2 Забазпечення комп'ютерної безпеки в державних, банківських та інших інформаційних системах

УДК 681.3

МІЖМЕРЕЖНІ ЕКРАНИ ЯК ОСНОВА БАГАТОРІВНЕВОГО ЗАХИСТУ ВІД ЗАГРОЗ В КОМУНІКАЦІЯХ РОЗПОДІЛЕНИХ МЕРЕЖ

Вячеслав Василенко
Національний авіаційний університет

Анотація: **Розглядаються питання захисту інформаційних ресурсів комунікаційної мережі зв'язку розподіленої обчислювальної мережі, наводиться варіант організації багаторівневого захисту ресурсів мережі, розглядаються механізми забезпечення функціональних послуг безпеки.**
Summary: **The questions of defense of informative resources of communication of DCN network are examined, the variant of organization of multilevel defense of resources of network is pointed, the mechanisms of providing of functional services of safety are examined.**
Ключові слова: **Багаторівневий захист, виявлення атак, загрози, контроль доступу, механізми безпеки, розподілена мережа, міжмережний екран.**

I Вступ

Одним із поширених методів захисту інформаційних ресурсів розподілених обчислювальних мереж (РОМ) є використання міжмережних екранів, які інтегруються в інфраструктуру РОМ і забезпечують виконання встановлених правил доступу до захищеної мережі вузлів РОМ та відслідковування протоколів і послуг із захисту, що використовуються [1].

В цьому випадку міжмережний екран є єдиною загальною точкою обміну даними кожного вузла РОМ із розподіленою мережею і використовується як бар'єр між захищеною і незахищеною мережами таким чином, що всі дані між мережами проходять безпосередньо через міжмережні екрани (МЕ). В міжмережних екранах, як правило, реалізуються механізми безпеки, які роблять цей інтерфейс безпечним і керованим. Механізми безпеки МЕ дозволяють: аналізувати дані, що проходять через нього; контролювати комунікаційне середовище і партнерів з обміну даними; регламентувати обмін даними відповідно до політики безпеки; реєструвати події, що мають відношення до безпеки.

II Осовна частина

Використання єдиної загальної точки обміну даними кожного вузла РОМ із розподіленою мережею дає декілька переваг: організація захисту є значно ефективнішою; простіша реалізація мережної політики безпеки; використовуються посилені методи автентифікації; забезпечується безпека через розподіл ресурсів; полегшується спостереження за сеансами обміну інформацією.

Основними завданнями МЕ є: контроль доступу на мережному рівні; контроль доступу на рівні користувачів; контроль доступу на рівні даних; керування правами доступу; контроль доступу на прикладному рівні; ізоляція послуг із захисту; реалізація функцій оповіщення; приховування інфраструктури мережі; конфіденційність комунікацій.

Для забезпечення захисту інформаційних ресурсів розподіленої мережі РОМ може бути реалізованим багаторівневий захист. Необхідність його реалізації обумовлюється, з одного боку, відсутністю універсальних засобів захисту, а з другого, тим, що жодний окремий компонент не може в достатній мірі захистити мережу. Для ефективного захисту необхідно використовувати множину компонентів, що сумісно працюють таким чином, що здійснення атаки буде неможливим або ускладненим.

Організація багаторівневого захисту пов'язана з визначенням периметра мережі, внутрішньої мережі і політики безпеки системи (фактор персоналу).

Периметр – це посилена границя мережі, яка може включати до свого складу: маршрутизатори (routers); міжмережні екрани (firewalls); систему виявлення атак чи вторгнень (СВА чи СВВ, IDS); пристрої віртуальної приватної мережі (ПВПМ, VPN); програмне забезпечення мережі; демілітаризовану зону (ДМЗ, DMZ) і екрановані підмережі.

Маршрутизатори здійснюють управління вхідним, вихідним трафіком та трафіком в середині мережі.

Пограничний маршрутизатор є останнім маршрутизатором перед виходом в незахищену мережу і виконує роль першого і останнього рубежу захисту мережі.

Міжмережний екран або брандмауер аналізує трафік із використанням набору правил, які дозволяють визначити можливість або неможливість передачі трафіка мережею. Область дії МЕ починається там, де закінчується область дії пограничного маршрутизатора.

Система виявлення атак дозволяє виявити і повідомити про вторгнення в мережу і про потенційно небезпечні події. Система може складатися з множини детекторів різного типу, що розміщені в найважливіших точках мережі. Детектори СВА шукають задані сигнатури критичних подій або виконують статистичний аналіз функціонування мережі і виявляють аномальні події. У разі виявлення критичних подій детектори СВА повідомляють адміністратора і/або здійснюють запис у журнал подій.

Демілітаризована зона – це підмережа, що містить ресурси загального користування і підключається до брандмауера або іншого фільтруючого пристрою, який захищає її від зовнішніх вторгнень. *Екранована підмережа* є областю, що розміщується поза МЕ. Екранована підмережа використовується для ізоляції серверів, до яких необхідно забезпечити доступ із незахищеної мережі і які використовуються користувачами внутрішньої захищеної підмережі.

Внутрішня мережа – це мережа, яка захищена периметром. Вона містить всі сервери, робочі станції та інформаційну інфраструктуру. Для забезпечення захисту внутрішньої мережі використовуються наступні пристрої "периметра": маршрутизатори для фільтрування вхідного та вихідного трафіка підмережі; внутрішні МЕ для розподілу ресурсів; проксі-брандмауери для підвищення безпеки; детектори СВА для моніторингу трафіка внутрішньої мережі. У внутрішній мережі також використовуються: персональні МЕ для посилення захисту хостів; антивірусне програмне забезпечення; посилення захисту операційної системи; керування конфігурацією системи; аудит.

Захист хоста – це процес зміни конфігурації операційної системи і додатків хоста з метою перекриття потенціальних вразливостей системи. Захист хоста є останнім рубежем оборони системи.

Управління конфігурацією – процес встановлення і підтримки визначеної конфігурації для систем і пристроїв, що входять до мережі. Управління конфігурацією – найкращий захід організації захищеної стандартної (базової) конфігурації, який призведе до зниження наслідків інцидентів до мінімуму. Управління конфігурацією дозволяє також контролювати неавторизоване встановлення програмного забезпечення.

Аудит – процес, який дозволяє контролювати стан захищеності мережі і своєчасно вносити зміни в архітектуру системи технічного захисту мережі.

Концепція багаторівневого захисту передбачає створення ефективної інфраструктури безпеки і визначає рівні та можливі механізми захисту інформаційних ресурсів мережі.

Комплекс засобів захисту комунікаційної мережі зв'язку (КМЗ) РОМ повинен забезпечувати реалізацію основних функціональних властивостей безпеки інформаційних ресурсів РОМ, передбачених вимогами Нормативних документів Системи технічного захисту інформації, таких як: конфіденційність; цілісність; доступність; спостереженість.

Нормативною базою для вибору і реалізації вимог із захисту інформації в РОМ є НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу" [3]. Профіль може бути або вибраний із профілів, описаних в [3], або визначений як упорядкована сукупність рівнів послуг згідно з вимогами зазначеного документа. Вимоги до гарантій визначаються насамперед характером (важливістю) оброблюваної інформації з обмеженим доступом і призначенням РОМ.

Як уже наголошувалося, забезпечення функціональних властивостей захищеності мережних ресурсів РОМ може досягатися шляхом використання *сукупності засобів та механізмів захисту*: маршрутизаторів, серверів доступу, міжмережних екранів, засобів криптографічного перетворення інформації, що передається відкритими каналами зв'язку, засобів контролю цілісності, засобів антивірусного захисту, систем резервного копіювання та відновлення інформації, програмних засобів централізованого керування системою захисту інформації, аудиту за станом захищеності системи і реагування на критичні події, що пов'язані зі спробами порушення встановленої власником РОМ політики безпеки.

Найбільш важливою частиною системи керування безпекою мережі є точна реалізація політики захисту мережі. Використання політики безпеки передбачає вибір, встановлення і налагодження відповідних засобів мережного захисту.

Політика захисту мережі має описувати технологію і процедури, що використовуються для моніторингу стану захисту системи. За допомогою моніторингу виявляються загрози мережі. Контроль активності в мережі може виявити спроби компрометації системи і допомагає виконати аналіз атак. Моніторинг забезпечує відповідність налагоджень засобів мережного захисту вимогам політики безпеки.

Він може включати аналіз повідомлень системних журналів маршрутизаторів периметра, брандмауерів і системи керування доступом.

Моніторинг може здійснюватися системою виявлення атак. Сенсори системи виявлення атак аналізують зміст окремих пакетів з метою виявлення наявності в мережному трафіку ознак (сигнатур) загрози або вторгнення. Якщо поведінка потоку даних є підозрілою, сенсори у реальному масштабі часу реєструють порушення політики безпеки і передають сигнал тривоги засобам управління інформаційною безпекою для своєчасного відключення порушника від мережі і недопущення подальшого розвитку атаки.

Політика захисту мережі має визначати процедури, що використовуються для аудита, тестування і підтримки захисту мережі. Аудит і тестування можуть допомогти при визначенні загального технічного стану та вразливостей мережних компонентів і всієї системи в цілому.

Використання засобів аудита і тестування є найкращим засобом перевірки ефективності існуючої інфраструктури системи захисту. В список задач, що виконуються в процесі аудита, мають включатися:

перевірка кожної нової системи, що встановлюється в мережі;

перевірка відповідності змін конфігурації мережних засобів діючої політики безпеки;

регулярні перевірки системи за допомогою додаткових автоматизованих засобів;

позапланові перевірки стану системи;

щоденні перевірки найважливіших системних файлів і файлів системного журналу;

контроль за активністю користувачів.

На основі результатів регулярних перевірок створюється загальна характеристика стану системи захисту. Такі перевірки можуть моделювати більшість варіантів проникнення порушників в систему. Також може бути уявлена і незаконна активність користувачів.

Позапланові перевірки можуть використовуватися для виявлення дій порушників, а також як тест для виявлення певних проблем захисту. Позапланові перевірки можуть використовуватися для контролю відповідності системи вимогам і стандартам політики безпеки.

Моніторинг і аудит можуть виявити слабкі місця системи захисту. На підставі результатів перевірок необхідно удосконалювати стан системи захисту, використовуючи останні поновлення програмних засобів, технічні рекомендації, нові версії існуючого програмного забезпечення, новітні технології. Безперервний контроль, супроводження і модифікація системи захисту забезпечує безпеку мережі. Основними напрямками вдосконалення системи є:

- регулярне відслідковування інформації про нові типи атак, точки вразливості;
- відслідковування інформації про нові технології захисту мереж і методи захисту обладнання і систем;
- своєчасне поновлення програмного забезпечення, “латок”, сервісних пакетів;
- поновлення політики безпеки і методів захисту інформаційних активів;
- підготовка персоналу з питань захисту інформації;
- використання нових технологій захисту, що дозволяють забезпечити наскрізний захист потоку даних між кінцевими пунктами;
- забезпечення розслідування, координації дій, документального підтвердження і необхідного оповіщення про інциденти захисту.

III Висновки

Таким чином, можливо визначити наступні основні групи задач захисту, що мають бути реалізовані комплексом засобів захисту кожного із вузлів РОМ:

захист периметра мережі вузлів РОМ;

захист віддаленого доступу до ресурсів РОМ;

захист інфраструктури мережі;

засоби антивірусного захисту мережних ресурсів вузлів;

забезпечення надійного (безперервного) функціонування КЗЗ.

*Література: **1**. Буточнов О. М., Гончар Г. В., Дерев’янко С. М., Короленко М. П. Захист інформації в комунікаційній мережі зв’язку ЄДАПС. // К.: Вісті Академії інженерних наук України. 2005, № 2, с. 37 − 58; **2**. Матов О. Я., Василенко В. С., Будько М. М Оцінка захищеності в локальних обчислювальних мережах. // К.: Вісті Академії інженерних наук України. 2005, № 2, с. 59 − 73; **3.** НД ТЗІ 2.5-005-99 “Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу”.*