МІНІСТЕРСТВО ОСВІТИ І НАУКИ,

МОЛОДІ ТА СПОРТУ УКРАЇНИ

МІЖНАРОДНИЙ ЕКОНОМІКО-ГУМАНІТАРНИЙ

УНІВЕРСИТЕТ ІМЕНІ АКАДЕМІКА

СТЕПАНА ДЕМ'ЯНЧУКА

М.М.ЛІСНЕВСЬКИЙ

ТЕХНОЛОГІ КОМП'ЮТЕРНОЇ БЕЗПЕКИ

Книга 2

Науковий керівник:

Р.М.Літнарович, доцент,к.т.н.

Рівне – 2012

УДК 614.2

Лісневський М.М. Технології комп'ютерної безпеки. Монографія. Книга 2. Науковий керівник Р.М.Літнарович. МЕГУ, Рівне, 2012.-100 с. Lisnevskiy M.M. Technologies of computer safety. Monograph. Book 2. Scientific leader R.M. Litnarovich. IEGU, Rivne, 2012.-100 p.

Рецензенти: В.Г.Бурачек, доктор технічних наук, професор
Є.С. Парняков, доктор технічних наук, професор
В.О.Боровий , доктор технічних наук, професор
Відповідальний за випуск: Й.В. Джунь, доктор фізико-математичних наук, професор

Послідовно розглядаються основні поняття побудови сучасних технологій комп'ютерної безпеки. Монографія містить актуальний матеріал довідково-аналітичного характеру по наступних темах: основи безпеки даних в комп'ютерних системах, ідентифікація і аутентифікація користувачів, захист даних від несанкціонованого доступу, основи захисту даних від комп'ютерних вірусів, основи криптографії, криптографічні методи захисту інформації, стандарти захисту інформації.

Ключові слова: комп'ютерна безпека, інформаційна безпека, захист, інформація.

Последовательно рассматриваются основные понятия построения современных технологий компьютерной безопасности. Монография содержит актуальный материал справочно аналитического характера по следующим темам: основы безопасности данных в компьютерных системах, идентификация и аутентификация пользователей, защита данных от несанкционированного доступа, основы защиты данных от компьютерных вирусов, основы криптографии, криптографические методы защиты информации, стандарты защиты информации.

Ключевые слова: компьютерная безопасность, информационная безопасность, защита, информация.

The basic concepts of construction of modern technologies of computer safety are consistently examined. A monograph contains aktual material certificate analytical character on the followings themes: bases of safety of information in the computer systems, authentication and authentification of users, protection of data from an unauthorized division, bases of protection of data from computer viruses, bases of cryptography, cryptographic methods of priv, standards of priv.

Keywords: computer safety, informative safety, defence, information

Мечислав Миколайович Лісневський, спеціаліст системотехнік, магістрант інформаційних технологій

ЗМІСТ

ВСТУП

В даний час дуже широко використовується термін "комп'ютерна безпека". Насправді комп'ютер схильний лише кільком ризикам, якщо він по мережі не підключений до інших комп'ютерів. За останній час відсоток використання комп'ютерних мереж (особливо Інтернету) значно виріс, тому сьогодні термін "комп'ютерна безпека" використовується для опису проблем, пов'язаних з мережевим використанням комп'ютерів і їх ресурсів. Основними технічними складовими комп'ютерної безпеки є:

- Конфіденційність;

- Цілісність;

- Аутентифікація;

- Доступність.

Для розуміння сутності комп'ютерної безпеки необхідно дати визначення всім перерахованим вище її компонентів:

- *Конфіденційність*, також відома як секретність, означає, що у неавторизованих користувачів не буде доступу до вашої інформації. Наслідки, які можуть бути викликані прогалинами в конфіденційності, можуть варіюватися від незначних до руйнівних.

- *Цілісність* означає, що ваша інформація захищена від неавторизованих змін, що не відноситься до авторизованих користувачам. Загрозу цілісності баз даних і ресурсів, як правило, представляє хакерство.

- *Аутентифікація* - це сервіс контролю доступу, який здійснює перевірку реєстраційної інформації користувача. Іншими словами це означає, що користувач - це є насправді той, за кого він себе видає.

- *Доступність* означає те, що ресурси доступні авторизованим користувачам.

Іншими важливими компонентами, яким велика увага приділяється професіоналами в області комп'ютерної безпеки, є контроль над доступом і суворе виконання зобов'язань. Контроль над доступом увазі не тільки факт, що користувач має доступ тільки до наявних ресурсів і послуг, але й той факт, що у нього є право доступу до ресурсів, які він законно очікує.

Що стосується суворого виконання зобов'язань, то це має на увазі неможливість відмови користувачам того, що він відправив повідомлення і навпаки.

Концепція комп'ютерної безпеки дуже велика, тому до даних технічним аспектам є й інші додатки. Коріння комп'ютерної безпеки закладені в дисципліні. Основними питаннями, пов'язаними з цим терміном, є комп'ютерний злочин (спроби запобігти, виявити атаки) та конфіденційність / анонімність в кіберпросторі.

Хоча конфіденційність, цілісність, аутентифікація є важливими компонентами комп'ютерної безпеки, для користувачів Інтернету найбільш важливою складовою є конфіденційність, тому що більшість користувачів думають, що їм нема чого приховувати або інформація, яку вони надають при реєстрації на сайті, не є секретною.

Потрібно пам'ятати, що в Інтернеті інформація дуже швидко поширюється серед компаній і потроху зібрана інформація з різних джерел може багато чого сказати про людину. Тому можливість контролю інформації, для чого вона збирається, хто і як може нею

скористатися є дуже серйозним і важливим питанням в контексті комп'ютерної безпеки.

Мережа і забезпечення її безпеки вимагає не тільки постійної роботи, але і особливої уваги, яку слід приділяти дрібницям. В той час, коли погроз немає і вся система працює в штатному режимі, постійна робота з мережею включає прогнозування можливих ходів недоброзичливців, формування і створення різних мерів захисту, і, що важливо, - навчання користувачів, яке повинне здійснюватися постійно. В тому випадку, якщо вторгнення в систему недоброзичливців відбулося, то системний адміністратор, що відповідає за безпеку, повинен виявити «слабку ланку» системи захисту, а так само визначити причину проникнення і те, яким чином це відбулося. Для формування політики безпеки першою дією, яку повинен зробити адміністратор, буде так звана інвентаризація наявних ресурсів, які і мають бути захищені. Фахівець здійснює ідентифікацію всіх користувачів мережі, організовує їм доступ до наявних ресурсів, а так само аналізує можливі джерела небезпеки, які загрожують кожному з наявних ресурсів. Оперуючи всією зібраною інформацією, стає можливим починати створення політики безпеки, дотримувати яку зобов'язані всі користувачі без виключення.

Потрібний за якістю рівень безпеки мережі обов'язково повинен включати наступні аспекти:

- **ризик і його оцінка**. Простіше кажучи - виявлення предмету захисту (що захищаємо і від кого). Цей аспект має на увазі виявлення цінностей, розташованих в мережі і знаходження потенційних джерел риски;

- **відповідальність**. Всі рішення по ухваленню тих або інших дій стосовно політики безпеки (будь то нові облікові записи, або виявлення порушників) повинні здійснюватися відповідальними особами, яких і необхідно вказати;

- **мережеві ресурси і правила їх використання**. У зведенні правил політики безпеки обов'язково мають бути присутніми (у очевидній формі) пояснення, які б показали користувачеві, що він має права робити, а що ні. Наприклад, використання ресурсів мережі в особистих цілях і вживання інформації не за призначенням - не допускається;

- **аспекти юридичного характеру**. Необхідно заручитися підтримкою грамотного юриста, яка б дозволила відповісти на всі питання про інформацію, що зберігається або оброблюваній в мережі. Всі отримані відомості обов'язково мають бути включені в документи про політику безпеки мережі;

- **відновлення системи безпеки і всі супутні процедури**. Слід точно позначити дії, які мають бути прийняті у разі порушення системи захисту. Плюс до цього мають бути визначені заходи, які будуть прийняті на аресу тих, хто став винуватцем порушення, що відбулося.

1. КЛАСИФІКАЦІЯ ВИДІВ ВТОРГНЕННЯ

Залежно від мети вторгнення, існує можливість визначити їх класи, які діляться на п'ять основних типів:

- **апаратні засоби**. Сервери, робочі станції, периферійні пристрої (принтери, сканери), мережеві кабелі і різноманітні дискові накопичувачі. У тому числі і мережеве устаткування: комутатори, маршрутизатори, мости;

- **програмне забезпечення**. То або інше програмне забезпечення, встановлене на будь-якому з комп'ютерів, який

включений в мережу, може стати можливим «ключем» для проникнення недоброзичливця. І не має значення, чи куплені ці програми у сторонніх розробників, або створені власним IT-відділом. Важливо відзначити, що операційні системи, що є базою для роботи всіх необхідних програмних продуктів, потребують регулярного оновлення (установка «патчів»);

- **інформація**. Найважливішою цінністю володіють дані, операція якими відбувається в комп'ютерній мережі. Якщо будь-яке програмне забезпечення і самі операційні системи можна відновити (або переустановити), то цілісність даних, як правило, не підлягає відновленню. Наприклад, список клієнтів, що потрапив до рук недоброзичливців, може вилитися в справжню катастрофу для всього бізнесу;

- **люди**. Користувачі, що працюють в єдиній мережі, завжди знаходяться в зоні риску.

- **документи**. Статистика показує, що різні паролі, дані і конфіденційну інформацію дуже часто переносять на паперовий носій (роздрук, записи на листах паперу і багато що інше). І, як правило, рано чи пізно вся подібна «паперова» інформація потрапляє в сміття і просто викидається. Недоброзичливець може цим скористатися і оволодіти закритою для нього інформацією. Слід знати, що будь-які паперові носії, перш ніж бути викинуті, мають бути знищені. Наприклад, за допомогою спеціального утилізатора паперу.

Політика безпеки, яку дійсно можна назвати хорошою і ефективною повинна, перш за все, бути зрозуміла всім користувачам. Проте, не все так просто, адже далеко не всі можуть все зрозуміти досконало. Для вирішення цієї проблеми рекомендується проводити постійні повторні ознайомлення робочого персоналу з наявною політикою безпеки. Це може бути виконано не тільки на спеціальних інструктажах, але і

безпосередньо на самому робочому місці. І найголовніше - не розцінювати подібні дії як просту формальність. Користувачі повинні розуміти всю узяту на себе відповідальності і сприяти збереженню інформації.

1.1. Безпека з фізичної точки зору

Несанкціонований доступ, а точніше його запобігання - це, перш за все, фізичне блокування доступу до мережі, що захищається. Плюс позбавлення доступу до комп'ютерів і серверів мережі, кабелів повідомлень і різних периферійних пристроїв. У тому випадку, коли мережа і підключення до неї виходять за рамки контрольованої зони (наприклад, вихід в інтернет через провайдера), необхідні особливі заходи, такі як організація віртуальних тунелів або шифрування. На додаток до цього, все устаткування, яке так чи інакше бере участь в обміні даними, повинне завжди знаходитися під контролем.

Всі сервери і сховища даних повинні знаходитися в закритих приміщеннях. У них повинні мати доступ тільки компетентні особи із строгим рівнем допуску. Подібними заходами захисту мають бути забезпечені і пристрої функціонування мережі (концентратори, маршрутизатори і інші пристрої). Всі комп'ютери повинні знаходитися в приміщеннях, що закриваються на замок, за якими здійснюватиметься спостереження. Існує багато способів організації контролю і спостереження за приміщеннями, наприклад - реєстраційний журнал і вказівка в нім всіх відвідувачів. Різні резервні копії даних, розміщені на носіях (лазерні диски, стрічки,

касети), повинні зберігатися в закритих місцях без загального доступу, наприклад - в сейфах.

1.2. Застарілі комп'ютери і їх утилізація

Достатньо часто парку обчислювальної техніки може потрібно комп'ютерна допомога. Ремонт, відновлення і багато інших операцій повинні проводитися тільки компетентними фахівцями. Проте, не рідкісні і ті випадки, коли необхідна модернізація устаткування (комп'ютери, сервери, сховища даних), або ж повна заміна застарілої техніки на нову. Все «списане» устаткування, як правило, передається в користування стороннім організаціям (комп'ютерні клуби, школи і інше). Будь-яка політика безпеки, організована на підприємстві або організації, повинна містити жорсткі правила по знищенню даних, які раніше або зараз представляють конфіденційність. Зрозуміло, подібні дії мають бути проведені зі всіма жорсткими дисками і іншими накопичувачами інформації списуваної техніки, щоб виключити ризик розповсюдження конфіденційної інформації. Так само мають бути описані алгоритми утилізації носіїв інформації з резервними копіями важливих даних. У багатьох випадках буде незамінна процедура фізичного знищення подібних носіїв. Це буде хорошим гарантом, який повністю виключить «просочування» конфіденційної інформації.

1.3. Програмний доступ до інформації

Окрім фізичного обмеження доступу до мережі слід прийняти заходи по програмному обмеженню. Проте, як показує статистика,

як би добре не була побудована система подібного обмеження, завжди відшукається людина, яка буде здатна її обійти. Отже, необхідно мати засоби контролю і спостереження за всіма подіями, що відбуваються в мережі і, у разі потреби, зуміти визначити вторгнення і його глибину.

Мають місце декілька алгоритмів управління мережевим доступом:

- захист ресурсів;
- ідентифікація на фізичному рівні;
- паролі і облікові записи користувачів.

Такий елемент як володіння ресурсами в багатьох операційних системах є ключовою ланкою політики безпеки. Так, наприклад, серверні операційні системи від компанії Microsoft (Windows 2000/2003) мають інструменти по відстежуванню дій користувачів, які контактують з тими або іншими ресурсами (наприклад, файли). Творці файлів мають безліч засобів вплинути на їх захист: обмежити доступ, заборонити його і багато що інше. Операційні системи Unix/linux так само мають подібні інструменти, хоч і відрізняються ними від MS Windows.

1.4. Користувачі і їх ідентифікація

В тому випадку, якщо які-небудь особливо секретні дані не зберігаються в мережі, то для їх доступу, а так само для доступу до інших ресурсів достатньо лише логіна і пароля. Подібна система проста і у багатьох випадках є оптимальним рішенням. Операційні системи Windows 2000/2003/xp дозволяють створювати так звані

домени, які є відособленими зонами управління зі встановленим рівнем захисту. Системний адміністратор може дуже гнучко управляти правами доступу домена, вирішуючи або забороняючи доступ конкретним користувачам не тільки на рядові обчислювальні машини, але і на сервер (сервери). Так само, можливі і такі дії, як довірчі стосунки між декількома доменами, де системні адміністратори можуть вирішити доступ для користувачів до ресурсів інших доменів. Подібні дії вимагають дозволів на рівні облікових записів і співпраці відповідальних осіб (системних адміністраторів). Серверні операційні системи Microsoft (Windows 2000/2003 і пізніші) підтримують групові політики безпеки, що надзвичайно ефективно дозволяє оперувати правами доступу до важливих ресурсів.

Для вирішення подібних завдань в Novell Netware використовується спеціальна служба Novel Directory Services. Кожен користувач отримує унікальне реєстраційне мережеве ім'я і представляється в певному каталозі об'єктом User. У даному об'єкті розташовується все інформація про користувача, будь то логін, з'єднання і інше.

Unix і подібні операційні системи не містять в своїй структурі доменних систем. Замість цього, кожен хост системи містить так званий файл паролів, де присутня інформація про всіх користувачів, у тому числі і їх паролі в зашифрованому вигляді. Так, наприклад, для доступу до інших мережевих ресурсів, користувач Unix повинен використовувати проксі, або ж пройти реєстрацію на комп'ютері іншої частини мережі, що відноситься до необхідних ресурсів. Варто пам'ятати, що такі мережеві утиліти, як FTP і Telnet можуть пересилати ідентифікаційну інформацію користувачів відкритим текстом без якого-небудь шифрування, а значить - можуть стати об'єктом уваги для недоброзичливців.

Звичайні мережеві операції (друк файлів, їх копіювання), а так само реєстрація на якій-небудь видаленій системі в операційній системі Unix виконується утилітами видаленої роботи. Зазвичай,

вони називаються «r-командами», де їх імена завжди починаються з букви «r».

Утиліти подібного класу надзвичайно ефективні в мережевому середовищі, якщо одному користувачеві доводиться здійснювати роботу на декількох обчислювальних машинах мережі. Проте, враховуючи той факт, що для виконання тієї або іншої команди на видаленому комп'ютері користувачеві цілком досить мати обліковий запис, то це може викликати проблеми із загальною безпекою системи.

Файл /etc/hosts.equiv, або ж .rhosts, а точніше запис в нім визначає права доступу. Комп'ютер, до якого виконується видалене підключення, «довіряє» тому комп'ютеру з якого виконується r-команда. Якщо комп'ютер знаходить відповідний запис в даному файлі, то вирішує доступ до запрошуваних ресурсів. Кожен із записів файлу /etc/hosts.equiv дозволяє ідентифікувати користувача, оскільки містить його ім'я і хост, які мають повноваження на виконання необхідної команди. Саме з цієї причини зовсім не обов'язковий пароль. Простіше кажучи, якщо користувач має реєстрацію на видаленому комп'ютері, то аутентифікація їм вже пройдена. Файл .rhosts розташовується в «домашньому» каталозі користувача і має такий самий алгоритм роботи. Вся робота видалених користувачів (їх доступ і права) грунтуються на записах наявних в цьому файлі.

В наші дні, в операційних системах Unix і Linux з'явилися спеціальні утиліти Secure Shell (утиліти захисної оболонки), які хоч і схожі по своєму дії з r-командами, але відрізняються від них наявністю шифрування і спеціальними алгоритмами аутентифікації.

Дані алгоритми безпеки системи мають схожість з довірчими стосунками, реалізованими в Windows Nt/2000/server 2003/xp, проте механіка їх роботи все ж таки різна. Так, наприклад, в системі Unix/linux недоброзичливець достатньо легко може представитися

видаленим комп'ютером і за допомогою r-команд дістати доступ до інформації, що захищається.

На серверах Windows здійснюються різноманітні фонові процеси, які виконують строго певні функції. Вони називаються службами. Операційні системи Unix так само мають схожі інструменти, які виконують подібну роботу і називаються «демонами». Всі дані процеси, як правило, виконуються автоматично і без інформування про це користувача. В деяких випадках вони можуть стати винуватцями порушень системи захисту.

Слідує чітко знати всі основні фонові процеси операційних систем і уміти оперувати з ними. Так, наприклад, в системах Unix існують певні демони, які так чи інакше стосуються роботи мережевих протоколів Tcp/ip. Можливі такі випадки, коли вони можуть негативно позначитися на безпеці всієї системи. Їх можна відключити і тим самим вирішити багато проблем.

Наприклад, служба tftp є спрощеною моделлю FTP. Дана спрощена служба відрізняється своєю компактністю і легкістю реалізації в апаратних засобах комп'ютера (перепрограмований ПЗП). У багатьох випадках використання цієї служби достатнє ефективно, але ця служба не має доступу до механіки (в порівнянні з FTP), що управляє, і не оперує обліковими даними користувача (логін і пароль). Враховуючи, що аутентифікації як такий немає, можуть виникнути серйозні проблеми з безпекою всієї системи.

Сервери, що працюють під управлінням операційних систем Windows, мають в своєму розпорядженні дві утиліти з набору Resource Kit, які дозволяють запускати практично будь-які програми у фоновому режимі. Одна з них - це INSTRV.EXE, яка встановлює виконувані програми. А друга - SRVANY.EXE, яка перетворює необхідну програму на службу.

Слід зазначити, що окрім технічного обслуговування обчислювальної техніки, будь то ремонт комп'ютерів і їх своєчасна

модернізація, слід розробити чітку концепцію корпоративної безпеки.

1.5. Елементи корпоративної безпеки

Основна мета: забезпечити надійні гарантії по правильному використанню обчислювальною технікою і телекомунікаційних ресурсів «Компанії» штатом її співробітників і іншими користувачами.

Всі користувачі зобов'язані оперувати обчислювальним засобам з урахуванням всіх норм і правил, і тим самим здійснювати на ній ефективну роботу. Дана політика безпеки стосується всіх користувачів обчислювальних машин, телекомунікаційних ресурсів і служб. Порушення політики безпеки може стати причиною дисциплінарної дії, звільнення і/або порушення кримінальної справи. В міру необхідності дана політика безпеки може видозмінюватися і переглядатися. Перевірку комп'ютерної системи

мають право здійснювати керівники компанії. Під їх компетентність потрапляє електронна пошта і багато інших інтерфейсів обміну даними. Подібна перевірка здійснюється з метою гарантувати повне дотримання всіх норм встановленої політики безпеки. Телекомунікаційна і обчислювальна системи є власністю Компанії і можуть бути використані тільки у вирішенні строго робочих завдань. Штат співробітників Компанії не повинен розраховувати на конфіденційність тієї інформації, яку вони створюють, відправляють або отримують за допомогою обчислювальних і комунікаційних засобів, що належать Компанії. Всім користувачам комп'ютерів Компанії належить керуватися приведеними нижче заходами безпеки і правилами, які стосуються обчислювальної техніки і телекомунікаційних ресурсів. Всі програмні ліцензії мають бути строго дотримані користувачами. Мають бути враховані авторські права і закони, що підкріплюють інтелектуальну власність. Будь-яку інформацію, що є невірною, непристойною, образливою, загрозливою або протизаконною, забороняється зберігати, отримувати або передавати за допомогою електронних ліній зв'язку (будь то електронна пошта або багато що інше), що належать Компанії. Будь-яка інформація, створена на комп'ютерах Компанії, будь то файли або листи електронної пошти, може бути проаналізована і вивчена керівниками Компанії. Програмне забезпечення, яке не отримало дозвіл на установку у системного адміністратора, не може бути встановлене на комп'ютери Компанії. Забороняється пересилка будь-якої інформації, без дозволу на те її власників. Будь-яка електронна кореспонденція від юриста Компанії або адвоката, що представляє її, повинна містити на кожній сторінці (у колонтитулі) позначку: "Захищено адвокатським правом/без дозволу не пересилати". Користувачі не мають права змінювати або копіювати яку-небудь інформацію (без відповідного не те дозволи), що належить іншим користувачам. Без особливого попереднього дозволу забороняється зберігати на комп'ютерах Компанії яку-небудь сторонню комерційну інформацію, будь то оголошення, рекламні матеріали і так далі. Так само, забороняється зберігання і

пересилка шкідливих програм - вірусів. Користувач несе відповідальність за власний обліковий запис і інформацію, що ідентифікує його (наприклад, особистий пароль на вхід в систему). Так само, забороняється роздруковувати подібну інформацію паперові носії і зберігати її в загальних мережевих ресурсах. Можливість входу в інші комп'ютерні мережі не дає користувачам права на підключення і взаємодію з цими мережами без наявності відповідного на те дозволу адміністратора.

2. ПРЕДМЕТ І ОБ'ЄКТ ЗАХИСТУ

2.1. Предмет захисту інформації

Питання інформаційної безпеки займають особливе місце і в зв'язку з віком-тане роллю в житті суспільства вимагають до себе все більшу увагу. Успіх практи-но будь-якої діяльності в чималому ступені залежить від уміння розпоряджатися такий цінністю, як інформація.

- «Інформаційні ресурси є об'єктами власності громадян, організацій , громадських об'єднань, держави »;
- «Інформація - відомості про осіб, предмети, події, явища і процеси (не-залежно від форми їх подання), відображені на матеріальних носіях, викори-зуемих з метою отримання знань і практичних рішень ».

Інформація має ряд особливостей:

- Не матеріальна;

- Зберігається і передається за допомогою матеріальних носіїв;

- Будь-який матеріальний об'єкт містить інформацію про самого себе або про інше об'єкті.

Інформація притаманні такі властивості:

Цінність інформації визначається ступенем її корисності для власника.

Конфіденційність інформації - суб'єктивно визначається (приписувана)характеристику (властивість) інформації, яка вказує на необхідність введення обмеження навколо суб'єктів, що мають доступ до цієї інформації, і забезпечувана здатністю системи (середовища) зберігати вказану інформацію в таємниці від суб'єктів, не мають повноважень доступу до неї. Об'єктивні передумови подібного обмеження доступності інформації для одних суб'єктів укладені в необхідності захисту їх законних інтересів від інших суб'єктів інформаційних відносин.

Державну таємницю можуть містити відомості, що належать державі (державній установі).

Достовірність інформації визначається достатньою для власника точністю відображати об'єкти і процеси навколишнього світу в певних тимчасових і просторових рамках. Інформація, викривлено представляє дійсність, яка може завдати власникові значний матеріальний і моральний збиток. Якщо інформації спотворена умисно, той її називають дезінформацією.

Предметом захисту є інформація, що зберігається, обробляється і передана в комп'ютерних (інформаційних) системах.

3. КЛАСИФІКАЦІЯ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

- Некомпетентне використання, класифікація всіх можливих загроз інформаційної безпеки АС може бути проведена по ряду базових ознак.

1. За природою виникнення.

Природні загрози - загрози, викликані впливами на АС та її компонентиоб'єктивних фізичних процесів або стихійних природних явищ, незалежних від людини.

Штучні загрози - загрози інформаційної безпеки АС, викликані деятельностью людини.

2. За ступенем навмисності прояви.

Загрози випадкового дії та загрози, викликані помилками або халатністю персоналу. Загрози, не пов'язані з навмисними діями зловмисників і реалізовані у випадкові моменти часу, називають випадковими . Класифікація за цією ознакою наведена на рис. 2.1.

- прояв помилок програмно-апаратних засобів АС;

-настроювання або не правомірне відключення засобів захисту персоналом служби безпеки;

- Ненавмисні дії, що призводять до часткового або повної відмови системи або руйнування апаратних, програмних, інформаційних ресурсів системи (не навмисне псування обладнання, видалення, спотворення файлів з важливою інформацією або програм, у тому числі системних і т.п.);

- Неправомірне включення устаткування або зміна режимів роботи устройств і програм;

- Ненавмисне псування носіїв інформації;

- Пересилання даних по хибному адресою абонента (пристрої);

- Введення помилкових даних;

- Ненавмисне пошкодження каналів зв'язку.

Загрози навмисного дії, наприклад:

- Традиційне або універсальне шпигунство і диверсії (підслуховування, візуальне спостереження; розкрадання документів і машинних носіїв, розкрадання програм і атрибутів системи захисту, підкуп і шантаж співробітників, збір і аналіз відходів машинних носіїв, підпали, вибухи); Реалізація загроз цього класу призводить до найбільших втрат інформації (до 80% Збитку). При цьому може відбуватися знищення, порушення цілісності, доступ-ності та конфіденційності інформації.

4. МОДЕЛЬ ПОШИРЕННЯ ПРАВ ДОСТУПУ TAKE-GRANT

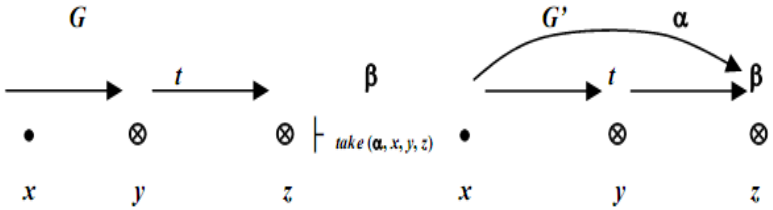
Модель розповсюдження прав доступу Take-Grant, запропонована в 1976 р., використовуэться для аналізу систем дискреційного розмежування доступу, в першу чергу, для аналізу шляхів поширення прав доступу в таких системах. В якості основних елементів моделі використовуються граф доступів і правила його перетворення. Мета моделі

- Дати відповідь на питання про можливість отримання прав доступу суб'єктом системи на об'єкт в стані, описуваному графом до-ступ. В даний час модель Take-Grant отримала продовження як розширена модель Take-Grant, в якій розглядають шляхи виникнення інформаційних потоків в системах з дискреційним розгалуженням доступу.

Переходячи до формального опису моделі Take-Grant, позначимо: O – безліч об'єктів (наприклад, файлів або сегментів пам'яті); S ⊆ O - безліч активних об'єктів та суб'єктів (наприклад, користувачів або процесів); R = {r1, r2, ..., rm} ∪ (t, g) - безліч прав доступу, де t (take) - право брати права доступу; g (grant) - право давати права доступу; G = (S, O, E) - кінцевий позначений орієнтований граф без петель, представляє поточні доступи в системі; безлічі S, O відповідають вершинам графа, які позначимо: ⊗ - об'єкти (елементи безлічі O \ S); • - суб'єкти (елементи безлічі S); елементи множини E ⊆ O × O × R представляють дуги графа, помічені непорожніми підмножинами з безлічі прав доступу R. Стан системи описується його графом доступів. Перехід системи з стану в стан визначається операціями або правилами перетворення графи доступу. Перетворення графа G в граф G 'в результаті виконання певного правила позначимо через G ├ op G '. У класичній моделі Take-Grant правило перетворення графи може бути одним з чотирьох, перерахованих нижче.

1. Правило «Брати» - take (α, x, y, z). Нехай x ∈ S, y, z ∈ O - різні вершини графа G, β ⊆ R, α ⊆ β. Правило визначає порядок отримання нової графи доступів G 'з графи G (рис. 4.1).

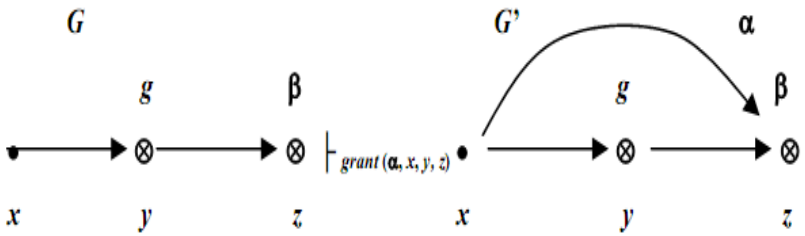
Рис. 4.1. Суб'єкт x бере в об'єкта y права α ⊆ β на об'єкт z



2. Правило «Давати» - grant (α, x, y, z). Нехай x ∈ S, y, z

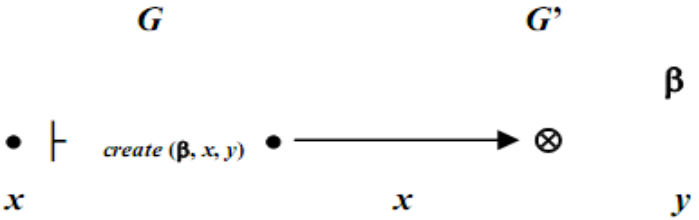
O - різні вершини графа G, β ⊆ R, α ⊆ β. Правило визначає порядок отримання нового графа G 'з графа G (рис. 4.2).

Рис. 4.2. Суб'єкт x дає об'єкту y права α ⊆ β на об'єкт z



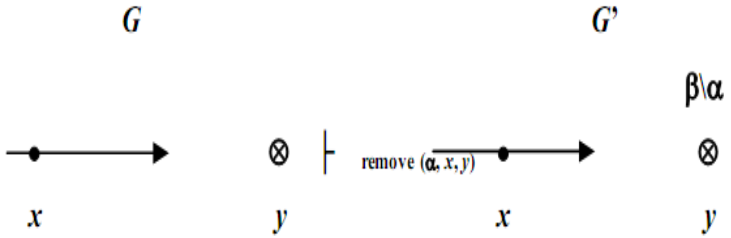
3.Правило «Створити» - create (β, x, y). Нехай x ∈ S, β ⊆ R, β ≠ ∅. Правило визначивши порядок отримання нової графи G 'з графи G; y ∈ O - новий об'єкт або суб'єкт (рис. 4.3).

Рис.4.3. Суб'єкт x створює новий β - доступний об'єкт y



4. Правило «Видалити» - remove (α, x, y). Нехай x ∈ S, y ∈ O - різні вершини графа G, β ⊆ R, α ⊆ β. Правило визначає порядок отримання нової графи G(рис. 4.4).

Рис. 4.4. Суб'єкт x видаляє права доступу α на об'єкт y



У моделі Take-Grant основна увага приділяється визначенню умов, при яких в системі можливе поширення прав доступа певним способом. Росдивимося умови реалізації: способу санкціонованого отримання прав доступу і способу викрадення прав доступу.

5. МОДЕЛЬ СИСТЕМИ БЕЗПЕКИ БЕЛЛА-ЛАПАДУЛА

Класична модель Белла-Лападула (БЛ) побудована для аналізу систем захисту, реалізують мандатне(повноважне) розмежування доступу. Можливість її використання в якості формальної моделі таких систем безпосередньо відзначена в критерії TCSEC («Помаранчева книга»). Модель БЛ була запропонована в 1975 р. Нехай визначені кінцеві множини: S - безліч суб'єктів системи (користувачі системи і програми); O - безліч об'єктів системи (наприклад, всі системні файли); R = (read, write, append, execute) - безліч видів доступу суб'єктів незалежно об'єктов з S до об'єктів з O, де read - доступ на читання, write - на запис, append – на запис у кінець об'єкта, execute - на виконання.

позначимо:

B = {b ⊆ S × O × R} - безліч можливих множин поточних доступів в системі; M = SO M - матриця дозволених доступів, де Mso ∈ R - дозволений доступ суб'єкта s до об'єкта o; L - безліч рівнів секретності, наприклад L = {U, C, S, TS}, де U <З <S <TS; (fs, fo, fc) ∈ F = Ls × Lo × Lc - Трійка функцій (fs, fo, fc), що визначають: fs: S → L - рівень допуску суб'єкта; fo: S → L - рівень секретності об'єкта; fc: S → L - поточний рівень допуску суб'єкта, при цьому ∀ s ∈ Sfc (s) ≤ fs (s); H - поточний рівень ієрархії об'єктів; V = B × M × F × H - безліч станів системи; Q - безліч запитів системі; D - безліч рішень по запитах, наприклад {yes, no, error}; W ∈ Q × D × V × V - безліч дій системи, де четвірка (q, d, v2, v1) ∈ W оз- початку, що система за запитом q з відповіддю d перейшла із стану v1 в стан v2; No - безліч значень часу {No = 0, 1, 2, ...}; X - безліч функцій x: No → Q, які задають всі можливі послідовності запитів до системи; Y - безліч функцій y: No → D, які задають всі можливі послідовності відповідей системи за запитами; Z - безліч функцій z: No → V, які задають всі можливі послідовності станів системи. Безпека системи

визначається за допомогою трьох властивостей: ss - властивості простий безпеки (simple security); *- Властивості зірки; ds - властивості дискретної безпеки (discretionary security). Оперуючи цими властивостями і їх поєднаннями можлива побудова захисту системи будь-якої складності.

6. МОДЕЛЬ LOW-WATER-MARK

Модель Low-Water-Mark (LWM) представляє близьку до моделі БЛ підхід до поділу властивостей системи безпеки, що реалізує мандатну (повноважну) політику безпеки. У моделі LWM пропонується порядок безпечного функціонування системи у випадку, коли за запитом суб'єкта йому завжди необхідно надавати доступ на запис в об'єкт. Нехай визначені кінцеві множини: S - безліч суб'єктів системи; O - безліч об'єктів системи; R = {read, write} - безліч видів доступу суб'єктів з S до об'єктів з O. Позначимо: B = {b ⊆ S × O × R} - безліч можливих множин поточних доступів в системі; L - безліч рівнів секретності; (fs, fo) ∈ ∈ F = Ls × Lo - Двійка функцій (fs, fo), визначають: fs: S → L - рівень допуску суб'єкта; рівень допуску суб'єкта і fo: S → L - рівень секретності об'єкта; V = B × F - безліч станів системи; W ⊆ OP × V × V безліч дій системи, де трійка (op, (b, f), (b *, f *)) ∈ W означає, що система в результаті виконання операції op ∈ OP перейшла із стану (b, f) у стан (b *, f *).

Безліч OP містить операції read, write, reset, описані в табл. 6.1.

6.1. Основні операції моделі LWM

Операція	Умови виконання	Результат виконання операції
read (s, o)	**fs(s) ≥ fo(o)**	**f * = f; b* = b ∪ {(s, o, read)}**
write (s, o)	**fs(s) = fo(o)**	**f *s = fs, ∀ o′≠ o f *o(o′) =fo(o), f*o(o) = fs(s), if (f*o(o′) < fo(o)) then o = ∅ , b* = b ∪ {(s, o, read)}**
reset (s, o)	**fs(s) > fo(o)**	**f*s = fs, ∀ o′≠ o f*o(o′) =fo(o′), f*o(o) = max (L)**

В результаті виконання операції write рівень секретності об'єкта знижується до рівня доступу суб'єкта. Якщо це зниження реально відбувається, то вся інформація в об'єкті стирається. В результаті виконання операції reset рівень секретності об'єкта стає максимально можливим в системі. Таким чином, розглянуті моделі Take-Grant, БЛ можуть бути виконані при побудові політики безпеки та аналізу детермінованих систем захисту , тобто систем, які не включають елементів, що мають імовірнісну природу. При дослідженні систем, закономірності функціонування яких складні або практично не піддаються опису, доцільно використовувати елементи теорії імовірності. До числа таких систем можна віднести глобальні обчислювальні мережі, наприклад Internet, або сучасні багатозадачні, розраховані на багато мережеві операційні системи.

7. МОДЕЛІ РОЛЕВОГО РОЗМЕЖУВАННЯ ДОСТУПУ

Базова модель ролевого розмежування доступу (РРД) визначає найзагальніші принципи побудови моделей РРД. Основними елементами базової моделі РРД є:

U - безліч користувачів;

R - безліч ролей;

P - безліч прав доступу на об'єкти системи;

S - безліч сесій користувачів;

PA: R → 2P - Функція, що визначає для кожної ролі безліч прав доступу; при цьому для кожного p ∈ P існує r ∈ R така, що p ∈ PA (r);

UA: U → 2R - Функція, що визначає для кожного користувача безліч ролей, на які він може бути авторизований; user: S → U - функція, що визначає для кожної сесії користувача, від імені якого вона активізована; roles: S → 2R - Функція, що визначає для користувача безліч ролей, на які він авторизований в даній сесії, при цьому в кожен момент часу для кожного s ∈ S виконується умова roles (s) ⊆ UA (user (s)). Принципово можуть існувати ролі, на які не авторизований жоден користувач. У базовій моделі РРД передбачається, що множини U, R, P і функції PA, UA не змінюються з часом. Безліч ролей, на які авторизується користовачем протягом однієї сесії, модифікується самим користувачем. У базовій моделі РРД відсутні механізми, що дозволяють одній сесії активізувати іншу сесію. Всі сесії активізуються користувачем. Для забезпечення відповідності реальним системам, кожен користувач яких займає певне положення

в службовій ієрархії, на безлічі ролей реалізовується ієрархічна структура.

Ієрархією ролей в базовій моделі РРД називається заданий на множині ролей R ставлення часткового порядку «≤» (відношення «≤» має властивості рефлексивності, антисиметричність і транзитивності). При цьому виконується умова для

$$u \in U, \text{ если } r, r' \in R, r \in UA(u) \text{ и } r' \le r, \text{ то } r' \in UA(u).$$

Таким чином, користувач повинен бути авторизований на всі ролі, в її нижчих рівнях ієрархії. Іншим важливим механізмом базової моделі РРД є обмеження, на які може бути авторизований користувач або на які він авторизується протягом однієї сесії. У базовій моделі РРД задані обмеження статичного взаємного виключення ролей або прав доступу, якщо виконуються умови:

$$R = R_1 \cup \ldots \cup R_n, \text{ где } R_i \cap R_j = \varnothing \text{ для } 1 \le i < j \le n;$$

$$|UA(u) \cap R_1| \le 1 \text{ для } u \in U, i \in 1, 2, \ldots, n;$$

$$P = P_1 \cup \ldots \cup R_m, \text{ где } P_i \cap P_j = \varnothing \text{ для } 1 \le i < j \le m;$$

$$|PA(r) \cap P_1| \le 1 \text{ для } p \in U, i \in 1, 2, \ldots, m.$$

Безліч ролей і безліч прав доступу розділяються на непересічні підмножини. При цьому кожен користувач може володіти не більше, ніж однієї роллю з кожної підмножини ролей, а кожна роль - не більше, ніж одним правом доступа з кожної підмножини прав доступу. У базовій моделі РРД задано обмеження динамічного взаємного виключення ролей, якщо виконуються умови:

$$R = R_1 \cup \ldots \cup R_n, \text{ где } R_i \cap R_j = \varnothing \text{ для } 1 \le i < j \le n;$$

$$|roles(s) \cap R_i| \le 1 \text{ для } s \in S,\ i \in 1, 2, \ldots, n.$$

Безліч ролей поділяється на непересічні підмножини. При цьому в кожній сесії користувач може володіти не більше, ніж однією роллю з кожного під-безлічі ролей. У базовій моделі РРД задані статичні кількісні обмеження на обладнаня роллю або правом доступу, якщо визначено дві функції:

$$\alpha : R \to N_0; \qquad \beta : P \to N_0,$$

де N0 - безліч натуральних чисел з нулем, і виконуються умови:

$$|UA^{-1}(r)| \le \alpha(r) \text{ для } r \in R;$$

$$|PA^{-1}(p)| \le \beta(p) \text{ для } p \in P.$$

Для кожної ролі встановлюється максимальне число користувачів, які можуть бути на неї авторизовані, а для кожного права доступу встановлюється максимальне число ролей, які можуть їм володіти.

У базовій моделі РРД задано динамічне кількісне обмеження на обладнання роллю, якщо визначена функція

$\gamma : R \to N0$

і виконується умова

$$|roles^{-1}(r)| \le \gamma(r) \text{ для } r \in R.$$

Для ролі встановлюється максимальне число сесій користувачів, які можуть одночасно бути на неї авторизовані. У базовій моделі РРД

задані статичні обмеження необхідного володіння роллю або правом доступу, якщо визначено дві функції:

$$\alpha : R \to 2^R; \qquad \beta : P \to 2^P,$$

і виконуються умови:

• для і ∈ U, якщо r, r '∈ R, r ∈ UA (u) і r' ∈ α (r), то r '∈ UA (u);

• для r ∈ R, якщо p, p '∈ P, p ∈ PA (r) і p' ∈ β (p), то p '∈ PA (r).

Для кожної ролі для того щоб на неї міг бути авторизований користувач, можуть бути визначені ролі, на які користувач також повинен бути авторизований. Для кожного права доступу, для того щоб їм володіла роль, можуть бути визначені права доступу, якими ця роль також повинна володіти.

8. КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

З поширенням писемності в людському суспільстві з'явилася потреба в обміні листами та повідомленнями, що викликало необхідність приховування вмісту письмових повідомлень від сторонніх. Методи приховування вмісту письмових повідомлень можна розділити на три групи. До першої групи відносяться методи маскировки або стеганографії, які здійснюють приховування самого факту наявності повідомлення; другу групу складають різні методи тайнопису або криптографії (від грецьких слів ktyptos - таємний і grapho - пишу); методи третьої групи орієнтовані на створення спеціальних технічних пристроїв, засекречування інформації. Практично одночасно з криптографією став розвиватися і

криптоаналіз та наука про розкриття шифрів (ключів) по шифр текста.

Друга світова війна дала новий поштовх розвитку криптографії і криптоаналізу, що було викликано застосуванням технічних засобів зв'язку і бойового управління. Для розробки нових шифрів та роботи в якості криптоаналітиків залучалися провідні вчені. У роки Другої світової війни був розроблений ряд механічних пристроїв для шифрування повідомлень.

У 1949 р. була опублікована стаття Клода Шеннона "Теорія зв'язку в секретних системах », яка підвела наукову базу під криптографію і криптоаналіз. З цього стали говорити про Криптологія (від грецького kryptos - таємний і logos - повіщення) - науці про перетворення інформації для забезпечення її таємності. Етап розвитку криптографії та криптоаналізу до 1949 р. стали називати донаучной криптології.

Криптографія є одним з найбільш потужних засобів забезпечення конфіденційність ціальностей і контролю цілісності інформації. У багатьох відношеннях вона займає центральне місце серед програмно-технічних регуляторів безпеки. наприклад, для портативних комп'ютерів, фізично захистити які вкрай важко, лише криптографія дозволяє гарантувати конфіденційність інформації навіть у разі крадіжки.

8.1. Класифікація методів криптографічного закриття інформації

В даний час відомо велика кількість методів криптографічного закриття інформації. Класифікація методів шифрування (криптоалгоритмів) може бути здійснення за такими ознаками:

• за типом ключів: симетричні і асиметричні криптоалгоритми;

• за розміром блоку інформації: потокові та блочні шифри;

• за характером впливів, вироблених над даними: метод заміни (перестановки), метод підстановки; аналітичні методи, адитивні методи (гамування), комбіновані методи. Кодування може бути смислове, символьне, комбіноване. Закриття інформації іншими способами може досягатися за допомогою , стиснення / проведення урочистих подій, розсічення / рознесення.

8.2. Основні визначення криптології

Захист даних за допомогою шифрування - одне з можливих рішень проблеми безпеки. Зашифровані дані стають доступними тільки тим, хто знає, як їх розшифрувати, і тому викрадення зашифрованих даних абсолютно бессмисленно для несанкціонованих користувачів. Коди і шифри використовувалися задовго до появи ЕОМ. З теоретичної точки зору не існує чіткої відмінності між кодами і шифрами. Проте в сучасній практиці відмінність між ними є досить чітким. Коди оперують лінгвістичними елементами, розділяючи шифрований текст на такі смислові елементи, як слова і склади. У шифрі завжди розрізняють два елементи: алгоритм і ключ.

Алгоритм дозволяє використовувати порівняно короткий ключ для шифрування як завгодно великого тексту. Визначимо ряд термінів, які використовуються в криптології.

Під шифром розуміється сукупність оборотних перетворень безлічі відкритих даних на безліч зашифрованих даних, заданих алгоритмом криптографічного перетворення.

Ключ - конкретне секретне стан деяких параметрів алгоритму крипто-графічного перетворення даних, що забезпечує вибір одного варіанта з сукупності всіляких для даного алгоритму.

Гаммирование - процес накладення за певним законом гами шифру на відкриті дані.

Гамма шифру - псевдослучайная двійкова послідовність, що виробляється на заданому алгоритму, для зашифрування відкритих даних і розшифрування зашифруванних даних.

Зашифрування даних називається процес перетворення відкритих даних в зашифрований за допомогою шифру, а розшифрування даних - процес перетворення закритих даних у відкриті за допомогою шифру.

Шифруванням називається процес зашифрування або розшифрування даних.

Дешифрованням називається процес перетворення закритих даних у відкриті при невідомому ключі і, можливо, невідомому алгоритмі.

Криптостійкості називається характеристика шифру, що визначає його стійкість до дешифруванню. Зазвичай ця характеристика визначається періодом часу, необхідним для дешифрування.

Імітозащити - захист від нав'язування помилкових даних. Для забезпечення захисту до зашифрованих даних додається Імітовставка, що представляє собою послідовність даних фіксованої довжини, отриману за певним правилом з відкритих даних і ключа.

Криптографічний захист - це захист даних за допомогою криптографічного перетворення, під яким розуміється перетворення даних шифруванням і (або) виробленням імітовставки.

Сінхропосилка - вихідні відкриті параметри алгоритму криптографічного перетворення.

Рівняння зашифрування (розшифрування) - співвідношення, що опис є процес зашифрованих (відкритих) даних з відкритих (зашифрованих) даних в результаті перетворень, заданих алгоритмом криптографічного перетворення.

Сучасні методи шифрування повинні відповідати наступним вимогам:

1. Стійкість шифру, проти стояти криптоаналізу повинна бути такою, щоб розшифрування його могло бути здійснено тільки шляхом вирішення завдання повного перебору ключів.

2. Крипостійкість забезпечується не секретністю алгоритму, а секретністю ключа.

3. Шифр текст не повинен суттєво більшим за вихідну інформацію.

4. Помилки, що виникають при шифруванні, не повинні призводити до спотворень і втрат інформації.

5. Час шифрування не повинно бути великим.

6. Вартість шифрування повинна бути узгоджена з вартістю закривання інформації.

9. **КОМБІНОВАНІ МЕТОДИ**

Шифрування комбінованими методами грунтується на результатах, отриманих К. Шенноном. Найбільш часто застосовуються такі комбінації, як підстановка і гамма, перестановка і гамма,

підстановка і перестановка, гамма і гамма. При складених комбінованих шифрів необхідно проявляти обережність, тому що неправильний вибір складання шифрів може привести до вихідного відкритого тексту.

Як приклад можна навести шифр, запропонований Д. Френдбергом, який комбінує підстановку з генератором ПСЧ. Особливість данного алгоритму полягає в тому, що при великому обсязі шифртекста частотні характеристики символів шифр текста близькі до рівномірного розподілу незалежно від змісту відкритого тексту.

Комбінація методів підстановки і перестановки була застосована в 1974 р. фірмою IBM при розробці системи Люцифер. Система Люцифер будується на базі блоків підстановки (S-блоків) і блоків перестановкіи (P-блоків). Блок підстановки включає лінійні і нелінійні перетворення.

Перший перетворювач S-блоку здійснює розгортку двійкового числа з n розрядів у число по підставі 2n. Другий перетворювач здійснює згортку цього числа. Блок перестановки здійснює перетворення n розрядного вхідного числа в n розрядне число. Вхідні дані (відкритий текст) послідовно проходять через шари 32-розрядних P-блоків і 8-розрядних S-блоків. Реалізація шифрування даних в системі Люцифер програмними засобами показала низьку продуктивність, тому P і S-блоки були реалізовані апаратно, що дозволило досягти швидкості шифрування до 100 Кбайт / с. Досвід, отриманий при розробці та експлуатації системи, дав можливість створити стандарт шифрування данних DES.

DES (*Data Encryption Standard*) є одним з найбільш поширених криптографічних стандартів на шифрування даних, що застосовуються в США. Першоначальний метод, який лежить в основі даного стандарту, був розроблений фірмою IBM для своїх цілей. Він був перевірений Агентством Національної Безпеки США, яке не виявило в ньому статистичних чи математичних вад. Це

означало, що де шифрування даних, захищених за допомогою DES, не могло бути виконане статиститичними (наприклад, за допомогою частотного словника) або математичними («прокручено зазростанням »в зворотному напрямку) методами. Після цього метод фірми IBM був прийнятий як федерального стандарту. Стандарт DES використовується федеральними департаментами і агентствами для захисту всіх досить важливих даних у комп'ютерах (виключаючи деякі дані, методи захисту яких визначаються спеціальними актами). Його застосовують багато не державних інститутів, в тому числі більшість банків і служб обігу грошей. Обумовлений в стандарті алгоритм криптографічного захисту даних опублікований для того, щоб більшість користувачів могли використовувати перевірений і алгоритм з хорошою криптостійкості. Однак, з одного боку, публікація алгоритму небажана, оскільки може призвести до спроб дешифрування закритої інформації, але, з іншого боку, це не настільки суттєво оскільки стандартний алгоритм шифрування даних повинен володіти такими характеристиками, щоб його опублікування не позначилося на його криптостійкості.

DES має блоки по 64 біт і заснований на 16 кратною перестановою даних, також для шифрування використовує ключ в 56 біт. Існує кілька режимів DES: Electronic Code Book (ECB) і Cipher Block Chaining (CBC). 56 біт - це 8 семібітових ASCII символів, тобто пароль не може бути більше ніж 8 букв. Якщо додатково використовувати тільки букви і цифри, то кількість можливих варіантів буде істотно менше максимально можливих 256.

Суть даного алгоритму полягає в наступному. Вхідний блок даних ділиться навпіл на ліву (L0) і праву (R0) частини. Після цього формується вихідний масив так, що його ліва частина L1 представлена правою частниною R0 вхідного, а права R1 формується як сума L0 і R0 операцій можна переконатися, що всі проведені операції можуть бути звернені і розшифрування здійснюється за число операцій, лінійно залежне від розміру блоку.

Після кількох таких збивань можна вважати, що кожен біт вихідного блоку шифровки може залежати від кожного біта повідомлення.

10. **АЛГОРИТМ RSA**

В даний час найбільш розвинутим методом криптографічного захисту інформацію з відомим ключем є RSA, названий так за початковими буквами прізвищ її винахідників (Rivest, Shamir і Adleman). Перед тим як приступити до викладу концепції методу RSA, необхідно визначити деякі терміни. Під простим числом будемо розуміти таке число, яке ділиться тільки на 1 і на саме себе. Взаємно простими числами будемо називати такі числа, які не мають ні одного загального дільника, крім 1. Під результатом операції i mod j будемо вважати залишок від цілочисельного ділення i на j. Щоб використовувати алгоритм RSA, треба спочатку згенерувати відкритий та секретний ключ, виконавши такі кроки.

Виберемо два дуже великих простих числа p і q, Визначимо n як результат множення p на q (n = pq). Виберемо велике випадкове число, яке назвемо d. Це число повинне бути простим з m результатом множення (p - 1) (q - 1). Визначимо таке число e, для якого є істинним наступне співвідношення

(e d) mod (m) = 1 або e = (1 mod (m)) / d.

Відкритим ключем будуть числа e і n, а секретним ключем - числа d і n. Тепер, щоб зашифрувати дані за відомим ключу {e, n}, необхідно зробити наступне:

- Розбити шифруємий текст на блоки, кожний з яких може бути представлений у вигляді числа M (i) = 0, 1, ..., n - 1;

- Зашифрувати текст, що розглядається як послідовність чисел M (i) за формулою C (i) = (M (i)e) Mod n.

Щоб розшифрувати дані, використовуючи секретний ключ {d, n}, необхідно виконати наступні обчислення: M (i) = (C (i)d) Mod n. В результаті вийде безліч чисел M (i), які представляють собою вихідний текст.

Приклад. Застосуємо метод RSA для шифрування повідомлення «ГАЗ». для простоти будемо використовувати дуже маленькі числа (на практиці використовуються набагато більші числа).

Виберемо p = 3 і q = 11.

Визначимо n = 3 · 11 = 33.

Знайдемо (p - 1) (q - 1) = 20. Отже, як d виберемо будь-яке число, яке є взаємно простим з 20, наприклад d = 3. Виберемо число e. В якості такого числа може бути взято будь-яке число, яке задовольняється співвідношення (e × 3) mod 20 = 1, наприклад 7.Уявімо шифруємо повідомлення як послідовність цілих чисел в диапазоні 0 ... 32. Нехай буква А зображується числом 1, буква Г - числом 4, а буква З - числом 9. Тоді повідомлення можна представити у вигляді послідовності чисел 4 1 9. Зашифруємо повідомлення, використовуючи ключ {7, 33}:

C1 = (4) mod 33 = 16 384 mod 33 = 16,

C2 = (17) Mod 33 = 1 mod 33 = 1,

C3 = (97) Mod 33 = 4782969 mod 33 = 15.

Шифр текст: «16 січня 15». Спробуємо розшифрувати повідомлення {16, 1, 15}, отримане в результаті зашиврування за відомим ключем, на основі секретного ключа {3, 33}:

M1 = (163) Mod 33 = 4096 mod 33 = 4,

M2 = (13) Mod 33 = 1 mod 33 = 1,

M3 = (153) Mod 33 = 3375 mod 33 = 9.

Таким чином, в результаті розшифрування повідомлення отримано початкове повідомлення «ГАЗ». Крипостійкість алгоритму RSA грунтується на припущенні, що важко визначити секретний ключ за відомим, оскільки для цього необхідно вирішити задачу про існування дільників цілого числа. Дане завдання є Np-повній і, як наслідок цього факту, не допускає в даний час ефективного(поліноміальною) рішення. Більше того, саме питання існування ефективних алгоритмів рішення np-повних задач є до теперішнього часу відкритим. У зв'язку з цим для чисел, що складаються з 200 цифр (а саме такі числа рекомендується використовувати традиційні методи вимагають виконання величезного числа операцій (близько 1023).

11. МЕТОДИ КОДУВАННЯ

Як уже зазначалося, під кодуванням розуміється заміна елементів відкритого тексту (букв, слів, фраз і т.п.) кодами. Розрізняють символьне і смислове кодування.

При символьному кодуванні кожен знак алфавіту відкритого тексту замінюється відповідним символом. Прикладом символьного кодування служить азбука Морзе, а також методи шифрування заміною і перестановкою. Розглянемо метод символьного кодування, який використовує попередні символи відкритого тексту. Цей метод, званий методом стопки книг, був запропонований Б.Я. Рябко. Припустимо, що потрібно передати повідомлення X з алфавіту A, в якому букви алфавіту ототожнені з числами 1, 2, ..., L, де L - число елементів алфавіту A. Кожної букви алфавіту відповідає код ki, 1 = 1

... L. При появі в повідомленні X очередної букви xj її код представляється кодом номера позиції j, займаної в даний момент буквою xj в списку. Це дає можливість на приймальному кінці за кодом номера позиції j визначити букву xj. Після кодування букви xj одночасно на приймальному і передавальних кінцях переміщують букву xj в початок списку, збільшуючи тим самим на одиницю номера букв, що стояли на позиціях від 1 до j - 1. Номери букв, що стояли на позиціях від j + 1 до L, залишаються без змін. В результаті кодування відкритого тексту на початку списку будуть знаходитися літери, які найбільш часто зустрічалися у відкритому тому тексті.

Цікавий метод кодування в 1992 р. запропонував С.П. Савчук. На відміну від метода стопки книг переміщенню піддається список кодів. Нехай алфавіт A = {a1, a2, ...,an}. Даному порядку розташування букв відповідає початковий список кодів K0 ={k1, k2, ..., kn}. При появі в кодованої повідомленні букви (ai) в якості коду вибирається відповідне її розташування код (ki). Після цього здійснюється зсув списка кодів:

{k1, k2, ..., ki, ..., kn} → {k2, k3, ..., kn, k1}.

Таким чином, список кодів утворює замкнуте кільце. Смислове кодування - це кодування, в якому в якості вихідного алфавіта використовуються не тільки окремі символи (літери), а й слова і навіть найбільш часто зустрічаються фрази. Розглянемо приклад одноалфавітного і багатоалфавітного смислового кодуванняня.

Приклад. Відкритий текст: «19.9.1992 РОКУ».

Таблиця кодування

Елементи відкритого тексту	Коди
1	**089 146 214 417**
2	**187 226 045 361**
9	**289 023 194 635**
РІК	**031 155 217 473**
.	**786 432 319 157**

Закодоване повідомлення при одноалфавітном кодуванні:

«089 289 786 289 786 089 289 289 187 031».

Закодоване повідомлення при багатоалфавітному кодуванні:

«089 289 786 023 432 146 194 635 187 031» (при багатоалфавітному кодуванні однакові символи замінюються кодами з наступного ряду). Серед різних кодів, що застосовуються для кодування природних мов, особбий інтерес викликає код Хаффмена, який дозволяє стискати відкритий текст. Суть його полягає в привласненні найбільш часто зустрічається буквам найбільш коротких кодів.

Рядок двійкових символів кодів Хаффмена єдиним чином розкладається на коди символів (такі коди називаються префіксним).

Приклад. Закодоване кодом Хаффмена повідомлення має вигляд:

«01101000100000010101111000100000».

Користуючись деревом для англійської мови, отримуємо 0110 = S.

Далі знову починаємо рух з вершини: 100 = E; 01000 = C;

10 1011 = R; 1010 = I; 001 = T; 00000 = Y.

Відкритий текст: «SECURITY».

12. ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС

В основі криптографічного контролю цілісності лежать два поняття: хеш-функція; електронний цифровий підпис (ЕЦП).

Хеш-функція - це труднообратне перетворення даних (односторонної функції), що реалізовується, як правило, засобами симетричного шифрування зі зв'язуванням блоків. Результат шифрування останнього блоку (залежний від усіх попередніх) і служить результатом хеш-функції.

Нехай є дані, цілісність яких повинна бути перевірена, хеш-функція

і раніше обчислений результат її застосування до вихідних даних (дайджест). хеш-функцію позначимо через h, вихідні дані - через T, перевіряються дані - через T '.

Контроль цілісності даних зводиться до перевірки рівності h (T) = h (T '). Якщо воно виконується, вважається, що T = T '. Збіг дайджестів для різних даних називаються колізією. В принципі колізії можливі (так як потужність безлічі дайджестов менше безлічі хешування даних), однак, виходячи з визначення хеш-функції, спеціально організувати колізію за прийнятний час неможливо.

Асиметричні методи дозволяють реалізувати так званий електронний цифровий підпис, або електронне засвідчення повідомлення. Ідея полягає в тому, що відправник посилає два примірники повідомлення - відкрите і дешифрувати його секретним ключем (природно, дешифрування незашифрованого повідомлення насправді є форма шифрування). Одержувач може зашифрувати за допомогою відкритого ключа відправника дешифрований примірник і порівняти з відкритим. Якщо вони співпадуть, лічність і підпис відправника можна вважати встановленими.

Нехай E (T) позначає результат шифрування тексту T за допомогою відкритого ключа, а D (T) - результат дешифрування тексту T за допомогою секретного ключа. Щоб асімметковий метод міг застосовуватися для реалізації електронного підпису, необхідно виконання тотожності E(D(T)) = D(E(T)) = T.

Проілюструємо рис. 12.1 процедуру ефективної генерації електронного підпису, що складається в шифруванні перетворенням D дайджесту h (T), а перевірка ефективно згенерованої електронного підпису може бути реалізована способом, зображеним на рис. 12.2.

З рівності E (S ') = h (T) випливає, S' = D (h (T ')). Отже, ЕЦП захищає цілісність повідомлення, засвідчує особу відправника і служить основою невідказності.

Рис.12.1. Вироблення електронного цифрового підпису

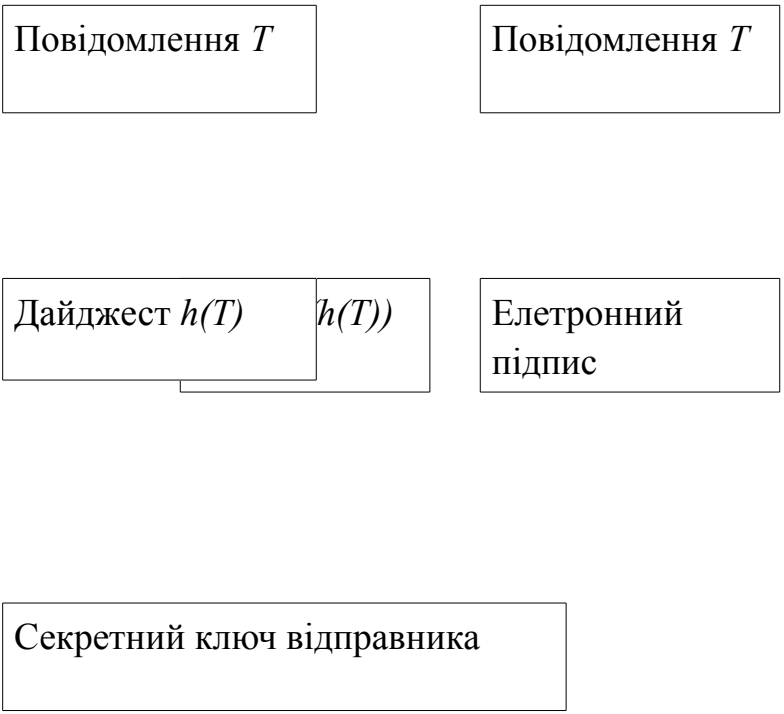
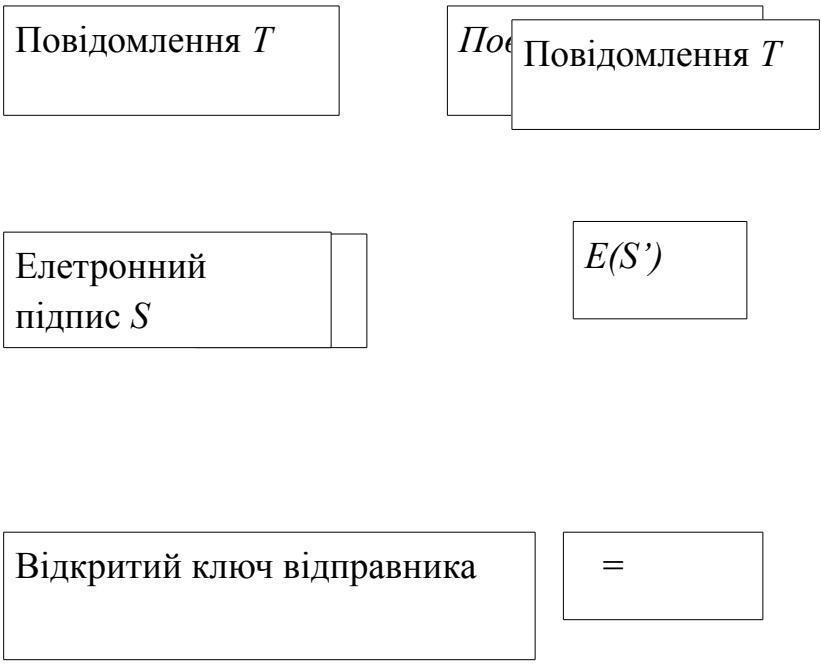


Рис.12.2. Перевірка електронного цифрового підпису



Звернемо увагу на те, що при використання асиметричних методів шифрування (зокрема ЕЦП) необхідно мати гарантію автентичності пари (ім'я, відкритий ключ) адресата. Для вирішення цього завдання в специфікаціях X.509 вводяться поняття цифрового сертифікату і сертифікаційного центру. Сертифікаційний центр - це компонент глобальної служби каталогів, що відповідає за управління криптографічними ключами користувачів, який посвідчує справжність пари ім'я, відкритий ключ адресата своїм підписом.

Цифрові сертифікати у форматі X.509 стали не тільки формальним, але й фактичним стандартом, підтримуваним численними сертифікаційними центрами. Зазначимо, що послуги, характерні для асиметричного шифрування, можна реалізовувати і за допомогою симетричних методів, якщо є надійна третя сторона, знаюча секретні ключі своїх клієнтів. Ця ідея покладена, наприклад, в основу сервера аутентифікації Kerberos.

13. КЛАСИФІКАЦІЯ КОМП'ЮТЕРНИХ ВІРУСІВ

Віруси можна розділити на класи за такими основними ознаками:

- середовище проживання;
- операційна система (ОС);
- особливості алгоритму роботи;

- деструктивні можливості.

Залежно від середовища існування віруси можна розділити на:

- Файлові;
- Завантажувальні;
- Макровіруси;
- Мережеві.

Файлові віруси або різними способами впроваджуються у виконувані файла, або створюють файли двійники (віруси-компаньйони), або використовують особливості організації файлової системи (link-віруси).

Завантажувальні віруси записують себе або в завантажувальний сектор диска (boot-сектор), або в сектор, що містить системний завантажувач вінчестера (Master Boot Record), або змінюють покажчик на активний boot сектор.

Макровіруси заражають файли-документи й електронні таблиці декількох популярних редакторів. Мережеві віруси використовують для свого поширення протоколи або команди комп'ютерних мереж і електронної пошти. Існує велика кількість сполучень, наприклад файлово-завантажувальні віруси, що заражають як файли, так і завантажувальні сектори дисків. Такі віруси, мають довільно складний алгоритм роботи, часто застосовують оригінальні методи проникненням в систему, використовують «стелс-» і поліморфік-технології. Інший приклад такого сполучення - мережний макровірус, який не тільки заражає редаговані документи, але і розсилає свої копії по електронній пошті.

Заражається операційна система є другим рівнем розподілу вірусів на класи. Кожен файловий чи мережний вірус заражає файли який-

небудь однієї або декількох ОС - DOS, Windows 95/98/Me/NT/2000/XP, OS / 2, UNIX і т. д. Макровіруси заражають файли форматів Word, Excel, інших додатків Microsoft Office. Загрузочні віруси орієнтовані на конкретні формати розташування системних даних у завантажувальних секторах дисків.

Серед особливостей алгоритму роботи вірусів виділяються наступні:

- резидентність;
- використання «стелс»-алгоритмів;
- самошифрування і поліморфічность;
- використання нестандартних прийомів.

Резидентний вірус при інфікуванні комп'ютера залишає в оперативній пам'яті свою резидентну частину, яка потім перехоплює звернення ОС до об'єктів зараження і впроваджуються в них. Резидентні віруси знаходяться в пам'яті і є активними до вимикання комп'ютера або перезавантаження ОС. Нерезидентні віруси не заражають пам'ять комп'ютера і зберігають активність обмежений час. Деякі віруси залишають в оперативній пам'яті невеликі резидентні програми, які не поширюють вірус. Такі віруси вважаються нерезидентними.

Резидентними можна вважати макровіруси, оскільки вони також присутні в пам'яті комп'ютера протягом усього часу роботи зараженого редактора. при цьому роль ОС бере на себе редактор, а поняття «перезавантаження операційної системи» трактується як вихід з редактора.

Використання «стелс»-алгоритмів дозволяє вірусам цілком або частково сховати себе в системі. Найбільш поширеним «стелс»-алгоритмом є перехват запитів ОС на читання запису заражених

об'єктів і потім «стелс»-віруси або тимчасово лікують їх, або підставляють замість себе незаражені ділянки інформації. В випадку макровірусів найбільш популярний спосіб - заборона викликів меню перегляду макросів.

Самошифрування і поліморфічность використовуються практично всіма типами вірусів для того, щоб максимально ускладнити процедуру виявлення вірусу. поліморфік - віруси (polymorphic) досить важко піддаються виявленню, вони не мають сигнатур, тобто не містять жодної постійної ділянки коду. У більшості випадків два зразки того самого поліморфік - вірусу не будуть мати жодного збігу. Це досягається шифруванням основного тіла вірусу і модифікаціями програми - розшифровувача.

Різні нестандартні прийоми часто використовуються у вірусах для того, щоб як найглибше сховати себе в ядрі ОС (як це робить вірус «ЗАРАЗА»), захистити від виявлення свою резидентну копію (віруси TPVO, Trout2), утруднити лікування від вірусу (наприклад, завадять свою копію в Flash-BIOS) і т.д.

За деструктивним можливостям віруси можна розділити на:

- нешкідливі, тобто ніяк не впливають на роботу комп'ютера (крім зменшення своєю вільною пам'ятю на диску при своєму поширенні);

- безпечні, вплив яких обмежується зменшенням вільної пам'яті на дискуі графічними, звуковими та іншими ефектами;

- небезпечні віруси, які можуть привести до серйозних збоїв у роботі комп'ютера;

- дуже небезпечні - в алгоритм їх роботи свідомо закладені деструктивні процедури (викликають втрату програм, знищення даних, або сприяють швидкому зносу рухомих частин механізмів).

Інші шкідливі програми. До шкідливих програм крім вірусів відносяться також «троянські коні», «логічні бомби», intended-віруси, конструктори вірусів і поліморфік-генератори.

«Троянський кінь» (логічні бомби) - це програма, що наносить будь-які руйнівні дії в залежності від певних умов або при кожному запуску, знищуючи інформацію на дисках, «веде» систему до зависання і т.д. Блешність відомих інфекцій такого роду підробляються під які небудь корисні програми, нові версії популярних утиліт або доповнення до них. Дуже часто вони россилаются по BBS-станціях або електронних конференціях. У порівнянні з вірусами «Троянські коні» не отримують широкого поширення по достатньо простим причинам: вони або знищують себе разом з іншими даними на диску, або маскують свою присутність і знищуються постраждалим користувачем.

До «троянським коням» також можна віднести «дроппер» вірусів - заражені файли, код яких підправлений таким чином, що відомі версії антивірусів не знаходять вірусу у файлі. Наприклад, файл шифрується будь-яким спеціальним чином або упаковується рідко використовуваним архіватором, що не дозволяє антивірусу «Побачити» зараження.

Слід відзначити також «злі жарти» (hoax). До них відносяться програми, які не заподіють комп'ютеру якоїсь прямої шкоди, проте виводять повідомлення про те, що така шкода вже заподіяна, або буде завдано при будь-яких умовах, або попереджають користувача про неіснуючу небезпеку. До «злих жартів" відносяться, наприклад, програми, які «лякають» користувача повідомленнями про форматування диска, визначають віруси в незаражених файлах, виводять дивні вірусоподібні повідомлення і т.д.

Intended-віруси. До таких вірусів відносяться програми, які на перший погляд є стовідсотковими вірусами, але не здатні розмножуватися через помилок. Наприклад, вірус, який при

зараженні «забуває» помістити в початок файлів команду передачі управління на код вірусу, або записує в неї неправильну адресу свого кода, або неправильно встановлює адресу перехоплюваних переривання (що в більшості випадків завішує комп'ютер) і т.д.

До категорії intended-вірусів також відносяться віруси, які за наведеними вище причин розмножуються тільки один раз з «авторської» копії. Заразивши якийсь або файл, вони втрачають здатність до подальшого розмноження.

Конструктори вірусів - це утиліта, призначена для виготовлення нових комп'ютерних вірусів. Відомі конструктори вірусів для DOS, Windows і макровірусів. Вони дозволяють генерувати вихідні тексти вірусів (ASM-файли), об'єктні модулі та / або безпосередньо заражені файли.

Деякі конструктори забезпечені стандартним віконним інтерфейсом, позволяючи за допомогою системи меню вибрати тип вірусу, групи об'єкти (COM та / або EXE) наявність або відсутність самошифровки, внутрішні текстові рядки, вибрати ефекти, що супроводжують роботу вірусу, і т. д.

Інші конструктори не мають інтерфейсу і зчитують інформацію про тип вірусу з конфігураційного файлу.

Поліморфні генератори, як і конструктори вірусів, не є вірусами в прямому сенсі цього слова, оскільки в їхній алгоритм не закладаються функції розмножения, тобто відкриття, закриття і запису у файли, читання і запису секторів і т.д.

Головною функцією подібного роду програм є шифрування тіла вірусу і генерація відповідного розшифровувача.

Резидентні віруси. Під терміном «резидентність» (DOS термін TSR - Terminate and Stay Resident) розуміється здатність вірусів залишати свої копії в операційній системі, перехоплювати деякі події

(наприклад, звернення до файлів або дисків) і викликати при цьому процедури зараження виявлених об'єктів (файлів і секторів). Таким чином, резидентні віруси активні не тільки в момент роботи інфікованої програми, але і після того як програма закінчила свою роботу.

Резидентні копії таких вірусів залишаються життєздатними аж до чергової перезагрузки, навіть якщо на диску знищені всі інфіковані файли.

Полиморфик-вірусами є ті, виявлення яких неможливо (або вкрай важко) здійснити за допомогою так званих вірусних масок - ділянок постійного коду, специфічних для конкретного вірусу. Досягається це двома основними способами - шифруванням основного коду вірусу з непостійним ключем і випадковим набором команд розшифровувача або зміною самого виконуваного коду вірусу.

Рівні поліморфізму. Існує розподіл поліморфік-вірусів на рівні в залежності від складності коду, який зустрічається в розшифровувача цих вірусів. Такий поділ вперше запропонував доктор Алан Соломон, через деякий час Весселін Бончев розширив його.

Рівень 1. Віруси, які мають деякий набір розшифровувача з постійним кодом і при зараженні вибирають один з них. Такі віруси є поле-морфікамі і носять також назву олігоморфік (oligomorphic).

Рівень 2. Розшифровувача вірусу містить одну або кілька постійних інстррукцій, основна ж його частина непостійна.

Рівень 3. Розшифровщик містить невикористовувані інструкції сміття типу NOP,CLI, STI і т.д.

Рівень 4. У розшифровувача використовуються взаємозамінні інструкції і зміна порядку проходження (перемішування) інструкцій. Алгоритм розшифровки при цьому не змінюється.

Рівень 5. Використовуються всі перераховані вище прийоми, алгоритм розшифровки непостійний, можливо повторне шифрування коду вірусу і навіть часткове шифрованя самого коду розшифровувача.

Рівень 6. Permutating-віруси. Зміні підлягає основний код вірусу - ділиться на блоки, які при зараженні переставляються в довільному порядку. Вірус при цьому залишається працездатним. Подібні віруси можуть бути не зашифровані.

Наведене поділ не вільно від недоліків, оскільки проводиться по єдиному критерію - можливості виявляти вірус по коду розшифровувача при допомозі стандартного прийому вірусних масок. Якщо зробити розподіл на рівні з точки зору антивірусів, що використовують системи автоматичного розшифрування коду вірусу (емулятори), то розподіл на рівні буде залежати від складності емуляції коду вірусу. Можливо, більш об'єктивним є поділ, в якому крім критерію вірусних масок беруть участь і інші параметри:

1. Ступінь складності поліморфік коду (відсоток від усіх інструкцій процесора, які можуть зустрітися в коді розшифровувача).

2. Використання антіемуляторних прийомів.

3. Сталість алгоритму розшифровувача.

4. Сталість довжини розшифровувача.

13.1. Види антивірусних програм

- Програми-детектори;

- Програми-доктори або фаги;

- Програми-монітори (ревізори);

- Програми фільтри;

- Програми-вакцини або іммунізатори.

Програми-детектори (сканери) здійснюють пошук характерної для конкретного вірусу послідовності байтів (сигнатури вірусу) в оперативній пам'яті у файлах і при виявленні видають відповідне повідомлення. Недоліком таких антивірусних програм є те, що вони можуть знаходити тільки ті віруси, які відомі розробникам.

У багатьох сканерах використовуються також алгоритми евристичного сканування, тобто аналіз послідовності команд в об'єкті, що перевіряється, набір деякої статистики і прийняття рішення («можливо, заражений» або «не заражений») для кожного провіряючого об'єкта.

До переваг сканерів відноситься їх універсальність, до недоліків – розміри антивірусних баз, які сканерам доводиться «тягати за собою», і не велика швидкість пошуку вірусів.

Програми-доктора або фаги, а також програми-вакцини не тільки знаходять заражені вірусами файли, але і «лікують» їх, тобто видаляють з файлу тіло програми віруса, повертаючи файли в початковий стан. На початку своєї роботи фаги шукають віруси в

оперативної пам'яті, знищуючи їх, і тільки потім переходять до «лікування» файлів. Седі фагів виділяють поліфаги, тобто програми-доктори, призначені для пошуку й знищення великої кількості вірусів. Найбільш відомими поліфагами є програми Aidstest, Scan, Norton AntiViris і Doctor Web.

Програми-ревізори (CRC-сканери) відносяться до найнадійніших засобів захисту від вірусів. Принцип роботи CRC-сканерів заснований на підрахунку CRC-сум (контрольних сум) для присутніх на диску файлів / системних секторів. Ці CRC-суми потім зберігаються в базі даних антивірусу, як, втім, і деяка інша інформація: довжини файлів, дати їх останньої модифікації і т.д. При подальшому запуску CRC-сканери звіряють дані, що містяться в базі даних, з реально підщитаними значеннями. Якщо інформація про файл, записана в базі даних, не збігається з реальними значеннями, то CRC-сканери сигналізують про те, що файл був змінений або заражений вірусом.

CRC-сканери, що використовують «антістелс»-алгоритми, є досить сильним зброєю проти вірусів: практично 100% вірусів виявляються виявленими почті відразу після їх появи на комп'ютері. Однак у цього типу антивірусів є недолік, який помітно знижує їх ефективність. Цей недолік відбувається в тому, що CRC-сканери не здатні зловити вірус у момент його появи в системі, а роблять це лише через деякий час, вже після того, як вірус розійшовся по комп'ютеру. CRC-сканери не можуть детектувати вірус в нових файлах, оскільки в їх базах даних немає інформації про цих файлах. Більше того, періодично появляють віруси, які використовують цю «слабкість» CRC-сканерів, заражають тільки новостворювані файли і залишаються невидимими для CRC-сканерів. До числа програм-ревізорів належить, наприклад, відома в Росії програма ADinf фірми «Діалог-наука».

Антивірусні монітори - це резидентні програми, що перехоплюють вірусо-небезпечні ситуації і повідомляють про це

користувача. До вірусоопасним відносяться виклики на відкриття для запису у виконувані файли запис у завантажувальні сектори дисків або MBR вінчестера, спроби програм залишитися резидентно і т.д., тобто виклики, які характерні для вірусів в моменти їхнього розмноження.До достоїнств моніторів є їхня здатність виявляти і блокувати вірус на ранній стадії його розмноження, що, до речі, буває дуже корисно в випадках, коли давно відомий вірус постійно "виповзає невідомо звідки». До недостатку відносяться існування шляхів обходу захисту монітора і велика кількість помилкових спрацьовувань.

Вакцини або іммунізатори - це резидентні програми, що мають зараження файлів. Вакцини застосовують, якщо відсутні програми-доктори, «лікують» цей вірус. Іммунізатори діляться на два типи: іммунізатори, що повідомляють про заражений файл, і іммунізатори, блокуючі зараження яким-небудь типом вірусу. Перші звичайні але записуються в кінець файлів (за принципом файлового вірусу і при запуску файлу кожен раз перевіряють його на зміну. Недолік у таких іммунізатори всього один, але він не значний : абсолютна нездатність повідомити про зараження «стелс»-вірусом. Тому такі іммунізатори, як і монітори, практично не використовуються в даний час.

Другий тип імунізації захищає систему від поразки вірусом якогось виділеного виду. Файли на дисках модифікуються таким чином, що вірус приймає їх за вже заражені. Для захисту від резидентного вірусу в пам'ять комп'ютера заноситься програма, що імітує копію вірусу, при запуску вірус натикається на неї і вважає, що система вже заражена.

Якість антивірусної програми визначається за такими позиціями, приведенними в порядку їх важливості:

1. Надійність і зручність роботи - відсутність зависань антивіруса та інших технічних проблем, що вимагають від користувача спеціальної підготовки.

2. Якість виявлення вірусів всіх поширених типів, сканування

всередині файлів документів / таблиць (MS Word, Excel, Office), упакованих та архівованних файлів. Відсутність «помилкових спрацьовувань». Можливість лікування заражених об'єктів (для сканерів - періодичність появи нових версій, тобто швидкість настройки сканера на нові віруси).

3. Існування версій антивіруса під всі популярні платформи (DOS, Windows 95/98/NT/Me/2000/XP, Novell NetWare, OS / 2, Alpha, UNIX, Linux і т. д.), Присутніх не тільки режиму «сканування за запитом», а й «нальоту».

14 . ТЕХНОЛОГІЇ КІБЕР-БЕЗПЕКИ

Є багато технологій кібер-безпеки пропонованих на сучасному ринку, які можуть служити гарантіями і контрзаходами щодо захисту агентств інформаційної технології (IT) інфраструктури. Ототожнюєм 18 технологій описавши те, що вони роблять, як вони працюють, і їх ефективності. Ці технології можуть бути класифіковані з контролю функціональності які вони забезпечують. Таблиця 1 визначає ці керуючі категорії:

Таблиця 1: Категорії управління кібер-безпеки:

Категорії управління	**Управління функціональністю**

Контроль доступу	Гарантує, що система і її дані не змінені або незаконно пошкоджені шкідливим кодом.
Криптографія	Включає в себе шифрування даних при передачі і при зберіганні в системі. Шифрування являє собою процес перетворення звичайних даних в код форми, так що інформація доступна тільки

Продовження таблиці 1.

Аудит і моніторинг	Допомога адміністраторам виконувати дослідження під час і після кібер-атаки.
Конфігурація управління та гарантія	Допомога адміністраторам переглядати та змінювати налаштування безпеки на їх частини та мережі, перевірте правильність безпеки настройки і підтримки операцій в захищеному режимі при умовах примусу.

Вибору і ефективного здійснення кібер-безпеки технологій вимагають адекватного розгляду ряду ключових факторів, у тому числі враховуючи унікальні IT-інфраструктури агенства і використання оборони глибокої стратегії.

Інформаційна безпека є важливим чинником для будь-якої організації , що залежить від інформаційних систем для виконання своєї роботи. різкого розширення в комп'ютері міжмережевої взаємодії і експонентний збільшення використання Інтернету, змінюють спосіб нашого уряду, нації, і велика частина світу спілкується і веде бізнес. Однак без належних гарантій, швидкість і доступність, що створює величезні переваги комп'ютерного століття може дозволити особам і груп з шкідливими намірами отримати не санкціонований доступ до системи і використовувати цей доступ для отримання конфіденційної інформації, вчинення шахрайства, порушення операцій або нападів на сайти інших організацій. Експерти сходяться на думці, що має місце стійкий прогрес у витонченості та ефективності атак технології. Зловмисники швидко розвивають атаки для експлуатації вразливостей, виявлених в продуктах. Крім того, вони можуть об'єднати ці напади з іншими формами технології з метою розвитку програми, які автоматично сканують мережу вразливих систем, атаки на них, скомпрометувавши їх, і використовувати їх для розповсюдження атаки ще більше. Ці атаки та інструменти стали легко доступні, і можуть бути легко бути завантажені з Інтернету, і використовуються для початку атаки. За даними Федерального бюроДослідження, терористи, транснаціональні злочинці, і спецслужби швидко стають відомі у використанні інформаційних інструментів експлуатації таких, як комп'ютерні віруси, троянські програми, черв'яки, логічні бомби, і підслуховування снифферов, які можуть зруйнувати, перехоплюваюси, погіршуючи цілісність, або заборону доступу до даних. Крім того, незадоволення інсайдерської організації значної загрози, оскільки такі особи часто мають знання, які дозволяє їм отримати необмежений доступ і наносять пошкодження або

крадіжки активів , не маючи багато знань про комп'ютерні вторгнення. Як велику суму грошей і більш чутливих економічних і комерційної інформацією обмінюються в електронному вигляді і в якості країни оборони і розвідки громади все більше покладаються на стандартизовані інформаційні технології, збільшується імовірність, що інформаційні атаки загрожуватимуть життєво важливим національним інтересам.

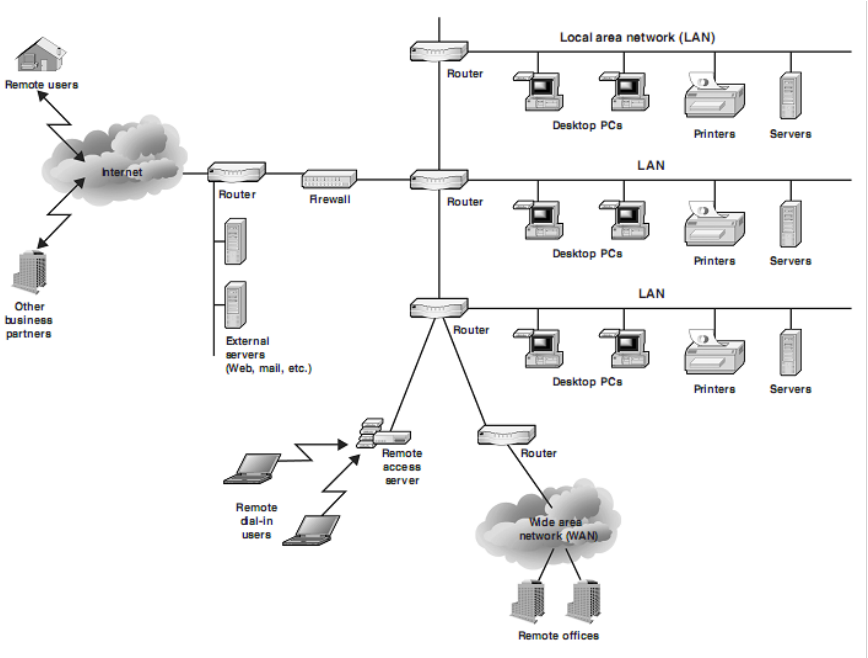
14.1. Ефективна реалізація комерційно доступних технологій можуть знизити ризики

Для виконання вимоги FISMA є ефективно здійснювати технічні засоби контролю. Безліч технологій кібербезпеки , які пропонуються в сучасному ринку може служити в якості гарантії і контрзаходу щодо захисту агентств IT-інфраструктури. Для надання допомоги установам у виявленні та враховуючи необхідність подальшого здійснення таких технологій, це документ забезпечує структуроване обговорення наявних у продажу, стані практиці технології кібербезпеки, що федеральні органи можуть використовувати для захисту своїх комп'ютерних систем. У ньому також обговорюються реалізації міркувань з доступних технологій. Як правило, інфраструктура установ будуються на декількох вузлах, в тому числі настільних персональних комп'ютерів (ПК), сервери та мейнфрейми. Дані ліній зв'язку та мережних пристроїв, таких як маршрутизатори, концентратори і перемикачі дозволяють сайту взаємодіяти один з одним через місцеву мережу (LAN) в межах

установи. Глобальні мережі (WAN) підключають локальні мережі у різних географічних точках. Крім того, агентства зазвичай підключені до Інтернет-колекції з усього світу мереж, управляє близько 10.000 інтернет-провайдерів (ISP). Прикладом типового IT-інфраструктура показано на рис. 1.

Конфіденційність ставиться до збереження уповноваженим обмеження на доступ інформації та розкриття інформації, включаючи засоби для захисту недоторканності приватного життя і власності інформації. Цілісність відноситься до захищення від неправильної модифікації або знищення інформації, включаючи забезпечення непідробленість інформації та автентичність. Доступність ставиться до забезпечення своєчасного і надійного доступу та використання інформації.

Рис. 1: Типові інфраструктури IT



Комерційно доступні технології кібер-безпеки можуть бути розгорнуті та захищають кожен з цих компонентів. Ці технології реалізують технічні засоби контролю. Ефективність управління є контроль за дотриманням агентства політики, а також обліку та аналізу інцидентів безпеки. Крім того, існуючі технології можуть значно допомогти агентству в переоцінці раніше виявлених ризиків, виявлення нових проблемних областей.

14.2. Контроль доступу

Технологіїя контролю доступу гарантує, що тільки авторизовані користувачі або системи можуть отримати доступ і використовувати комп'ютери, мережі та інформацію яка зберігаються на цих системах, і ця технологія допомагає захистити конфіденційність даних та систем. Контроль доступу спрощує мережеву безпеку за рахунок зниження кількості шляхів, що зловмисники можуть використовувати, щоб проникнути в систему або в мережевий захист. Контроль доступу включає в себе три різних типи управління: прикордонної охорони, перевірки автентичності та авторизації. Гранична технології захисту може бути використана для захисту мережі (наприклад, мережевими екранами) або одного комп'ютера (наприклад, персональні міжмережеві екрани). Як правило, ці технології для запобігання доступу до мережі або комп'ютера від зовнішніх неавторизованих користувачів. Ще один тип прикордонної технології охорони є управління контентом, також може бути використана для обмеження здатності уповноваженої системи або мережі доступу користувачів до систем або мереж.

Перевірка справжності технологій зв'язують користувача з визначенням ідентичності. Люди проходять перевірку автентичності трьома основними способами: щось вони знають, щось у них є, або щось вони є. Люди і системи регулярно використовують ці кошти для виявлення людей в повсякденному житті. Наприклад, члени громади регулярно дізнаються один від одного по тому, як вони виглядають або як їхні голоси звучать, у чому вони є. Банкомати визнають, клієнтів, тому що вони представляють банківську карту, що вони є і вони входять в персональний ідентифікаційний номер (PIN).

У той час як використання паролів є прикладом аутентифікації на основі чого користувачі щось знають. Є кілька технологій,

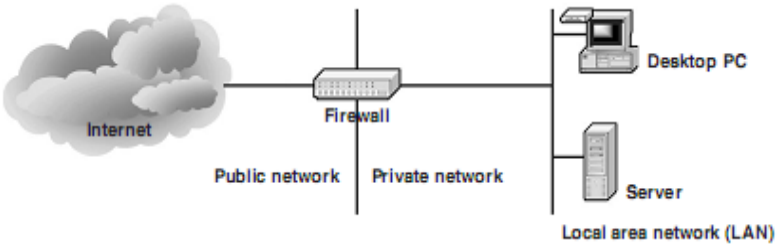
заснованих на тому що користувачі мають. Безпека маркери можуть бути використані для аутентифікації користувачів. Інформація користувача може бути закодована на знак з використанням на магнітних носіях (Наприклад, банківські картки) або оптичних носіях (наприклад, компакт-диск типу засобу масової інформації). Кілька розумних технологій містять інтегральну схему чіп, який може зберігати й обробляти дані, також доступні. Біометрична технологія автоматизації та ідентифікації людей за допомогою одного або декількох їх ,різних фізичних або поведінкових характеристик аутентифікації, заснованої на користувачу.

Використання маркерів безпеки або біометричних технологій, вимагає встановлення відповідної аутенфікації на мережу і точки доступу до комп'ютера. Як тільки користувач пройшов перевірку автентичності, та авторизацію яку використовують для того щоб запобігти діям, яким користувач відповідає заздалегідь визначеним правилам. Користувачам може бути наданий доступ до даних систем або виконавши певні дії системи. Авторизація технології підтримують принципи законного використання, мінімальних привілеїв і поділу обов'язків. Контроль доступу може бути ідентифікації користувача, ролі, членства в групах, або іншу інформацію, до відома системи. Більшість операційних систем та деякі програми забезпечують деяку аутентифікацію та авторизацію функціональності. Наприклад, користувач ідентифікаційного номера (ІН) коду та пароля найбільш часто використовують технологію аутентифікації. Системні адміністратори можуть призначати права користувачів і привілеї для додатків і файлів даних на основі ідентифікатора користувача. Деякі операційні системи дозволяють угруповання користувачам спростити адміністрування груп користувачів, яким потрібен той же рівень доступу до файлів і додатків.

14.3. **Граничний захист: Брандмауери**

Міжмережеві екрани мережевих пристроїв або систем під управлінням спеціального програмного забезпечення, що контролює потоки мережевого трафіку між мережами або між хост та мережею. Брандмауер налаштований на одну точку, яка через комунікації повинна пройти. Що дозволяє брандмауеру захисний бар'єр між захищеною мережею і будь-якими зовнішніми мережами. Будь яка інформація залишаючи внутрішню мережу може бути примушена пройти через брандмауера, оскільки це захишає мережі. Міжмережеві екрани зазвичай розгортаються де корпоративна мережа підключається до Інтернету. Тим не менш, міжмережеві екрани також можуть бути використані всередині країни, щоб охороняти області організації від несанкціонованого внутрішнього доступу. Наприклад, багато корпоративних мереж використовують брандмауери для обмеження доступу до внутрішніх мереж, які виконують важливі функції, такі, як бухгалтерський облік або персоналу. Персональні комп'ютери можуть мати міжмережеві екрани, які називається, що захистять їх від несанкціонованого доступу по мережі. Такі особисті брандмауери коштують порівняно недорого ,програмного забезпечення яке може бути встановлене на персональних комп'ютерах для фільтрації всього мережевого трафіку. По суті, брандмауер тримає небажані зовнішні дані, і чутливі внутрішні дані. (див. рис. 2).

Рис. 2: Типовий брандмауер: Захист хостів приватної мережі та громадської мережи.



Як працює технологія

Як правило, брандмауер мережевого пристрою або вузла з двома або більше мережних інтерфейсів, один з яких підключено до захищеної внутрішньої мережі, а інший підключений до незахищених мереж, таким як Інтернет. Брандмауері працює програмне забезпечення, яка досліджує мережеві пакети, що приходять на свою мережу і вживає відповідних заходів на основі набору правил. Визначивши ці правила, які дозволяють тільки вповноваженим мережевим трафіком потоку між двома інтерфейсами. Налаштування брандмауера передбачає створення правил належним чином. Одна конфігурація стратегії полягає у відмові всього мережевого трафіку, а потім включати тільки обмежений набір мережевих пакетів, щоб пройти брандмауера. Уповноважений мережевий трафік буде включати в себе з'єднання необхідних для виконання функцій, таких як відвідування веб-сайтів і отримання електронної пошти.

NIST(Національний Інститут Стандартів і Технологій) описує вісім видів брандмауерів: брандмауери пакетного фільтра, із збереженням стану перевірки брандмауерів, застосування брандмауерів з проксі-шлюзом, проксі міжмережевих екранів, гібридні технології

міжмережевого екрану, трансляція мережевих адрес, хост-брандмауери, а також персональних брандмауерів / персональний брандмауер техніки. Пакетний фільтр маршрутизації пристроя брандмауера, включає всебе контроль доступу функціональності системи адрес і сеансів зв'язку.

Управління доступом функціональності брандмауера та пакетного фільтра регулюється набір правил який дозволяє блокувати мережеві пакети на основі числа та їх характеристики, у тому числі адресу відправника і одержувача, мережевий протокол, а також джерело і номера порту призначення. Пакет Фільтр брандмауери звичайно містяться на зовнішньому кордоні з ненадійною мережею, і вони утворюють першу лінію оборони.

Брандмауерами відслідковують мережні з'єднання, що використовують мережеві програми для надійної передачі даних. Коли програма використовує мережеве підключення для створення сеансу з віддаленої хост-системи, порт також відкриваєься у вихідній системі. Цей порт отримує мережевий трафік від призначення системи. для успішного зв'язку, пакетний фільтр брандмауера повинен дозволяти вхідні пакети з призначення системи. Відкриття багатьох портів, щоб вхідний трафік створює ризик вторгнення несанкціонованих користувачів, які можуть використовувати різні методи зловживання конвенцій очікування мережевих протоколів, таких як протокол управління передачею (TCP). Брандмауери вирішили цю проблему шляхом створення каталогу вихідних мережних сполук, а також відповідний порт клієнта в кожній сесії.

Додаток брандмауери проксі-шлюз забезпечує додатковий захист від вставки брандмауер в якості посередника між внутрішнім додатком, спроба зв'язатися з зовнішніми серверами, такими як веб-сервер. Наприклад, веб-проксі отримує запити на зовнішні веб-сторінки у усередині брандмауера і передає їх у узовнішній веб-сервер , і наче Брандмауер буде посилати запит до веб-клієнта.

Зовнішній веб-сервер реагує на брандмауер і сервер переадресовує відповідь , ніби клієнт брандмауера були з веб-сервера. Немає прямого підключення до мережі зробленого з хост клієнта всередину, зовнішнього веб-сервера.

Виділені сервери проксі зазвичай розгортаються за традиційні Брандмауер платформ. У типовому використанні, основний брандмауер може приймати вхідні мережевого трафіку, визначити, які програми стають мішенню, а потім передавати трафік на відповідний проксі-сервер (наприклад, по електронній пошті Проксі-сервер). Проксі-сервер звичайно буде виконувати фільтрацію на трафік, а потім направити його до внутрішніх систем . Проксі-сервер або вихідний трафік безпосередньо з внутрішньої системи, фільтрів або трафіку, а потім його передати в брандмауер вихідної поставки. Багато організацій дозволяють кешування часто використовувати веб-сторінки на проксі-сервер, тим самим знижуючи трафік брандмауера.

В додаток на володіння аутентифікації і ведення журналу, проксі-сервери корисні для веб-електронного сканування змісту поштою.

Гібридні технології брандмауера є брандмауер продуктів, які включають функціональність декількох різних типів брандмауерів платформ. Наприклад, багато виробників фільтр пакетів або брандмауерів з потокової перевіркою Пакетний фільтр брандмауери реалізували основні проксі-сервера функціональністю, щоб компенсувати деякі недоліки, пов'язані з їх платформамми. У більшості випадків, ці постачальники реалізації програм проксі-сервери, щоб забезпечити поліпшену реєстрації мережевого трафіку і користувачів аутентифікації. Майже всі великі постачальники брандмауерів ввели кілька функції у свої продукти якимось чином, тому не завжди просто вирішити, який конкретний продукт брандмауера найбільш відповідний для цього додатка або інфраструктури підприємства. Вибір гібридного продукту

брандмауера повинен бути заснований на підтримуваних наборів функцій , що підприємству необхідно.

Трансляція мережевих адрес (NAT), технології є ефективним інструментом для мережевої адреси внутрішньої мережі за брандмауером навколишнього середовища. По суті, NAT дозволяє організації для розгортання мережі в адресному плані за своїм вибором за фаєрволом при збереженні можливості підключення до зовнішніх систем через брандмауер. Мережева трансляція адрес здійснюється одним із трьох методів: статичні, хования, і порт. У статичному NAT, кожен внутрішньої системи на приватні мережі має відповідний зовнішній, маршрутизований протокол Інтернету (IP) адресу, пов'язану з ним. Даний метод використовується рідко бо унікальні IP-адреси в дефіциті. З хования NAT, всі системи за брандмауером одні й ті ж зовнішні, маршрутизовані адреси IP, в той час як внутрішні системи використовують приватні IP-адреси. Таким чином NAT системи, за фаєрволом виявиться єдину систему. З порту трансляції адрес, можна розмістити хост за брандмауером системи і до цих пір робить їх доступними для вибіркових зовнішніх користувачів.

Хост-брандмауерів є брандмауер програмні компоненти, які доступні у деяких операційних системах або як доповнення. Оскільки мережеві брандмауер не може повністю захистити внутрішні сервери, локальні брандмауери можуть бути використовуватися для захисту окремих вузлів.

Персональні брандмауери та особистої техніки брандмауер використовуються для ПК у віддалених місцевостях. Ці міжмережеві екрани мають важливе значення тому що багато дистанційного персоналу або роботи на дому і доступу конфіденційних даних. Домашні користувачі набору Інтернет-провайдерів можуть потенційно мати обмежений захист брандмауера , тому Інтернет-провайдер застосовує різну політику безпеки. Таким чином, персональні міжмережеві екрани були

розроблені для забезпечення надійного захисту віддалених систем, а також виконувати безліч тих же функцій, що й великі брандмауери. Ці продукти, як правило, реалізовані в одній з двох конфігурацій. Первісна конфігурація персональний міжмережевий екран, який встановлений в системі який захищає; персональні міжмережеві екрани, як правило, не забезпечують захист в інших системах або ресурсах. Крім того, персональні міжмережеві екрани зазвичай не забезпечують контроль мережевого трафіку, проходження комп'ютерної мережі, вони захищають тільки комп'ютер, на якому вони встановлені. Друга конфігурація є персональний брандмауер пристрою. У більшості випадків, особисті Брандмауер техніки призначені для захисту невеликих мереж, таких як мереж, які можуть бути знайдені в домашніх офісах. Ці пристрої зазвичай працюють на спеціалізованих апаратних та інтегрують деякі інші різновиди мережевих компонентів інфраструктури в брандмауері, в тому числі такі: кабель або цифрової абонентської лінії широкосмугового модему з мережевої маршрутизації, центральний вузол мережі, мережевого комутатора, протокол динамічної конфігурації хоста (DHCP), сервера, Simple Network Management Protocol (SNMP) агент, і агентами проксі програми. З точки зору стратегії , особисті брандмауери та зазвичай проблемними є адреса підключення , пов'язані з віддаленням філій. Тим не менш, деякі організації використовують ці прилади на їх організаційних інтернетах, практикуючи багаторівневу стратегію захисту.

Централізоване управління розподіленими брандмауерами Адміністратор безпеки, а не користувачі, визначає і підтримує політику безпеки. Це накладає відповідальність і можливості визначення політики безпеки , які можуть правильно заблокувати цільові системи. Централізовано керована система немає необхідності керувати кожною системою окремо. Належним чином розподілена система включає брандмауер винятком безпеки.Більш просунуті системи включають в себе можливість застосування відповідної політики, що проводиться в життя в залежності від

розташування брандмауера. Централізоване управління розподіленими брандмауери можуть бути , програмне забезпечення або апаратні брандмауери. Централізоване управління розподілення програмного забезпечення функцій брандмауера схожі на основі хоста чи особистих міжмережевих екранів, але їхня політика безпеки централізовано визначається і управляється. Централізоване управління розподіленими апаратними брандмауерами об'єднує можливості фільтрації міжмережевих екранів з можливістю підключення за традиційним з'єднанням.

Ефективність технології

При правильному налаштуванні всіх брандмауерів може захистити мережі або ПК від несанкціонованого доступу по мережі. Хоча брандмауери захисту певних ресурсів діють в рамках організації. Є деякі загрози, що брандмауери не можуть захистити від: сполуки, які обходять міжмережевий екран, нові загрози, які ще не були визначені, і віруси, які були введені в внутрішню мережу. Це важливо враховувати ці недоліки, крім самого брандмауера з метою протидії ці додаткові загрози і забезпечують комплексне рішення безпеки. Кожен тип брандмауера платформа має свої сильні і слабкі сторони.

Пакетний фільтр брандмауера мають дві основні переваги: швидкість і гнучкість. Пакетний фільтр брандмауера можуть бути використані для забезпечення практично будь-який типів мережевих комунікацій або протоколу. В пакет фільтрів брандмауера є кілька недоліків: вони не можуть запобігати атакам, які використовуються конкретними програмами вразливостей або функції, вони можуть увійти тільки мінімальна кількість інформації, таких як адреса джерела, місця призначення адреси і тип трафіку, вони не підтримують аутентифікацію користувачів, і вони уразливі для атак , які використовують недоліки в TCP / IP протокол, наприклад, IP-спуфінга адрес.

Брандмауерами Stateful Inspection частка сильних і слабких сторін пакета фільтра міжмережевих екранів, але через реалізацію таблиці станів, вони як правило, вважається більш безпечним, ніж фільтр пакетів брандмауерів. Stateful Inspection брандмауери можуть розміститися в інших мережевих протоколів в таким же чином, що пакетні фільтри роблять, але динамічна перевірка технології відноситься тільки до TCP / IP протоколу.

Брандмауери проксі-шлюзу мають численні переваги порівняно з пакетним фільтром брандмауера і брандмауерів інспекції. По-перше, застосування проксі-брандмауера шлюзу можуть вивчити весь пакет мережі а не тільки мережевих адрес і портів. Це дозволяє цим брандмауерам забезпечення більш розширених можливостей реєстрацій подій, ніж пакетні фільтри або брандмауери роблять динамічну перевірку. Іншою перевагою є те, що застосування проксі-брандмауера, шлюз може виконувати перевірку автентичності користувачів безпосередньо, в той час як фільтр пакетів брандмауерів звичайно є огляд аутентифікації користувачів на основі мережевих адрес їх системи (наприклад, джерела, місця призначення, типу). Враховуючи, що мережеві адреси можна легко підробити, можливі аутентифікації властиві шлюзу прикладного проксі перевершують ті, що в пакеті фільтра або з збереженням стану перевірка брандмауерів. Передові функціональні можливості проксі програми шлюз брандмауера також наводить ряд недоліків в порівнянні з функціональністю фільтр пакетів або брандмауер з відстеженням стану інспекції. По-перше, через "повний усвідомлений пакет" зустрічається в проксі програми шлюзи, брандмауер змушений витрачати значний час і читання інтерпретації кожного пакета. Таким чином, застосування брандмауерів проксі-шлюзу як правило, не підходять з високою пропускною здатністю або додатків реального часу. Щоб зменшити навантаження на брандмауер, проксі-сервер може бути використовувати менше часу для безпеки, чутливих послуг, таким як електронна пошта і більшість веб-трафіку.

Іншим недоліком є те, що застосування брандмауерів проксі-шлюзу, часто обмежені в плані підтримки нових мережевих програм і протоколів. Окремі, специфічні для програми агента проксі , потрібна для кожного типу мережевого трафіку, яка повинна пройти через брандмауер. Більшість виробників проксі програм надають загальний агент проксі для підтримки невизначених мережевих протоколів і додатків.

Виділені сервери проксі дозволяє організації для забезпечення користувачів вимоги до перевірки достовірності та інші фільтрації та перевірку будь-якого трафіку , який проходить через проксі-сервер. Це означає, що організація може обмежити вихідний трафік на певних місцях, перевірити всі вихідні повідомлення електронної пошти на наявність вірусів, або обмежити внутрішнім користувачам запис в організації Веб-сервер. Оскільки більшість проблем безпеки виходять зсередини організації, проксі-сервери можуть допомогти в зриві внутрішніх атак або зловмисних поведінок.

З точки зору сильних і слабких сторін кожного типу NAT-статичний, або Порт-застосований в певних ситуаціях; мінлива кількість гнучкість конструкції, пропоновані кожного типу. Статичний NAT пропонує найбільшу гнучкість, але це не завжди практично через брак IP адрес. Приховування NAT технології, рідко використовується, тому що адреса порту пропонує додаткові можливості. Port Address Translation часто є найбільш зручним і безпечним рішенням.

Хост-пакетів брандмауера як правило, надають можливість контролю доступу для обмеження трафіку та сервера. Недоліком локальних брандмауерів є те, що вони повинні бути введені окремо, так і підтримувати безпеку стає все більш складно, як число налаштованих пристроїв збільшується.

Централізоване управління розподіленими брандмауерів є вигода, єдиний корпоративний нагляд за брандмауером реалізації на

окремих машинах. Тим не менш, вони залишаються вразливими для атак на хост операційну систему від мережі, а також навмисних або ненавмисних фальсифікацій на користувачів, підключених до системи, яка в даний час захищена. Обладнання розподілених брандмауерів може бути призначені для не локальних або мережевих атак через хост операційну систему.

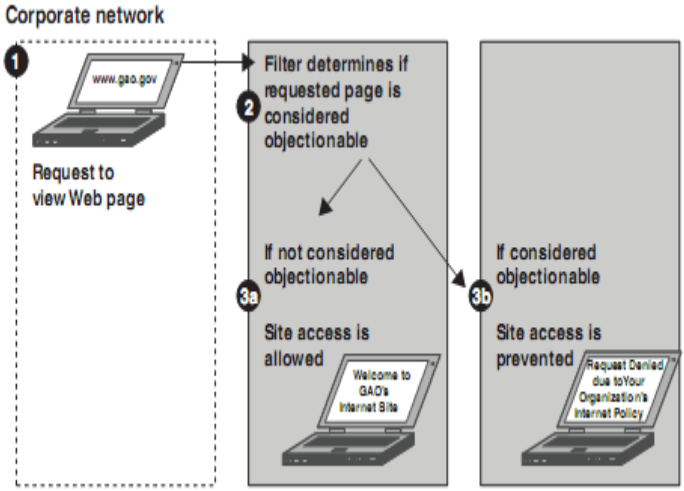
14.4. Зміст управління прикордонної охорони

Вміст фільтра і веб-додатків обміну повідомленнями за неналежним змісту, спаму, порушень інтелектуальної власності, недотримання організації політики безпеки, і заборонення типів файлів. Фільтри можуть допомагають підтримувати незаконні матеріали із системи організації, зниження мережевого трафіку від спаму, а також припинити різні типи атак. Вони можуть також відстежувати, які користувачі переглядають веб, де, і як довго.

Фільтри: (1) веб-фільтри, які виключити з доступу веб-сторінки, які вважаються небажаними або не пов'язані з бізнесом. (2) повідомлення фільтрів, які існують три основні типи контент-додатків обміну повідомленнями, такі як електронна пошта, миттєві повідомлення, короткі повідомлення служби, та точка-однолітків для спаму або іншого небажаного змісту, а також (3) веб цілісності фільтрів, які забезпечують цілісність веб-підприємства сторінок.

Як працює технологія

Рис 3: Як працює Web Filter



Веб-фільтр блокує небажані веб-сторінки шляхом (1) перехоплення запиту користувача на перегляд веб-сторінок, (2) визначення того, що запитувана сторінка містить небажаного змісту, і (3) забороняють користувачеві доступ до цієї веб-сторінці (див. рис. 3). Веб-фільтри можуть спостерігати і реагувати на запити за двома основними напрямками. Один з методів, наскрізну технологію, вимагає програмного забезпечення веб фільтрації, щоб бути інтегрована з іншими мережами пристроями,таких як проксі-серверів або шлюзів. Це гарантує, що всі запити проходять через веб-фільтр, щоб бути прийнятой або відхиленой. Інший метод обробки запитів, відомий як передача за технологією, вимагає, щоб веб фільтрація програмного забезпечення встановлювалась на окремий сервер і поміщена на мережі машин, що для фільтрації. Веб-фільтр, отримує весь трафік, який існує в мережі. Якщо запит зроблено для обмеженої веб-сторінки, веб-фільтр буде відображати повідомлення про помилку , що доступ користувача до веб-сторінки

було відмовлено. Зв’язок користувача з веб-сайтом є закритим, то веб-сервер відправляє додаткову інформацію на комп'ютер користувача. Веб-фільтри також різняться за методами визначення, якщо запрос веб-сторінки містить небажаний матеріал:

• **Сайт технологію класифікації** порівнює запрос сайту на бази даних веб-сторінок, які вважаються небажаними. як правило, постачальники надають основну базу даних небажаних веб-сторінку як частини програмного забезпечення веб-фільтру, який потім може бути змінений адміністратором. Продавці часто надають абонентське обслуговування так як бази даних клієнтів можуть бути автоматично оновлюваними з новими сайтами, які були визнані запереченними. База даних складається в основному зі списку веб-сайту адреси, як правило, розділені на групи, такі як азартні ігри, дорослі матеріали і спорту. Адміністратор може потім вирішити, які сайти повинні бути заблоковані. Якщо запитуваний веб-сайт перебуває у списку небажаних веб-сайтів, веб-фільтр буде відображати повідомлення, що інформує користувача, що він або вона не були позбавлені доступу до Веб-сторінки.

• **Зміст класифікації** використовує штучний інтелект в поєднанні з сайту класифікації методів підтримування оновленої бази даних. Перед користувачем можна переглянути веб-сайт, веб-фільтр, перевірити текстовий зміст веб-сторінки, вихідного коду. Сумнівний зміст визначається за наявності ключових слів або фраз або поєднанням ключових слів і рівня непристойних слів. Знайдені веб-сайти будуть небажаними в залежності від їх змісту та можуть бути додані в базу даних небажаних сайтів. Веб-сайти не повинні бути заблоковані для всієї організації, але може бути заблоковані на основі IP-діапазону адрес, імен хостів, або іншими критеріями.

Повідомлення фільтрів працюють за аналогією з веб-фільтрів і може досліджувати зміст повідомлення для фільтрації спаму, образи, або рекреаційних електронної пошти, які знижують продуктивність працівників.

Повідомлення на основі типу вкладень і відправників електронної пошти, як це визначено політикою організації.Виключення файлів засновані на їх розширенях файлу, або останніх частин їхніх імен, що свідчить про тип файлу. Файли можуть бути виключені для обмеження незаконного обігу матеріалу, зупинити проникнення вірусів у мережі, обмежувати інтелектуальну власність порушень або здійснювати інші такі функції, спрямовані на підвищення безпеки організації. Розширення файлів, які зазвичай виключені в MP3 (музичні файли), JPG (графічні файли), MPEG (відео файлів), і EXE (Виконувані файли), серед інших. Веб-фільтр забезпечує цілісність змісту веб-сторінки. Якщо веб-сервер піддається нападу або стає недоступним для користувачів, веб цілісність фільтра зберігає неавторизований доступ до інформації від надбанням громадськості. Фільтр контенту є окремим пристроєм в мережі, розташованої між веб-сервером і маршрутизатор або брандмауер. Пристрій містить колекцію цифрових підписів уповноважених веб-вмісту, що, як відомо,є законними. При запиті до веб-серверу, кожний цифровий об'єкт, підпис порівнюється з цифровим підписом, що було , зібрано раніше.

Якщо цифрові підписи не збігаються, то сторінка вважається несанкціонована і буде негайно замінена з архів копія оригінальної сторінки, і програмне забезпечення повідомляє відповідний персонал по телефону, електронною поштою.

Ефективність технології:

Вміст фільтрів мають значні темпи як помилково приймаючи небажані сайти і блокування сайтів, які не є небажаними. Якщо все зроблено правильно, фільтрація може скоротити обсяг небажаних і небажаних повідомлень електронної пошти. Тим не менш, це не зовсім точні, і законні повідомлення які можуть бути заблоковані. Крім того, контент-фільтри не працюють у всіх операційних

системах. Хоча наскрізна технологія може бути ефективна при зупинці вказаного трафіку.

Тим не менш, недолік передачі в тому, що окремий сервер повинен бути присвячений виконання моніторингу та фільтрації функцій. Сайт класифікації є ефективним відповідно доступу користувачів до сайтів, які було визначено, за небажаним змістом. Однак через Розмір і ріст Інтернету, ця технологія стикається з проблемами в зберіганні повних і точних списків небажаних сайтів. По-перше, веб-сайти , які в переважно графічний характер, можуть, не містяти достатнього ключа для програми по категоріям сайтів. По-друге, є деякі теми, які настільки неоднозначні, що це дуже важко класифікувати їх, та зміст. По-третє, користувачі можуть обійти фільтрацію списків за допомогою проксі- сайтів.

15. АУНТЕНФІКАЦІЯ: БІОМЕТРІЯ

Термін *біометрія* охоплює широкий спектр технологій, які використовуються щоб засвідчити особу за допомогою вимірювання та аналізу людських характеристик. Біометричні технології аутентифікації методів, які спираються на вимірювання та аналізу фізіологічних або поведінкових характеристик. Фізіологічні характеристики людини включають в себе вимір частини тіла, наприклад, пальців або очей і риси, визначення поведінкових характеристик включають в себе.

Біометрія теоретично дуже ефективна в особистих ідентифікаторах, оскільки характеристики які вони вимірюють, є різними для кожної людини. На відміну від традиційних методів ідентифікації, які використовують щось у вас є (Наприклад, смарт-карта), або щось ви знаєте (наприклад, пароль), ці характеристики є невід'ємною частиною .

Як працює технологія

Хоча біометричні технології різняться за складністю, можливості та продуктивності, всі вони мають кілька елементів. Біометричні системи істотно системах розпізнавання образів. Вони використовують придбання пристроїв, таких як камери і скануючих пристроїв для захоплення зображення, записів або вимірювання характеристик особистості, і використання комп'ютерної техніки та програмного забезпечення для витягання, кодування, зберігання і порівньюють ці характеристики. Тому що процес автоматизований, біометричного прийняття рішень, як правило, дуже швидко, в більшості випадків приймають тільки через кілька секунд у режимі реального часу. Різних типів біометричних технологій вимірювання різних характеристик. Проте всі вони пов'язані з аналогічними процес, який може бути розділений на два окремих етапи: (1) реєстрації та (2) перевірки чи ідентифікації.

Реєстрації . Придбання таких пристроїв, як камери та сканери використовуватися для захоплення зображень, записів або вимірів характеристики людини та комп'ютерного обладнання та програмного забезпечення використовуються для вилучення, кодування, зберігання, і порівняння цих характеристик. У реєстраційному етапі захоплені зразки є усередненими й обробляються для створення унікального цифрового представлення характерно, називається контрольним шаблоном , яка зберігається для майбутніх порівнянь. Неможливо відтворити зразки, таких як відбитки пальців, з шаблону. Шаблони можуть бути збережені централізовано на комп'ютерній базі даних, в самому пристрої, або на смарт- карті.

Перевірка або ідентифікації стадії. Залежно від програми, біометричні технології можуть бути використані в одному з двох режимів: перевірка або ідентифікації. Перевірка використовується, щоб засвідчити особу людини, відповідаючи на питання: "Чи є це людина, яка себе видає?" Ідентифікація використовується для

встановити особу людини, порівнюючи біометричних людини з усіма зберігатися біометричні записи, щоб відповісти на питання: "Хто ця людина?"

Поточний біометричних технологій, які використовуються для захисту комп'ютерних систем від несанкціонованого доступу включають розпізнавання відбитків пальців, райдужної оболонки ока, і динамік визнання. Ці технології використовуються деякими особами в замінити паролі як спосіб аутентифікації осіб, які намагаються для доступу до комп'ютерів та мереж.

15.1. **Аутентифікація: Смарт Жетони**

Смарт-токен (smart token)легко портативний пристрій, який містить вбудовану інтегральну схему, які здатні як зберігати й обробляти дані. Більшість смарт-жетонів використовуються замість статичного ідентифікатора користувачів і паролі забезпечити більш надійним та зручним засобом для користувачів, щоб визначити і аутентифікацію до комп'ютерів і мереж. Хоча аутентифікація для деяких комп'ютерних систем базується виключно на володіння маркером,для реалізації також потрібно користувачеві надати те, що він або вона знає (наприклад, пароль) в Щоб успішно використовувати смарт-маркер.

Як працює технологія

Загалом, жетони можуть бути класифіковані відповідно з фізичними характеристиками, інтерфейсу і протоколу,які використовувані. Ці класифікації не є взаємовиключними.

1. **Фізичні характеристики**. Смарт маркери можуть бути розділені на дві фізичні групи: смарт-карт та інших маркерів.

Смарт-карта виглядає як кредитна карточка, але включає в себе вбудований мікропроцесор. Смарт жетони , які не є смарт-карти можуть виглядати як калькулятори, ключі або інші невеликі об'єктів.

2. Інтерфейси.

Два фізичних інтерфейси для смарт-карт були стандартизовані Міжнародною організацією зі стандартизації, в результаті чого є два типи смарт-карт. Перший тип, відомий як картки контактів, роботи вставивши картку в зчитувач смарт-карт, у той час як другий тип, відомий як безконтактні картки, використовує радіосигнали частотою, і карта повинна тільки бути передана в безпосередній близькості від карти терміналу для передачі інформації. Смарт-карти можуть бути налаштовані на контакти які включають в себе як і безконтактні можливості, а тому, що стандарти для двох технології дуже різні, два окремих інтерфейсу буде

необхідності.

3. Протоколи. Смарт жетони використовують три основні методи аутентифікації, на основі різних протоколів. Перший метод, статичний пароль обмін, вимагає, щоб користувач спочатку ідентифікував себе маркером до маркера може аутентифікації користувача на комп'ютері.

Дві інші методи відомі як час синхронізуються і завдання-відповідь, і засновані на криптографії. Ці методи використовують одноразовий пароль, який є паролем або передача коду, який може бути використаний тільки один раз, за короткий проміжок часу, а потім вже не діє. Якщо це перехопили в будь-якому випадку, пароль такий обмежений терміном служби, який швидко втрачає свою силу. доступ до системи, то він чи вона повинні вийти на

Час синхронізації маркера та формування унікального значення, що змінює регулярні інтервали (наприклад, раз на хвилину). Центральний сервер відстежує маркера згенерованого пароля для

порівняння вхідного проти очікуваного значення. Щоб увійти на систему, користувач вводить одноразовий пароль, який складається їх особистого PIN-коду та наступного унікального значення маркера. PIN-код допомагає центральним сервером для ідентифікації користувача і пароля значення, яке має бути введено. Якщо число, введене користувачем і той, що генеруються сервером тому ж, користувачеві буде надано доступ до системи. На малюнку 7 показаний приклад часу синхронізації маркера.

Рис. 7: Приклад часу синхронізованого маркера

Запит-відповідь жетони використовувати центральний сервер для генерації виклик (Наприклад, випадковий набір цифр), яке користувач буде потім увійти в маркер. Маркер потім обчислює відповідь, яка служить колишній цифровий пароль, який вводиться в систему. Якщо відповіді від Користувач же, як і очікується відповідь від сервера, користувач буде надано доступ до системи. У деяких реалізаціях, користувач повинен ввести PIN-код, перш ніж сервер буде генерувати виклик. На малюнку 8 Прикладом запит-відповідь маркер.

Рис. 8: Приклад запит-відповідь маркера

Ефективність технології

Якщо вони будуть реалізовані правильно, розумні жетони можуть допомогти в створенні безпечне середовище аутентифікації. Одноразовий пароль усунення Проблема електронного моніторингу, або "Пароль нюхають", і маркери, які вимагають використання PIN-коду допомагають знизити ризик

15.2. Аудит і моніторинг

Аудит і моніторинг технології можуть допомогти адміністраторам безпеки для регулярного оцінювання комп'ютерної безпеки, проводити дослідження під час і після атаки.

Ми описуємо чотири типи аудиту та моніторингу технологій: вторгнення ,Системи виявлення, системи запобігання вторгнень, безпека події кореляції інструментів та комп'ютерної експертизи. Виявлення вторгнень і системи запобігання вторгнень моніторингу та аналізу подій, що відбуваються на системи або мережі, і або оповіщення відповідного персоналу або запобігти нападу з виробництва. Зважаючи на великий обсяг даних, зібраних на деяких системах і мереж, ці інструменти можуть визначити ключову інформацію з використанням кореляційного аналізу. Програмно-технічна експертиза включає в себе виявлення, збереження, вилучення та документування комп'ютерної заснований доказів. Програмно-технічна експертиза використовуються під час дослідження комп'ютерної злочинності, виявити злочинця і методи, які використовувалися для проведення атаки.

15.2.1. **Система виявлення вторгнення**

Система виявлення вторгнень (IDS) виявляє, неправильну, або аномальну активність, спрямованої на підрив конфіденційності, доступності чи цілісності мережі, захищеної комп'ютерної системи. IDS збирає інформацію про мережу, аналізує інформацію про основний попередній набір правил, а потім відповідає на аналіз. Особливий тип IDS, відомий як приманка, діє як приманка сервера або система, яка збирає інформацію про нападаючий або охоронно такі, як метод вторгнень і уразливості, які використовуються з метою підвищення е безпеки. Щоб привернути нападників, приманка, містить важливі дані, але замість цього вони

містять неправдиві відомості. Приманки можуть бути налаштовані на оповіщення системного адміністратора атаки по електронній пошті або на пейджер, дозволяє адміністратору, переконатися, що принада не використовується як плацдарм для майбутніх атак.

Як працює технологія

Є три загальних типу IDS, класифікуються за джерелом інформацію, яку вони використовують для виявлення вторгнень: мережевий, на базі хоста, а також на базі додатків.

Мережеві системи IDS виявлення атак шляхом захоплення і аналізу мережевих пакетів. Мережеві системи IDS часто складаються з набору вузькоспеціалізованих датчиків або вузлів, розміщених в різних точках мережі. Ці пристрої моніторингу мережевого трафіку, виконують локальний аналіз, що трафіку і звітності атаки центральної консольного управління. тому що ці датчики обмежуються запуском програми IDS тільки, вони можуть легше бути захищені від атак. Багато з цих датчиків призначені для роботи в "стелс" режимі, що робить його більш важким для атакуючого виявити їх присутність та місце знаходження. Хост-системи IDS збирають інформацію з окремого комп'ютера і використовують цю інформацію для виявлення вторгнень. Хост-система IDS може визначити, які саме процеси і облікові записи користувачів, що беруть участь в зокрема нападу на системи. Крім

того, на відміну від електричної IDS, хост-системи IDS можуть більш легко розпізнати очікуваний результат атак, тому що вони можуть отримати прямий доступ і контроль даних файла та системних процесів. Хост- IDS, зазвичай використовують два типи джерел інформації: операційна система аудиту та системний журнал. Операційна система аудиту зазвичай генерується на внутрішньому рівні операційної системи, тому система аудиту більш докладно і краще захищена, ніж системні журнали. Деякі хост-системи IDS призначені для підтримки централізованого управління IDS та звітності інфраструктури, яка може дозволити єдиної консолі управління для відстеження багатьох хостів. Інші генерувати повідомлення у форматах, сумісні з системою управління мережею.

Програма на базі системи IDS є спеціальні підмножини хост-системи IDS, що аналізують події, що відбуваються на конкретні програми. Найбільш поширеними джерелами інформації використовується на базі програм IDS, є програми файли журналу транзакцій. Тому що вони безпосередньо взаємодіють з застосування і конкретних знань, на основі програми виявлення вторгнень можуть виявити дії авторизованих користувачів, які намагаються перевищують їх дозвіл. Це тому, що такі проблеми частіше з'явилися в взаємодію між користувачем даних та програми. Ці системи IDS характеризуються чотирма основними якостями: джерело інформації, метод аналізу, термінів, і відповідні заходи. IDS, є два основних способи проведення аналізу. Підпис (Іноді їх називають, заснованої на знаннях, або на основі шаблонів) аналіз спирається на попередні відомі атаки, щоб виявили атаку, яка відбувається. IDS аналіз активності системи, дивлячись на події, які відповідають визначеним картин подій, в якій описані відомі атаки. Аналіз порівнює поточну роботу системи або мережі від дійсним або приймають поведінку системи. В основі аномалії IDS створює базові норми (дійсним або приймається) поведінки через різні методи. Якщо поточна поведінка системи не буде в

межах норми межі поведінки, то це буде інтерпретуватися, як IDS атаки. IDS, можна використовувати як інтервал основі або в режимі реального часу терміни методом. інтервал, заснований на тимчасових методах аналізу даних по заданому графіком. Цей метод дозволяє IDS для збору великої кількості даних.

В режимі реального часу метод аналізу реагує на дані по мірі їх надходження, дозволяючи адміністраторам реагувати в режимі реального часу для атак. IDS, можуть реагувати на можливі атаки з використанням активних або пасивних стратегій реагування. Активні IDS відповідає за вторгнення системи запобігання (IPS). Пасивний IDS відповідає, за генерування сигналізації для адміністратора. Тривога може з'явитися на екран адміністратора і забезпечує адміністратора інформацію, таку як тип атаки, розташування атаки, рівень загрози і, можливо, атака є успішною. Пасивна відповідь IDS залежить від людини вживання заходів у відповідь на попередження.

Ефективність технології

IDS, не може миттєво виявити, звіт або відповідати на атаки, коли є важкі мережі або обчислювального навантаження. Таким чином, системи IDS є уразлива для атак та відмови в обслуговуванні; зловмисникові може відправити великий обсяг інформації через мережу та придушити IDS, дозволяє людині почати ще один напад, яке потім непомітно для IDS. Ефективність IDS може бути кілька, визначається числом помилкових спрацьовувань і помилкових негативів, які він генерує. Помилкове спрацьовування відбувається, коли IDS попередження, що є атака та відбувається, коли насправді немає атаки. Адміністратори повинні присвятити достатню кількість часу, щоб регулярно переглядати IDS журнали і тонка настройка IDS, щоб обмежити число помилкових

спрацьовувань. Іноді IDS можуть бути відключені для зручності. Зловмисник може використовувати цю вразливість, повільно змінювати роботу системи або мережі IDS. Аномалії в основі системи IDS також є змінна кількості часу, щоб обчислити дійсний або прийняті поведінки, так що для певного періоду часу IDS не буде ефективним методом виявлення атак.

15.2.2. **Система запобігання вторгнення**

Як ми вже говорили, систем запобігання вторгнень IDS, які є активною стратегією реагування. Це означає, що IPSS не тільки дозволяє виявляти інтрузівну діяльність, вони також можуть спробувати зупинити діяльність, в ідеалі, перш ніж він досягає своєї мети. Система попередження вторгнень є набагато ціннішим, ніж виявлення вторгнень, виявлення вторгнень, оскільки просто спостерігає події не роблячи жодних зусиль, щоб зупинити їх. IPSS часто поєднують найкращий міжмережевий екран, виявлення вторгнень, антивірус, і оцінки вразливості технології. Їх увагу, проте, по запобіганню виявлених атак, які могли б експлуатувати існуючі уразливості в захищену мережу або хост-системи.

<u>Як працює технологія</u>

Як IDS, IPSS або мережі чи хост. Вони виконують IDS функції і, якщо вони виявляють вторгнення, вживання заходів, такі як

блокування мережевого трафіку для запобігання атак з виробництва. Мережеві IPSS можутю просто монітор мережного трафіку або ж вони можуть бути "в лінії ", що означає, що діяльність повинна проходити через них. Мережеві IPSS ретельно контрулюють трафік даних, звичайно за допомогою спеціалізованого обладнання для компенсації витрат на обробку, що інспекція споживає.

Якщо IPS відповідає на напад вжити заходи проти порушника (режим роботи зазвичай називають як атаки назад або ударно-назад), він може почати серію атак проти зловмисника.

Ефективність технології

Системи запобігання вторгнень є логічним розвитком вторгнень системи виявлення. Замість того, щоб впоратися з постійним попередженням тривоги IDS, IPSS можуть запобігти атаки шляхом блокування підозрілого трафіку мережі.

Головна цінність деяких IPSS є їх здатність "вчитися", що становить прийнятної поведінки і припинити діяльність, яка nNetwork основі IPSS пропозицію в оперативний контроль потоків даних по всій мережі і надають можливість для запобігання спроб вторгнення.

Хост-IPSS дозволяє системам та програм які повинні бути індивідуально налаштованою для запобігання нападів на операційній системи або додатків. Ці IPSS підходять заходи з надання допомоги охороняючи непропатченних і експлуатованих

систем від атак, але вони вимагають значної користувача адміністрації.

На жаль, IPSS сприйнятливі до помилок виявлення вторгнень. Якщо виявлення інцидентів не є точним, то IPS може блокувати законні заходи, які неправильно класифікуються як шкідливі. Будь-яка організація, яка хоче використовувати системи запобігання вторгнень слід звернути особливу увагу на точність виявлення при виборі продукту.

Користувачі IPSS також стикаються з проблемою підтримки бази даних останніх сигнатури атак, так що системи можуть бути захищені від недавнього нападу стратегій. Крім того, IPSS причиною вузьких місць в мережевому трафіку, зниження пропускної по мережі.

15.2.3. **Контролювання подій безпеки**

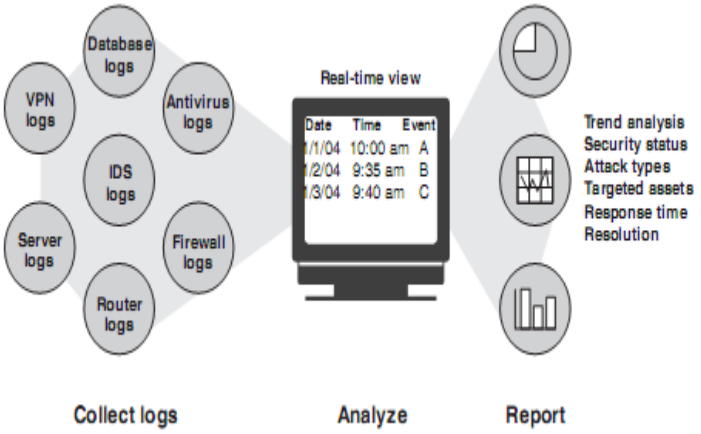
Засоби безпеки контрулювання подій збирають журнали, або списки дій, які відбулися, з операційних систем, мережевих екранів та програм, виявлення вторгнень та інших мережевих пристроїв. Потім кореляці інструментів аналізу журналів в режимі реального часу, розрізняють, чи нападстався, і реагувати на безпеку .

Огляд і аналіз журналу створюють динамічну картину поточних системних заходів, які можуть бути використані для перевірки того, що система працює відповідно до політики організації. Аналіз журналів є недостатньо, щоб отримати повну відомість всієї діяльності системи , але розмір, число, і труднощі читання через

реєстрування кожного інструменту файлів є непростим завданням для адміністратора.

Автоматизовані засоби аудиту забезпечують засоби для істотного скорочення необхідного часу огляду, і друкування звіту (Заздалегідь та налаштувати), які узагальнюють вміст журналу з набору конкретних видів діяльності (див. рис. 15).

Рис. 15: Типові Експлуатація Засобу безпеки кореляції подій



Як працює технологія

Засоби безпеки контрулювання подій з першу консолідують лог-файли з різних джерел, таких як операційні системи, міжмережеві екрани, додатки, системи IDS, антивірусні програми, сервери та віртуальні приватні мережі. Часто журнали різних джерел

надходять в різних пропрієтарних форматів, які роблять складні порівняння. В рамках процесу консолідації, подій безпеки кореляції інструментів нормалізації входить в стандартний формат, наприклад, Extensible Markup Language (як правило, називають XML). Після процесу нормалізації, непотрібні дані можуть бути усунені для того, щоб зменшити імовірність помилки.

Нормований журнали потім порівнюється (чи взаємозалежних) з метою визначення чи нападу та місце. Різноманітність кореляційних методів можуть бути використані, у тому числі складні на основі шаблонів аналізу, які можуть ідентифікувати аналогічної діяльності на різних журналів, які походять від нападу.

Об'єднуючи журнали різних IDS, кореляції інструменти можуть виявити цей тип атаки. Другий метод називається виявлення аномалій. У цьому методі базовим нормальним є активність користувачів яких було прийнято, і увійшли заходи в порівнянні з базовою лінією.

Якщо атака виявлена, інструменти можуть реагувати або пасивно або активно. Пасивна реакція означає, що ніякі дії не робляться за інструментом щоб зупинити загрозу безпосередньо. Наприклад, повідомлення може бути відправлене на системи адміністратора через пейджери або електронною поштою, інциденти можуть бути зареєстровані, і IP- адреси можуть бути додані до зловмисника або списки активів . Активну реакцію являє собою автоматизована дія, які вжиті інструментом для пом'якшення ризиків. Наприклад, одна активна відповідь, щоб блокувати атаки через інтерфейси з брандмауерами або маршрутизаторів.

Ефективність технології

Кореляція інструментів обмежена в своїх можливостях для взаємодії з численними безпеками продуктів, вони можуть бути не в змозі зібрати і співвіднести журнали певних продуктів. Крім того, ці інструменти залежать від достатності та точності журналів,

і вони не можуть виявляти атаки, які обійшли різні пристрої безпеки, такі як брандмауер і IDS. Якщо зловмисник зміг піти на компроміс журналу, то контролювання подій безпеки, інструментом можна було б проаналізувати неправдиву інформацію. Шифрування і аутентифікація в забезпечення безпеки і цілісності даних може знизити цей ризик.

15.2.4. **Інструменти компютерної експертизи**

Програмно-технічна експертиза використовуються для ідентифікації, зберігати, витягати документ комп'ютерних доказів. Вони можуть визначити паролі, лог- додатків та іншу інформацію у файлах, які були видалені, зашифровані або пошкоджені. У ході розслідування комп'ютерних злочинів, ці інструменти використовується для визначення винного і методи, які були використані для атаки.

Існують дві основні категорії комп'ютерної експертизи інструментів: (1) докази збереження та засоби збору, які запобігають випадковому або умисному зміні комп'ютерних даних і створення логічних та фізичну копію оригінального доказу, і (2) інструменти аналізу, які забезпечує відновлення даних і відкриття функцій. Кілька комерційно доступні комп'ютерної експертизи продукції включає риси обох категорії і претендує на повний набір інструментів судово-медичної експертизи.

15.2.5. Збереження фактичних даних та інструментів збору

Захист від запису і створення образу диска програмного забезпечення, яке використовують для збереження та копіювання доказів на комп'ютер при збереженні її цілісності. Є кілька методів, які використовуються програмним забезпеченням захисту від запису, який перешкоджає або забороняє спроби користувача для зміни даних на жорсткому диску комп'ютера або на іншому комп'ютері засобу масової інформації. В одному з методів, програмного забезпечення, захисту від запису та спроби отримати

ексклюзивний доступ до засобів масової інформації за допомогою механізмів, характерних для операційної системи. Якщо ексклюзивний доступ може бути отриманий, все інше програмне забезпечення заявки будуть позбавлені можливості доступу і заблоковані засоби масової інформації. Інший метод використовує окремий компонент програмного забезпечення, яке встановлений як частина операційної системи і завантажується при операційних на початку роботи . Образ диска це процес, який намагається скопіювати кожен біт даних з одного фізичного середовища комп'ютера на інші, аналогічні середовища. Цей тип дублювання відомий як фізична копія диска, і вона включає в себе копіювання всіх даних, включаючи файли, імена файлів і даних, які не пов'язані з файлом.

16. **УПРАВЛІННЯ МЕРЕЖЕЮ**

Управління мережею є можливість контролю моніторингу комп'ютерної мережі з єдиного центру. Системи мережевого управління складається з програмного забезпечення та спеціалізованих апаратних засобів комп'ютера. Перегляд всієї мережі є уніфікована архітектура для того, щоб отримати статус даних з мережі, компоненти, які вносили зміни в конфігурацію, а також попереджали мережевим адміністраторам проблеми. Міжнародна організація по стандартизації визначає концептуальну модель для опису п'яти основних функціональних областей мережі управління (і основні функції мережевих систем управління):

• **Несправність управління** вказує на проблеми, у вузлах мережі, і мережі операції, Для того потрібно визначити їх причини і вжити заходів.

• **Управління конфігурацією** моніторів та конфігурації інформації в мережі , так що вплив конкретних апаратних засобів і програмного забезпечення може бути управлятися і відслідковуватись.

• **Бухгалтерський облік** заходи з управління використанням мережі окремими користувачами або групи, щоб забезпечити платіжну інформацію, регулюють користувачів або

групи, і допомагає зберегти продуктивність мережі на прийнятному рівні.

• **Ефективність заходів** з управління різними аспектами мережі продуктивності, в тому числі збору та аналізу статистичних даних систем, з тим що продуктивність може підтримуватися на прийнятному рівні.

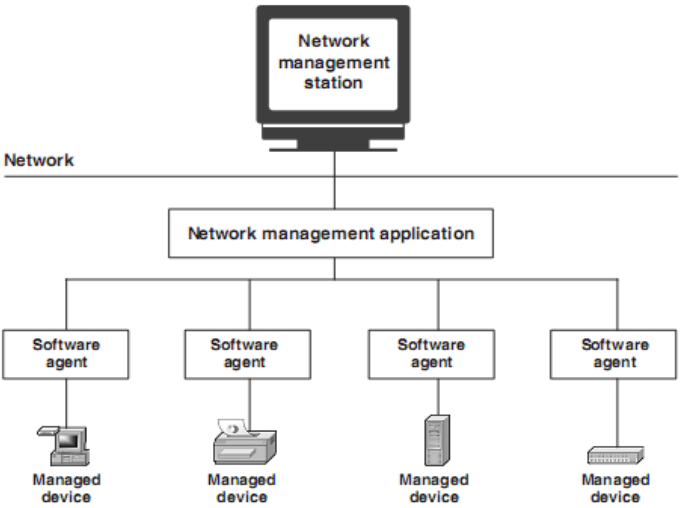
• **Управління безпекою** управляє доступом до мережевих ресурсів, обмежуючи доступ до мережевих ресурсів, а також шляхом надання повідомлення про безпеку порушень, так що інформація не може бути отримана без авторизації.

Як працює технологія:

Система управління мережею зазвичай складається з керованих пристроїв (мережевих хостів); програмні агенти, які використовують інформацію про керовані пристрої; застосування мережевого управління, яка збирає і обробляє інформацію від агентів, а також керування мережею станції, що дозволяє

оператору переглядати графічне представлення мережі, контроль керованих пристроїв у мережі, і програми мережевого керування програми. Рис 16 є прикладом типового мережевого управління архітектури.

Рис. 16: Типова архітектура управління мережею



Станції управління мережею, отримує і обробляє події мережевих елементів і виступає в якості головної консолі для мережевих операцій.

Станції управління мережею відображає графічну карту мережі, яка основні робочі стану критичних мережних пристроїв, таких як маршрутизаторів і комутаторів. Кожний мережевий пристрій представлено графічний елемент на консоль управління станцією,

а також різні кольори використовується для представлення поточний робочий станів мережних пристроїв, заснованих

про статус повідомлень, спрямованих пристроїв. Ці повідомлення (як правило, викликаються події) які знаходяться у файлі журналу.

Функціональність програмного забезпечення для управління мережею (мережеве управління програми та агенти) залежить від конкретного мережевого управління протоколу, програмне забезпечення базується на. більшість систем використовують відкриті протоколи. Тим не менш, деяке програмне забезпечення мережевого управління засноване на виробника конкретних протоколів. Два найбільш поширених мереж управління протоколів є простий протокол управління мережею (SNMP) і управління загальними Information Protocol (CMIP). SNMP які широко використовується в більшості середовищ ЛВС. CMIP використовується в телекомунікаційних середовищах, де мережі, як правило, великі і комплексні.

Ефективність технології

Системи управління мережею може бути досить дорогим, і вони часто комплексні. Складність полягає насамперед в управління мережею, протоколів і структури даних, які пов'язані з мережею управління інформацією. Крім того, ці системи вимагають спеціальну підготовку, для ефективного налаштування, обслуговування та експлуатації

системи управління мережею. Багато систем управління мережею не може підтримувати мережеві пристрої, використання конкретного виробника протоколів.

17. ІНСТРУМЕНТИ БЕЗПЕРЕВНИХ ОПЕРАЦІЙ

Безперервність операцій забезпечують повну інфраструктуру резервного копіювання ,зберігати дані підприємства, ресурси мережі й доступні в декількох місцях у разі надзвичайних ситуацій або планового технічного обслуговування, таких як системи або програмного забезпечення, модернізації. Вони підтримують оперативну спадкоємність зберігання пристроїв і хост і бази даних. Безперервність операцій включають системи високої готовності, які з'єднують два або більше комп'ютерів разом, щоб забезпечити безперервний доступ до даних за допомогою систем надмірності (відомий як кластеризація); журнал файлових систем, які підтримують конкретну інформацію про дані, щоб уникнути помилок файлової системи і корупції; балансування навантаження технологій, яка ефективно розподіляє трафік між мережевиви серверами таким чином, щоб сервер який перевантажений, і надлишковий масив незалежних дисків (RAID), що дозволяє двом або більш жорстких дисків для роботи в концерті для підвищення відмовостійкості та підвищення продуктивності.

Як працює технологія

Висока доступність системи використовують кластеризацію, яка відноситься до двох або більше серверів які створені таким чином, що якщо додаток, що працює на одному сервері не вдається, він може бути автоматично перезапущений або відновлений на іншому сервері. Це називається, як перемикання з одного сервера або вузла в кластер інший. Висока доступність системи використовують при збої операції автоматично перемикається на резервну базу даних сервера або мережі, якщо первинна система дає збій або тимчасово закрита для обслуговування. Деяка високопоставлена наявність системи може також виконувати віддалене резервне копіювання,

віддалених взаємних поглинань, паралельних операцій доступу і віддаленого відновлення системи. Ці функції описані нижче.

• При одночасному доступі, системи на обох сайтах одночасно поновлюється база даних.

• У віддаленого відновленні системи, дані можуть синхронізувати. Відновлена робота може бути реінтегрована з віддаленого резерву. У процесі, відомому як файл дзеркального відображення, що відмовила системи оновлюються з поточними даними програми та файлів, які були оброблені. Система резервного копіювання після провалу системи припинили свою діяльність. На завершення відновлення до сучасних даних і файлів дзеркала, висока наявність системи відновить синхронізовані системні операції, у тому числі Дзеркальне відображення в реальному часі дані і файли між системою сайтів. Це може виникнути під час віддаленого резервного копіювання що знаходиться у використанні.

Журнальна файлова система гарантує, що дані на диску були відновлені їх провали конфігурації. Він також відновлює збережені дані і зберігає їх у призначені місця, що робить важливу особливість для критичних додатків. Журналювання угоди файлової системи звертається послідовність зміни як одна операція, і відстежує зміни в метаданих файлової системи і призначені для користувача дані. Угода гарантує, що всі або жоден з файлів система оновлення .

Наприклад, процес створення нового файлу змінює деякі метадані цінностей. Перед файловою системою робить ці зміни, які створює умови для запису планованих змін. Як тільки угода була записаних на диску, файлова система змінює метадані, які зберігаються в журнальну файлову систему. У випадку збою системи, файлова

система відновлюється в попередній стан, повторюючи операції, перерахованих в журналі. Замість того, щоб розглянути всі метадані, Файлова система перевіряє тільки ті частини метаданих, які нещодавно змінилися.

Балансування навантаження розподіляє технології обробки та передачі рівномірно по комп'ютерній мережі шляхом передачі завдань від навантажених процесорів з тими, що більш вільні навантаженнями. Балансування навантаження грунтуються на трьох політиках: інформаційна політика, яка визначає кількість навантаження інформації, яка буде надаватися; передачі політики, яка визначає поточне навантаження на хост і розмір роботу, а також розміщення політики, яка визначає належний розподіл процесів для різних процесорів комп'ютера.

RAID-системи забезпечують великі обсяги зберігання, зробивши дані які є доступними для файлових серверів, хост-комп'ютерів, або мережі як єдине ціле (відомий як масив). Дизайн масиву дисків є важливим фактором, що визначає продуктивність і доступність даних в RAID-системи. На додаток до розгортання масиву дисків, RAID-системи включають контролер-інтелектуального електронних пристроїв, маршрутів, буферів, і управляє потоком даних між комп'ютером і мережею масиву дисків. RAID-контролери можуть організовувати дані на дисках в декількох напрямках з метою оптимізації продуктивності і надійності системи різних типів додатків. RAID може бути реалізований у програмному забезпеченні.

Ефективність технології

Безперервність в операційних технологій можуть допомогти агентствам збільшити доступність своїх важливих додатків. Деякі з технологій, такі як RAID і журнал файлових систем, підвищують здатність одного сервера, щоб зменьшити число відмов. Для багатьох агентств, комбінація з RAID. Журнал роботи файлової

системи та резервне джерело живлення може забезпечити адекватний захист від збоїв. Організації, які не переносять додаток відключення більш ніж кілька хвилин можуть розгорнути високу доступність системи, яка використовує кластеризацію. Кластеризації має доведений послужний список яке гарним рішенням для збільшення доступність додатків. Тим не менш, кластеризаці вимагає додаткових апаратних і програмних засобів кластеризації, і більш, складна в управлінні, ніж єдина система.

18. СКАНЕРИ

Сканування допомагає виявити мережі або безпеки уразливості системи.

Існують різні засоби сканування, в тому числі сканерів портів, вразливі сканери, сканери і модему.

Сканери портів використовуються для зіставлення мереж та визначення служби, що працюють на кожному комп'ютері, виявляючи відкриті TCP і User Datagram Protocol (UDP) порти. Уразливість сканера використовуються для ідентифікації вразливостей комп'ютерних хостів та мереж, а також використовувати результати, які були попередню скановані порти. Багато сканерів тепер обладнані автоматичним виправленням обраних вразливостей.

Як працює технологія

Порт сканери використовують методи, відомі як пінг і сканування портів на мережевій карті та ідентифікації сервісів, які знаходяться у використанні. Ping зачисток вважаються основной технікой для сканування мережі. Пінг визначає який діапазон IP-адрес карт на

комп'ютері, які підключені до відправника запитів зв'язку (відомої як Internet Message управління Протоколом [ICMP] ECHO запити) на кілька адрес IP. Якщо комп'ютер цільового адресу включений, то він поверне конкретну відповідь ICMP ECHO. В скануванні портів, сканер відправляє повідомлення на певний порт на цільовий комп'ютер і чекає відповіді. Відповідь на сканування може дозволити сканер для визначення: (1), які порти відкриті і (2) операційна система комп'ютера яка працює під управлінням (деякі сканування портів працюють тільки на певних операційних системах.

Хост- сканери повинні бути встановлені на кожному комп'ютері та повинні бути протестовані, і зазвичай вони вимагають адміністративного рівня доступу до роботи. Мережеві сканери працюють на мережі організації та визначають вразливі місця на декількох комп'ютерах. Сканери використовують великі бази даних відомих вразливостей для ідентифікації вразливостей, які

часто використовуються операційними системами і додатками. Коли знайдена вразливість , сканер попередить оператора, про можливі уразливості. На рис. 17 наведено приклад екрану сканер вразливостей.

Рис. 17: Приклад екрану сканера уразливостей

Модем сканери - це програми, які автоматично набере визначений діапазон телефонних номерів і відстеження успішних з'єднань в базі даних.

Деякі модем сканери можуть також визначити конкретну операційну систему, запущених на комп'ютері, і вони можуть бути налаштовані на спроби отримати доступ до системи, запустивши через заданий список загальні

імена користувачів і паролі.

Список літератури

1. INFORMATION SECURITY Technologies to Secure Federal Systems , The Honorable Tom Davis ,March 9, 2004, 76 c.
2. COMPUTER SECURITY Technologi planning study , James P.Anderson,October 1972. 104 c.
3. Информационная безопасность компютерных систем и сетей В.Ф. Шаньгин , Москва ИД<<Форум>> - ИНФРА-М .2008 г.
4. Руководство по защите от внутренних угроз информационной безопасности , Владимир Скиба, Владимир Курбатов, Питер, 2008. — 320 с: ил. ISBN 978-5-91180-855-6
5. Методы и средства защиты компьютерной информации : учебное пособие / А.А. Безбогов, А.В. Яковлев, В.Н. Шамкин. – Тамбов : Изд-во Тамб. гос. техн. ун-та, 2006. – 196 с. – 100 экз. – ISBN 5-8265-05044.
6. Информационная безопасность , Блинов А.М. , СПбГУЭФ -2010 г, 96с.
7. Управление доступом к информационным ресурсам , Гатчин Ю.А., Коробейников А.Г., Краснов А.Г, 2010 г, 45 с.
8. Introduction to Network Security , Neal Krawetz , Course Technology PTR-2007 , ISBN: 1-58450-643-1 . 608 c.
9. Серьезная литература по информационной безопасности
10. http://www.warning.dp.ua/compsec/index.html

11. http://csrc.nist.gov

12. http://arhiv-statey.pp.ua/index.php?newsid=26223

13. http://www.warning.dp.ua/compsec/index.html

14. www.gloffs.com/computer_security.htm

15. www.armor2net.com/knowledge/computer_security.htm

Мечислав Миколайович Лісневський,

спеціаліст системотехнік, магістрант

інформаційних технологій

ТЕХНОЛОГІЇ

КОМП'ЮТЕРНОЇ БЕЗПЕКИ

ІН 11М

Комп'ютерний набір, верстка і макетування та дизайн в редакторі Microsoft®Office® Word 2007 М.М.Лісневський

Науковий керівник Р. М. Літнарович, доцент, кандидат технічних наук

Міжнародний Економіко-Гуманітарний Університет ім. акад. Степана Дем'янчука

Кафедра математичного моделювання

33027,м.Рівне,Україна

Вул.акад. С.Дем'янчука,4, корпус 1

Телефон:(+00380) 362 23-73-09

Факс:(+00380) 362 23-01-86

E-mail:mail@regi.rovno.ua

E-mail:Mark_kornet@mail.ru