Люта М.В., магістр, Одокієнко С.М., к.т.н., доц.
Київський національний університет технологій та дизайну

МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД АТАК В МЕРЕЖІ INTERNET

Анотація. *У статті розглянуто методи захисту інформації від атак в мережі Internet. Проведено аналіз існуючих методів атак та на основі їх аналізу виявлено особливості захисту від атак.*

Ключові слова: *інформаційні мережі; захист інформаційних систем; атака; мережа Internet.*

Liuta M.V., Odokienko S.M.
Kyiv National University of Technologies and Design

METHODS OF PROTECTION OF INFORMATION FROM ATTACKS ON THE INTERNET

Abstract. *The article considers methods of protecting information from attacks on the Internet. The analysis of existing methods of attacks is carried out and the peculiarities of protection from attacks are revealed on the basis of their analysis.*

Keywords: *information networks; information systems protection; attack; Internet.*

Вступ. Інформаційна безпека має першорядне значення у зв'язку із значним поширенням атак, яким постійно піддаються як окремі мережі підприємств, так і національні мережі в цілому.

В результаті аналізу публікацій виявлено, що в багатьох роботах недостатньо висвітлено методи захисту інформації користувача в мережі Internet та їх особливості.

Перед керівниками держав і компаній гостро постає проблема втілення термінових заходів щодо захисту своїх активів, оскільки вони, у більшості випадків, не забезпечені навіть базовими методами захисту і є нестача професіоналів, здатних їх сформувати, впровадити й експлуатувати.

Постановка завдання. Мета статті полягає в аналізі методів забезпечення інформаційної безпеки користувачів в мережі Internet.

Результати досліджень. Особливість мережі Internet в тому, що 99% відсотків інформаційних ресурсів мережі є загальнодоступними. Віддалений доступ до цих ресурсів може здійснюватися анонімно будь-яким неавторизованим користувачем мережі. Прикладом подібного несанкціонованого доступу до загальнодоступних ресурсів є підключення до WWW- або FTP-серверів, в тому випадку, якщо подібний доступ дозволений. Визначившись, до яких ресурсів мережі Internet користувач має намір отримати доступ, необхідно зрозуміти чи збирається користувач дозволяти віддалений доступ з мережі до своїх ресурсів. Якщо ні, то тоді має сенс використовувати в якості мережевої ОС, яка не містить програм-серверів, а, отже, віддалений доступ до даної системи в принципі неможливий, так як він просто програмно не передбачено, правда з одним але: під дані системи дійсно немає серверів FTP, TELNET, WWW і т. д., але не можна забувати про вбудовану в них можливість надання віддаленого доступу до файлової системи, так зване поділ (share) ресурсів. Але якщо згадати щонайменше дивну позицію фірми Microsoft по відношенню до забезпечення безпеки своїх систем, потрібно серйозно подумати, перш ніж зупинити вибір на продуктах даної фірми. Останній приклад: в Internet з'явилася програма, що надає атакуючому несанкціонований віддалений доступ до файлової системи ОС Windows. Вибір клієнтської операційної системи може вирішити багато проблем з безпекою мережі для даного користувача (адже не можна отримати доступ до ресурсу, якого не має). Однак в цьому випадку погіршується функціональність системи. В такому випадку потрібно своєчасно сформулювати, основну аксіому безпеки [1, 5].

Аксіома безпеки. Принципи доступності, зручності, швидкодії і функціональності обчислювальної системи антагоністичні принципам її безпеки.

Дана аксіома, в принципі, очевидна: чим більш доступна, зручна, швидка і багатофункціональна ОС, тим вона менш безпечна. Прикладів можна привести масу. Наприклад, служба DNS: зручно, але небезпечно.

Повернемося до вибору користувачем клієнтської мережевої ОС. До речі, це, один з великих кроків, що ведуть до мережевої політики ізоляціонізму. Дана мережева політика безпеки полягає в здійсненні як можна більш повної ізоляції своєї обчислювальної системи від зовнішнього світу. Також одним з кроків до забезпечення цієї політики є, наприклад, використання систем Firewall, що дозволяють створити виділений захищений сегмент (наприклад, приватну мережу), відокремлений від глобальної мережі. Звичайно, ніщо не заважає довести цю політику мережевого ізоляціонізму до абсурду – просто висмикнути мережевий кабель (повна ізоляція від зовнішнього світу). Не забувайте, це теж "рішення" всіх проблем з віддаленими атаками і мережевою безпекою (в зв'язку с повною відсутністю інших).

Отже, нехай користувач мережі Internet вирішив використовувати для доступу в мережу тільки клієнтську мережну ОС і здійснювати за допомогою неї тільки неавторизований доступ. Так проблему з безпекою не буде вирішено Все було б добре, якби не було так погано. Для атаки "Відмова в обслуговуванні" абсолютно не має значення ні вид доступу, застосовуваний користувачем, ні тип мережевої ОС (хоча клієнтська ОС з точки зору захисту від атаки дещо краще). Ця атака, використовуючи фундаментальні прогалини в безпеці протоколів та інфраструктури мережі Internet, вражає мережну ОС на хості користувача з однією єдиною метою - порушити його працездатність. Для атаки, пов'язаної з нав'язуванням хибного маршруту за допомогою протоколу ICMP, метою якої є відмова в обслуговуванні, ОС Windows – найкраща ціль. В такому випадку користувачу залишається надіятись, що його хост не цікавить «хакера», який може порушити його роботу бажаючи просто нашкодити [3].

Адміністративні засоби захисту від віддалених атак у мережі Internet. Правильним кроком в цьому випадку буде запрошення спеціаліста з інформаційної безпеки, який разом з вами постарається забезпечити необхідний рівень безпеки для вашої розподіленої ОС. Це досить складне комплексне завдання, для вирішення якого необхідно визначити, що (список контрольованих об'єктів і ресурсів РОС), від чого (аналіз можливих загроз даної РОС) і як (вироблення вимог, визначення політики безпеки і вироблення адміністративних і програмно-апаратних заходів по забезпеченню на практиці розробленої політики безпеки) захищати. Мабуть, самими простими і дешевими є саме адміністративні методи захисту атак.

1. Метод захисту від аналізу мережевого трафіку.

Існує атака, що дозволяє «хакеру» за допомогою програмного прослуховування каналу передачі повідомлень в мережі перехоплювати будь-яку інформацію, якою обмінюються віддалені користувачі, якщо по каналу передаються тільки нешифровані повідомлення. Також можна показати, що базові прикладні протоколи віддаленого доступу TELNET і FTP не передбачають елементарну криптозахист переданих по мережі навіть ідентифікаторів (імен) і аутентифікатор (паролів) користувачів. Тому адміністраторам мереж, очевидно, можна порекомендувати не допускати використання цих фундаментальних протоколів для надання віддаленого авторизованого доступу до ресурсів своїх систем і вважати аналіз мережевого трафіку постійно присутньою загрозою, яку неможливо усунути, але можна зробити її здійснення по суті безглуздим [2, 3].

2. Метод захисту від помилкового ARP-сервера.

У тому випадку, якщо у мережевої ОС відсутня інформація про відповідність IP- і Ethernet-адрес хостів в середині одного сегмента IP-мережі, даний протокол дозволяє посилати широкомовний ARP-запит на пошук необхідної Ethernet-адреси, на яку атакуючий може надіслати запит, і, в подальшому, весь трафік на канальному рівні виявиться перехопленим «хакером» і пройде через хибний ARP-сервер. Очевидно, що для ліквідації даної атаки необхідно усунути причину, по якій можливо її здійснення. Основна причина успіху даної віддаленої атаки – відсутність необхідної інформації у ОС кожного хоста про відповідні IP- і Ethernet-адреси всіх інших хостів всередині даного сегменту мережі. Таким чином, найпростішим рішенням буде створення статичної ARP-таблиці у вигляді файлу (в ОС UNIX зазвичай / etc / ethers), куди необхідно внести відповідну інформацію про адреси. Даний файл встановлюється на кожен хост всередині сегмента, після чого, у мережевій ОС відпадає необхідність у використанні віддаленого ARP-пошуку [2, 4].

3. Метод захисту від помилкового DNS-сервера.

Використання в мережі Internet служби DNS в її нинішньому вигляді може дозволити «хакеру» отримати глобальний контроль над з'єднаннями шляхом нав'язування помилкового маршруту через хост «хакера» – помилковий DNS-сервер. Здійснення цієї віддаленої атаки, заснованої на потенційних вразливості служби DNS, може привести до катастрофічних наслідків для величезного числа користувачів Internet і стати причиною масового порушення інформаційної безпеки даної глобальної мережі. У наступних двох пунктах пропонуються можливі адміністративні методи щодо запобігання або ускладнення даної віддаленої атаки для адміністраторів і користувачів мережі і для адміністраторів DNS-серверів (рис. 1).

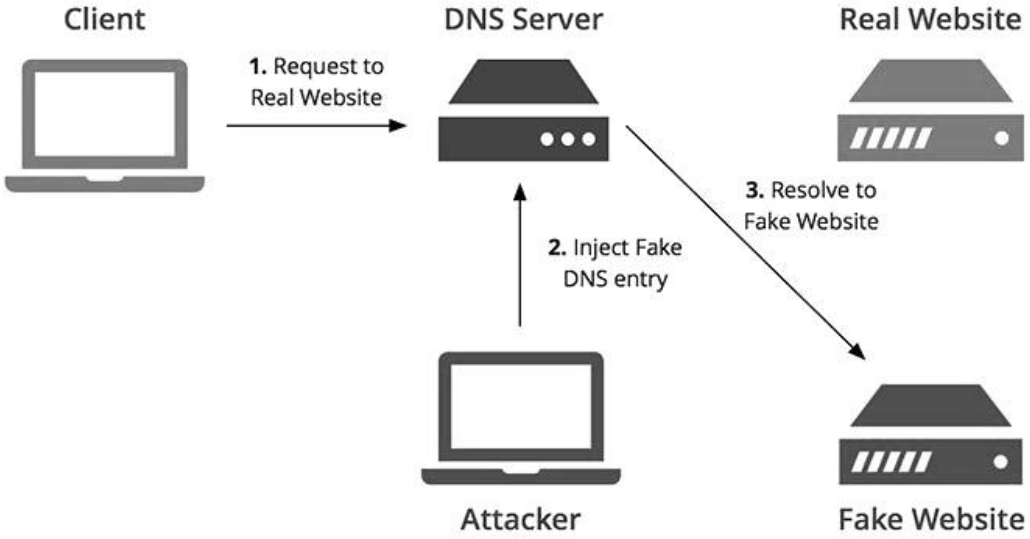

Рис. 1. **DNS-Server**

Адміністративно та програмно повністю не можна захиститися від атаки на існуючу версію служби DNS. Оптимальним з точки зору безпеки рішенням буде взагалі відмовитися від використання служби DNS в вашому захищеному сегменті. Звичайно, зовсім відмовитися від використання імен при зверненні до хостам для користувачів буде дуже не зручно. Тому можна запропонувати наступне компромісне рішення: використовувати імена, але відмовитися від механізму віддаленого DNS-пошуку. Ви правильно здогадалися, що це повернення до схеми, що використовувалася до появи служби DNS з виділеними DNS-серверами. Тоді на кожній машині в мережі існував hosts

файл, в якому знаходилася інформація про відповідні імена і IP-адреси всіх хостів в мережі. очевидно, що на сьогоднішній день адміністратору можна внести в подібний файл інформацію про лише найбільш часто відвідуваних користувачами даного сегмента серверах мережі. Тому використання на практиці даного рішення надзвичайно складне і, мабуть, нереально. Для ускладнення здійснення даної віддаленої атаки можна запропонувати адміністраторам використовувати для служби DNS замість протоколу UDP, який встановлюється за умовчанням, протокол TCP (хоча з документації далеко не очевидно, як його змінити). Це істотно ускладнить для атакуючого передачу на хост помилкового DNS-відповіді без прийому DNS-запиту. Загальний невтішний висновок такий: в мережі Internet при використанні існуючої версії служби DNS не існує прийнятного рішення для захисту від помилкового DNS-сервера (і не відмовишся, як у випадку з ARP, і використовувати небезпечно).

Єдиним способом ускладнити здійснення даної віддаленої атаки, це використовувати для спілкування з хостами і з іншими DNS-серверами тільки протокол TCP, а не UDP. Проте, це лише ускладнить виконання атаки - не забувайте як про можливе перехоплення DNS-запиту, так і про можливість математичного передбачення початкового значення TCP-ідентифікатора ISN.

На закінчення можна порекомендувати для всієї мережі Internet скоріше перейти або до нової більш захищеною версією служби DNS, або прийняти єдиний стандарт на захищений протокол. Зробити цей перехід, незважаючи на всі колосальні витрати, просто необхідно, інакше мережа Internet може бути просто поставлена на коліна перед всезростаючими успішними спробами порушення її безпеки за допомогою даної служби [2, 6].

4. Метод захисту від нав'язування помилкового маршруту при використанні протоколу ICMP.

Атака, яка полягала у передачі на хост помилкового ICMP Redirect повідомлення про зміну вихідного маршруту приводила як до перехоплення атакуючим інформації, так і до порушення працездатності атакованого хоста. Для того, щоб захиститися від даної віддаленої атаки, необхідно або фільтрувати дане повідомлення (використовуючи Firewall чи фільтруючий маршрутизатор), не допускаючи його попадання на кінцеву систему, або відповідним чином вибирати мережеву ОС, яка буде ігнорувати це повідомлення. Однак зазвичай не існує адміністративних способів вплинути на мережеву ОС так, щоб заборонити їй змінювати маршрут і реагувати на дане повідомлення. Єдиний спосіб, наприклад, в разі ОС Linux або FreeBSD полягає в тому, щоб змінити вихідні тексти і перекомпілювати ядро ОС. очевидно, що такий екзотичний для багатьох спосіб можливий тільки для вільно розповсюджуваних разом з вихідними текстами операційних систем. Зазвичай на практиці не існує іншого способу дізнатися реакцію використовуваної у вас ОС на ICMP Redirect повідомлення, як послати це повідомлення і подивитися, яким буде результат. Експерименти показали, що дане повідомлення дозволяє змінити маршрутизацію на ОС Linux та Windows. Слід зазначити, що продукти компанії Microsoft не відрізняються особливою захищеністю від можливих віддалених атак, властивих IP-мереж. Отже, використовувати дані ОС в захищеному сегменті IP-мережі є небажаним. Це і буде тим самим адміністративним рішенням по захисту сегмента мережі від даної віддаленій атаки [2, 4].

5. Метод захисту від відмови в обслуговуванні.

Немає і не може бути прийнятних способів захисту від відмови в обслуговуванні в існуючому стандарті IPv4 мережі Internet. Це пов'язано з тим, що в даному стандарті неможливий контроль за маршрутом повідомлень. Тому неможливо забезпечити надійний контроль за мережевими з'єднаннями, так як у одного суб'єкта мережної взаємодії існує можливість зайняти необмежене число каналів зв'язку з віддаленим

об'єктом і при цьому залишитися анонімним. Через це будь-який сервер в мережі Internet може бути повністю паралізований за допомогою віддаленої атаки. Єдине, що можна запропонувати для підвищення надійності роботи системи, що піддається даній атаці, - це використовувати якомога потужніші комп'ютери. Чим більше число і частота роботи процесорів, чим більший об'єм оперативної пам'яті, тим більш надійною буде робота мережевої ОС, коли на неї буде надсилатись велика кількість помилкових запитів на створення з'єднання. Крім того, необхідно використання відповідних вашим обчислювальним потужностям операційних систем з внутрішньою чергою, яка вміщує велику кількість запитів на підключення. Адже від того, що ви, наприклад, поставите на супер ЕОМ операційну систему Linux або Windows NT, у яких довжина черги для одночасно оброблюваних запитів близько 10, а тайм-аут очищення черги кілька хвилин, то, незважаючи на всі обчислювальні потужності комп'ютера, ОС буде повністю паралізована атакуючим [2, 3].

6. Метод захисту від підміни однієї зі сторін при взаємодії з використанням базових протоколів сімейства TCP / IP.

Як зазначалося раніше, єдиним базовим протоколом сімейства TCP / IP, в якому спочатку передбачена функція забезпечення безпеки з'єднання і його абонентів, є протокол транспортного рівня – протокол TCP. Що стосується базових протоколів прикладного рівня: FTP, TELNET, r-служба, NFS, HTTP, DNS, SMTP, то жоден з них не передбачає додатковий захист з'єднання на своєму рівні і залишає рішення всіх проблем щодо забезпечення безпеки з'єднання протоколу нижчого транспортного рівня – TCP. Однак, згадавши про можливі атаки на TCP-з'єднання, що при знаходженні атакуючого в одному сегменті з метою атаки захиститися від заміни одного з абонентів TCP-з'єднання в принципі неможливо, а у разі знаходження в різних сегментах через можливість математичного передбачення ідентифікатора TCP-з'єднання ISN також реальна підміна одного з абонентів, нескладно зробити висновок, що при використанні базових протоколів сімейства TCP / IP забезпечити безпеку з'єднання практично неможливо. Це відбувається через те, що, на жаль, всі базові протоколи мережі Internet з точки зору забезпечення інформаційної безпеки неймовірно застаріли.

Єдине, що можна порекомендувати мережевим адміністраторам для захисту тільки від міжсегментних атак на з'єднання – в якості базового «захищеного» протоколу використовувати протокол TCP і мережеві ОС, в яких початкове значення ідентифікатора TCP-з'єднання дійсно генерується випадковим чином (непоганий псевдовипадковий алгоритм генерації використовується в останніх версіях ОС FreeBSD) [2, 6].

7. Криптографічний метод захисту інформації.

Радикальне розв'язання проблем захисту інформації, що циркулює у високопродуктивних телекомунікаційних системах, може бути отримане на базі використання криптографічного захисту інформації. Криптографічний захист може забезпечити виконання умов збереження конфіденційності й цілісності даних, що передаються у відкритих мережах, а також анонімність об'єкта й умови його причетності до дій, що здійснюються в телекомунікаційних системах [7, 8].

Висновки. Запропоновано рішення проблеми як звичайного користувача мережі Internet, так і для користувачів корпоративними мережами. Проаналізовано безліч методів для захищення інформації користувача в мережі Internet.

В мережі необхідно розміщувати інформацію, поширення якої бажано її власнику. При цьому завжди необхідно враховувати той факт, що в будь-який момент ця інформація може бути перехоплена, перекручена або може стати недоступною. Вихід із становища полягає в чіткому розмежуванні інформації, що становить життєвий інтерес для суб'єктів – користувачів – і створення спеціалізованих систем її обробки. Отже, мова

повинна йти не про захищеність Internet, а про забезпечення розумної достатності інформаційної безпеки мережі [6].

Список використаної літератури

1. Андреєв О. С. Аналіз та оцінка загроз на інформаційні ресурси комп'ютерних систем, які працюють в режимі реального часу / О. С. Андреєв, М. В. Захарова, М. В. Люта // Вісник КНУТД. – 2013. – № 5. – С. 88–92.
2. Лукацкий А. В. Обнаружение атак / А. В. Лукацкий. – СПб.: БХВ-Петербург, 2001. – 624 с.
3. Медведовский И. Д. Атака из Internet / И. Д. Медведовский. – М.: Изд-во "СОЛОН-Пресс", 2002. – 368 с.
4. Медведовский И. Д. Атака на Internet / И. Д. Медведовский, П. В. Семьянов, Д. Г. Леонов. – 2-е изд., перераб. и доп. – М.: ДМК-Прес. 2006. – 336 с.
5. Нікітченко В. П. Аналіз сучасних систем керування проектами / В. П. Нікітченко, М. В. Захарова, М. В. Люта // Логос. Мистецтво наукової думки. – 2019. – № 3. – С. 95–97.
6. Олифер В. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов / В. Олифер, Н. Олифер. – 2-е изд. – СПб.: Питер, 2002. – 864 с.
7. Розломій І. О. Підвищення ефективності захисту персональних медичних даних на основі моделі розмежування доступу Take-Grant / І. О. Розломій, М. В. Захарова, М. В. Люта // Вісник КНУТД. – 2016. – № 4. – С. 29–33.
8. Телекомунікаційні системи та мережі. Структура та основні функції [Електронний ресурс] / В. В. Поповський та ін. – Друге видання, доповнене. – Х.: СМІТ, 2018. – Т. 1. – Режим доступу: http://www.znanius.com/3851.html.