АНАЛІЗ КРИТИЧНИХ РЕСУРСІВ І ПОТЕНЦІЙНИХ ЗАГРОЗ КОМП'ЮТЕРНОЇ МЕРЕЖІ

Віталій Самсон, Орест Полотай
Львівський державний університет безпеки життєдіяльності

Описано ресурси комп'ютерної мережі, які вважаються критичними і потребують особливого захисту. Також наведено перелік усіх потенційних загроз комп'ютерної мережі.
Ключові слова: комп'ютерна мережа, ресурси мережі, загрози мережі.

Describes computer network resources that are considered critical and require special protection. It also lists all the potential threats to your computer network.
Keywords: the computer network, network resources, network threats.

На сьогоднішній день існує безліч цілей забезпечення мережевої безпеки, але найбільшої уваги заслуговують три основні: конфіденційність, доступність і цілісність інформації.

Цілісність даних гарантує збереження як в разі зловмисних дій, помилок, так і випадковостей. Одне з найскладніших завдань мережевої безпеки - це забезпечення цілісності даних.

Забезпечення конфіденційності даних – це одна з основних цілей побудови інформаційної безпеки. До конфіденційної інформації можна віднести наступні дані:

- особиста інформація користувачів;
- облікові записи (імена і паролі);
- бухгалтерська інформація;
- дані про розробки і різні внутрішні документи;
- дані банківських карт.

Доступність – це одна з важливих цілей, адже, якщо користувач не може працювати з даними, який сенс говорити про їх захист. До ресурсів, які використовуються в локальній мережі відносяться:

- сервери;
- робочі пристрої;
- пристрої для забезпечення діяльності;
- дані користувачів;
- будь-які критичні дані, необхідні для роботи.

Для побудови безпеки комп'ютерної мережі потрібно розглянути загрози і перешкоди. Їх можна розділити на дві великі групи: технічні загрози і людський фактор [1].

Технічні загрози:

- комп'ютерні віруси;
- помилки в програмному забезпеченні;
- різні DoS- і DDoS-атаки;
- технічні засоби знімання інформації;
- аналізатори протоколів і прослуховують програми

Комп'ютерні віруси – це одна з найстаріших категорій небезпек, яка в чистому вигляді практично не зустрічається. Через активне застосування мережевих технологій для передачі даних, віруси все тісніше інтегруються з троянськими компонентами і мережними хробаками. На даний момент комп'ютерні віруси використовують для свого поширення чи уразливості в програмному забезпеченні, або електронну пошту.

Помилки в програмному забезпеченні полягають у тому, що через те, що програмне забезпечення для таких пристроїв як: сервери, маршрутизатори, робочі станції і т.д. написано розробниками, тобто людьми, воно не може не містити помилки. Це робить програмне забезпечення одним з найбільш вузьких місцем будь-якої мережі. Чим вище складність програмного забезпечення, тим більша ймовірність присутності в ньому помилок і

вразливостей. Для усунення даного виду вразливостей виробники програмного забезпечення регулярно випускають пакети оновлень. І необхідною умовою безпеки мережі є своєчасна установка цих оновлень.

DOS- і DDOS-атаки – DOS (Denial Of Service або відмову в обслуговуванні) – це особливий тип атак, який спрямований на виведення мережі або сегмента мережі з робочого стану. При атаках даного типу можуть використовуватися помилки в ПЗ, але в великих масштабах. Новий тип атак DDoS (Distributed Denial Of Service або розподілена атака типу відмова в обслуговуванні) – перевантажує канал трафіком і заважає проходженню інформації по каналах зв'язку, а часто і повністю блокує передачу по ним корисної інформації [3].

Технічні засоби знімання інформації – такі пристрої, як камери, клавіатурні жучки, реєстратори віброакустичних коливань і т.д. Дана категорія використовується не так часто, так як для установки пристроїв знімання інформації потрібен доступ в приміщення, де знаходяться складові мережі.

Аналізатори протоколів і «сніфери» – засоби перехоплення переданих в мережі даних. Зазвичай дані в мережі передаються у відкритому вигляді, це і дозволяє всередині локальної мережі перехопити їх зловмисникові. Деякі протоколи роботи з мережею не використовують шифрування паролів, в наслідок цього у зловмисника з'являється можливість перехопити їх для подальшого використання. Найбільш гостро ця проблема постає при передачі інформації з глобальних мереж [3].

Людський фактор:

- недбалість;
- низька кваліфікація;
- звільнені або незадоволені співробітники;
- промислове шпигунство.

Недбалість – одна з найпоширеніших категорій зловживань, таких як: недотримання інструкцій при роботі з секретною інформацією, використання несанкціонованих пристроїв для обміну інформацією в мережі і т.п. Підсумком недбалості є можливість зловмисників отримати безперешкодний доступ до ресурсів мережі.

Низька кваліфікація користувачів впливає на їх нерозуміння реальної загрози витоку інформації і т.п., а також не може визначити яку саме інформацію можна розголошувати, а яка є конфіденційною.

Звільнені і незадоволені співробітники можуть вкрасти будь-які дані для того, щоб потім продати цю інформацію або шантажувати керівництво. В особливу групу хотілося б виділити системних адміністраторів, які при звільненні або при незадоволенні умовами роботи можуть використовувати ресурси мережі в своїх цілях, в тому числі для своєї матеріальної вигоди.

Промислове шпигунство – найскладніша категорія, так як при прийомі на роботу керівництво не знає, чи є ця людина підставною особою з іншої організації, і влаштовується ця людина на роботу з метою передачі конфіденційної інформації організації, що найняла його [2].

Отже, для стабільної та ефективної роботи комп’ютерної мережі, системні адміністратори повинні враховувати всі перераховані загрози щодо найбільш важливих ресурсів мережі.

Література

1. Галатенко В.А. Основы информационной безопасности / Под ред. члена-корреспондента РАН В.Б. Бетелина – М.: ИНТУИТ.РУ «Интернет-Университет Информационных Технологий», 2003.
2. Грайворонський М. В. Безпека інформаційно-комунікаційних систем: підруч. для студ. вищ. навч. закл., які навчаються за напрямами "Безпека інформаційних і комунікаційних систем", "Системи технічного захисту інформації", "Управління інформаційною безпекою" / М. В. Грайворонський, О. М. Новіков. – К. : Вид-во BHV, 2009. – 608 с.
3. Студопедія. [Електронний ресурс]. Режим доступу з studopedia.org/4-122974.html