# Тема 7. Технологія захисту інформації при роботі у мережі. Види загроз безпеки інформаційної системи. Методи захисту

# Технологія захисту інформації при роботі у мережі

Ризики, що виникають у наслідок помилок у програмному забезпеченні залежать від міри відкритості системи, наявності помилок у операційній системі, швидкості їх виправлення.

Засоби захисту інформаційних ресурсів:

1. Перевірка системних установок (або її незмінність з часу останньої перевірки здійснюється за допомогою програм класу «сканер безпеки». Такі програмні продукти існують для більшості ОС. До них належать:
* ASET (компонент ОС Solaris);
* KSA (для платформ NetWare и NT);
* SSS (System Security Scanner) (Unix-платформи).

Ці програми аналізують стан безпеки як зовні, так і всередині мережі.

При аналізі зовнішніх загроз тестування проводиться по глобальній мережі з використання спеціальної програми (наприклад Internet Scanner, що входить до складу System Security Scanner). При аналізі внутрішні загроз тестування проводиться з самої ОС комп’ютера, а саме здійснюється:

* перевірка прав доступу;
* перевірка прав власності файлів;
* конфігурація мережевих сервісів;
* перевіряються програми аутентифікації, (наприклад, паролі);
* перевіряється поточна конфігурація (до неї відносяться файли конфігурації, версії ПЗ, незвичайні файли перевірка небезпечних змін у системі).
1. Перевірка небезпечних змін у системі (перевіряються сліди несанкціонованого доступу до системи:
* зміна розмірів файлів;
* зміна прав доступу до файлів;
* зміна змісту окремих файлів;
* зміна в установках ресурсів користувача;
* переключення мережевого інтерфейсу в режими робота, що дозволяють передавати дані на зовнішні комп’ютери.

За результатами сканування створюється звіт.

1. Аналіз захисту мережних сервісів. Прикладами таких засобів захисту є:
* пакет програм SATAN, автор F.Venema) програма розповсюджується безкоштовно. До складу системи входять більш ніж 20 тестів для перевірки вразливості системи;
* пакет Internet Scanner SAFEsuite. Цей пакет надає можливість ідентифікувати та корегувати більш ніж 140 відомих вразливих місць та постійно спостерігати за станом безпеки мережевих технічних засобів, що працюють з TCP/IP.
1. Засоби автоматичного реагування на спроби несанкціонованого доступу. Прикладом такого засобу є продукт RealSecure компании Internet Security Systems (США). Цей інструментальний засіб призначений адміністративного управління великими обсягами мережної інформації:
* відслідковує події, що порушують безпеку системи цілодобово;
* реєструє спроби несанкціонованого доступу;
* організовує комплекс активних засобів захисту. Пакет працює під ОС SunOS, Solaris и Linux.

Вимоги до захисту інформації, що передається по мережі.

З метою захисту інформації, що передається по мережі необхідного забезпечити виконання наступних вимог:

1. Інформація, що передається по мережі повинна бути закритою, тобто повідомлення може бути прочитане тільки тим кому воно адресоване;
2. Цілісність, випадкове чи навмисне пошкодження повідомлення повинно бути виявлене при його прийомі;
3. Необхідно встановлювати аутентичність відправника (при прийомі повідомлення одночасно виявляти хто його відправив).

# Види загроз безпеки інформаційної системи. Методи захисту

У реальному світі ми багато уваги приділяємо фізичній безпеці, а у світі електронної комерції доводиться піклуватися про засоби захисту даних, комунікацій і транзакцій. Маючи справу з мережевими системами Internet та Intranet, треба пам’ятати про існування декількох можливих загроз:

* дані навмисно перехоплюються, читаються чи змінюються;
* користувачі навмисно ідентифікують себе неправильно;
* користувач одержує несанкціонований доступ з однієї мережі до іншої. Вказані загрози реалізуються через такі уразливі місця, а саме.
1. Уразливості сервісів ТСР/ІР – ряд сервісів ТСР/ІР є небезпечними і можуть бути скомпрометовані розумними зловмисниками. Особливо вразливі сервіси, що використовуються в локальних обчислювальних мережах (ЛОМ) для поліпшення управління мережею.
2. Легкість спостереження за каналами та перехоплення інформації – більшість трафіку Інтернет не зашифровано. Електронна пошта, паролі та файли, що передаються, можуть бути перехоплені при використанні легкодоступних програм. Потім зловмисники можуть використати паролі для проникнення в системи електронної комерції.
3. Відсутність політики – багато мереж можуть бути сконфігуровані через незнання так, що даватимуть можливість доступу до них з Інтернету, не враховуючи можливих зловживань. Значна кількість мереж допускає використання більшої кількості сервісів ТСР/ІР, ніж це потрібно для діяльності їх організації. Адміністратори таких мереж не намагаються обмежити доступ до інформації з комп’ютерів. Це може допомогти зловмисникам проникнути до мережі.
4. Складність конфігурування – ресурси управління доступом до мереж у хостах часто є складними в налаштуванні та контролі за ними. Неправильно сконфігуровані засоби часто призводять до неавторизованого доступу.
5. Помилки при конфігуруванні хоста або ресурсів управління доступом, які або погано встановлені, або настільки складні, що важко адмініструються.
6. Роль та важливість адміністрування системи, які часто не враховуються під час опису посадових обов’язків співробітників (більшість адміністраторів наймаються на неповний робочий день є низькокваліфікованими).
7. Слабка аутентифікація.
8. Можливість легкого спостереження за даними, що передаються.
9. Можливість легкого маскування під інших.
10. Недоліки служб ЛОМ та взаємної довіри хостів один до одного.
11. Складність конфігурування і заходів захисту.
12. Слабкий захист на рівні хостів.

При здійсненні комерційних операцій (купівлі товарів в електронних магазинах) в електронній комерції для користувача існують такі загрози:

* підміна сторінки веб-сервера електронного магазину. Основний спосіб реалізації – переадресація запитів користувача на інший сервер. Проводиться шляхом заміни записів в таблицях DNS-серверів або в таблицях маршрутизаторів. Особливо це небезпечно, коли замовник вводить номер своєї кредитної картки;
* створення помилкових замовлень і шахрайство з боку співробітників електронного магазину. Проникнення в базу даних і зміна процедур обробки замовлень дозволяє незаконно маніпулювати з базою даних. За статистикою більше половини всіх комп’ютерних інцидентів пов’язано з власними співробітниками;
* перехоплення даних, переданих в системі електронної комерції. Особливу небезпеку являє собою перехоплення інформації про кредитну карту замовника;
* проникнення у внутрішню мережу компанії і компрометація компонентів електронного магазину. Реалізація атак типу «відмова в обслуговуванні» і порушення функціонування або виведення з ладу вузла електронної комерції;
* порушення доступності вузлів електронної комерції і неправильне налаштування програмного і апаратного забезпечення електронного магазину.

У результаті всіх цих загроз компанія втрачає довіру клієнтів і втрачає гроші від недосконалих угод. У деяких випадках цієї компанії можна пред’явити позов за розкриття номерів кредитних карт. У разі реалізації атак типу «відмова в обслуговуванні» на відновлення працездатності витрачаються тимчасові і матеріальні ресурси на заміну обладнання. Перехоплення даних не залежить від використовуваного програмного і апаратного забезпечення. Це пов’язано з незахищеністю версії протоколу IP. Рішення проблеми – використання криптографічних засобів або перехід на шосту версію протоколу IP. В обох випадках існують свої проблеми. У першому випадку застосування криптографії має бути ліцензоване у відповідному відомстві. У другому випадку виникають організаційні проблеми.

Все це говорить про необхідність комплексного захисту.

Реально захист часто обмежується використанням криптографії (40-бітової версії протоколу SSL) для захисту інформації між браузером клієнта і сервером електронного магазину і фільтром на маршрутизаторі.

Комплексна система захисту повинна будуватися з урахуванням чотирьох рівнів будь-якої інформаційної системи:

* рівень прикладного програмного забезпечення (ПО), що відповідає за взаємодію з користувачем. Прикладом елементів цього рівня – текстовий редактор WinWord, редактор електронних таблиць Excel, поштова програма Outlook, браузер Internet Explorer;
* рівень системи управління базами даних (СКБД), що відповідає за зберігання і обробку даних інформаційної системи. Прикладом елементів цього рівня – СУБД Oracle, MS SQL Server, Sybase і MS Access;
* рівень операційної системи (ОС), що відповідає за обслуговування СУБД і прикладного програмного забезпечення. Приклади – ОС MS Windows NT, Sun Solaris, Novell Netware;
* рівень мережі, що відповідає за взаємодію вузлів інформаційної системи. Приклади – протоколи TCP/IP, IPS/SPX і SMB/NetBIOS.

Система захисту повинна ефективно працювати на всіх рівнях. Інакше зловмисник зможе реалізувати атаку на ресурси електронного магазину.

Небезпечні і зовнішні і внутрішні атаки. За статистикою основна небезпека виходить від внутрішніх користувачів електронного магазину (операторів системи).

Для отримання несанкціонованого доступу до інформації про замовлення в базі даних є такі можливості:

* прочитати записи БД з MS Query, який дозволяє отримувати доступ до записів багатьох СУБД за допомогою механізму ODBC або SQL-запитів;
* прочитати потрібні дані засобами самої СУБД (рівень СУБД);
* прочитати файли бази даних безпосередньо на рівні операційної системи;
* відправити по мережі пакети зі сформованими запитами на отримання необхідних даних від СУБД. Або перехопити ці дані в процесі їх передачі по каналах зв’язку (рівень мережі).

Зазвичай основна увага приділяється нижнім двом рівням – рівню мережі і операційної системи. На рівні мережі застосовуються маршрутизатори і між мережеві екрани. На рівні ОС – вбудовані засоби розмежування доступу.

Взагалі, чисто технічними засобами вирішити завдання побудови комплексної системи захисту неможливо. Необхідний комплекс організаційних, законодавчих, фізичних і технічних заходів.

Безперервний розвиток мережних технологій при відсутності постійного аналізу безпеки призводить до того, що з плином часу захищеність мережі падає. З’являються нові невраховані загрози та уразливості системи.

Є поняття – адаптивна безпека мережі. Вона дозволяє забезпечувати захист у реальному режимі часу, адаптуючись до постійних змін в інформаційній інфраструктурі. ***Складається з трьох основних елементів*** – технології аналізу захищеності, технології виявлення атак, технології управління ризиками.

***Технології аналізу захищеності*** є дієвим методом, що дозволяє проаналізувати і реалізувати політику мережевої безпеки. Системи аналізу захищеності проводять пошук уразливостей, але нарощуючи число перевірок і досліджуючи всі її рівні. ***Уразливість*** – це деяка слабкість системи безпеки, яка може стати причиною нанесення пошкоджень системі електронної комерції.

***Виявлення атак*** – оцінка підозрілих дій, які відбуваються в корпоративній мережі. ***Атакою*** називається дія деякого суб’єкта системи електронної комерції (користувача, програми, процесу тощо), що використовує вразливість комп’ютерної системи електронної комерції для досягнення цілей, які виходять за межі авторизації даного суб’єкта в комп’ютерній системі. Виявлення атак реалізується за допомогою аналізу журналів реєстрації операційної системи і прикладного ПЗ та мережного трафіку в реальному часі. Компоненти виявлення атак, розміщені на вузлах або сегментах мережі, оцінюють різні дії.

***Управлінням*** у термінології безпеки називається захисний механізм (дія, пристрій, процедура, технологія тощо), що зменшує вразливість системи електронної комерції.