Фінальною метою всього цього є заспокоєння емоційного фону та взяття його під контроль підставного агента. Якщо говорити детальніше, агент повинен задати спільну мети та дати розуміння, що таким чином досягти тієї чи іншої мети нереально та є більш гуманні та врівноважені методи.

Цей метод діє на дійовий та конвенційний натовп у випадку коли в натовпі немає лідера. У цих видах головною задачею є об'єднання людей в одну велику групу та заспокоєння їх емоційного фону. Особливістю такого методу є використання малих людських ресурсів, для подолання великого скупчення людей.

Отже, у світі на даний момент існує багато моделей, які можна використовувати, але вони не доведені до ідеалу. Представлений метод базується на судженнях З. Фрейда, які були представлені не тільки як теорія, а метод протидії неконтрольованого натовпу.

Список використаних джерел

1. [Електронний ресурс] : огляд діяль-ності. – Режим доступу : https://uk.wikipedia.org/wiki/%D0%9C%D0%BE%D0%B4%D0%B5%D0%BB%D1%8E%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F_%D1%82%D0%B8%D0%BF%D1%83_%D1%81%D0%BA%D1%83%D0%BF%D1%87%D0%B5%D0%BD%D0%BD%D1%8F – Моделювання типу скупчення.

2. [Електронний ресурс] : огляд діяль-ності. – Режим доступу : http://loveread.ec/read_book.php?id=63684&p=1 – Психология масс и анализ Я

УДК 004.056.5

МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ В БЕЗДРОТОВИХ МЕРЕЖАХ

Петренко Т. А., к.т.н., доц.,
Вильотніков В. В., здобувач вищої освіти, гр. МКБп-201
Національний університет «Чернігівська політехніка»

Незважаючи на багато переваг бездротових локальних мереж, при їх впровадженні та використанні зростає загроза атак кіберзлочинців на їх користувачів та інфраструктуру загалом, а втрата особистої чи комерційної інформації може привести до фінансових збитків всієї компанії. При цьому виникає необхідність захисту переданої інформації в таких типах мереж. Так як загрози інформаційним ресурсам, в деяких випадках, можуть бути великими і катастрофічними. Тому актуальним є дослідження методів підвищення ефективності захисту інформації в бездротових комп'ютерних мережах.

Методи захисту інформації - це сукупність прийомів і засобів, що забезпечують конфіденційність, цілісність, повноту і доступність інформації, і протидіють внутрішнім і зовнішнім загрозам. Кожному виду загроз притаманні свої специфічні методи та способи захисту інформації.[1]

Забезпечення інформаційної безпеки при використанні бездротових мереж досягається системою методів, спрямованих:

- на попередження загроз - це превентивні заходи щодо забезпечення інформаційної безпеки в інтересах попередження можливості їх виникнення;
- на виявлення загроз - виражається в систематичному аналізі та контролі можливості появи реальних або потенційних загроз і своєчасних заходів щодо їх попередження;
- на визначенні загроз - має на меті визначення реальної загрози виконання конкретних злочинних дій;
- на локалізацію злочинних дій і вжиття заходів щодо ліквідації загрози або конкретних злочинних дій;

- на ліквідацію наслідків загроз і кібератак і відновлення повної функціональності бездротової мережі. [2]

Кращі світові практики в галузі управління інформаційною безпекою описані в міжнародному стандарті на системи менеджменту інформаційної безпеки ISO/IEC27001 (ISO 27001). Зазначений стандарт встановлює вимоги до системи менеджменту інформаційної безпеки для демонстрації здатності організації захищати свої інформаційні ресурси.[3]

На основі даного стандарту можуть бути виділені основні групи методів впровадження яких приведуть до зниження ймовірності порушення політики безпеки бездротової мережі в організації:

1. Організаційні методи з навчання користувачів та адміністраторів - представляють собою деякий набір інструкцій, що визначає обов'язкові для всіх користувачів порядок і правила використання комп'ютерів. А також обмеження за правилами доступу в комп'ютерні приміщення.

2. Контроль підключень до мережі. Рівень ризику, пов'язаного з підключенням несанкціонованої точки доступу або клієнта бездротової мережі, можна знизити шляхом відключення невикористовуваних портів комутаторів, фільтрації по MAC-адресами (port-security), аутентифікації 802.1X, систем виявлення атак і сканерів безпеки, контролюючих поява нових мережевих об'єктів, тощо;

3. Методи контролю фізичної безпеки. Контроль принесених на територію пристроїв дозволяє обмежити ймовірність підключення до мережі бездротових пристроїв. Обмеження доступу користувачів і відвідувачів до мережевих портів і слотів розширення комп'ютера знижує ймовірність підключення бездротового пристрою;

4. Мінімізація привілеїв користувача. Якщо користувач працює на комп'ютері з мінімально необхідними правами, то знижується ймовірність самовільної зміни налаштувань бездротових інтерфейсів;

5. Контроль політики безпеки. Методи аналізу захищеності, такі як сканери уразливостей, дозволяють виявляти появу в мережі нових пристроїв і визначити їх тип (функції визначення версій ОС і мережевих додатків), а також відстежувати відхилення параметрів клієнтів від заданого профілю. Технічне завдання на проведення робіт з аудиту зовнішніми консультантами має враховувати вимоги політики щодо бездротових мереж;

6. Інвентаризація ресурсів. Наявність актуального оновлюваного списку мережевих ресурсів полегшує виявлення нових мережевих об'єктів;

7. Виявлення атак. Застосування систем виявлення атак як традиційних, так і бездротових дає можливість своєчасно визначати спроби несанкціонованого доступу;

8. Методи розслідування інцидентів. Інциденти, пов'язані з бездротовими мережами мало відрізняються від інших подібних ситуацій, однак процедури їх розслідування повинні бути визначені;

9. Методи внутрішнього і зовнішнього аудиту. При проведенні робіт з оцінки захищеності повинні враховуватися вимоги політики щодо бездротових мереж.

10. Методи поділу мереж. У зв'язку зі специфікою бездротових мереж бажано виділяти точки бездротового доступу в окремий мережевий сегмент за допомогою брандмауера, особливо коли мова стосується гостьового доступу;

11. Методи шифрування. Використання криптографічних засобів захисту. Повинні бути визначені використовувані протоколи і алгоритми шифрування трафіку в бездротової мережі (WPA або 802.11i). При використанні технології 802.1X визначаються вимоги до протоколів ЕЦП і довжині ключа підпису сертифікатів, які використовуються для цілей;

12. Методи автентифікації. Повинні бути визначені вимоги до зберігання даних автентифікації, їх зміні, складності, безпеки при передачі по мережі. Можуть бути явно визначені використовувані методи EAP, методи захисту загального ключа сервера RADIUS;

13. Прив'язка програм і даних до конкретного комп'ютера (мережі або ключу) - метод, вельми динамічний з розвитку реалізують його засобів захисту.

14. Допустимість використання програмного та апаратного забезпечення. Цей метод включає в себе формування чітких вимоги до точок доступу, бездротовим комутаторів і клієнтів бездротової мережі;

15. Методи розпізнавання атак. Повинні бути визначені вимоги до систем виявлення бездротових атак, закріплена відповідальність за аналіз подій;

16. Протоколювання і аналіз подій безпеки. Даний метод передбачає додавання в список контрольованих подій, специфічних для бездротових мереж;

17. Контроль віддаленого доступу до мережі. У більшості випадків користувачів бездротової мережі логічно відносити до користувачів систем віддаленого доступу. Це обумовлено аналогічними загрозами і як наслідок - контрзаходами, характерними для даних компонентів ІС.

Специфічні мережеві методи і засоби забезпечення безпеки даних пов'язані з поняттям проміжної мережі, яка являє собою сукупність обладнання, розташованого між двома об'єднаними мережами. Так, наприклад, на базі цього обладнання можуть бути сформовані так звані «міжмережеві екрани» або брандмауери - це програмні, апаратні або програмно-апаратні механізми захисту мережі від зовнішнього світу, які служать бар'єром, що обмежує поширення інформації з однієї мережі в іншу.

До специфічних мережевих засобів забезпечення безпеки належать також засоби посилення захисту мережі - це деякі пристрої проміжної мережі і окремі технологічні рішення, наприклад:

- перемикаючі мости на концентраторі, які, під час контролю напрямку трафіку в мережі і виробляючи додаткову фільтрацію пакетів, створюють ще один бар'єр для хакерів;
- шлюзи рівня віртуального каналу дозволяють користувачам з'єднуватися і обмінюватися пакетами з сервером, при цьому кожен пакет окремо не перевіряється, а після перевірки адресних даних приймаються відразу кілька пакетів, можуть використовуватися для повної заборони прямих контактів комп'ютерів внутрішньої мережі зовнішньої мережею;
- ізоляція протоколів, заснована на використанні протоколу TCP/IP тільки для зв'язку з Internet. У внутрішній (локальної) мережі використовуються інші протоколи, несумісні з TCP/IP, а доступ в Internet здійснюється через шлюз прикладного рівня;
- створення віртуальної приватної мережі, якщо передбачається підключення віддалених користувачів до КВС.[4]

Організація моніторингу та аудиту мережі також складають основу для забезпечення безпеки. Більшість мережевих ОС мають вбудовані або додатково поставляються програми, що забезпечують проведення цієї роботи.

У складі специфічних мережевих методів знаходяться і архітектурні методи захисту, до яких зараховують рішення, що приймаються на рівні топології та архітектури мережі і підвищують її захищеність в цілому:

- фізична ізоляція закритого сегмента внутрішньої мережі, що містить конфіденційну інформацію, від зовнішньої мережі. Зв'язок із зовнішньою мережею підтримується через відкритий сегмент внутрішньої мережі;
- функціональний розподіл внутрішньої мережі на підмережі, При якому в кожній підмережі працюють користувачі (співробітники компанії), об'єднані за професійними інтересами;
- сеансове (короткочасне) підключення внутрішньо мережі до сегменту мережі, що підключений до Internet, за допомогою комутатора і/або перемикаючого моста.[5]

Багато заходів забезпечення безпеки на рівні архітектури проміжної мережі пов'язані з реалізацією компонентів багаторівневого захисту. Якщо проміжна мережа включає маршрутизатор, комп'ютер, виділений для брандмауера, і концентратор, з'єднаний безпосередньо з сервером внутрішньої мережі, то засоби захисту можуть бути реалізовані на кожному з цих пристроїв. Наприклад, на маршрутизаторі - фільтрація пакетів, на комп'ютері - міжмережевий екран, на концентраторі - перемикається міст і віртуальна ЛВС, на сервері внутрішньої мережі - ще один міжмережевий екран.

Таким чином, надійний захист телекомунікаційних мереж від загроз та кібератак можливий тільки на основі побудови комплексної системи безпеки інформації на всіх етапах розробки, введення в дію, модернізації апаратно-програмних засобів телекомунікацій, а також при обробці, зберіганні і передачі інформації по каналах зв'язку з широким застосуванням сучасних методів захисту інформації в бездротових мережах, яка б включала в себе взаємопов'язані заходи різних рівнів: нормативно-правового; організаційного (адміністративного); програмно-апаратного; технічного та ін.

Список використаних джерел

1. Богуш В. В., Соколов В. Ю. Дослідження захищеності Wi-Fi мереж. Зв'язок. 2009. №4 (88). С. 29–31.
2. Бурячок В. Л., Астапеня В. М., Соколов В. Ю. Способы повышения доступности информации в беспроводных системах стандарта IEEE 802.11 с MIMO. Сучасний захист інформації. 2016. №2. С. 60–68.
3. Платоненко А.В. Захист інформації у бездротових мережах WI-FI / Платоненко А.В. // Науково-технічна конференція «Актуальні проблеми забезпечення інформаційної безпеки держави» – Київ: ДУТ, 2014 – С.40-41.
4. Соколов В. Ю., Карацюба К. І. Використання дерев атак для аналізу захищеності бездротових технологій стандарту IEEE 802.11. Вісник ДУІКТ. 2012. Т. 10, №1. С. 42–49.
5. Чернобай К. Ю., Грибков С. В. Аналіз та шляхи вирішення проблем захисту комерційних бездротових локальних мереж WI-FI // Вісник національного університету "Львівська політехніка" . - № 880 (2017), с. 99-103

УДК 004.056.5

ІНФОРМАЦІЙНА БЕЗПЕКА. МЕТОДИ ПСИХОЛОГІЧНОГО ВПЛИВУ

Плакса А. О здобувач вищої освіти гр.КБ-171
Науковий керівник: **Мехед Д. Б.,** к.п.н., доцент
Національний університет «Чернігівська політехніка»

За останні роки кількість унікальних кібератак збільшувалася з кварталу в квартал та за підсумками 2020 року на 19% перевищила число кібератак в 2019 році. Найбільш часто кібератакам піддавалися держустанови, промисловість, медицина, сфера науки і освіти, фінансова галузь. На ці галузі припадає понад половини всіх кібератак на юридичні особи (54%). Частка атак на промислові компанії збільшилась до 10% проти 4% в 2019 році. Цю галузь атакують переважно з використанням шкідливого ПЗ (подібних атак 90%). Цілеспрямованих атак було істотно більше, ніж масових. Їх частка склала 73%, що на 13 % більше, ніж в 2019 році. Одна з причин - зростання числа APT-атак. Протягом року відзначалась висока активність до 27 APT-груп. Інформація як і раніше представляє високу цінність для кіберзлочинної спільноти. Частка кампаній, спрямованих на отримання даних, склала 60% і 57% в атаках проти юридичних та приватних осіб відповідно. Найбільший інтерес для зловмисників представляли персональні дані, облікові записи та дані банківських карт [3;с.158]. Загальна кількість заражень шкідливим ПЗ в 2020 році на 38% перевищила аналогічний показник 2019 року. Успіху шкідливих компаній сприяла модернізація як самого ШПЗ, так і засобів його постачання. Шифрувальники - одна з найбільш актуальних кіберзагроз для компаній по всьому світу. На їх частку припав 31% заражень ШПЗ серед юридичних осіб. Середня сума виплат в 2019- 20 роках досягла кількох сотень тисяч доларів США. Оператори шифрувальників шантажують жертв публікацією викрадених перед шифруванням даних у разі відмови платити викуп. Протягом всього року регулярно