ЗАХИСТ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

Богдан Цибуляк
Львівський державний університет безпеки життєдіяльності,
вул. Клепарівська 35, Львів, 79007, Україна, bohdan_ts@yahoo.com

Постійне зростання ролі інформації – одна з головних тенденцій у сучасному світі. Частка науково-дослідних і дослідно-конструкторських робіт у ціні товару зараз може сягати понад 50%. Окрім того з'явилася ряд навіть таких специфічних галузей виробництва, які майже на 100% складаються лише з однієї інформації, наприклад, створення програмного забезпечення, дизайн, реклама та інші галузі пов'язані з програмним забезпеченням (ПЗ). Так, всі витрати при розробці ПЗ йдуть на створення першого зразка, а подальше його тиражування не варте нічого.

Окрім того, зростання обсягів інформації суттєво вплинуло на телекомунікаційні мережі її обміну. Значно зросла пропускна здатність та швидкодія міжнародних телекомунікаційних мереж, а також для підключення до них створено необхідне обладнання та розроблено досить зручні, надійні, дешеві і широко застосовувані доступні програми. Однак інформація, яка передається від одного комп'ютера до іншого, не завжди прихована від інших комп'ютерів, підключених до тієї ж мережі. Це може призвести до шпигунства, крадіжки даних чи їх спотворення.

Широкий розвиток корпоративних мереж, інтеграція їх з інформаційними системами загального користування крім переваг породжує нові загрози безпеки інформації. Причини виникнення нових загроз характеризуються:

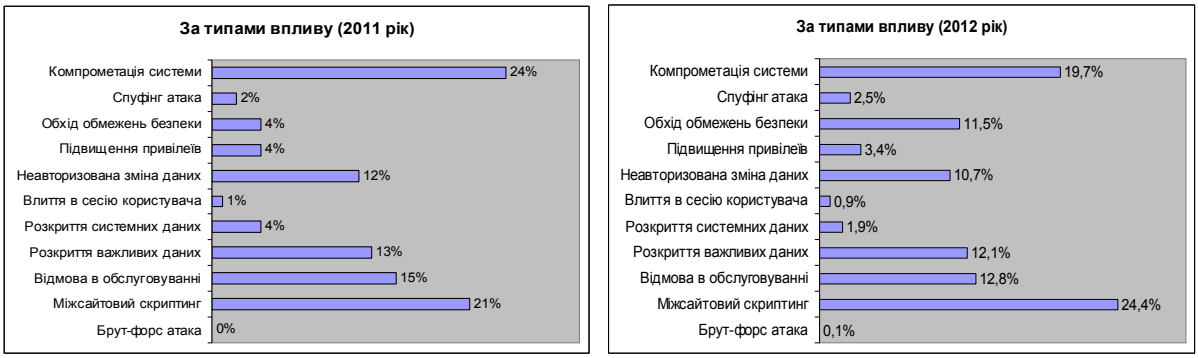
- складністю і різнорідністю використовуваного програмного й апаратного забезпечення корпоративних мереж;
- великим числом вузлів мережі, що беруть участь в електронному обміні інформацією, їх територіальним розподілом і відсутністю можливості контролю всіх налаштувань;
- доступністю інформації корпоративних систем зовнішнім користувачам (клієнтам, партнерам та ін.) через її розташування на фізично з'єднаних носіях.

Вбудовані в операційні системи механізми захисту інформації не дозволяють повною мірою ліквідувати ці загрози. Наявність постійних або тимчасових фізичних з'єднань є найважливішим фактором, який впливає на підвищення вразливості корпоративних систем через проломи у використовуваних захисних та програмних засобах і витік інформації внаслідок помилкових або неграмотних дій персоналу.

Портал по інформаційній безпеці SecutityLab.ru опублікував звіт, що містить статистику комп'ютерних зламів за 2011 рік (рис. 1, А) [1]. До найгучніших з них можна віднести, наприклад, злам весною – літом 2011 року іранськими хакерами серверів засвідчуючих центрів Comodo і DigiNotar, причому частина з викрадених сертифікатів безпеки належали іноземним спецслужбам, таким як ЦРУ, Моссад та MI-6. Зламавши сервера компанії RSA Security в середині березня 2011 року, невідомі хакери поставили під загрозу надійність цифрових підписів RSA SecurID. Цими ключами користувались понад 40 млн. працівників для отримання доступу до закритих мереж.

Всього за минулий рік було описано 4733 злами. Розробники програмного забезпечення змогли ліквідувати до 1 січня тільки 58% з них, а ще для 7% випустили інструкції з ліквідації несправностей. Таким чином понад третина вражених систем залишилась відкритою для кіберзлочинців.

Аналогічні тенденції щодо кіберзлочинності прослідковуються і у даних за 2012 рік (рис. 1, Б).



А Б

Рис. 1. Розподіл зламів комп'ютерних мереж за типами дії в 2011 р. (А), 2012 р. (Б).

Станом на 1 квітня 2012 року розробники ліквідували 1533 злами систем, для 54 з них було запропоновано тимчасове рішення. Не було усунено 465 з них, що складає 35% від загальної кількості.

Тому з підвищенням значущості та цінності інформації відповідно зростає і важливість її захисту. Захист інформації можна визначити як організаційні та технологічні заходи для обмеження доступу до інформації для будь-яких осіб, а також для посвідчення автентичності та незмінності інформації. Ця проблема на сьогодні є одним з найактуальніших завдань. Її можна звести до мінімуму, якщо заздалегідь планувати забезпечення безпеки програмних продуктів [2].

Напевно ніхто не зможе назвати точну цифру сумарних втрат від комп'ютерних злочинів, пов'язаних з несанкціонованим доступом до інформації. Це пояснюється, перш за все, небажанням постраждалих компаній оприлюднювати інформацію про свої втрати, а також тим, що не завжди втрати від розкрадання інформації можна точно оцінити в грошовому еквіваленті, або вчасно виявити саме викрадення.

Причин активізації комп'ютерних злочинів і пов'язаних з ними фінансових втрат досить багато, істотними з них є:

- перехід від традиційної "паперової технології" зберігання та передачі відомостей на електронну і недостатній при цьому розвиток технології захисту інформації в таких технологіях;
- об'єднання обчислювальних систем, створення глобальних мереж і розширення доступу до інформаційних ресурсів;
- збільшення складності програмних засобів і пов'язане з цим зменшення їх надійності і збільшення числа вразливих моментів.

Будь-яке сучасне підприємство незалежно від виду діяльності та форми власності не в змозі успішно розвиватися і вести господарську діяльність без створення на ньому умов для надійного функціонування системи захисту власної інформації. Створення ефективної системи захисту інформації на сьогоднішній день цілком реально. Надійність захисту інформації, перш за все, буде визначатися повнотою вирішення цілого комплексу завдань.

Ефективність захисту інформації в автоматизованих системах досягається застосуванням засобів захисту інформації (ЗЗІ). Під засобом захисту інформації розуміється технічний, програмний засіб або матеріали, призначені для захисту інформації.

Зараз на ринку представлено багато різноманітних ЗЗІ, які умовно можна розділити на кілька груп засобів, які забезпечують:

- розмежування доступу до інформації в автоматизованих системах;
- захист інформації при передачі її по каналах зв'язку;
- захист від витоку інформації по різних фізичних полях, що виникають при роботі технічних засобів автоматизованих систем;
- захист від впливу програм-вірусів;
- безпеку зберігання, транспортування носіїв інформації і захист їх від копіювання.

Інформація, що має певну цінність, потребує захисту, як від звичайного користувача, так і від навмисного несанкціонованого доступу. Серед способів захисту даних можна виділити декілька категорій. До першої категорії відноситься захист інформації з використанням паролів, до другої категорії можна віднести способи, пов’язані з модифікацією вихідного файлу, до третьої категорії захисту відноситься шифрування важливої інформації.

Оскільки основна загроза інформаційної безпеки баз даних, як свідчить статистика кіберзлочинів, надходить у першу чергу безпосередньо від співробітників, тому доцільно є максимально обмежити коло працівників, які мають доступ до конфіденційної бази даних, а також обсяг даних, до яких вони допускаються.

Захист інформації паролем закриває доступ до неї для звичайних користувачів. Однак досвідчений користувач може відкрити запаролену інформацію, обійшовши захист, вивчивши вихідні тексти процедур або скориставшись достатньою кількістю безкоштовних чи платних утиліт, які відображають пароль, у тому числі доступні вихідні коди коду на Visual Basic дозволяють прочитати такий пароль. Тому простим і дієвим захистом інформації від ряду таких програм буде введення в пароль кириличних символів, оскільки основні світові розробники переважно враховують латинку. У такому випадку пароль, як правило, вони розкриють, але те, що видають в якості пароля, розібрати неможливо.

Підвищення рівня захисту інформації досягається з використанням встановлення спеціалізованого ПЗ, наприклад, ESMART ® CryptoDisk, яке дозволяє створювати на будь-яких носіях інформації захищені області для зберігання секретних даних [3]. Фізично захищена область - це особливий файл, інформація всередині якого зберігається в зашифрованому вигляді. Відкрити даний файл і отримати доступ до збереженої в ньому інформації можна тільки за допомогою програми ESMART ® CryptoDisk. Для спільного використання секретного диска передбачена функція розмежування прав доступу: читання/запис, тільки читання, перегляд журналу користування тощо.

Отже, не завжди використання найскладніших підходів по забезпеченню секретності інформації чи дорогих програмних засобів захисту є виправданим. Проте, обмеження прав доступу користувачів та комплексне використання кількох засобів захисту різних виробників дає цілком задовільний рівень захисту конфіденційної інформації.

[1] http://www.securitylab.ru/analytics/422328.php
[2] А.Ю. Ефремов, Н.Б. Еремеев Защита информации / Учеб. пособие по лаб. практикуму. Харьков: Нац. аэрокосм. ун-т «Харьк. авиац. ин-т» (2004). 45 с.
[3] http://www.esmart.ru/_products/product_/show_4/