пристроїв, від тостерів до пральних машин. Ці пристрої можуть бути вразливими для атак ланцюжка поставок – коли обладнання змінено, щоб дозволити використовувати пристрої для атак на мережі Wi-Fi [19].

2.3 Оцінка можливих збитків від атак

Технології продовжують розвиватися. Сьогодні особисті стосунки, робочі графіки та бізнес-рішення не тільки використовують технологічні інструменти, вони часто покладаються на них, і це відкриває двері для хакерів. Легкий доступ до величезних масивів конфіденційної інформації означає, що все більше і більше організацій піддаються цілій низці кібер-ризиків, від крадіжки даних і програм-вимагачів до корпоративного шпигунства – вони можуть навіть не знати про це.

Перші 48 годин мають вирішальне значення при мінімізації збитків від кібератаки.

Кіберзагрози зростають – 21% підприємств постраждали від кіберінцидентів. Ці атаки можуть бути дуже дорогими. Згідно з дослідженням вартості витоку даних, проведеним IBM Ponemon Institute у 2020 році, середня вартість витоку даних у Канаді становить 4,5 мільйона доларів США.

Кібер-ризик зазвичай відноситься до будь-якого ризику фінансових втрат, збоїв чи шкоди репутації організації внаслідок збою її систем інформаційних технологій. Кібер-ризик може матеріалізуватися різними способами, наприклад:

- умисні та несанкціоновані порушення безпеки з метою отримання доступу до інформаційних систем;

- ненавмисні або випадкові порушення безпеки;

- операційні IT-ризики через такі чинники, як погана цілісність системи.

У багатьох випадках, чим складніші та масштабніші цифрові операції бізнесу, тим вищий кібер-ризик.

Деякі з найсерйозніших кіберзагроз пов’язані з переходом на нові технології, такі як Інтернет речей (IoT). У міру того, як мережі розосереджуються і все більше пристроїв розвивають ширші можливості підключення, заходи безпеки також повинні розвиватись.

Імітація фішинг-атаки з потенційними користувачами Wi-Fi може бути дуже ефективним засобом навчання. Крім того, інвестиції в хорошу систему захисту матимуть своє значення. Використовуючи кілька рівнів контролю безпеки – брандмауер, систему запобігання вторгненням (IPS) та систему захисту від вторгнень (IDS) – користувач отримує гарантію, що система матиме адекватну резервну копію на випадок використання вразливості. Ідея полягає в тому, щоб мати відповідну форму захисту від будь-яких атак.

Також, доречно створити протокол на випадок втрати або крадіжки пристрою.

Також, користувачеві доречно бути готовим до надзвичайної ситуації. Неможливо передбачити, коли відбудеться атака, тому завжди корисно мати стратегії резервного копіювання та відновлення готові до роботи. Шифрувати всю конфіденційну інформацію при її зберіганні або передачі, але також мати план дій у разі непередбачених обставин, якщо системи вийдуть з ладу.

Кібер-ризик зростає в міру розвитку кіберзлочинності, і ніколи не було так важливо мати систему запобіжних заходів [20].

Успішна кібератака може завдати серйозних збитків. Це може вплинути на прибуток, а також на репутацію бізнесу та довіру споживачів. Наслідки порушення безпеки можна умовно поділити на три категорії: фінансові, репутаційні та юридичні.

1. Економічна вартість кібератаки. Кібератаки часто призводять до значних фінансових втрат у результаті:

- крадіжки корпоративної інформації;

- крадіжки фінансової інформації (наприклад, банківських реквізитів або даних платіжної картки);

- крадіжки грошей;

- збоїв у торгівлі (наприклад, неможливість проводити транзакції в Інтернеті);

- втрати бізнесу чи контракту.

Підприємства, які постраждали від поганої кібербезпеки, також зазвичай несуть витрати, пов’язані з ремонтом порушених систем, мереж та пристроїв [21].

2. Репутаційні збитки. Довіра – важливий елемент взаємовідносин із клієнтами. Кібератаки можуть завдати шкоди репутації бізнесу та підірвати довіру клієнтів. Це, своєю чергою, потенційно може призвести до:

- втрати клієнтів;
- втрати продажів;
- зниження прибутку.

Вплив репутаційної шкоди може навіть вплинути на постачальників або вплинути на відносини, які можуть бути у із партнерами, інвесторами та іншими третіми сторонами, залученими до бізнесу [22].

3. Правові наслідки кібербезпеки. Закони про захист даних та конфіденційність вимагають, керування безпекою всіх особистих даних. Якщо ці дані були випадково або навмисно скомпрометовані, і користувач не зміг застосувати відповідних заходів безпеки, можна зіткнутися зі штрафами та санкціями регулюючих органів.

Для мінімізації можливих збитків від кібератак потрібно використовувати керування ризиками. Після атаки ефективний план реагування на інциденти кібербезпеки може допомогти:

- зменшити вплив атаки;
- повідомити про кіберзлочин у відповідний орган;
- очистити уражені системи;
- налагодити бізнес у найкоротші терміни [23].

Сьогодні кібератаки можуть бути спрямовані на будь-яку компанію чи організацію, що має підключення до Інтернету, а успішна атака може знищити цінні цифрові активи.

В проведеному дослідженні цифровими активами вважаються електронні набори даних, які мають майбутню економічну цінність і мають законні правові власності. Прикладами таких активів є програмне забезпечення, комп’ютерний

код, відеоігри, цифрові зображення, файли WAV, анімація, цифрові записи (такі як бази даних, електронні документи та електронні книги), веб-сторінки, презентації PowerPoint та залишкова інформація.

У порівнянні з фізичними даними, цифрові відрізняються простотою передачі та зміни. Якщо ці активи пошкоджені або знищені, традиційна оцінка збитків не може охопити розмір понесених збитків. Без розуміння всіх змінних, які впливають на визначення збитків, важко визначити повну втрату цифрових активів компанії або прийняти зважені бізнес-рішення.

Існує кілька причин для точної кількісної оцінки втрат активів від кібератак.

По-перше, правильна оцінка збитків необхідна під час повідомлення про напад до правоохоронних органів. У більшості юрисдикцій такі злочини повинні перевищувати визначену суму, щоб вважатися злочином, передбаченим законом.

Ще однією причиною для точної оцінки збитків є подання заявки на страхове відшкодування. Залежно від свого страхового покриття, організація може бути в змозі відшкодувати частину своїх збитків від страхового перевізника.

Третя причина точної кількісної оцінки збитків пов’язана зі здатністю компанії приймати правильні бізнес-рішення. Наприклад, якщо потрібно порівняти рентабельність інвестицій, потрібна оцінка вартості цифрового активу.

Звичайно метою кібератаки є вимагання, фінансове шахрайство, отримання широкого доступу до комп’ютерних ресурсів, запуск зловмисних атак через Інтернет, заподіяння випадкової шкоди або крадіжка інтелектуальної власності, але ці злочини не повинні мати жодної злочинної мети.

Збитками від атак вважаються пошкодження матеріальних активів або нематеріальні втрати інформації чи даних, або майбутні бізнес-інтереси та ресурси організації. Крім того, можуть виникнути нематеріальні збитки. Кібервтрати виникають внаслідок несанкціонованого видалення та продажу конфіденційної інформації; вартість відновлення знищеного або викраденого коду; знищення від шкідливого програмного забезпечення, запровадженого в мережу; втрата партнерських відносин, що виникли внаслідок кібератаки; витрати

та збитки, понесені в судових процесах після кібератаки; витрати на перевірку та реконструкцію систем; зниження репутації компанії; і втрата довіри акціонерів і ринкової капіталізації.

Перелік витрат і збитків:

1) витрати на перевірку систем (діагностика відновлення);

2) витрати на відновлення системи в режимі онлайн (тестування);

3) вартість заміни знищеного майна чи послуг;

4) втрачений прибуток;

5) завдана шкода;

6) втрата комп'ютерного часу (втрата продуктивності);

7) вартість заміни втрачених даних [24].

2.4 Огляд існуючих бездротових систем виявлення та запобігання вторгнень

Експерт Карен Скарфоне вивчає найкращі системи запобігання вторгненням у бездротові мережі (WIPS), щоб допомогти користувачам визначити, яка з них найкраще підходить для них.

Корпоративні системи запобігання вторгненням у бездротову мережу вже досить давно допомагають організаціям виявляти та блокувати атаки на бездротові локальні мережі (LAN). Раніше продукти для запобігання бездротовим вторгненням найчастіше використовувалися для виявлення несанкціонованих точок бездротового доступу (AP), але з того часу вони еволюціонували для захисту від широкого спектру атак на бездротові локальні мережі (WLAN). У зв'язку з різким зростанням використання бездротових технологій, особливо для ноутбуків, смартфонів і планшетів, організації вважають все більш важливим використання бездротових систем запобігання вторгненням.

Система запобігання вторгненням у бездротові мережі (WIPS) може швидко зупинити загрози WLAN, наприклад, запобігти несанкціонованому доступу до WLAN та клієнтським пристроям. Такий доступ, у свою чергу, можна використовувати для отримання несанкціонованого доступу до провідних мереж, систем та даних організації.

Існує три моделі розгортання WIPS:

Точка доступу частково виконує функції WIPS, чергуючи їх зі своїми звичайними функціями підключення до мережі. Точка доступу має вбудовані спеціальні функції WIPS, тому вона може постійно виконувати функції підключення до мережі та функції WIPS.

WIPS розгортається через виділені датчики замість точок доступу.

Оскільки він може спричинити значне уповільнення роботи мережі, а також найменш ефективний при виявленні атак, перша модель розгортання значною мірою вийшла із вживання. Дві інші моделі – виділені WIPS, вбудовані в точки доступу, та виділені датчики WIPS – широко використовуються.

Кожна організація має власні унікальні вимоги до безпеки, а також різні технології та архітектури WLAN, тому кожна організація повинна проводити свій власний процес оцінки, щоб гарантувати, що рішення буде оптимальним для неї.

Критерій №1: управління пристроєм.

При оцінці продуктів WIPS необхідно враховувати два аспекти управління пристроями: управління самими пристроями WIPS, такими як датчики, та управління точками доступу WLAN, клієнтськими пристроями та іншими компонентами.

Що стосується управління пристроями WIPS, то всі продукти WIPS, в яких використовуються виділені датчики, пропонують централізований механізм керування цими датчиками. Так само для продуктів, реалізованих за допомогою можливостей WIPS, вбудованих у точки доступу, існують централізовані механізми управління.

Використання WIPS для керування самими компонентами WLAN – це можливість, яку не пропонують багато продуктів. Aruba RFProtect – виняток; він дозволяє, наприклад, заблокувати конфігурації бездротових пристроїв із центральної консолі. Крім того, продукти AirTight WIPS та HP Mobility Security IDS/IPS дозволяють централізовано впроваджувати індивідуальні політики безпеки. Проте більшість організацій вже мають інші засоби для налаштування та моніторингу безпеки своїх бездротових пристроїв, тому в цій конкретній можливості управління пристроями часто немає необхідності.

Критерій №2: виявлення атаки.

Такі програми, як AirTight WIPS, Aruba (тепер HP) RFProtect, Cisco Adaptive Wireless IPS, Fluke Networks AirMagnet Enterprise, HP Mobility Security IDS / IPS і Zebra Technologies AirDefense (від Motorola), мають базові можливості виявлення атак WIPS: виявляти несанкціоновані точки доступу і виявляти несанкціоновані підключення, включаючи неавторизовані клієнтські пристрої та неавторизовані одноранговi мережі. Жодних інших подробиць про те, що Zebra Technologies AirDefense може зробити з точки зору виявлення атак, не відомо, але всі інші продукти пропонують одну або кілька додаткових можливостей, включаючи:

- виявлення атак типу «відмова в обслуговуванні»;

- виявлення атак типу man-in-the-middle та підробки клієнта;

- відображення фізичного розташування пристроїв WLAN, включаючи клієнтські пристрої та точки доступу (як авторизовані, так і несанкціоновані).

Два продукти, Cisco Adaptive Wireless IPS та HP Mobility Security IDS/IPS, також сприяють виявленню спроб активної автентифікації та злому шифрування. Фактично ці два продукти є єдиними проаналізованими продуктами, які підтримують весь спектр можливостей виявлення атак, досліджених за цим критерієм.

Критерій №3: дотримання правил.

Важливо мати можливість виконувати докладні звіти щодо відповідності політикам на WIPS, щоб документувати дотримання різноманітних ініціатив

щодо забезпечення відповідності. Одна організація може бути об’єктом кількох цих ініціатив, тому для цих організацій наявність звітів про відповідність, заздалегідь визначених для кожної ініціативи, може значно заощадити час. Організація також може потребувати звітності про відповідність політиці для інших цілей, таких як внутрішній або зовнішній аудит.

Хоча всі продукти пропонують своєрідні можливості звітності, п’ять спеціально просувають власну підтримку звітності про відповідність нормативним вимогам: Aruba RFProtect, Cisco Adaptive Wireless IPS, Fluke Networks AirMagnet Enterprise, HP Mobility Security IDS/IPS та Zebra Technologies AirDefense.

Критерій №4: захист від атаки.

Кожен продукт WIPS пропонує вбудовані можливості захисту від атак, інакше це була б бездротова система виявлення вторгнень (WIDS), а не WIPS. Проте існують різні методи захисту різних видів атак, і іноді є кілька варіантів для зупинки одного типу атаки. Деякі методи викликають менше незручностей для інших користувачів та пристроїв у порівнянні з іншими методами, але їх легко обійти. Таким чином, залежно від потреб організації в безпеці один метод може бути кращим за інший.

Так само, як немає докладних списків сигнатур атак WLAN, наданих постачальниками WIPS, немає відповідних списків варіантів техніки захисту від атак для зупинення кожного типу атаки WLAN. І навіть якби вони були, знадобилося б багато зусиль, щоб розглянути варіанти та оцінити відносні сильні та слабкі сторони кожного з усіх можливостей WIPS. Більш реалістично запитати постачальників WIPS про основні методи, які вони використовують для зупинення атак, а потім переконатися, що ці методи відповідають вимогам організації.

Ще одне важливе міркування, пов’язане із захистом від атак, – це точність виявлення з погляду хибних спрацьовувань. На відміну від постачальників IPS для провідних мереж та хостів, які часто розрізняють свої продукти, посилаючись

на хибнопозитивні та негативні статистичні дані, постачальники WIPS не надають оцінок цих показників. Організації, зацікавлені у придбанні продуктів WIPS, повинні приділяти особливу увагу їх підтримці для налаштування виявлення атак та відповідей, що має дозволити організації звести до мінімуму помилкові спрацьовування та негативні результати, тим самим полегшуючи блокування атак.

Критерій №5: ціна.

Моделі ціноутворення дуже різняться залежно від продуктів WIPS. Це значною мірою пов’язане з різними архітектурами, що вони використовують. Деякі продукти, такі як Aruba RFProtect, є програмним модулем, який можна встановити та активувати на існуючому обладнанні; у цьому випадку програмне забезпечення ліцензується залежно від кількості точок доступу, що підтримуються. Інші продукти пропонують як варіанти апаратного, так і віртуального пристрою; для цих продуктів може знадобитися придбання ліцензій для кожного датчика, що підтримується. На додаток до цих варіантів, пристрій AirTight WIPS надає хмарні послуги, і модель ціноутворення для них повністю відрізнятиметься від програмних або апаратних реалізацій.

При оцінці систем запобігання вторгненням у бездротові мережі, безумовно, важливо визначити витрати на придбання та встановлення програмного забезпечення сервера керування, консолі та датчика / точки доступу. Однак не слід упускати з уваги витрати на обслуговування. Для будь-якого WIPS потрібен постійний моніторинг, щоб адміністратори могли реагувати на успішні атаки, а часте налаштування сигнатур і правил виявлення атак WIPS також критично важливе для підвищення точності виявлення та мінімізації помилкових спрацьовувань та негативних результатів.

При оцінці систем запобігання вторгненням у бездротові мережі необхідно враховувати багато факторів. Деякі з них, наприклад ціна і продуктивність, сильно різняться для кожної організації в залежності від обраної архітектури WIPS (наприклад, точки доступу з вбудованим WIPS, виділені датчики WIPS),

існуючого характеру інфраструктури WLAN та моделі розгортання WIPS (програмне забезпечення, апаратний пристрій, віртуальний пристрій, хмарний сервіс).

Продукти Cisco Adaptive Wireless IPS та HP Mobility Security IDS/IPS пропонують широкий спектр можливостей виявлення атак високого рівня, включаючи активну автентифікацію та виявлення злому шифрування. Продукти Cisco Adaptive Wireless IPS та Fluke Networks AirMagnet Enterprise надають можливості захоплення пакетів. А продукти Aruba RFProtect, Cisco Adaptive Wireless IPS та Fluke Networks AirMagnet Enterprise пропонують архітектури високої доступності з автоматичним перемиканням при відмові між серверами керування.

Виходячи з цих критеріїв, продукт Cisco Adaptive Wireless IPS має бути ретельно розглянутий будь-якою організацією, яка шукає надійний продукт WIPS. Проте, як правило, він найкраще підходить для великих організацій, тому малим та середнім організаціям слід обов’язково оцінити продукти серії Fluke Networks AirMagnet Enterprise та HP Mobility Security IDS/IPS System. Всі ці три продукти пропонують надійний баланс функцій виявлення атак, можливостей криміналістичної обробки даних, а також можливостей масштабування та високої доступності [25].

Системи виявлення вторгнень і системи запобігання вторгнень йдуть пліч-о-пліч настільки, що й відповідні абревіатури часто змішуються (наприклад, IDS IPS, IDPS тощо).

У той час як системи виявлення вторгнень контролюють мережу щодо активних або неминучих порушень політики безпеки, запобігання вторгненням йде ще далі, щоб запобігти таким порушенням. Отже, не може бути IPS без IDS.

Доступно кілька різновидів систем виявлення вторгнень. Розглянемо чотири найбільш поширені:

1. Мережева система виявлення вторгнень (NIPS, IDS IPS).

2. Аналіз мережевої поведінки (NBA).

3. Система запобігання вторгненням у бездротові мережі (WIPS).

4. Система запобігання вторгненням на основі хоста (HIPS).

1. Мережеві системи запобігання вторгненням (NIPS, IDS IPS).

NIPS виявляє та запобігає шкідливій активності, аналізуючи пакети протоколу по всій мережі. Їх часто називають IDS IPS або системами виявлення та запобігання вторгненням.

Після встановлення NIPS збирає інформацію з консолі хоста та мережі для визначення дозволених хостів, додатків та операційних систем, які зазвичай використовуються в мережі. Вони також реєструють інформацію про характеристики звичайного мережевого трафіку для виявлення будь-яких підозрілих змін у мережі.

NIPS може запобігати атакам різними способами, такими як завершення TCP-з'єднання для запобігання атакі, обмеження використання смуги пропускання або навіть відхилення підозрілої мережної активності. Сьогоднішні NIPS навіть здатні керувати брандмауерами та маршрутизаторами, щоб блокувати підозрілу активність. NIPS зазвичай не аналізує зашифрований мережевий трафік, не обробляє високі навантаження трафіку і обробляє прямі атаки на IDS IPS.

NIPS в першу чергу використовує виявлення загроз на основі сигнатур. Виявлення на основі сигнатур шукає шаблони або сигнатури розпізнаних раніше загроз для виявлення потенційних нових загроз.

AccessEnforcer, міжмережевий екран UTM від Calyptix, включає IDS IPS як частину стандартної служби всім моделей [26].

2. Аналіз мережевої поведінки (NBA).

Датчики та програми NBA досліджують мережевий трафік для виявлення загроз безпеки, які створюють незвичайні потоки трафіку, таких як розподілені атаки типу «відмова в обслуговуванні» (DDoS), певні форми шкідливого програмного забезпечення та порушення політики безпеки. Виявлення NBA в першу чергу включає наступні два методи:

1) виявлення на основі аномалій шукає відхилення від так званої «нормальної» поведінки в системі чи мережевій активності. При запуску виявлення аномалій потрібен період навчання, протягом якого створюється профіль про те, що вважається нормальною поведінкою системи. Невідповідності з цим профілем позначаються як шкідливі.

Виявлення на основі аномалій відмінно підходить для виявлення нових загроз, але можуть виникнути проблеми, якщо мережа буде скомпрометована під час періоду навчання, оскільки шкідлива поведінка може реєструватися як завжди під час створення профілю. Крім того, виявлення на основі аномалій також дає багато помилкових спрацьовувань через доброякісну активність, яка не була виявлена під час початкового періоду навчання.

2) виявлення аналізу протоколу з відстеження стану аналогічно виявленню на основі аномалій в тому, що він шукає відхилення від нормальної поведінки мережі або системи. Базовий рівень нормальної поведінки викладено в універсальних профілях, створених постачальником. Аналіз протоколів з відстеженням стану призначений для розрізнення доброякісної та підозрілої активності в автентифікованому та не автентифікованому станах.

За допомогою NBA пороги підозрілої активності автоматично оновлюються на постійній основі, а також можуть бути встановлені вручну. Система NBA має використовуватися як розширення NIPS чи IDS IPS для забезпечення багаторівневого захисту.

AccessEnforcer, мережевий брандмауер від Calyptix, включає мережевий аналіз протоколів з відстеження стану як частина стандартної послуги, що надається всім клієнтам.

3. Системи запобігання бездротовим вторгненням (WIPS).

WIPS аналізує радіочастотний спектр по всій бездротовій мережі, щоб виявляти вторгнення, порушення мережевої політики та несанкціоноване використання та повідомляти про них. WIPS можна реалізувати трьома основними способами:

1) моніторинг оверлею. Бездротові датчики розміщуються всюди у фізичній області мережі (наприклад, у коридорах, туалеті, стелях), щоб забезпечити підключення до мережі та моніторинг мережі;

2) комплексний моніторинг. Існуючі консолі точок доступу використовуються для забезпечення безпеки та підключення замість бездротових датчиків;

3) гібридний моніторинг. І датчики, і консолі AP використовуються для моніторингу та підключення.

WIPS може збирати інформацію про пристрої, підключені до мережі, і дуже ефективно виявляти і запобігати різноманітним шкідливим подіям, включаючи шахрайські точки доступу, DoS-атаки, несанкціонований доступ, спеціальні мережі, спуфінг та посередництво. Вони навіть можуть припинити з'єднання при виявленні загрози.

Однак накладення та інтегрований моніторинг мають унікальні обмеження, тому сьогодні більшість організацій використовують гібридний WIPS для комплексного моніторингу.

Наприклад, інтегрована консоль моніторингу може бути єдиною точкою відмови і не може сканувати розширені канали, такі як оверлейні монітори. Хоча оверлейні монітори спеціально розроблені з такою можливістю перемикання каналів, вони не ідеальні для постійного моніторингу одного каналу [27].

4. Система запобігання вторгненням на основі хоста (HIPS).

Системи запобігання вторгненням на основі хоста, або HIPS, аналізують активність на одному хості для виявлення та запобігання шкідливій активності. HIPS в першу чергу аналізує поведінку коду, використовуючи методи виявлення на основі сигнатур та аномалій для виявлення підозрілої активності. Їх часто хвалять за запобігання атакам, які використовують шифрування.

HIPS також може запобігти доступу до конфіденційної інформації, розташованої на хості, тим самим запобігаючи будь-якій потенційній шкоді, заподіяній руткітами або троянськими конями. Нарешті, HIPS може запобігти

обробці хост-машиною шкідливої активності у мережі. Оскільки HIPS забезпечує безпеку тільки для одного хост-комп’ютера або сервера, його найкраще використовувати разом з IDS IPS та WIPS, щоб забезпечити повне управління загрозами у всій мережі.

Будь-який брандмауер UTM повинен включати IPS IDS зі стандартним сервісом, поєднуючи його з фільтрацією електронної пошти, веб-фільтрацією, VPN та додатковими функціями для забезпечення безпеки та ефективності мережі [28].

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ТА МЕТОДИК УСУНЕННЯ ВРАЗЛИВОСТЕЙ ТОЧОК ДОСТУПУ ПО КАНАЛУ WI-FI

3.1 Рекомендації зі зміни налаштувань, їх обґрунтування

Бездротові локальні мережі (WLAN) забезпечують неймовірну продуктивність і нову ефективність організаціям будь-якого розміру. Розвиток функцій і можливостей WLAN дозволяє організаціям пропонувати переваги бездротового зв’язку своїм співробітникам, не жертвуючи безпекою. При правильному розгортанні WLAN можуть бути такими ж безпечними, як і дротові мережі.

Нижче запропоновано п’ять кроків до створення безпечної інфраструктури WLAN.

WLAN вийшли на новий новий рівень продуктивності та свободи як всередині організації, так і за її межами. Однак, хоча продуктивність зросла, виникли нові проблеми безпеки. За конструкцією бездротові сигнали поширюються за фізичні межі організації, скасовуючи традиційну безпеку всередині організації. Сигнали із незахищених мереж WLAN, що поширюються за межі корпоративної мережі, можуть бути знайдені та використані неавторизованим персоналом або навіть зловмисними хакерами.

Хоча бездротовий носій має особливі унікальні характеристики, основні заходи безпеки WLAN не дуже відрізняються від тих, які необхідні для створення надійної дротової безпеки, і IT-адміністратори можуть підтримувати корпоративну конфіденційність за допомогою належних заходів безпеки WLAN.

Хоча IT-адміністратори, можливо, вже знають про належні методи захисту самого середовища WLAN, вони можуть бути здивовані, дізнавшись, що однієї лише безпеки WLAN недостатньо для захисту організації.

Найпоширенішою є шахрайська точка доступу, про яку йшла мова у розділі 2 та буде детально розглянута у пункті 3.3. Крім того, стратегія Cisco Self-Defending Network (SDN) захищає від нових загроз безпеці, створених бездротовими технологіями, значно покращуючи здатність мережі автоматично ідентифікувати, запобігати та адаптуватися до загроз безпеки. У рамках цієї стратегії уніфікована бездротова мережа Cisco надає комплексне рішення для захисту мережі від бездротових загроз і забезпечення безпечного приватного зв'язку через авторизовану бездротову локальну мережу. Кожен пристрій у мережі — від клієнтів до точок доступу до бездротових контролерів і системи керування — відіграє певну роль у захисті середовища бездротової мережі за допомогою розподіленого захисту. Через його мобільний характер потрібен багаторівневий підхід до безпеки. Cisco Systems рекомендує наступний п'ятиетапний підхід для зменшення ризиків для мережі від бездротових загроз:

1) створити політику безпеки WLAN;

2) захистити WLAN;

3) захистити дротову (Ethernet) мережу від бездротових загроз;

4) захистити організацію від зовнішніх загроз;

5) залучити працівників до охорони мережі [29].

Створити політику безпеки WLAN. Подібно до політики безпеки, яка існує для дротового доступу, письмова політика бездротової мережі, яка охоплює авторизоване використання та безпеку, є необхідним першим кроком. Як правило, документи політики безпеки включають такі розділи: мета, сфера політики, обов'язки, застосування, визначення, історія переглядів.

Перед створенням політики безпеки необхідно ретельно дослідити – більшість порушень безпеки можна простежити через недогляд або помилки в реалізації політики безпеки.

Забезпечення WLAN. Розгортання WLAN значно зросло за останні роки, розвиваючись від гостьового доступу в конференц-залах, обмежених гарячих зон підключення в організації до повного покриття всієї організації. На жаль, багато з

цих розгортань є небезпечними, що дає можливість цікавим або зловмисним хакерам спробувати отримати доступ до конфіденційної інформації, як вже було з'ясовано у дослідженні. Захист WLAN не складний. Технологічні досягнення в галузі та уніфікована бездротова мережа Cisco, наприклад, роблять це простіше, ніж будь-коли. Захист мережі базується на розширенні стратегії Cisco Self-Defending Network, яка базується на трьох стовпах: безпечний зв'язок, контроль і стримування загроз, а також управління політикою та відповідністю. Зважаючи на ці три аспекти, нижче наведено найкращі методи захисту уніфікованої бездротової мережі Cisco.

- безпечний зв'язок. Захищений зв'язок передбачає як шифрування даних, так і аутентифікацію користувачів у мережі. У бездротовій мережі, подібно до дротової мережі, ці два компоненти не потрібно поєднувати, але для більшості мереж Cisco рекомендує використовувати обидва. Крім того, унікальні характеристики бездротового середовища вимагають застосування інших методів безпеки для захисту мережі;

- змінення SSID за замовчуванням. Точки доступу мають стандартне ім'я мережі, яке передається клієнтам, щоб повідомляти про доступність точки доступу. Необхідно змінити це налаштування відразу після встановлення. При перейменуванні ідентифікатора набору послуг (SSID) точки доступу вибрати щось, що не має прямого відношення до користувача; не вибирати назву компанії, ПІБ, номер телефону чи іншу доступну інформацію, яку легко вгадати чи знайти в Інтернеті. За замовчуванням точки доступу передають SSID будь-якому бездротовому клієнту в межах досяжності. Для деяких програм, таких як точки доступу або гостьовий доступ, ця можливість дозволяє користувачам знаходити мережу без сторонньої допомоги. Однак для корпоративних чи домашніх мереж слід вимкнути трансляцію, щоб обмежити тих, хто випадково шукає відкриту бездротову мережу. Уніфікована бездротова мережа Cisco забезпечує доступ до всіх клієнтів протягом заданої оператором кількості спроб. Якщо клієнту не вдається отримати доступ у межах цього ліміту, він автоматично виключається

(блокується від доступу), доки не закінчиться встановлений оператором таймер. Операційна система також може вимкнути трансляцію SSID для кожної мережі WLAN, що ще більше зменшує частоту випадкових перевірок;

- використання сильного шифрування. Однією з найбільших перешкод для розгортання WLAN було шифрування еквівалентної конфіденційності бездротової мережі (WEP), яке є слабким автономним методом шифрування. Крім того, складність додаткових рішень безпеки завадила багатьом IT-менеджерам скористатися перевагами останніх досягнень у безпеці WLAN. Уніфікована бездротова мережа Cisco об'єднує компоненти безпеки в простий менеджер політик, який налаштовує політику безпеки в системі для кожної мережі. Щоб забезпечити зручне підключення клієнта, точки доступу, як правило, не налаштовуються виробником для шифрування по повітрю. Після розгортання цей крок легко забути, але це найпоширеніший спосіб злому або використання мереж WLAN неавторизованими користувачами. Тому слід налаштувати метод захисту по повітрю відразу після розгортання. Cisco рекомендує використовувати найбезпечніше шифрування по повітрю — IEEE 802.11i або VPN. IEEE 802.11i, також відомий як Wi-Fi Protected Access 2 (WPA2), коли точка доступу, сертифікована Wi-Fi Alliance, використовує розширений стандарт шифрування (AES) для шифрування даних. AES є найвищим стандартом шифрування на даний момент і замінює WEP. Необхідно використовувати WPA2 з AES, коли це можливо або WPA3. Його попередник, WPA, є тимчасовою формою безпеки, сертифікованою Wi-Fi Alliance, поки стандарт 802.11i ще не був ратифікований. Стандарт 802.11i, WPA3 і WPA2 вимагають використання сервера RADIUS для надання кожному клієнту унікальних ключів шифрування. Уніфікована бездротова мережа Cisco взаємодіє із сервером керування безпечним доступом Cisco (ACS), а також із серверами RADIUS, сумісними з 802.11i та WPA інших виробників. Крім того, на відміну від інших клієнтів, де може знадобитися програмне забезпечення сторонніх виробників, щоб увімкнути можливості IEEE 802.11i, клієнти Cisco готові до підключення в безпечному режимі WPA3 або

WPA2 до інфраструктури об’єднаної бездротової мережі Cisco. Важливо зазначити, що для персональної версії WPA2 і WPA3 не потрібен сервер RADIUS. Таким чином, рекомендовано для реалізацій безпечного будинку або малого офісу/домашнього офісу (SOHO) програму Cisco Compatible Extensions, що допомагає забезпечити взаємодію широкого спектру клієнтських пристроїв WLAN з інноваційними функціями продуктів інфраструктури Cisco WLAN та їх підтримку. В результаті IT-менеджери можуть впевнено розгортати WLAN, навіть якщо ці WLAN обслуговують багато типів клієнтських пристроїв.

Cisco Compatible Extensions — це важлива ініціатива, яка дозволяє забезпечити наскрізну продуктивність, керування радіочастотами, якість обслуговування (QoS) та можливості безпеки, необхідні в бездротовій мережі. Кілька основних покращень безпеки, доступних через програму, включають режими аутентифікації Cisco LEAP, захищений протокол розширеної аутентифікації (PEAP) і гнучку автентифікацію за допомогою розширеного протоколу аутентифікації через безпечне тунелювання (EAP-FAST), а також безпечний швидкий роумінг із кешуванням ключів. для програм, чутливих до затримок, таких як голос через WLAN. Деякі з цих функцій були прийняті органами стандартизації з часом, і Cisco надала їх після ратифікації.

Оскільки можливості клієнта є невід’ємною частиною загальної безпеки мережі, Cisco і Intel тісно співпрацюють у рамках програми Cisco Compatible Extensions. Intel, стратегічний партнер альянсу, отримав статус Cisco Compatibility для своєї технології Centrino Mobile, яка доступна в багатьох ноутбуках. Основні постачальники ноутбуків, включаючи Acer, Dell, Fujitsu, IBM, HP і Toshiba, надають ноутбуки, сумісні з Cisco.

VPN є наступним найкращим рішенням для захисту від повітряного клієнтського підключення. VPN у поєднанні з сегментацією мережі з використанням кількох SSID і VLAN забезпечує надійне рішення для мереж з різними клієнтами. VPN-сервіси IP Security (IPSec) і Secure Sockets Layer (SSL) забезпечують такий же рівень безпеки, як 802.11i. Контролери бездротової

локальної мережі Cisco припиняють роботу тунелів IPSec VPN, усуваючи потенційні вузькі місця централізованих серверів VPN. Крім того, уніфікована бездротова мережа Cisco підтримує прозорий роумінг через підмережі, тому програми, чутливі до затримок, такі як бездротова передача голосу через IP (VoIP) або Citrix, не втрачатимуть підключення під час роумінгу через довгі затримки.

Якщо жоден з цих методів неможливий, слід налаштувати WEP. Хоча широко відомо, що WEP легко скомпрометувати інструментами, доступними в Інтернеті, він, принаймні, є стримуючим фактором для випадкових шпигунів. У поєднанні з сегментацією користувачів на основі VLAN, WEP значно зменшує ризик безпеки. Рішення Cisco WLAN також підтримує локальну та RADIUS фільтрацію MAC, що найкраще підходить для невеликих груп клієнтів із відомим списком MAC-адрес карт доступу 802.11. При використанні цього методу слід негайно розробити план встановлення більш сильної форми безпеки. Незалежно від вибраного рішення безпеки бездротового зв’язку, усі дротові комунікації рівня 2 між контролерами бездротової локальної мережі Cisco і точками доступу Cisco Aironet, що працюють за протоколом Lightweight Access Point Protocol (LWAPP), захищаються шляхом передачі даних через тунелі LWAPP. І як додатковий захід безпеки, вимкнення також використовується для автоматичного блокування доступу до рівня 2 після встановленої оператором кількості невдалих спроб автентифікації. Рекомендовано використовувати функцію ідентифікації мережі для сегментації користувачів на відповідні ресурси. Багато різних типів користувачів повинні отримати доступ до мережі WLAN. Адміністратори замовлень вимагають доступу до систем введення замовлень та доставки; працівникам бухгалтерії та фінансів необхідний доступ до рахунків, а також до інших фінансових систем; а відділам маркетингу та продажів може знадобитися доступ до даних про результати продажів. Уніфікована бездротова мережа Cisco підтримує мережу ідентифікаційних даних — концепцію, за якою політики WLAN призначаються та застосовуються на основі ідентифікації бездротового клієнта, а не його фізичного розташування. При встановленні ідентифікаційної

мережі бездротові пристрої повинні пройти автентифікацію лише один раз у системі WLAN. Контекстна інформація слідує за пристроями, коли вони переміщуються, допомагаючи забезпечити прозору мобільність. Коли WLAN пов’язана з певною VLAN, користувач може отримати доступ до мережевих ресурсів лише в цій VLAN [29].

Багато корпорацій використовують сканери штрих-кодів для відстеження запасів під час доставки та отримання, або використовують мобільні принтери на виробничих цехах. Вищенаведене налаштування разом із частими змінами ключа шифрування та контрольними списками MAC-адрес зменшує потенційні ризики безпеки.

Нарешті, багато організацій зацікавлені в тому, щоб допомогти гостям, партнерам і клієнтам отримати доступ до Інтернету. Бездротова гостьова мережа – це простий спосіб надати доступ, усуваючи потребу для IT-персоналу авторизувати окремих користувачів. Гостьові мережі використовують відкритий метод безпеки, розділений за певним SSID, який направляє трафік до VLAN, яка має доступ лише до загальнодоступного Інтернету.

У цьому випадку SSID зазвичай транслюється, тому гості можуть знайти його без сторонньої допомоги. Вхід користувача можна здійснити через веб-сторінку приєднаного порталу, щоб перевіряти використання та погодитися з будь-якими умовами, перш ніж гість скористається послугою.

У такому випадку доцільно переконатися, що порти керування захищені. Інтерфейси керування системою WLAN повинні підтримувати безпечні, аутентифіковані методи керування. Переналаштування точки доступу через порт керування — це один із методів, який хакер може використовувати для доступу до корпоративної мережі. Уніфікована бездротова мережа Cisco підтримує інтерфейси Simple Network Management Protocol версії 3 (SNMPv3), Secure Shell (SSH) (захищений Інтернет) і SSL (захищений Telnet) до системи бездротового керування Cisco (WCS). Крім того, Cisco WCS можна налаштувати таким чином, що керування неможливе по повітрю, і він підтримує окреме VLAN керування,

тому лише станції в певній VLAN можуть змінювати налаштування мережі WLAN.

Легкі точки доступу Cisco не зберігають шифрування чи іншу інформацію безпеки локально, тому мережу не можна скомпрометувати, якщо точку доступу вкрадено. Крім того, всі точки доступу автоматично аутентифікуються, що запобігає додаванню неавторизованих точок доступу до мережі.

Рекомендується захистити точки доступу від несанкціонованого доступу, щоб запобігти незапланованим змінам радіочастотного покриття. Оскільки сигнали точки доступу виходять за межі периметра більшості будівель, хтось може підключитися всередині, сидячи на автостоянці або через дорогу. Якщо охоронні патрулі або відеоспостереження вже використовуються, персонал служби безпеки повинен бути попереджений про транспортні засоби або людей, які, здається, блукають поблизу об’єкта протягом тривалого періоду часу.

Уніфікована бездротова мережа Cisco використовує запатентовані алгоритми управління радіоресурсами Cisco (RRM), які виявляють і адаптуються до змін повітряного простору в реальному часі. Можна використовувати Cisco RRM, щоб зменшити поширення радіочастот за межами фізичного периметра будівлі.

Забезпечення мережі від загроз бездротової лінії. Ініціативою Cisco Self-Defending Network є контроль і стримування загроз, що стосується як бездротової, так і дротової мережі. Як і в інших політиках безпеки, простого попередження співробітників про загрози зазвичай недостатньо. Хорошим прикладом є антивірусна політика не відкривати вкладення електронної пошти від невідомих відправників. Більшість організацій не можуть покладатися лише на це застереження — навіть одна помилка може завдати значної шкоди мережі, що спричинить значні простої та втрату продуктивності. Аналогічно, контроль і стримування бездротових загроз є життєво важливими, особливо в епоху, коли відсутність контролю загроз може призвести до порушень регуляторних заходів або законодавчих актів. Навіть політика «без Wi-Fi» не є гарантією безпеки від

цих загроз. Співробітники можуть вводити несанкціоновані точки доступу, а ноутбуки можуть підключатися до сусідніх мереж. Обидві вразливості такі ж реальні, як віруси, хробаки та спам. Традиційні дротові методи безпеки, такі як брандмауери та VPN, не виявляють ці типи загроз, оскільки вони виникають по повітрю, але об'єднана бездротова мережа Cisco розроблена для активного моніторингу та запобігання таких випадків. У об'єднаній бездротовій мережі Cisco точки доступу одночасно діють як повітряні монітори та пристрої пересилання даних. Це налаштування дозволяє точкам доступу передавати інформацію про бездротовий зв'язок у режимі реального часу домену, включаючи потенційні загрози безпеці для контролерів бездротової локальної мережі Cisco, без переривання служби. Усі загрози безпеці швидко ідентифікуються та представляються адміністраторам мережі через Cisco WCS, де можна проводити точний аналіз та вживати заходів щодо їх усунення.

Cisco Systems надає єдину систему WLAN, яка пропонує одночасний захист бездротової мережі та надання послуг WLAN, допомагаючи забезпечити повний захист WLAN без зайвих витрат на обладнання або додаткові пристрої моніторингу. Назавжди видаліть шахрайський пристрій із відстеженням місцезнаходження. Щоб гарантувати, що бездротова загроза назавжди усунена, необхідно фізично видалити шахрайський пристрій. Традиційно портативні аналізатори використовувалися в загальній області, де було виявлено шахрайський пристрій. Однак, оскільки бездротове розповсюдження може поширюватися досить далеко, це рішення може зайняти багато часу, особливо для багатоповерхових об'єктів.

Рішення Cisco Location Appliance з Cisco WCS може точно відстежувати до 1500 пристроїв із підтримкою Wi-Fi, таких як мітки радіочастотної ідентифікації (RFID), голосовий зв'язок через Wi-Fi телефони, ноутбуки та персональні цифрові помічники (КПК).

Захистит від зовнішніх загроз. Мережа повинна бути захищена від загроз безпеці, таких як віруси, хробаки та шпигунські програми, поки мобільні пристрої

знаходяться далеко від офісу. Ці загрози безпеці заважають бізнесу, спричиняючи простої та постійні виправлення. Керування політикою та відповідністю є останньою опорою стратегії Cisco Self-Defending Network для проактивного моніторингу та карантину зловмисного програмного забезпечення для підтримки цілісності мережі. Програма відповідності має включати моніторинг, щоб знати, коли системні та мережеві політики порушуються. Без цього IT-адміністратори не можуть знати, чи дотримуються їх політики безпеки. Управління політикою та відповідністю надає такі ж послуги безпеки для мобільного пристрою, що й мережа компанії. Зокрема, ноутбук потребує такого ж захисту, що й мережа компанії. Брандмауери, VPN та антивірусне програмне забезпечення допомагають захистити його від багатьох загроз, з якими ці пристрої стикаються під час підключення до Інтернету. Такі інструменти, як Cisco Security Agent, об'єднують в одному агенті функції безпеки кінцевої точки, такі як брандмауер, запобігання вторгненням, захист від шпигунського та рекламного програмного забезпечення та багато іншого. Тому що Cisco Security Agent швидше аналізує поведінку ніж покладається на відповідність сигнатур, його ніколи не потрібно оновлювати, щоб зупинити нову атаку. Ця архітектура «нульового оновлення» забезпечує захист зі зниженими експлуатаційними витратами і може ідентифікувати загрози «нульовий день». По суті, Cisco Security Agent дозволяє організаціям застосовувати політику безпеки на окремих кінцевих точках.

Як і мережа компанії, аутентифікація користувачів для контролю доступу та шифрування даних може значно посилити заходи безпеки. Аутентифікацію користувача можна виконувати за допомогою паролів, USB-токенів або смарт-карт. Хоча в цілому ці методи ефективні, вони не завадять тому, хто видаляє жорсткий диск, щоб отримати доступ до конфіденційних даних. На цьому етапі слід розглянути питання шифрування, але щоб шифрування працювало, воно повинно бути автоматичним і прозорим для користувача. Якщо користувач повинен увімкнути його для певних файлів, воно, швидше за все, не буде ефективним через людську помилку. Заражені або вразливі кінцеві точки мають

бути автоматично виявлені, ізольовані та очищені. Network Admission Control (NAC) — це набір технологій і рішень, створених на основі галузевої ініціативи, очолюваної Cisco Systems. NAC використовує мережеву інфраструктуру для забезпечення дотримання політики безпеки на всіх пристроях, які прагнуть отримати доступ до мережевих обчислювальних ресурсів, тим самим обмежуючи шкоду від нових загроз безпеки, таких як віруси, хробаки та шпигунські програми. Клієнти, які використовують NAC, можуть дозволити доступ до мережі лише сумісним і надійним кінцевим пристроям і можуть обмежити доступ несумісних пристроїв. NAC є важливою частиною самозахистуючої мережі Cisco.

Cisco пропонує підходи до NAC як на основі пристроїв, так і на основі архітектури, які відповідають функціональним та оперативним потребам будь-якої організації, незалежно від того, чи має вона просту вимогу політики безпеки, чи вимагає підтримки для комплексної реалізації безпеки за участю численних постачальників безпеки в поєднанні з корпоративним керуванням робочим столом. Рішення Cisco NAC Appliance (Cisco Clean Access), так і Cisco NAC Framework забезпечують захист від загроз безпеки для WLAN. Ці рішення забезпечують дотримання політики безпеки пристроїв, коли клієнти WLAN намагаються отримати доступ до мережі, шляхом поміщення в карантин невідповідних клієнтів WLAN та надання послуг з відновлення для забезпечення відповідності. Обидва рішення повністю сумісні з уніфікованою бездротовою мережею Cisco. Архітектура пристрою Cisco NAC для уніфікованої бездротової мережі Cisco зображена на рис. 3.1.

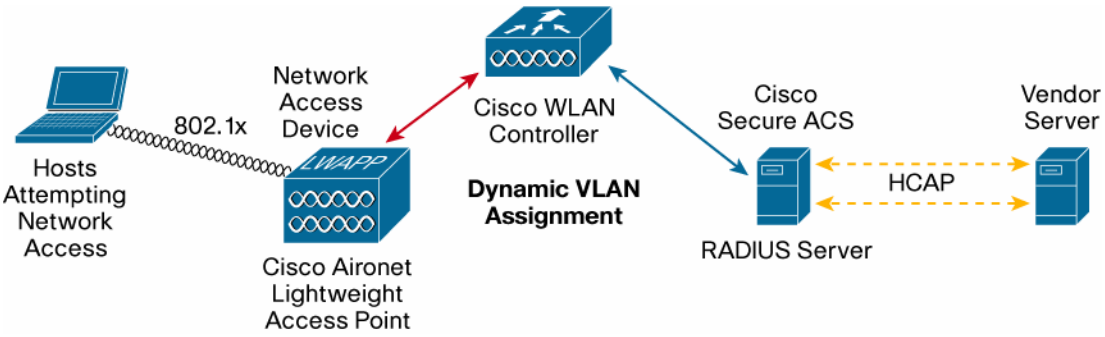

Рисунок 3.1 – Архітектура пристрою Cisco NAC

Соціальна інженерія часто є найефективнішим інструментом для захисту мережі. Більшість співробітників просто не усвідомлюють ризиків без освіти — наприклад, більшість людей не усвідомлює, що простий акт підключення точки доступу до роз'єму Ethernet загрожує безпеці корпоративної мережі. Навчання співробітників — інформаційні плакати або тренінги з найкращих методів безпеки (наприклад, вибір пароля та конфіденційність) — виявилося ефективним у допомозі компаніям зберігати конфіденційну інформацію та мережу в безпеці.

Уніфіковану бездротову мережу Cisco спочатку можна безпечно розгорнути як бездротове рішення IPS, а потім перетворити на службу WLAN [29].

Якщо всі ці кроки будуть використані, компанія значно зменшить ризики для WLAN та бездротових загроз.

Отже, рекомендовано:

1) створити політику безпеки WLAN;

2) захистити WLAN:

- змінити стандартний SSID;

- використовувати надійне шифрування;

- розгорнути взаємну аутентифікацію між клієнтом і мережею;

- використовувати VPN або WEP у поєднанні зі списками керування MAC-адресами для захисту пристроїв;

- використовувати мережу ідентифікації в поєднанні з VLAN, щоб обмежити доступ до мережевих ресурсів;

- переконатися, що порти керування захищені;

- розгортати легкі точки доступу, оскільки вони не зберігають інформацію безпеки локально;

- фізично приховати або захистити точки доступу, щоб запобігти несанкціонованому доступу;

- відстежувати зовнішню будівлю та сайт на предмет підозрілої діяльності;

3) захистити мережу від бездротових загроз:

- розгорнути та ввімкнути бездротові IPS, щоб запобігти шахрайським точкам доступу та іншим бездротовим загрозам;

- назавжди видалити будь-які шахрайські пристрої за допомогою відстеження розташування;

4) захиститися від зовнішніх загроз:

- обладнати мобільні пристрої такими ж службами безпеки, як мережа компанії або домашня мережа (брандмауери, VPN, антивірусне програмне забезпечення);

- переконатися, що політика безпеки мобільних пристроїв відповідає вимогам NAC;

5) залучити користувачів до захисту мережі через навчання.

3.2 Рекомендації щодо відбиття різних типів атак різними способами

Для запобігання можливим атакам на безпровідну мережу по каналу Wi-Fi, важливо усвідомити, що для відбиття та попередження різних видів атак необхідні різні заходи та ПО. Проте, дослідженням виявлено, що існують і універсальні програми, які можуть допомогти при більшості можливих атак.

Важливо зазначити, що жодна система не на 100% вільна від уразливостей або захищена від хакерів. Якщо зловмисник має достатньо часу, ресурсів і робочої сили для початку атаки, швидше за все, він знайде вихід.

Мережеві атаки – це будь-які спроби використовувати вразливість або слабке місце в мережі або її системах, включаючи сервери, брандмауери, комп’ютери, маршрутизатори, комутатори, принтери. Метою атаки може бути крадіжка, зміна або видалення доступу до цінних даних. Або це може бути відключення мережі.

Типи атак на безпеку мережі включають: відмову в обслуговуванні (DoS), розподілену відмову в обслуговуванні (DDoS), атаки переповнення буфера, пінг-атаки, SYN флуд, посилення DNS, чорний хід, спуфінг, смурф атаки, злом TCP/IP, атаки людина в центрі; відтворення атак, отруєння DNS, отруєння ARP, кайтінг домену, typosquatting, атаки на стороні клієнта, атаки на водопій, атаки нульового дня [30]. Більшість з даних атак розглядалися у дослідженні у першому та другому розділах.

1) при атаці типу «відмова в обслуговуванні» (DoS) зловмисник перевантажує сервер даними, перешкоджаючи надходженню дійсного запиту від реальних клієнтів у мережі. DoS-атака також може виконуватися у всій мережі, оскільки атака націлена на центральний маршрутизатор або міжмережевий екран. В результаті пропускна спроможність мережі скомпрометована, що забороняє доступ до всіх систем цієї мережі, а не тільки до однієї.

Для запобігання даній атаці доречно:

- купити більшу пропускну спроможність;
- створити надмірність у інфраструктурі;
- розгорнути апаратні та програмні модулі Anti-DoS;
- розгорнути захист від DoS;
- захистити сервери DNS.

2) при протидії розподіленій атаці типу «відмова в обслуговуванні» (DDoS) можна вжити наступних заходів:

- розробити план реагування на відмову у обслуговуванні;
- забезпечити безпеку мережної інфраструктури;
- фільтрувати маршрутизатори на краю мережі для виявлення та видалення DDoS-з’єднань;
- блокувати сайт, на який проводиться DDoS-атака, тим самим спрямовуючи весь трафік на недійсну адресу.

3) при атаці переповнення буфера програма отримує більше вхідних даних, ніж очікує. В результаті помилка наражає системну пам’ять на шкідливу загрозу.

Хоча переповнення буфера саме собою не завдає шкоди, воно виявляє вразливість. Потім зловмисники можуть отримати доступ до ділянок пам’яті за межами буфера програми, що дозволяє їм записувати шкідливий код у цю область пам’яті. Під час запуску програми запускається шкідливий код.

Можна запобігти атаці переповнення буфера:

- виконувати рутинний аудит коду (автоматизованого або ручного);

- забезпечти навчання, включаючи перевірку кордонів, використання небезпечних функцій та групових стандартів;

- використовувати інструменти компілятора, такі як StackShield, StackGuard та Libsafe;

- використовувати безпечні функції, такі як strncat замість strcat, strncpy замість strcpy;

- регулярно оновлювати веб-сервери та сервери програм та проглядати звіти про помилки, пов’язані з програмами, від яких залежить код;

- періодично сканувати програму за допомогою одного або декількох широко доступних сканерів, які шукають помилки переповнення буфера у серверних продуктах та користувацьких веб-додатках.

4) ping-атака – атака, призначена для придушення або переповнення цільового пристрою за допомогою exo-запитів ICMP (Internet Control Message Protocol). У звичайних ситуаціях exo-запит використовується для перевірки зв’язку між джерелом і цільовим пристроєм за допомогою exo-запитів ICMP і повідомлень exo-відповіді.

З іншого боку, Ping Attack навмисно затоплює цільовий пристрій пакетами запитів. Пристрій призначення змушений відповідати рівною кількістю пакетів у відповідь і в кінцевому підсумку не може впоратися з обсягом запитів. Це призводить до того, що ціль стає недоступною для звичайного трафіку і не відповідає на звичайні запити ping.

Запобігти атаці Ping можна наступним чином:

- налаштування брандмауера для блокування доступу ICMP-запитів до мережі по периметру;

- додавання фільтрів, які повідомляють маршрутизатору, що потрібно виявляти та відкидати спотворені пакети даних або ті, що надходять із підозрілих джерел;

- пошук підроблених пакетів, що не виходять з мережі, що також відомо як вихідна фільтрація;

- встановлення програмного забезпечення для моніторингу мережі, щоб попередити про незвичайні моделі трафіку;

- регулярне сканування мережі на предмет відкритих портів, що виходять за рамки базового рівня.

5) При SYN флуді, серверу доводиться витрачати ресурси очікування напіввідкритих з’єднань, які можуть споживати достатньо ресурсів, щоб система перестала відповідати на законний трафік. SYN-флуд – це форма атаки типу «відмова в обслуговуванні».

Заходи протидії SYN флуд:

- налаштування IPS для виявлення аномальних шаблонів трафіку;

- налаштування локального брандмауера для визначення порогових значень SYN-атак та захисту від SYN-флуду;

- встановлення сучасного мережевого обладнання з можливістю обмеження швидкості;

- установка комерційних інструментів для забезпечення видимості у всій мережі з можливістю бачити і аналізувати трафік з частин мережі.

6) атака з посиленням сервера доменних імен (DNS) – це популярна форма розподіленої відмови в обслуговуванні (DDoS), коли зловмисники використовують загальнодоступні відкриті DNS-сервери для повені цільової системи трафіком відповідей DNS.

Основний метод полягає в тому, що зловмисник відправляє запит пошуку DNS-імені на відкритий DNS-сервер із підміненою адресою джерела, що є адресою мети.

Запобігання атакам DNS Amplification:

- реалізація перевірки вихідної IP-адреси на мережному пристрої;

- вимкнення рекурсії на авторитетних серверах імен;

- обмеження рекурсії для авторизованих клієнтів;

- впровадження налаштування обмеження швидкості відповіді (RRL) на DNS-сервері.

7) бекдор (чорний хід) – тип шкідливого програмного забезпечення, яке скасовує звичайні процедури автентифікації для доступу до системи. В результаті віддалений доступ надається до ресурсів у додатку, таких як бази даних та файлові сервери, що дає зловмисникам можливість віддалено виконувати системні команди та оновлювати зловмисне програмне забезпечення.

Встановлення бекдору досягається за рахунок використання вразливих компонентів у веб-програмі. Після встановлення виявлення утруднено, оскільки файли мають тенденцію бути дуже заплутаними.

Можна запобігти атакам через чорний хід:

- використовуючи антивірусне програмне забезпечення;

- використовуючи інструменти моніторингу мережі;

- використовуючи рішення для виявлення ненадійного програмного забезпечення на кінцевих точках;

- забезпечуючи захист кожного пристрою брандмауером хоста.

8) спуфінг-атака – атака із заміною, відбувається, коли зловмисник видає себе за інший пристрій або користувача в мережі, щоб запустити атаки на мережні вузли, вкрасти дані, поширити зловмисне програмне забезпечення або обійти засоби контролю доступу.

Існує кілька різних типів атак спуфінгу, які зловмисники можуть використати для цього. Деякі з найбільш поширених методів включають атаки з заміною IP-адреси, атаки з заміною ARP і атаки з заміною DNS-сервера.

Запобігти атаці спуфінгу можна таким чином:

- використовуючи пакетну фільтрацію;

- уникати довірчих відносин із невідомими об’єктами;

- використовуючи програмне забезпечення для виявлення спуфінгу;

- увімкнути криптографічні мережеві протоколи, такі як Transport Layer Security (TLS), Secure Shell (SSH), HTTP Secure (HTTPS).

9) атака Smurf – це форма DDoS-атаки, яка викликає повінь пакетів на жертву шляхом використання / зловживання протоколом ICMP. При розгортанні великі пакети створюються з допомогою методу, званого «спуфінг». Smurf-атаки – стара техніка, але вона залишається актуальною через популярність розгортання та необхідну тактику превентивного запобігання.

Запобігти атаці смурфів:

- блокуючи спрямований широкомовний трафік, що надходить до мережі;

- налаштувавши хости та маршрутизатори так, щоб вони не відповідали на exo запити ICMP;

- розгонувши вбудовану або очищувальну технологію запобігання DDoS-атакам;

- використовувати вхідну фільтрацію для перевірки всіх вхідних пакетів.

10) злом TCP – це кібератака, при якій авторизований користувач отримує доступ до законного з’єднання іншого клієнта у мережі. Захопивши сеанс TCP/IP, зловмисник може читати і змінювати пакети даних, що передаються, а також відправляти свої запити адресату.

Методи протидії захопленню TCP/IP:

- використання SSL під час автентифікації користувачів або виконання конфіденційних операцій;

- повторне створення ідентифікатора сеансу при зміні рівня безпеки (наприклад, під час входу до системи);

- реалізація тайм-аутів сеансу;

- зберігати дані автентифікації на сервері та не надсилати такі дані, як ім’я користувача, cookie;

- блокування доступу до сеансів у файловій системі або використання налоштовуваної обробки сеансів.

11) атака Man-in-the-Middle (MitM) – коли зловмисник перехоплює повідомлення між двома сторонами, щоб таємно перехопити чи змінити трафік між ними. Зловмисники можуть використовувати атаки MitM для крадіжки облікових даних або особистої інформації, стеження за жертвою, саботажу зв’язку або пошкодження даних.

Можна запобігти атаці MITM таким чином:

- включення останньої версії протоколів шифрування, таких як TLS 1.3, до активів інфраструктури;

- навчати персонал, щоб вони не використовували відкриті загальнодоступні мережі Wi-Fi або пропозиції Wi-Fi у громадських місцях, де це можливо;

- навчання персоналу розпізнавання попереджень браузера з сайтів або підключень, які можуть бути незаконними;

- використання VPN для забезпечення безпечних підключень;

- реалізація багатофакторної автентифікації.

12) атака повторного відтворення відбувається, коли кіберзлочинець підслуховує захищене мережне з’єднання, перехоплює його, а потім шахрайським чином затримує або повторно відправляє його, щоб змусити одержувача зробити те, що хоче хакер.

Можна запобігти повторній атаці:

- створити унікальні та випадкові ключі сеансу зв’язку між відправником та одержувачем;

- використати тимчасові позначки цифрових підписів у всіх повідомленнях;

- забезпечити пароль для кожної транзакції, яка використовується лише один раз і відкидається;

- реалізувати заборони дублювання повідомлень;

13) отруєння DNS (також відоме як отруєння кеша DNS або підміна DNS) – тип атаки, який використовує проломи в безпеці протоколу системи доменних імен (DNS) для перенаправлення інтернет-трафіку на шкідливі веб-сайти.

Запобігти зараженню DNS можливо якщо:

- увімкнути DNSSEC на внутрішніх серверах DNS;

- не дозволяти корпоративним DNS-серверам відповідати на DNS-запити в Інтернеті;

- звертати увагу на відповіді DNS;

- вимкнути дозволи файлів хоста на клієнтах та серверах;

- використовувати DNS-сервери пересилання лише для перевірених DNS-серверів.

14) отруєння ARP (також відоме як ARP Spoofing) – це тип кібератаки, що здійснюється через локальну мережу (LAN), яка включає відправлення шкідливих пакетів ARP на стандартний шлюз в локальній мережі, щоб змінити пари в його IP-адресі на MAC. Атака полягає в тому, що зловмисник відправляє хибне повідомлення у відповідь ARP на мережевий шлюз за замовчуванням, інформуючи його про те, що його або її MAC-адреса повинна бути пов’язана з IP-адресою його або її мети (і навпаки, тому MAC-адреса його або її мети тепер пов’язана з IP-адресою зловмисника) [30].

Можна запобігти отруєнню ARP такими способами:

- використання статичних записів ARP;

- реалізація шифрування веб-трафіку;

- використання VPN;

- увімкнення мережевого брандмауера для фільтрації та блокування шкідливих пакетів.

15) комплектування доменів – це практика багаторазової реєстрації та видалення доменного імені, щоб реєстрант міг фактично володіти доменним ім’ям, не сплачуючи за нього. Основна причина кайтінг домену – це додатковий заробіток на рекламі та маркетингових методах, при цьому не потрібно платити за домен.

Можна запобігти кайтинг домену таким чином:

- бути в курсі законодавства ICANN;

- купувати доменні імена лише у надійних постачальників веб-хостингу;

- використовувати технології веб-фільтрації для виявлення припаркованих доменів;

- використовувати веб-технології у браузері для визначення репутації веб-сайту.

16) typosquatting, також відомий як перехоплення URL-адрес, є формою кіберсквоттингу (сидіння на сайтах під чиїмось брендом або авторським правом), націлений на користувачів Інтернету, які неправильно вводять адресу веб-сайту у своєму веб-браузері.

Можна запобігти атакам typosquatting такими способами:

- зареєструвати торгову марка домену;

- купити всі пов’язані URL-адреси, які можуть бути легко написані з помилками;

- надсилати користувачів на офіційний сайт зі сторонніх сайтів;

- використовувати інструмент з відкритим вихідним кодом, такий як DNS Twist, для автоматичного сканування домену компанії щодо будь-яких поточних атак типу сквоттингу.

17) атаки на стороні клієнта вимагають взаємодії з користувачем, який зазвичай ініціюється з веб-браузера на веб-сайт. Тактика, яка використовується для запуску атаки, зрозуміла для кінцевого користувача, наприклад, спонукати його клацнути посилання, відкрити документ або завантажити шкідливий контент.

Можна запобігти атакам на стороні клієнта такими способами:

- визначення дозволів для затверджених сторонніх постачальників, яким можна дозволити доступ до даних або заблокувати від отримання будь-яких конкретних типів даних;

- аудит нових скриптів;

- забезпечення очищення даних і перевірки введення;

- комплексна звітність про відвідуваність сайту та активність користувачів у режимі реального часу для виявлення будь-яких підозрілих шаблонів або мережевих запитів.

18) атака водопою – це цілеспрямована атака, кінцева мета якої – заразити комп'ютер користувача та отримати доступ до мережі організації. Атаки Watering Hole, також відомі як атаки зі стратегічним зломом веб-сайтів, мають обмежений обсяг, оскільки вони покладаються на елемент успіху. Проте вони стають більш ефективними у поєднанні із запрошеннями електронною поштою для залучення користувачів на веб-сайти.

Можна запобігти нападу наступним чином:

- встановлення веб-шлюзів для захисту підприємства від випадкових завантажень;

- використання рішення для захисту електронної пошти, яке фільтрує вихідну та вхідну електронну пошту;

- створення та забезпечення дотримання програми навчання з питань безпеки;

- здійснення динамічного аналізу шкідливих програм.

19) атаки нульового дня. Якщо хакеру вдається скористатися вразливістю до того, як розробники програмного забезпечення зможуть знайти виправлення, цей експлойт стане відомим як атака нульового дня. Вразливості нульового дня можуть набувати практично будь-якої форми, тому що вони можуть виявлятися як будь-який тип ширшої вразливості програмного забезпечення. Наприклад, вони можуть набувати форми відсутнього шифрування даних, SQL-ін'єкції,

переповнення буфера, відсутності авторизації, непрацюючих алгоритмів, перенаправлення URL-адрес, помилок або проблем з безпекою паролів [30].

Можна запобігти атакам нульового дня такими способами:

- бути в курсі, приєднуючись до списків загроз від авторитетних організацій безпеки;

- використовувати WAF (брандмауер веб-додатків) для відстеження вхідного трафіку;

- оновлювати системи до останніх програмних та апаратних виправлень;

- моніторити вхідний та вихідний трафік щодо шкідливого трафіку;

- використовувати IPS-рішення.

20) еманація даних – форма атаки, коли дані компрометуються шляхом отримання аналогового виведення від пристрою і передачі побічного продукту на інший ресурс. Джерелом атаки може бути звук клацання клавіатури, світло світлодіодів та відбите світло.

Можна запобігти атакам, пов’язаним з передачею даних:

- не розміщувати точки доступу біля зовнішніх стін;

- проводити обстеження майданчика для визначення зони покриття та оптимального розміщення точок бездротового доступу для запобігання виходу сигналів за встановлені межі;

- реалізовувати клітину Фарадея для зменшення емісії даних;

- шифрувати всіх дані, що передаються через точку доступу;

- використовувати брандмауери на кожній точці доступу до мережі;

21) джемінг – це тип атаки типу «відмова в обслуговуванні» (DoS), націлений на бездротові мережі. Атака відбувається, коли радіочастоти заважають роботі бездротової мережі. Зазвичай глушення не є зловмисним і викликано наявністю інших бездротових пристроїв, що працюють на тій самій частоті, що і бездротова мережа.

Можна запобігти атакам Jamming за допомогою:

- використання стеганографії;

- реалізації схеми приховування криптографічної головоломки;

- реалізації шифрування Triple DES;

- встановлення приманок.

22) деякі методи атак орієнтовані безпосередньо на пристрої Bluetooth: атаки Bluejacking Bluetooth, Bluetooth-атаки через Bluetooth, атаки Bluebugging Bluetooth.

Запобігти атакам через вразливість Bluetooth можна якщо:

- увімкнути служби «знайди мій пристрій» на телефоні через надійну організацію, таку як Apple або Google, щоб був спосіб використовувати їх технології для пошуку та віддаленого блокування телефону у разі його втрати;

- уникати використання Bluetooth для передачі конфіденційної інформації, наприклад паролів;

- не залишати Bluetooth у режимі «виявлений», коли підключається новий периферійний пристрій до телефона або ноутбука;

- вимкнути Bluetooth, коли ним не користуються.

23) атаки безпеки та ризики, які можуть виникнути у NFC, пов’язані з фізичною природою датчиків NFC та їх робочим механізмом, який використовує небезпечний канал зв’язку. Зв’язок NFC схильний до перехоплення, клонування квитків, пошкодження даних, модифікації даних, вставки даних та атак типу «відмова в обслуговуванні» (DoS).

Можна запобігти атакам зв’язку ближнього поля за допомогою:

- вимкнення мережевих функцій, що не використовуються;

- моніторингу оновлень NFC та оперативному виправленню пристрою;

- обмеження максимальної затримки;

24) атака злого близнюка – це атака хакера, при якій хакер встановлює підроблену мережу Wi-Fi, яка виглядає як законна точка доступу, для крадіжки конфіденційних даних жертв. Атака може бути виконана як атака «людина посередині» (MITM).

Можна запобігти подвійним атакам:

-не входити до облікових записів у загальнодоступному Wi-Fi;

- уникати підключення до точок доступу Wi-Fi з написом «Небезпечно», навіть якщо вони мають знайоме ім’я;

- використовувати двофакторну автентифікацію для всіх конфіденційних облікових записів. Навчитися розпізнавати атаки соціальної інженерії, фішинг та підроблені URL-адреси;

- відвідувати лише веб-сайти HTTPS, особливо у відкритих мережах;

- використовувати VPN під час кожного підключення до загальнодоступної точки доступу.

25) атака деаутентифікації - це тип атаки типу «відмова в обслуговуванні», націлений на обмін даними між користувачем та точкою доступу Wi-Fi. Зловмисник може підробити MAC-адресу жертв і відправити кадр деаутентифікації точці доступу від імені жертви; через це з’єднання з клієнтом розривається. Програма aireplay-ng – найкращий інструмент для виконання атаки деаутентифікації.

Можна запобігти атакам деаутентифікації та дисоціації такими способами:

- переконатися, що мережа використовує шифрування WPA2;

- створити надійну парольну фразу Wi-Fi;

- змінити обліковий запис адміністратора за умовчанням для маршрутизатора, на якому увімкнено Wi-Fi.

26) warchalking – це коли хтось малює символи або позначки області, щоб вказати на відкритий Wi-Fi. Цей тип атаки відносно нешкідливий.

Можна запобігти атакам шляхом:

- вимкнення WPS на бездротовому маршрутизаторі;

- утримання від загальнодоступного Wi-Fi;

- використання програмного забезпечення, яке виявляє несанкціоновані точки доступу;

- запобігання трансляції SSID.

27) атака з перехопленням інформації, також відома як атака зі стеженням або перехопленням, є крадіжкою інформації, що передається по мережі комп’ютером, смартфоном або іншим підключеним пристроєм.

Атака використовує незахищені мережні з’єднання для доступа до даних, які надсилаються або приймаються користувачем.

Атаку з підслуховуванням може бути важко виявити, тому що передача даних через мережу буде працювати нормально.

Можна запобігти підслуховуванню та перехопленню пакетів такими способами:

- використовувати персональний брандмауер;

- постійно оновлювати антивірусне програмне забезпечення;

- використовувати VPN;

- використовувати надійний пароль та часто змінювати його;

- переконатися, що на смартфоні встановлена остання версія.

28) проста, але ефективна стратегія для бездротового DoS – це відтворення локально підслуханих пакетів даних. Ці пакети потім переносяться іншими вузлами пересилання, що призводить до збільшення рівня перевантаження у більш широкому масштабі. Існують варіанти атаки, при яких відтворюються або пакети, що управляють, або пакети даних.

Можна запобігти атакам повторного відтворення (бездротовою мережею) такими способами:

- розміщення точок доступу в окремих віртуальних локальних мережах та реалізація певного типу виявлення вторгнень, щоб допомогти визначити, коли зловмисник намагається налаштувати шахрайську точку доступу або використовує атаку методом грубої сили для отримання доступу;

- шифрування всіх даних, що передаються через точку доступу;

- налаштування точки доступу на прийом лише адреси керування доступом до середовища (MAC);

- використання брандмауерів на кожній точці доступу до мережі;

- вимкнення трансляції SSID з усіх точок доступу;

- використання EAP-TLS для використання різних ключів для шифрування та широкомовного трафіку;

- налаштування сервера RADIUS та центру сертифікації.

29) атака WPS відносно проста за допомогою інструмента з відкритим вихідним кодом Reaver. Reaver працює шляхом грубої сили атаки на PIN-код WPS.

Можна запобігти атакам WPS:

- впровадження інструментів для виявлення несанкціонованих точок бездротового доступу (WAP);

- вимкнення WPS;

- налаштування контролю MAC-адрес на точках доступу;

- переконатися, що бездротовий маршрутизатор підтримує блокування зловмисника WPS для PIN-коду WPS.

30) атаки WEP / WPA. На жаль, WPA (захищений доступ Wi-Fi) піддається атакам зі зломом паролів, особливо коли в мережі використовується слабкий PSK або парольна фраза.

Можна запобігти атакам WEP / WPA такими способами:

- зміна SSID та паролів за умовчанням;

- оновлення прошивки пристроїв, маршрутизаторів та іншого обладнання з підтримкою Wi-Fi у міру появи оновлень;

- увімкнення брандмауера для додаткової безпеки на пристроях або використання віртуальної приватної мережі (VPN), особливо при віддаленому доступі до активів;

- підвищення обізнаності компанії про ризики, пов’язані з небезпечним підключенням та використанням бездротових мереж на роботі та вдома;

- використання мережного моніторингу для спостереження за підключеними пристроями та веб-трафіком;

- регулярний перегляд журналів пристрою та результатів моніторингу щодо підозрілої активності;

- використання засобів автентифікації, таких як двофакторна автентифікація.

31) атака IV також відома як атака вектора ініціалізації. Це свого роду атака на бездротову мережу, яка може становити серйозну загрозу для мережі. Це пов'язано з тим, що це викликає деякі зміни у векторі ініціалізації бездротового пакета, який зашифровано під час передачі.

Після такої атаки зловмисник може отримати багато інформації про відкритий текст одного пакета і згенерувати інший ключ шифрування, який він може використовувати для дешифрування інших пакетів з використанням того ж вектора ініціалізації. З таким ключем дешифрування зловмисники можуть використовувати його для створення таблиці дешифрування, яку вони використовують для дешифрування кожного пакета, що надсилається мережею.

Можна запобігти атакам:

- позбавитися зашифрованого одноразового номера;

- ініціалізувати весь блок розміром 128 біт випадковим значенням IV для шифрування пакетних даних;

- зашифрувати IV окремо, як єдиний блок;

- додати 16-бітне поле для довжини пакета перед його шифруванням.

32) WPA2 атаки. На жаль, у 2017 році було виявлено метод атаки під назвою KRACK (Key Reinstallation AttaCK), який порушує шифрування WPA2, дозволяючи хакеру зчитувати інформацію, що передається між пристроєм та його точкою бездротового доступу.

Можна запобігти атакам WPA2 такими способами:

- забезпечення оновлення пристроїв з підтримкою Wi-Fi одразу після виходу оновлення програмного забезпечення;

- бути впевненим, що на бездротовому маршрутизаторі встановлено останню версію мікропрограми;

- використання надійного рішення VPN на всіх мобільних пристроях та комп’ютерах перед підключенням до Wi-Fi;

- перегляд лише URL-адрес HTTPS під час перегляду веб-сторінок через з’єднання Wi-Fi [30].

3.3 Рекомендації щодо удосконалення методів захисту даних

Як було з’ясовано у розділі 2, шахрайська точка доступу – це точка бездротового доступу, встановлена в захищеній мережі без відома системного адміністратора. Відповідно до стандарту PCI DSS, неавторизовані бездротові пристрої можуть бути приховані всередині комп’ютера або іншого компонента системи, підключені до них або можуть бути підключені безпосередньо до мережного порту або мережного пристрою, наприклад, комутатора або маршрутизатора.

Шахрайська точка доступу може бути невеликою точкою бездротового доступу, підключеною до існуючого міжмережевого екрану або комутатора, або до мережевого роз’єму, що не використовується (наприклад, на персональному столі). Це може бути мобільний пристрій, підключений до USB, який створює бездротове з’єднання. точка доступу або навіть бездротова картка, підключена до сервера.

Оскільки вони встановлені за брандмауером організації, то несанкціоновані точки доступу можуть бути смертельними для безпеки.

Три основні небезпеки шахрайської точки доступу:

- комусь, хто пройшов аутентифікацію, дозволено доступ до мережі;

- системний адміністратор не контролює та не керує нею;

- вона не відповідає звичайним процедурам безпеки інших точок бездротового доступу в тій самій мережі.

Як насправді зловмисник встановлює шахрайську точку доступу? Є безліч способів, але один простий приклад – соціальна інженерія. Якщо зловмисник використовує соціальну інженерію, щоб уникнути фізичного захисту організації, підключає невелику точку бездротового доступу до відкритого мережного порту або, можливо, USB-пристрій Wi-Fi до авторизованого ноутбука і поєднує з'єднання зі своєю точкою бездротового доступу через цей портативний комп'ютер [31].

Точка бездротового доступу не обов'язково повинна встановлюватися хакером, щоб вважатися шахрайською. Фактично авторизовані користувачі організації можуть створити ризик несанкціонованої точки доступу у середовище.

Хоча співробітники можуть не мати злого наміру, точки доступу, що встановлені або використовуються без дозволу системного адміністратора, вважаються шахрайськими. Ось кілька можливих ситуацій:

1) IT-відділ може неправильно налаштувати або випадково продублювати бездротову мережу;

2) співробітники могли використовувати власні точки доступу, щоб спростити підключення мобільних пристроїв, iPad або домашніх ноутбуків до корпоративної мережі;

3) роздратований співробітник, якому набридає повільний корпоративний Wi-Fi, може придбати та встановити приватний бездротовий пристрій у провідній корпоративній мережі.

Всі вони вважаються шахрайськими, тому що вони не перебувають під тими самими заходами безпеки, що й інші точки бездротового доступу в середовищі. Це означає, що системні адміністратори не бачать безпеки цього бездротового середовища. Крім того, співробітники, ймовірно, не включатимуть налаштування безпеки на своїх точках доступу, що спрощує зловмисникам використання цієї точки доступу для перехоплення мережевого трафіку.

Хакери використовують шахрайські точки доступу як простий спосіб отримати доступ до бізнес-систем для збирання конфіденційних даних.

Один із хитрих способів використання шахрайських точок доступу хакерами – використання злих близнюків (також званих ананасами Wi-Fi), які розбиралися у розділі 2.

Якщо точка бездротового доступу виглядає надійною з тим же ім’ям бездротової мережі, унікальним 32-значним ідентифікатором (SSID) та MAC-адресою, пристрої співробітників можуть автоматично підключатися до неї. Якщо злий близнюк успішний, зловмисник може легко підключитися до ноутбука користувача, щоб вкрасти облікові дані для автентифікації та отримати доступ до мережі під авторизованим ім’ям.

Технології бездротового сканування працюють шляхом створення вихідної бази даних точок доступу в середовищі, включаючи IP- та MAC-адреси. Під час сканування воно визначає, порівнює та позначає точки доступу, які не узгоджуються з головним списком. Системний адміністратор повинен вручну дослідити результати сканування та визначити, чи є вони хибними.

Існує кілька процесів, які організації можуть використовувати для виконання вимог Стандарту безпеки даних індустрії платіжних карток (PCI DSS), але більшість підприємств використовують безкоштовний комерційний інструмент сканування. Інші можливі методи тестування несанкціонованих точок доступу включають перевірку фізичних компонентів або бездротові системи виявлення вторгнень (IDS) [31].

Нижче наводиться розбивка по п’яти основних етапах процесу сканування точки бездротового доступу.

1. Знайти бездротові пристрої.

Важко визначити, які бездротові пристрої слід видалити, якщо відсутній точний список усіх пристроїв, які знаходяться у розпорядженні користувача. Ось чому Рада PCI вимагає, щоб проводилося сканування всіх пристроїв бездротового доступу.

Це також чудовий час, щоб переконатися, що фізично убезпечено всі бездротові пристрої, щоб вони були недоступні для широкого загалу.

2. Отримати інструмент сканування та правильно налаштувати його.

Для боротьби з шахрайськими бездротовими мережами використовується або бездротовий сканер, або система виявлення/запобігання вторгненням (IDS/IPS).

Під час пошуку відповідного інструмента необхідно переконатися, що він є бездротовим, а не дротовим. Інструменти дротового сканування використовуються багатьма організаціями для додаткової безпеки, але, згідно з PCI DSS, вони мають високий рівень помилкових спрацьовувань і не допоможуть виконати вимогу 11.1.

Рекомендовано бездротове сканування та технології IDS, такі як Fluke Networks AirMagnet, Snort (з відкритим вихідним кодом), Alert Logic та Cisco.

Після того, як обрано інструмент, настав час для налаштування. Конфігурація бездротового скануючого пристрою не надто складна, але важливо враховувати функції керування журналами та попередження цього інструменту. Необхідно увімкнути автоматичні оповіщення та механізм стримування для усунення несанкціонованих бездротових точок.

3. Просканувати середовище.

Оскільки шахрайський пристрій потенційно може з’явитися у будь-якій частині середовища, важливо звертати увагу на те, де проходить сканування. Відповідно до PCI DSS, місця, де зберігаються, обробляються або передаються дані мають або регулярно скануватися, або в цих місцях повинні бути реалізовані бездротові IDS/IPS.

4. Усунення всіх виявлених шахрайських точок доступу.

Не кожне попередження, яке виявляєте під час сканування, обов’язково є хибним. Можливо, сканування виявило помилкові спрацьовування. Іноді сканер визначає точку доступу як шахрайську, коли сервер автоматично призначає IP-адресу новому легітимному портативному комп’ютеру. Документація має вирішальне значення, щоб визначити, чи справді спрацювання хибне.

Однак, якщо сканування дійсно виявило законну шахрайську точку бездротового доступу, необхідно негайно усунути шахрайську загрозу відповідно до вимог PCI DSS 12.9 і повторно просканувати середовище.

5. Підтримувати регулярний розклад сканування.

Хакерам потрібні дані, і якщо вони виявлять слабке місце, яке дозволяє їм встановити шахрайську точку доступу, вони це зроблять. Ось чому відповідність ніколи не є моментом часу. Це процес.

Стандарт PCI DSS говорить, що всі організації повинні щокварталу сканувати несанкціоновані точки бездротового доступу. Чим вища частота сканування, тим швидше отримання результату.

Шахрайська точка доступу робить мережу та її конфіденційні дані вразливими для зловмисників, які мають бездротове з’єднання. Судячи з онлайн-уроків злих близнюків і підроблених точок доступу Wi-Fi, зрозуміло, що хакери все ще використовують шахрайські точки доступу для атак як корпоративних, так і особистих мереж.

Сьогоднішні хакери докладають зусиль, щоб приховати свої дії, а це означає, що виявлення несанкціонованих точок бездротового доступу в майбутньому може стати набагато складнішим. На даний момент важливо сканувати щокварталу, щоб переконатися, що скануєте правильні розташування у середовищі, і мати план гри для будь-яких виявлених шахрайських точок доступу [31].