УДК 621.39

ЗАХОДИ ДЛЯ ЗАХИСТУ ВІД АТАК ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ОРГАНІЗАЦІЙ

Пчелінцев І.С., Григоренко О.Г.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: olenagri@ukr.net

Activities for protection from the attack to ensure cybersecurity of organizations

The main types of attacks on network infrastructures of organizations and their consequences are given. These activities to protect against attacks to provide cyber security of organizations.

В роботі наведено основні типи атак на мережні інфраструктури організацій та їх наслідки. Зазначені заходи для захисту від атак для забезпечення кібербезпеки організацій.

Однією з ознак сучасного суспільства є його цифровізація на основі постійно зростаючого розвитку інформаційно-комунікаційних технологій. Згідно прогнозів Cisco, опублікованих в звіті Cisco Visual Networking Index ™ Complete Forecast, Cisco VNI, в період з 2016 по 2021 рр. число інтернет-користувачів зросте з 3,3 до 4,6 млрд, тобто 58% світового населення, світовий обсяг IP-трафіку збільшиться в 3 рази і до 2021 р досягне 3,3 зеттабайт (в 2016 р аналогічний показник становив 1,2 зеттабайт) [1]. Велика кількість даних, що передаються і зберігаються, є привабливою для кіберзлочинців, які намагаються використати кібервразливості для отримання інформації з метою особистої або фінансової вигоди. Тому забезпечення кібербезпеки в державі є стратегічним завданням.

Метою Стратегії кібербезпеки України є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави [2].

Згідно Закону «Про основні засади забезпечення кібербезпеки України» [3] кібербезпека - захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. Кіберпростір - середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних [3].

Дедалі частіше об'єктами кібератак та кіберзлочинів стають інформаційні ресурси фінансових установ, підприємств транспорту та енергозабезпечення, державних органів, які гарантують безпеку, оборону, захист від надзвичайних ситуацій. Новітні технології застосовуються не лише для скоєння традиційних

видів злочинів, але і для скоєння принципово нових видів злочинів, притаманних суспільству з високим рівнем інформатизації. [2]

Основними типами атак на мережну інфраструктуру організацій [4,5], підприємств є встановлення шкідливого програмного забезпечення, атаки через браузер та електронну пошту, атаки DoS та DDoS, Sniffing, Spoofing, Man-in-the-middle.

Шкідливе програмне забезпечення (ПЗ) порушує роботу комп'ютерів або отримує до них доступ без відому або дозволу користувача. До шкідливого програмного коду відносяться комп'ютерні віруси, черв'яки, троянські коні, програми-вимагачі, шпигунські програми, рекламне ПЗ, псевдоантивіруси та ін. Деяке шкідливе ПЗ виявити легко, проте дію іншого виявити практично неможливо.

Атака типу "Відмова в обслуговуванні" (DoS) перериває доступ користувачів, пристроїв або додатків до мережних сервісів. Така атака реалізується або через перевантаження мережі, хоста чи додатка великою кількістю трафіку, або через надсилання пакетів даних неправильного формату хосту або додатку. В першому випадку результатом є аварійне завершення роботи пристрою чи сервісу, в другому - програма не може ідентифікувати пакети, що містять помилки або неналежним чином відформатовані, і приймач припиняє роботу.

Розподілена DoS атака (DDoS) походить з декількох скоординованих джерел. Кіберзлочинець створює мережу заражених хостів – ботнет, які заражають інші хости. За допомогою спеціальної керуючої системи ботнет виконує DDoS атаку.

Аналіз трафіку (Sniffing) виконується, коли весь мережний трафік, який проходить через мережну інтерфейсну карту (NIC), аналізується кіберзлочинцями за допомогою програмного забезпечення, апаратного пристрою або їх комбінації.

Атака типу підміна (Spoofing) відбувається за рахунок використання довірчих відносин між двома системами, якщо дві системи підтримують єдину аутентифікацію. Підміна MAC-адреси відбувається, коли один комп'ютер приймає пакети даних, адресовані на MAC-адресу іншого комп'ютера. Надсилання IP-пакетів з підробленої IP-адреси джерела для маскування своєї справжньої адреси – це IP-spoofing. При ARP підміні зловмисник розсилає підроблені ARP повідомлення мережею для того, щоб зв'язати свою MAC-адресу з IP-адресою авторизованого користувача мережі. При підміні системи DNS відбувається модифікація DNS-сервера для перенаправлення певного доменного імені на іншу IP-адресу, контрольовану кіберзлочинцем.

Атака «людина посередині» Man-in-the-middle (MitM) полягає в перехопленні кіберзлочинцем повідомлень, якими обмінюються комп'ютери, щоб викрасти інформацію, яка проходить мережею. Зловмисник також може передавати підставні дані між хостами, оскільки вузли не усвідомлюють, що відбулася модифікація повідомлень. MitM дозволяє злочинцю контролювати пристрій без відому користувача.

Для забезпечення кібербезпеки в організації [4,5] потрібно запровадити наступні першочергові заходи для захисту від різноманітних атак:

Регулярне оновлення програмного забезпечення та антивірусних програм.

Налаштування міжмережних екранів для заборони будь-яких пакетів, що надходять ззовні мережі, але мають адреси, які вказують на їх походження з внутрішньої мережі. Така ситуація є незвичайною, і це вказує на те, що кіберзлочинець спробував здійснити атаку з підміною адреси.

Для запобігання DoS та DDoS атакам патчі та оновлення повинні бути актуальними, навантаження між серверними системами треба розподілити, зовнішні ICMP пакети на межі периметру треба заборонити.

Запровадження шифрування трафіку та файлів, що зберігаються, використання криптографічної аутентифікації, включення часових міток до кожної частини повідомлення.

Для запобігання встановленню аналізаторів трафіку у внутрішній мережі організації забезпечити фізичну безпеку.

Для боротьби зі спамом потрібно включення фільтрації електронної пошти, навчання користувачів щодо обережного ставлення до підозрілих електронних листів і перевірки вкладень електронної пошти перед тим, як їх відкрити, також використання фільтрів на хостах/серверах.

Для запобігання подальших атак необхідно здійснювати регулярний аналіз ризиків.

Окрім вище зазначених заходів потрібно запровадити політику безпеки організації та ознайомити з нею працівників. Важливо також пам'ятати, що забезпечення кібербезпеки – це не одноразова акція, а постійний процес, що потребує постійного вдосконалення заходів захисту, використовуючи нові розробки в галузі кібербезпеки, відстежуючи вразливості та навчаючи співробітників.

Література

1. Звіт Cisco Visual Networking Index ™ Complete Forecast/ [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/ru_ru/about/press/press-releases/2017/06-09b.html.
2. Стратегія кібербезпеки України/ [Електронний ресурс] – Режим доступу: https://zakon5.rada.gov.ua/laws/show/96/2016.
3. Закон України «Про основні засади забезпечення кібербезпеки України»/ Із змінами, внесеними згідно із Законом № 2469-VIII від 21.06.2018, ВВР, 2018, № 31, ст.241 / [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19.
4. Внимание, это кибератака: как понять, что ваша компания в зоне риска, и защититься/ [Електронний ресурс] – Режим доступу: https://delo.ua/special/vnimanie-eto-kiberataka-kak-ponjat-chto-vasha-k-348941/.
5. Палаева Л.В. Основные виды кибератак на автоматизированные системы управления технологическим процессом и средства защиты от них/ Л.В.Палаева, А.М.Хафизов, А.М.Гилязетдинова, А.Р.Вахитова, К.Н.Давыдова, Е.Р.Сиротина // Фундаментальные исследования. – 2017. – № 10-3. – С. 507-511. [Електронний ресурс] – Режим доступу: https://www.fundamental-research.ru/ru/article/view?id=41866.