УДК 004.056 **doi: 10.26906/SUNZ.2022.2.091**

А. С. Янко, Р. А. Вигівський

Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна

СИСТЕМА ЗАХИСТУ КОМП'ЮТЕРНОЇ МЕРЕЖІ

Анотація. В даній статті висвітлено основи захисту інформації у комп'ютерних системах від несанкціонованого доступу. Розглянуті головні фактори, які необхідно врахувати при проектуванні безпечної мережі. Проаналізовано найпоширеніші методи Інтернет-атак та інших загроз в сучасних комп'ютерних мережах. Досліджено механізми безпеки до набору протоколів Інтернету на різних рівнях, що забезпечують логічний захист одиниць даних, коли вони переміщуються по мережі. Оцінено наслідки для безпеки поточної та нової версій Інтернет-протоколу. А також висвітлено сучасні технології безпеки в Інтернеті та систем виявлення вторгнень в мережу.

Ключові слова: аспекти безпеки, Інтернет-атака, Інтернет-протокол, комп'ютерна мережа, криптографічні системи,мережева безпека, програмного забезпечення мережевої безпеки, система виявлень вторгнень.

Вступ

Завдяки Інтернету та новим мережевим технологіям світ стає все більш взаємопов'язаним. У всьому світі існує величезна кількість особистої, комерційної, військової та урядової інформації про мережеві інфраструктури. Через легкість, з якою інтелектуальну власність можна придбати через Інтернет, безпека мережі стає все більш важливою. Інтелектуальна власність може бути порушена. Існує два типи мереж: мережі передачі даних і синхронні мережі, що складаються з комутаторів.

Інтернет класифікується як мережа передачі даних. Оскільки поточна мережа даних складається з комп'ютерних маршрутизаторів, спеціальні програми, такі як «троянські коні», закладені в маршрутизатори, можуть отримувати інформацію. Оскільки синхронна мережа, яка складається з комутаторів, не буферизує дані, вона не вразлива для зловмисників. Ось чому мережі передачі даних, такі як Інтернет, та інші мережі, які підключаються до Інтернету, надають перевагу безпеці.

На сьогодні мережева безпека це великий набір вимог та політик, які пред'являються до мережевої корпоративної інфраструктури для аналізу її роботи та недопущення доступу до даних зловмисників, зміни цих даних, їх модифікації, а також відмови роботи мережі чи її окремих ресурсів.

Незалежно від масштабу та виду підприємства скрізь, де використовується мережна інфраструктура, необхідні апаратні рішення та програмні продукти, які дозволяють забезпечити безпеку мережі.

У глобальному сенсі необхідно дотримуватися основних принципів, виконання яких дозволить говорити про безпеку мережі на підприємстві, наприклад, захист кінцевих мережевих пристроїв. Забезпечити достатній рівень безпеки пристрою можна лише у разі використання останніх технологій. Наприклад, персональні комп'ютери можуть бути атаковані за допомогою вірусів, хробаків або вразливостей під час роботи з веб-браузерами. Використання корпоративних антивірусів із оновленими базами сигнатур дозволяє скоротити ризик атаки.

Відмовостійкість таких пристроїв, можливість їх відновлення. Моніторинг інфраструктури – обов'язкова дія захисту мережі.

Для того, щоб розуміти, в якому статусі знаходяться сервіси та програми, необхідно використовувати засоби захисту доступу до мережі.

Постійний контроль пропускної спроможності мережі. Успішно виконана атака завжди призводить до витрат на відновлення інфраструктури. У разі використання засобів захисту від цільових атак, а також засобів запобігання вторгненням ризики значно зменшуються, і шанси зловмисників на успішну атаку скорочуються. Це, у свою чергу, дозволяє організувати безперервний робочий процес і знизити витрати компанії за простої.

Відмовостійкість внутрішньої мережі організації та можливість її відновлення після атаки. Захистити периметр компанії на 100% все ж таки не вдається, і в такому випадку варто продумати можливість переходу з одного ресурсу на інший у разі відмови першого, причому непомітно для користувачів.

Тема безпеки мережі досліджується шляхом дослідження наступного: архітектура Інтернету та вразливі аспекти безпеки Інтернету; типи Інтернет-атак і заходи безпеки; безпека мережі для мереж, підключених до Інтернету; поточна розробка обладнання та програмного забезпечення мережевої безпеки.

Аналіз останніх досліджень і публікацій. Інформаційні загрози для комп'ютерних мереж мають стійку тенденцію до зростання та модифікації. На даний час в області виявлення вторгнень в комп'ютерні мережі переважає підхід виявлення зловживань, який ґрунтується на побудові моделі атаки безпосередньо, як на систему в цілому. Однак цей підхід має очевидний недолік, пов'язаний, перш за все, з недостатнім урахуванням впливу комп'ютерного середовища та уразливих аспекти безпеки в Інтернет-архітектурі. Загальнотеоретичні аспекти дослідження безпеки комп'ютерної мережі представлені в публікаціях В. Г. Оліфер, Н. О. Оліфер, О. О. Єрофєєва, В. М. Лопатіна, та інших провідних вчених. Аналізуючи дослідження та попередні напрацювання в даній, було прийнято рішення більш детально описати уразливі аспекти безпеки в Інтернет-архітектури, а також для оцінки необхідних змін у технології безпеки проаналізувати загрози комп'ютерної мережі та Інтернет-протокол.

Метою статті є розробка надійної системи захисту комп'ютерної мережі на основі використання ефективних механізмів захисту та виявлення атак.

Виклад основного матеріалу

Системні та мережеві технології необхідні для широкого кола застосувань. Для мереж і програм необхідна безпека. Незважаючи на те, що безпека мережі є важливою вимогою, існує значний недолік методів безпеки, які можна легко реалізувати.

Між розробниками технологій безпеки та мережевими розробниками існує «комунікаційний розрив».

Модель інтерфейсу відкритих систем (OSI) лежить в основі проектування мережі, що є добре розробленим процесом.

Протоколи різних рівнів можна легко комбінувати, щоб утворити стеки, які дозволяють розробляти модульну систему.

Реалізація окремих шарів може бути змінена пізніше, не впливаючи на інші шари, що забезпечує гнучкість розробки.

Проектування безпечної мережі, на відміну від проектування мережі, не є добре розробленим процесом. Немає методології для вирішення складності вимог безпеки [1].

Проектування безпечної мережі не дає тих же переваг, що й проектування мережі. Безпека мережі не передбачає захисту обох кінців мережі. Канал зв'язку не повинен бути вразливим для атак під час передачі даних. Потенційний хакер може націлитися на канал зв'язку, отримати зашифровані дані, розшифрувати їх, а потім знову ввести помилкове повідомлення. Захистити середню мережу так само важливо, як захистити комп'ютери та зашифрувати повідомлення.

При проектуванні безпечної мережі необхідно враховувати такі фактори:

- Доступ – авторизованим користувачам надається можливість спілкуватися з певною мережею та з неї.
- Конфіденційність – дані в мережі залишаються конфіденційними.
- Аутентифікація – переконайтеся, що користувачі мережі є тими, за кого себе видають.
- Цілісність – переконайтеся, що повідомлення не було змінено під час передачі.
- Невідмовність – переконайтеся, що користувач не заперечує використання мережі.

Ефективний план безпеки мережі розробляється з розумінням проблем безпеки, потенційних зловмисників, необхідного рівня безпеки та факторів, які роблять мережу вразливою для атак. Існує безліч продуктів, які роблять комп'ютер менш вразливим до мережевих атак.

Прикладами цих інструментів є шифрування, брандмауери, механізми виявлення вторгнень, керування безпекою та аутентифікації.

Підприємства в усьому світі використовують комбінацію деяких із цих інструментів. «Інтранети» підключені до Інтернету та достатньо захищені від нього.

Інтернет-архітектура сама по собі керує в результаті недоліків мережі розуміння проблем Інтернет-безпеки значною мірою допомагає у розробці безпечних рішень для захисту мереж від Інтернету.

Також необхідно вивчати типи Інтернет-атак, щоб їх виявити та захистити від них. Системи виявлення вторгнень побудовані на основі найпоширеніших типів атак. При вторгненні в мережу пакети вводяться, щоб викликати проблеми з таких причин:

- Неналежне використання ресурсів
- Втручання у призначену функцію будь-якого системного ресурсу
- Отримання системних знань, таких як паролі та логіни, які можна використовувати під час наступних атак.

Безпека даних – це аспект безпеки, який дозволяє перетворювати дані клієнта в незрозумілі дані для передачі. Навіть якщо ці незрозумілі дані будуть перехоплені, для декодування повідомлення потрібен ключ. Певною мірою цей метод безпеки є ефективним.

У минулому міцна криптографія легко зламалася; однак це вже не так. Через розвиток хакерів криптографічні методи повинні постійно розвиватися, щоб залишатися на крок попереду.

Під час передачі шифрованого тексту по мережі вигідно використовувати захищену мережу. Це захистить шифрований текст, зменшуючи ймовірність того, що багато людей спробують зламати код. Захищена мережа також запобігає вставлянню в мережу несанкціонованих повідомлень.

В результаті потрібні жорсткі шифри і жорсткі мережі для атаки.

Організації використовують захищені приватні мережі або «інтранети» через занепокоєння щодо порушень безпеки в Інтернеті. Спеціальна група з розробки Інтернету IETF додала механізми безпеки до набору протоколів Інтернету на різних рівнях. Ці механізми безпеки забезпечують логічний захист одиниць даних, коли вони переміщуються по мережі. Оцінюються наслідки для безпеки поточної та нової версій Інтернет-протоколу. Хоча в протоколі існує безпека, не всі атаки захищені. Ці атаки перевіряються, щоб визначити, чи потрібні додаткові заходи безпеки.

Архітектура IP-безпеки Інтернет-протоколу є стандартизацією Інтернет-безпеки. IP-безпека, або IP-сек, відноситься як до нового покоління IP (IPv6), так і до поточної версії (IPv4). Хоча нові методи, такі як IP sec, були розроблені для усунення деяких з найбільш відомих недоліків Інтернету, їх виявляється недостатньо [2].

IPsec – це протокол «точка-точка», в якому одна сторона шифрує, інша розшифровує, і обидві сторони мають однаковий ключ або ключі (рис. 1). IPsec має два режими роботи: транспортний і тунельний режим [3].

Поширені методи Інтернет-атаки. Класифіковано найпоширеніші методи Інтернет-атаки. Деякі атаки, такі як підслуховування та фішинг, отримують знання системи або особисту інформацію. Можливі напади.

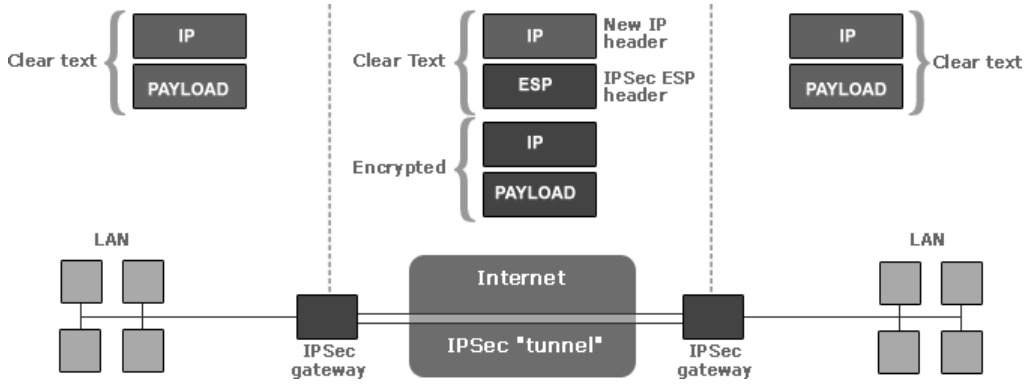

Рис. 1. Візуальне представлення реалізації IPsec для забезпечення безпечного зв'язку

Віруси, хробаки та трояни також можуть перешкоджати призначеній роботі системи. Інший тип атаки – це коли ресурси системи використовуються неефективно, що може бути викликано атакою відмови в обслуговуванні (DoS). Інші типи мережевих вторгнень включають атаки на землю, атаки серфінгу та атаки із сльозою.

Ці атаки не так відомі, як DoS-атаки, але вони все ще використовуються в тій чи іншій формі, навіть якщо вони не згадуються по імені [4]. Найбільшими загрозами безпеки комп'ютерних мереж на сьогоднішній день є:

- Віруси: віруси – це програми, що саморозмножуються, що заражають і поширюються файлами . Коли файл відкривається, вірус проникає в систему і стає активним.
- Трояни: трояни можуть здаватися користувачеві нешкідливими програмами, але насправді вони служать шкідливій меті. Трояни зазвичай переносять корисне навантаження, наприклад вірус.
- Підслуховування: підслуховування – це перехоплення комунікацій несанкціонованою стороною. Пасивне підслуховування відбувається, коли людина таємно слухає лише мережеві повідомлення. З іншого боку, активне прослуховування відбувається, коли зловмисник слухає і вставляє щось у потік комунікації. В результаті повідомлення можуть спотворюватися. Цей метод можна використовувати для викрадення конфіденційної інформації.
- Фішинг: спроба отримати конфіденційну інформацію від окремої особи, групи чи організації відома як фішинг. Фішери обманом обманюють користувачів, щоб вони розкрили конфіденційну інформацію, таку як номери кредитних карток, облікові дані онлайн-банкінгу та іншу особисту інформацію.
- Відмова в обслуговуванні: відмова в обслуговуванні – це атака, яка виникає, коли система отримує надмірну кількість запитів і не може спілкуватися з запитувачами . Під час очікування завершення рукостискання система споживає ресурси. Зрештою, система не зможе відповісти на будь-які подальші запити, що зробить її непрацездатною.
- Спуфінг IP: спуфінг означає, що адреса комп'ютера відображає адресу надійного комп'ютера, щоб отримати доступ до інших комп'ютерів. Особистість зловмисника приховується різними способами, що ускладнює виявлення та запобігання. Підроблені IP-пакети не можуть бути усунені за допомогою поточної технології протоколу IP.

Технології безпеки в Інтернеті. Інтернет-загрози залишатимуться серйозною проблемою у світовому співтоваристві, доки можна отримати доступ до інформації та її передачу через Інтернет. Для боротьби з цими атаками були розроблені різні механізми захисту та виявлення:

- Брандмауер: брандмауер – це загальний механізм контролю кордонів або захисту периметра. Метою брандмауера є блокування трафіку ззовні, але його також можна використовувати для блокування трафіку зсередини. Брандмауер - це перша лінія захисту від зловмисників. Це система, яка запобігає несанкціонованому доступу до або з приватної мережі. Брандмауери можуть бути реалізовані як в апаратному, так і в програмному забезпеченні, або в гібриді обох [5].
- Криптографічні системи. Сьогодні криптографія є цінним і широко використовуваним інструментом в інженерії безпеки. Це передбачало використання кодів і шифрів для перетворення інформації в незрозумілі дані. В результаті ці незрозумілі дані безпечно передаються по мережі.
- Secure Socket Layer: набір протоколів Secure Socket Layer (SSL) є стандартним методом для досягнення високого рівня безпеки між веб-браузером і веб-сайтом. SSL призначений для створення безпечного каналу або тунелю між веб-браузером і веб-сервером, щоб захищати будь-яку інформацію, якою обмінюється в захищеному тунелі. Завдяки використанню сертифікатів SSL дозволяє клієнтам аутентифікуватися на серверах. Щоб підтвердити свою особу, клієнти надають серверу сертифікат.
- Система виявлення вторгнень: система виявлення вторгнень (IDS) – це додатковий захід безпеки, який допомагає в попередження комп'ютерних вторгнень. Системи IDS можуть бути обидві програмні та апаратні пристрої, які виявляють атаки. IDS продукти використовуються для моніторингу з'єднань, щоб визначити, чи були запущені атаки. Деякі системи виявлення вторгнень (IDS) просто контролюють і оповіщають коли відбувається напад, тоді як інші намагаються запобігти напад.

Сфера мережевої безпеки йде по стопах своїх попередників. З додаванням біометричної ідентифікації використовуються ті ж методики. Біометрія є

більш безпечним методом аутентифікації, ніж паролі. Це може значно зменшити несанкціонований доступ до захищених систем. Програмний аспект мережевої безпеки постійно розвивається. Постійно впроваджуються нові брандмауери та схеми шифрування. Дослідження, що проводяться, допомагають зрозуміти поточні події, а також спроектувати майбутні події в цій галузі. У мережевій безпеці визначено два основних розгортання: розгортання програмного забезпечення та розгортання обладнання.

Набір програм вплине на безпеку в Інтернеті більше за все інше. У майбутньому безпека може нагадувати як імунна система. Імунна система захищає від атакує і готується протистояти більш складним ворогам.

Аналогічно, мережева безпека зможе виконувати роль імунна система. Біометричний рух, можливо, почався деякий час тому, але, судячи з усього, він не переслідується агресивно. Багато подій безпеки відбуваються всередині одного набору технології безпеки, які зараз використовуються, з мінімальними змінами. Після стількох років еволюції є деякі лазійки, тобто обхід або зміна заходів безпеки які потрібно змінити і які необхідно забезпечити. Кілька рівнів заходи безпеки можуть запобігти їм.

Висновки

Безпека мережі є важливою сферою, яка набирає обертів, оскільки Інтернет-атаки та інші різновиди загроз зростають в геометричних розмірах. Щоб оцінити необхідні зміни в техніці систем безпеки комп'ютерних мереж, були проаналізовані загрози безпеки та Інтернет-протокол. Більшість технологій безпеки базується на програмному забезпеченні, але на даний час маємо необхідно додатково використовувати апаратні засоби систем захисту.

Ефективний план безпеки мережі розробляється з розумінням проблем безпеки, потенційних зловмисників, необхідного рівня безпеки та факторів, які роблять мережу вразливою для атак. Існує безліч продуктів, які роблять комп'ютер менш вразливим до мережевих атак. Прикладами цих інструментів є шифрування, брандмауери, механізми виявлення вторгнень, керування безпекою та аутентифікації. Мережеві пристрої повинні бути стійкими до відмов та передбачати можливість швидкого відновлення. Важливо систематично виконувати моніторинг інфраструктури, щоб розуміти, в якому стані знаходиться той чи інший пристрій, додаток, сервіс і при необхідності впроваджувати засоби їх захисту. Поточний стан безпеки будь-якої мережі зовсім відносне питання, тому постійно необхідно використовувати нові підходи до безпеки, як апаратні, так і програмне забезпечення, аналізувати трафік мережі та проводити постійні інструктажі безпеки з користувачами мережі. Прогрес систем безпеки комп'ютерних мереж відбувалася не лише створенням нових концепцій та методів, а часто заключається в модифікації тих самих технологій, які вже використовуються.

Найближчим часом поєднання протоколу IPv6 та елементів безпеки, такі заходи, як брандмауери, виявлення вторгнень та процедури аутентифікації будуть успішними для захисту мереж.

СПИСОК ЛІТЕРАТУРИ

1. Грайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Грайворонський, О. М. Новіков – К.: Видавнича група BHV, 2009. – 608 с.
2. Bound (ed.), "IPv6 Enterprise Network Scenarios". IETF Internet Draft. July 2004.
3. Durand, S. Roy, and J. Paugh, "Issues with Dual Stack IPv6 on by Default". IETF Internet Draft. July 2004.
4. Михайлюта С. Л., Степанушко І. В., Бабич Б. О., Ткаченко В. Ю., Лавринович В. С. Дослідження мережевих DOS-атак, що ґрунтуються на використанні протоколу ICMP // Вісник Інженерної академії України. - К.: 2009. – № 2. – С. 146–149.
5. Вертузаєв М. С., Юрченко О. М. Захист інформації в комп'ютерних системах від несанкціонованого доступу: Навч. посібник / За ред. С. ГЛаптєва,— К.: Вид-во Європ. ун-ту, 2001.— 321 с.

Received (Надійшла) 28.02.2022
Accepted for publication (Прийнята до друку) 20.04.2022

Computer network protectionsystem

A. Yanko, R. Vyhivskyi

Abstract. This article highlights the basics of protecting information in computer systems from unauthorized access. Because network security is an important area that is gaining momentum, as Internet attacks and other threats grow exponentially. Security threats and the Internet Protocol were analyzed to assess the necessary changes in the security of computer network systems. Most security technologies are based on software, but we currently need to use additional hardware protection systems. The main factors that must be taken into account when designing a secure network are considered. The most common methods of Internet attacks and other threats in modern computer networks are analyzed. The security mechanisms for a set of Internet protocols at different levels, which provide logical protection of data units when they move on the network, have been studied. The security implications of the current and new versions of the Internet Protocol have been assessed. It also covers modern security technologies on the Internet and intrusion detection systems. The advancement of computer network security systems has not only been the creation of new concepts and methods, but often the modification of the same technologies that are already in use. In the near future, a combination of IPv6 and security features, such as firewalls, intrusion detection, and authentication procedures, will be successful in protecting networks. An effective network security plan has been developed with an understanding of security issues, potential attackers, the required level of security, and the factors that make the network vulnerable to attacks. As a result, a reliable algorithm of the computer network protection system has been developed based on the use of effective protection and attack detection mechanisms.

Keywords: security aspects, Internet attack, Internet protocol, computer network, cryptographic systems, network security, network security software, intrusion detection system.