Тема 15. Захист інформації в комп'ютерних мережах

Захист інформації – сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умов впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам інформації.

Термін вживається в Україні для опису комплексу заходів по забезпеченню інформаційної безпеки.

Захист інформації ведеться для підтримки таких властивостей інформації:

Цілісність – неможливість модифікації інформації неавторизованим користувачем.

Конфіденційність – інформація не може бути отримана неавторизованим користувачем.

Доступність – полягає в тому, що авторизований користувач може використовувати інформацію відповідно до правил, встановлених політикою безпеки не очікуючи довше заданого (прийнятного) інтервалу часу.

15.1 Технічний захист інформації

Одним з напрямків захисту інформації в комп'ютерних системах є технічний захист інформації (ТЗІ). В свою чергу, питання ТЗІ розбиваються на два великих класи задач:

– захист інформації від несанкціонованого доступу (НСД)

– захист інформації від витоку технічними каналами.

Для забезпечення ТЗІ створюється комплекс технічного захисту інформації, що є складовою системи захисту інформації.

Під НСД звичайно розуміється доступ до інформації, що порушує встановлену в інформаційній системі політику розмежування доступу. Під технічними каналами розглядаються канали побічних електромагнітних випромінювань і наводок (ПЕМВН), акустичні канали, оптичні канали та інші.

Захист від НСД може здійснюватися в різних складових інформаційної системи:

– прикладне та системне ПЗ.
– апаратна частина серверів та робочих станцій.
– комунікаційне обладнання та канали зв’язку.
– периметр інформаційної системи.

Для захисту інформації на рівні прикладного та системного ПЗ використовуються:

– системи розмежування доступу до інформації;
– системи ідентифікації та автентифікації;
– системи аудиту та моніторингу;
– системи антивірусного захисту.

Для захисту інформації на рівні апаратного забезпечення використовуються:

– апаратні ключі.
– системи сигналізації.
– засоби блокування пристроїв та інтерфейс вводу-виводу інформації.

В комунікаційних системах використовуються наступні засоби мережевого захисту інформації:

– міжмережеві екрани (Firewall)
– системи виявлення вторгнень (Intrusion Detection System)
– засоби створення віртуальних приватних мереж (Virtual Private Network)
  – для організації захищених каналів передачі даних через незахищене середовище (Symantec Enterprise VPN, Cisco IOS VPN, Cisco VPN concentrator). Віртуальні приватні мережі забезпечують прозоре для користувача сполучення локальних мереж, зберігаючи при цьому конфіденційність та цілісність інформації шляхом її динамічного шифрування.

– засоби аналізу захищеності – для аналізу захищеності корпоративної мережі та виявлення можливих каналів реалізації загроз інформації (Symantec Enterprise Security Manager, Symantec NetRecon). Їх застосування дозволяє попередити можливі атаки на корпоративну мережу, оптимізувати витрати на захист інформації та контролювати поточний стан захищеності мережі.

Захист інформації від її витоку технічними каналами зв'язку забезпечується такими засобами та заходами:

– використання екранованого кабелю та прокладка проводів та кабелів в екранованих конструкціях;
– встановлення на лініях зв'язку високочастотних фільтрів;
– побудова екранованих приміщень («капсул»);
– використання екранованого обладнання;
– встановлення активних систем зашумлення;
– створення контрольованої зони.

15.2 Мережевий екран

Міжмережевий екран, Мережевий екран, брендмауер, фаєрвол (Firewall, буквально «вогняна стіна») – пристрій або набір пристроїв, сконфігурованих, щоб допускати, відмовляти, шифрувати, пропускати через проксі весь комп'ютерний трафік між областями різної безпеки згідно з набором правил та інших критеріїв.

Фаєрвол може бути у вигляді окремого приладу (так званий маршрутизатор або роутер), або програмного забезпечення, що встановлюється на персональний комп'ютер чи проксі-сервер. Простий та дешевий фаєрвол може не мати такої гнучкої системи налаштувань правил фільтрації пакетів та трансляції адрес вхідного та вихідного трафіку (функція редиректу).

В залежності від активних з'єднань, що відслідковуються, фаєрволи розділяють на:

– stateless (проста фільтрація), які не відслідковують поточні з’єднання (наприклад TCP), а фільтрують потік даних виключно на основі статичних правил;
– stateful (фільтрація з врахуванням контексту), з відслідковуванням поточних з’єднань та пропуском тільки таких пакетів, що задовольняють логіці й алгоритмам роботи відповідних протоколів та програм. Такі типи фаєрволів дозволяють ефективніше боротися з різноманітними DDoS-атаками та вразливістю деяких протоколів мереж.

Для того щоб задовольнити вимогам широкого кола користувачів, існує три типи фаєрволів: мережевого рівня, прикладного рівня і рівня з’єднання. Кожен з цих трьох типів використовує свій, відмінний від інших підхід до захисту мережі.

Фаєрвол мережевого рівня представлений екрануючим маршрутизатором. Він контролює лише дані службової інформації пакетів мережевого і транспортного рівнів моделі OSI. Мінусом таких маршрутизаторів є те, що ще п’ять рівнів залишаються неконтрольованими. Нарешті, адміністратори, які працюють з екрануючими маршрутизаторами, повинні пам’ятати, що у більшості приладів, що здійснюють фільтрацію пакетів, відсутні механізми аудиту та подачі сигналу тривоги. Іншими словами, маршрутизатори можуть піддаватися атакам і відбивати велику їх кількість, а адміністратори навіть не будуть проінформовані.

Фаєрвол прикладного рівня також відомий як проксі-сервер (сервер-посередник). Фаєрволи прикладного рівня встановлюють певний фізичний поділ між локальною мережею і Internet, тому вони відповідають найвищим вимогам безпеки. Проте, оскільки програма повинна аналізувати пакети і приймати рішення щодо контролю доступу до них, фаєрволи прикладного рівня неминуче зменшують продуктивність мережі, тому як сервер-посередник використовуються швидші комп’ютери.

Фаєрвол рівня з'єднання схожий на фаєрвол прикладного рівня тим, що обидва вони є серверами-посередниками. Відмінність полягає в тому, що

фаєрволи прикладного рівня вимагають спеціального програмного забезпечення для кожної мережевої служби на зразок FTP або HTTP. Натомість, фаєрволи рівня з'єднання обслуговують велику кількість протоколів.

15.3 Система виявлення вторгнень

Система виявлення атак (вторгнень) – програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу в комп'ютерну систему або мережу або несанкціонованого управління ними в основному через Інтернет. Відповідний англійський термін – Intrusion Detection System (IDS). Системи виявлення вторгнень забезпечують додатковий рівень захисту комп'ютерних систем разом з системою запобігання вторгненням (IPS – Intrusion Prevention System).

IDS можуть сповістити про початок атаки на мережу, причому деякі з них здатні виявляти раніше невідомі атаки. IPS не обмежуються лише оповіщенням, але й здійснюють різні заходи, спрямовані на блокування атаки (наприклад. розрив з'єднання або виконання скрипта, заданого адміністратором). На практиці досить часто програмно-апаратні рішення поєднують у собі функціональністъ двох типів систем. Їх об'єднання тоді називають IDPS.

Хоча і IDS, і міжмережевий екран відносяться до засобів забезпечення інформаційної безпеки, міжмережевий екран відрізняється тим, що обмежує надходження на хост або підмережу певних видів трафіку для запобігання вторгнень і не відслідковує вторгнення, які відбуваються всередині мережі. IDS, навпаки, пропускає трафік, аналізуючи його і сигналізуючи при виявленні підозрілої активності. Виявлення порушення безпеки проводиться звичайно з використанням евристичних правил та аналізу сигнатур відомих комп'ютерних атак.

15.3.1 Статичні і динамічні IDS

Статичні засоби роблять «знімки» (snapshot) середовища та здійснюють їх аналіз, розшукуючи вразливе ПЗ, помилки в конфігураціях і т.д. Статичні IDS

перевіряють версії прикладних програм на наявність відомих вразливостей і слабких паролів, перевіряють вміст спеціальних файлів в директоріях користувачів або перевіряють конфігурацію відкритих мережевих сервісів. Статичні IDS виявляють сліди вторгнення.

Динамічні IDS здійснюють моніторинг у реальному часі всіх дій, що відбуваються в системі, переглядаючи файли аудиту або мережні пакети, що передаються за певний проміжок часу. Динамічні IDS реалізують аналіз в реальному часі і дозволяють постійно стежити за безпекою системи.

15.3.2 Мережеві та системні IDS

Мережеві (Network-based IDS, NIDS) контролюють пакети в мережевому оточенні і виявляють спроби зловмисника проникнути всередину системи або реалізувати атаку «відмова в обслуговуванні». Ці IDS працюють з мережевими потоками даних. Типовий приклад NIDS – система, яка контролює велике число TPC-запитів на з'єднання (SYN) з багатьма портами на обраному комп'ютері, виявляючи, таким чином, що хтось намагається здійснити сканування TCP-портів. Мережева IDS може запускатися або на окремому комп'ютері, який контролює свій власний трафік, або на виділеному комп'ютері, прозоро переглядають весь трафік у мережі (концентратор, маршрутизатор). Мережеві IDS контролюють багато комп'ютерів, тоді як інші IDS контролюють тільки один. Прикладом мережевої IDS є Snort.

IDS, які встановлюються на хості і виявляють зловмисні дії на ньому називаються хостовими або системними IDS. Прикладами хостових IDS можуть бути системи контролю цілісності файлів, які перевіряють системні файли з метою визначення, коли в них були внесені зміни. Монітори реєстраційних файлів, контролюють реєстраційні файли, створювані мережевими сервісами і службами. Обманні системи, що працюють з псевдосервісами, мета яких полягає у відтворенні добре відомих вразливостей для обману зловмисників.

15.3.3 Аналіз сигнатур і протоколів

Аналіз сигнатур був першим методом, застосованим для виявлення вторгнень. Він базується на простому понятті збігу послідовності зі зразком. У вхідному пакеті проглядається байт за байтом і порівнюється з сигнатурою (підписом) – характерним рядком програми, що вказує на характеристику шкідливого трафіку. Такий підпис може містити ключову фразу або команду, яка пов’язана з нападом. Якщо збіг знайдено, оголошується тривога.

Другий метод аналізу полягає в розгляді строго форматованих даних трафіку мережі, відомих як протоколи. Кожен пакет супроводжується різними протоколами. Кожен протокол має кілька полів з очікуваними або нормальними значеннями. Якщо що-небудь порушує ці стандарти, то ймовірна зловмисність. IDS переглядає кожне поле всіх протоколів вхідних пакетів: IP, TCP, і UDP. Якщо є порушення протоколу, наприклад, якщо він містить несподівані значення в одному з полів, оголошується тривога.

PIDS (Protocol based IDS) являє собою систему (або агента), яка відстежує і аналізує комунікаційні протоколи з пов’язаними системами або користувачами. Для веб-сервера подібна IDS зазвичай веде спостереження за HTTP і HTTPS протоколами. При використанні HTTPS IDS повинна розташовуватися на такому інтерфейсі, щоб переглядати HTTPS пакети ще до їх шифрування і відправки в мережу.

APIDS (Application Protocol based IDS) – це система (або агент), яка веде спостереження та аналіз даних, переданих з використанням специфічних для певних програм протоколів. Наприклад, на веб-сервері з SQL базою даних IDS буде відслідковувати вміст SQL команд, що передаються на сервер.