План:

1. Інформація як об’єкт захисту.
2. Характеристика загроз безпеки інформації.
3. Несанкціонований доступ до інформації і його мета.
4. Порушники безпеки інформації.

**Сучасний стан інформаційної безпеки. Проблеми захисту комп’ютерної інформації**

**1 Інформація як об’єкт захисту**

Широке використання інформаційних технологій у всіх сферах життя суспільства робить досить актуальною проблему захисту інформації, її користувачів, інформаційних ресурсів, каналів передачі даних від злочинних зазіхань зловмисників.

Концентрація інформації в комп'ютерах (аналогічно концентрації готівки в банках) змушує одних усе більш підсилювати пошуки шляхів доступу до інформації, а інших, відповідно, підсилювати контроль над нею з метою захисту.

Складність створення системи захисту інформації визначається тим, що дані можуть бути викрадені з комп'ютера (скопійовані), одночасно залишаючись на місці. Цінність деяких даних полягає у володінні ними, а не в їх знищенні або зміні.

Забезпечення безпеки інформації - справа дорога, і не стільки через витрати на закупівлю або установку різних технічних або програмних засобів, скільки через те, що важко кваліфіковано визначити межі розумної безпеки і відповідної підтримки системи в працездатному стані.

Об'єктами зазіхань можуть бути як самі матеріальні технічні засоби (комп'ютери і периферія), так і програмне забезпечення і бази даних.

Кожен збій роботи комп'ютерної мережі - це не тільки моральний збиток для працівників підприємства і мережевих адміністраторів. В міру розвитку технологій електронних платежів, «безпаперового» документообігу серйозний збій локальних мереж може паралізувати роботу цілих підприємств, що приведе до відчутних збитків. Не випадково захист даних у комп'ютерних мережах стає однією із найгостріших проблем.

Забезпечення безпеки інформації в комп'ютерних мережах припускає створення перешкод для будь-яких несанкціонованих спроб розкрадання або модифікації даних, переданих у мережі. При цьому дуже важливо зберегти такі властивості інформації, як:

* доступність,
* цілісність,
* конфіденційність

Доступність інформації - здатність забезпечувати своєчасний і безперешкодний доступ користувачів до інформації, яка їх цікавить.

Цілісність інформації полягає в її існуванні в неспотвореному вигляді (незмінному стосовно деякого фіксованого її стану).

Конфіденційність - це властивість, що вказує на необхідність введення обмежень доступу до даної інформації для визначеного кола користувачів.

Для того, щоб правильно оцінити можливий реальний збиток від втрати інформації, що зберігається на комп'ютері, необхідно знати, які загрози при цьому можуть виникнути і які адекватні заходи для її захисту необхідно приймати.

2 Характеристика загроз безпеки інформації

Неправомірне перекручування, фальсифікація, знищення або розголошення конфіденційної інформації може нанести серйозні, а іноді й непоправні матеріальні або моральні втрати. У цьому випадку, досить важливим є забезпечення безпеки інформації без збитку для інтересів тих, кому вона призначена.

Щоб забезпечити гарантований захист інформації в комп'ютерних системах обробки даних, потрібно насамперед сформулювати мету захисту інформації і визначити перелік необхідних заходів, які забезпечують захист. Для цього необхідно, в першу чергу, розглянути і систематизувати всі можливі фактори (загрози), що можуть привести до втрати або перекручування вихідної інформації.

Під загрозою безпеки комп'ютерної системи розуміється подія (вплив), що у випадку своєї реалізації стане причиною порушення цілісності інформації, її втрати або заміни. Загрози можуть бути як випадковими, так і навмисними.

До випадкових загроз відносяться:

1. помилки обслуговуючого персоналу і користувачів;
2. втрата інформації, обумовлена неправильним збереженням архівних даних;
3. випадкове знищення або зміна даних;
4. збої устаткування і електроживлення;
5. збої кабельної системи;
6. перебої електроживлення;
7. збої дискових систем;
8. збої систем архівування даних;
9. збої роботи серверів, робочих станцій, мережевих карт і т.д.;
10. некоректна робота програмного забезпечення;
11. зміна даних при помилках у програмному забезпеченні;
12. зараження системи комп'ютерними вірусами;
13. несанкціонований доступ;
14. випадкове ознайомлення з конфіденційною інформацією сторонніх осіб.

Найчастіше збиток наноситься не через чийсь злий намір, а просто через елементарні помилки користувачів, що випадково псують або видаляють дані, життєво важливі для системи. У зв'язку з цим, крім контролю доступу, необхідним елементом захисту комп’ютерної інформації є розмежування повноважень користувачів. Крім того, ймовірність помилок обслуговуючого персоналу і користувачів мережі може бути значно зменшена, якщо їх правильно навчати і, крім того, періодично контролювати їх дії зі сторони, наприклад, адміністратора мережі.

Надійний засіб запобігання втрат інформації при короткочасному відключенні електроенергії - установка джерел безперебійного живлення (UPS). Різні по своїх технічних і споживчих характеристиках, подібні пристрої можуть забезпечити живлення всієї локальної мережі або окремого комп'ютера упродовж часу, достатнього для відновлення подачі напруги або для збереження інформації на магнітних носіях. Більшість UPS виконують функції ще і стабілізатора напруги, що є додатковим захистом від стрибків напруги в мережі. Багато сучасних мережевих пристроїв (сервери, концентратори і ін.) оснащені власними дубльованими системами електроживлення.

Основний, найбільш розповсюджений, метод захисту інформації і устаткування від стихійних лих (пожеж, землетрусів, повеней і т.п.) полягає в створенні і збереженні архівних копій даних.

Особливістю комп'ютерних технологій є те, що безпомилкових програм, у принципі, не буває. Якщо проект практично в будь-якій області техніки можна виконати з величезним запасом надійності, то в області програмування така надійність досить умовна, а іноді майже недосяжна. І це стосується не тільки окремих програм, але і цілого ряду програмних продуктів фірм, відомих в усім світі.

Через недоліки в програмних продуктах Microsoft, зв'язаних із забезпеченням безпеки даних у мережі Internet, «хакери» можуть захоплювати особисті ключі шифрів користувачів і діяти від їх імені.

На сьогоднішній день більше половини користувачів випробували «на собі» дію вірусів. Найбільш розповсюдженим методом захисту від вірусів дотепер залишається використання різних антивірусних програм.

Рівень зазначених загроз значною мірою знижується за рахунок підвищення кваліфікації обслуговуючого персоналу і користувачів, а також надійності апаратно-програмних і технічних засобів.

Однак найбільш небезпечним джерелом загроз інформації є навмисні дії зловмисників.

Стандартність архітектурних принципів побудови устаткування і програм забезпечує порівняно легкий доступ професіонала до інформації, що знаходиться в персональному комп'ютері. Обмеження доступу до ПК шляхом введення кодів не гарантує стовідсотковий захист інформації.

Включити комп'ютер і зняти код доступу до системи не викликає особливих утруднень: досить відключити акумулятор на материнській платі. На деяких моделях материнських плат для цього передбачений спеціальний перемикач. Також у кожного виготовлювача програми BIOS (AMI, AWARD і ін.) є коди, що мають пріоритет перед будь-якими кодами користувачів, набравши які можна одержати доступ до системи. У крайньому випадку, можна вкрасти системний блок комп'ютера або витягти жорсткий диск і вже в спокійній обстановці одержати доступ до необхідної інформації.

Загрози, що навмисно створюються зловмисником або групою осіб (навмисні загрози), заслуговують більш детального аналізу, тому що часто носять витончений характер і приводять до важких наслідків. Тому розглянемо їх докладно.

До навмисних загроз відносяться:

* несанкціонований доступ до інформації і мережевих ресурсів;
* розкриття і модифікація даних і програм, їх копіювання;
* розкриття, модифікація або підміна трафіка обчислювальної мережі;
* розробка і поширення комп'ютерних вірусів, введення в програмне забезпечення логічних бомб;
* крадіжка магнітних носіїв і розрахункових документів;
* руйнування архівної інформації або навмисне її знищення;
* фальсифікація повідомлень, відмова від факту одержання інформації або зміна часу його прийому;
* перехоплення та ознайомлення з інформацією, яка передана по каналах зв'язку тощо.

Виділяють три основних види загроз безпеки: загрози розкриття, цілісності і відмови в обслуговуванні (рис. 1.1).



Рис. 1.1 Види загроз безпеки інформації в комп’ютерних мережах

Загроза розкриття полягає в тім, що інформація стає відомою тому, кому не потрібно її знати. Іноді замість слова «розкриття» використовуються терміни «крадіжка» або «витік».

Загроза порушення цілісності - будь-яка навмисна зміна (модифікація або навіть видалення) даних, що зберігаються в обчислювальній системі або передаються з однієї системи в іншу. Звичайно вважається, що загрозі розкриття піддаються в більшому ступені державні структури, а загрозі порушення цілісності - ділові або комерційні.

Загроза відмови в обслуговуванні виникає всякий раз, коли в результаті певних дій блокується доступ до деякого ресурсу обчислювальної системи.

3 Несанкціонований доступ до інформації і його мета

Спосіб несанкціонованого доступу (НСД) - це сукупність прийомів і порядок дій з метою одержання (добування) інформації, що охороняється, незаконним протиправним шляхом і забезпечення можливості впливати на цю інформацію (наприклад: підмінити, знищити і т.п.).

При здійсненні несанкціонованого доступу, зловмисник переслідує три мети:

* одержати необхідну інформацію для конкурентної боротьби;
* мати можливість вносити зміни в інформаційні потоки конкурента у відповідності зі своїми інтересами;
* завдати шкоди конкурентові шляхом знищення матеріалу інформаційних цінностей.

Повний обсяг даних про діяльність конкурента не може бути отриманий тільки яким-небудь одним з можливих способів доступу до інформації. Від мети залежить як вибір способів дій, так і кількісний і якісний склад сил і засобів добування інформації.

4 Порушники безпеки інформації

Спроба одержати несанкціонований доступ до комп'ютерної мережі з метою ознайомитися з нею, залишити інформацію, виконати, знищити, змінити або викрасти програму або іншу інформацію кваліфікується як «комп'ютерне піратство»*.*

Для запобігання можливих загроз, фірми повинні не тільки забезпечити захист операційних систем, програмного забезпечення і контроль доступу, але і спробувати виявити категорії порушників і ті методи, які вони використовують.

У залежності від мотивів, мети і методів, дії порушників безпеки інформації можна розділити на чотири категорії:

* шукачі пригод;
* ідейні «хакери»;
* «хакери»-професіонали;
* ненадійні (неблагополучні) співробітники.



Рис. 1.2 Способи НСД до конфіденційної інформації

Шукач пригод*,* як правило, студент або старшокласник, і в нього рідко є продуманий план атаки. Він вибирає мету випадковим чином і звичайно відступає, зіштовхнувшись зі складнощами. Знайшовши діру в системі безпеки, він намагається зібрати закриту інформацію, але практично ніколи не намагається її таємно змінити. Своїми перемогами такий шукач пригод ділиться тільки зі своїми близькими друзями-колегами.

Ідейний «хакер» *-* це той же шукач пригод, але більш майстерний. Він уже вибирає собі конкретні цілі (хости і ресурси) на підставі своїх переконань. Його улюбленим видом атаки є зміна інформаційного наповнення Web-сервера або, у більш рідких випадках, блокування роботи ресурсу, що атакується. У порівнянні із шукачем пригод, ідейний «хакер» розповідає про успішні атаки набагато більш широкої аудиторії, звичайно розміщаючи інформацію на хакерському Web-вузлі.

«Хакер»-професіонал має чіткий план дій і націлюється на визначені ресурси. Його атаки добре продумані і звичайно здійснюються в кілька етапів. Спочатку він збирає попередню інформацію (тип ОС, надані сервіси і міри захисту). Потім він складає план атаки з урахуванням зібраних даних і підбирає (або навіть розробляє) відповідні інструменти. Далі, провівши атаку, він одержує закриту інформацію і, нарешті, знищує всі сліди своїх дій. Такий професіонал звичайно добре фінансується і може працювати один або в складі команди професіоналів.

Ненадійний (неблагополучний) співробітник своїми діями може спричинити стільки ж проблем (буває і більше), скільки промисловий шпигун, до того ж, його присутність звичайно складніше знайти. Крім того, йому доводиться переборювати не зовнішній захист мережі, а тільки, як правило, менш жорсткіший внутрішній. Він не такий витончений у способах атаки, як промисловий шпигун, і тому частіше допускає помилки і тим самим може видати свою присутність. Однак, у цьому випадку, небезпека його несанкціонованого доступу до корпоративним даних набагато вища, ніж будь-якого іншого зловмисника.

Перераховані категорії порушників безпеки інформації можна згрупувати по їхній кваліфікації: початківець (шукач пригод), фахівець(ідейний «хакер», ненадійний співробітник), професіонал («хакер»-професіонал). А якщо з цими групами зіставити мотиви порушення безпеки і технічну оснащеність кожної групи, то можна одержати узагальнену модель порушника безпеки інформації, як це показано на рис. 1.3.

Порушник безпеки інформація, як правило, будучи фахівцем визначеної кваліфікації, намагається довідатися все про комп'ютерні системи і мережі, зокрема, про засоби їх захисту. Тому модель порушника визначає:

* категорії осіб, у числі яких може виявитися порушник;
* можливі цілі порушника і їх градації по ступені важливості і небезпеки;
* припущення про його кваліфікації;
* оцінка його технічної озброєності;
* обмеження і припущення про характер його дій.

Діапазон спонукальних мотивів одержання доступу до системи досить широкий: від бажання випробувати емоційний підйом під час гри з комп'ютером до відчуття влади над ненависним менеджером. Займаються цим не тільки новачки, що бажають побавитися, але і професійні програмісти. Паролі вони добувають, або в результаті підбору або здогадування, або шляхом обміну з іншими «хакерами».

Частина з них, однак, починає не тільки переглядати файли, але і виявляти інтерес саме до їх змісту, а це вже являє серйозну загрозу, оскільки в даному випадку важко відрізнити звичайну цікавість від злочинних дій.



Рис. 1.3 Модель порушника безпеки інформації.

Донедавна викликали занепокоєння випадки, коли незадоволені керівником службовці, зловживаючи своїм положенням, псували системи, допускаючи до них сторонніх або залишаючи системи без догляду в робочому стані. Спонукальними мотивами таких дій є:

* реакція на догану або зауваження з боку керівника;
* невдоволення тим, що фірма не оплатила понаднормові години роботи (хоча найчастіше понаднормова робота виникає через неефективне використання робочого часу);
* злий намір у якості, наприклад, реваншу з метою послабити фірму як конкурента якої-небудь новоствореної фірми.

Професійні «хакери» - це комп'ютерні фанати, що прекрасно знають обчислювальну техніку і системи зв'язку. Вони затратили масу часу на обмірковування способів проникнення в системи і ще більше, експериментуючи із самими системами. Для входження в систему професіонали найчастіше використовують деяку систематичність та експерименти, а не розраховують на удачу або інтуїцію. Їх мета - виявити і перебороти захист, вивчити можливості обчислювальної установки і потім вийти з неї, довівши можливість досягнення своєї мети.

До категорії хакерів-професіоналів звичайно відносять наступних осіб:

* таких, що входять у злочинні угруповання, які переслідують політичні цілі;
* прагнучих одержати інформацію з метою промислового шпигунства;
* «хакер» або угруповання «хакерів», що прагнуть до наживи.

Сьогодні, зі стрімким розвитком Internet, «хакери» стають справжньою загрозою для державних і корпоративних комп'ютерних мереж. Так, за оцінками експертів США, напади «хакерів» на комп'ютери і мережі федеральних державних систем відбуваються в цій країні не рідше 50-ти раз на день. Багато великих компаній і організації піддаються атакам кілька разів у тиждень, а деякі навіть щодня. Виходять такі атаки не завжди ззовні, 70% спроб зловмисного проникнення в комп'ютерні системи мають джерело всередині самої організації.

**Література**

1. Соколов А.В., Степанюк О.М. Защита от компьютерного терроризма. Справочное пособие. – СПб.: БХВ – Петербург; Арлит 2002. – 496 с.;
2. Баранов В М. и др. Защита информации в системах и средствах информатизации и связи. Учебное пособие. – СПб.: 1996. – 111 с.
3. Мельников В.В. Защита информации в компьютерных системах. М.: Финансы и статистика. – 1997. – 364 с.