УДК 681.3

А.З. Піскозуб, Л.Т. Пархуць
Національний університет “Львівська політехніка”,
кафедра “Автоматика і телемеханіка”

ЗАХИСТ КОРПОРАТИВНОЇ СИСТЕМИ ПІДПРИЄМСТВА: ОСНОВНІ ЕТАПИ ТА СПОСОБИ РЕАЛІЗАЦІЇ

Розглянуто основні етапи та способи реалізації захисту комп’ютерної системи підприємства, даються рекомендації з вибору необхідного програмного та програмно-апаратного забезпечення.

In the given article there have been considered basic phases and security realization methods of computer system of a company and given recommendations how to choose the necessary software and hardware.

Із постійним вдосконаленням інформаційних технологій і глибшим їх проникненням в різні сфери нашого життя зростають і вимоги до забезпечення відповідного рівня захисту даних підприємства чи підрозділу. Сьогодні вже нікого не здивуєш термінами “промисловий шпіонаж” чи “хакер”. І в першому, і в другому випадках йдеться про несанкціоноване отримання інформації. Що ж повинно бути враховано при проектуванні комп’ютерної інфраструктури підрозділу?

Захист системи загалом можна розглядати з погляду можливих каналів витоку інформації – організаційно-технічний захист, захист від технічних, програмно-апаратних каналів витоку інформації та захист, коли каналом витоку є самі люди.

Отже, захист слід розпочинати з організаційно-технічних заходів (захист приміщення, де буде розташована комп’ютерна система, доступ до приміщення лише обмеженій групі людей тощо).

Захист від технічних каналів витоку інформації відіграє сьогодні важливу роль. Враховуючи бурхливий розвиток за останні роки арсеналу засобів, пов’язаних із несанкціонованим отриманням інформації, тобто шпіонажем, зазначимо, що кваліфіковану консультацію з цього питання може надати лише фахівець. Причому у кожному конкретному випадку залежно від місця розташування підприємства, цінності самої інформації, наявності потенційних конкурентів, які не гребують нічим заради отримання інформації та ще багатьох факторів, рекомендації можуть бути абсолютно різними. Прикладами таких технічних каналів витоку інформації можуть бути: підслуховування розмов по радіоканалу (підслуховування розмов в приміщенні за допомогою занесеної туди радіозакладки – “жучка”), за допомогою лазерної накачки чи через звичайний телефон на основі “мікрофонного ефекту”, отримання інформації з комп’ютера через наявність в останнього побічних електромагнітних наводок тощо. До речі, рівень побічних електромагнітних наводок можна істотно зменшити, якщо застосовується технологія спеціального екранування комп’ютера екрануючим напиленням. Ряд провідних українських фірм-виробників комп’ютерного обладнання мають в своєму асортименті комп’ютерну техніку з істотно зниженим показником побічних електромагнітних наводок.

Не слід забувати і про людський фактор. Керівник повинен оточити себе надійними працівниками – це може відіграти ключову роль там, де, здавалось, усі абсолютно заходи із забезпечення захисту інформації були враховані.

Найпоширеніші сьогодні програмно-апаратні канали витоку інформації і тому ми детальніше розглянемо саме їх та методи захисту від них.

Насамперед необхідно оцінити ризик компрометації ваших конфіденційних даних, – чим вища їх цінність, тим вищий ризик їх компрометації, і тим ефективніші засоби і методи захисту повинні бути застосовані. Іншими словами, вартість засобів захисту має бути адекватна вартості даних, що підлягають захисту.

Розглянемо тепер, як забезпечити необхідний рівень захисту комп'ютерної системи підприємства. Його реалізація складається з чотирьох етапів – планування та проектування системи, реалізації архітектури безпеки та обов'язкового дотримання усіх пунктів політики безпеки. Розглянемо ці етапи.

Чим детальніше ви плануєте проект, тим менше проблем ви будете мати потім– ця теза є особливо актуальною для реалізації захисту інформації у вашій мережі. Планування слід розпочинати зі створення чіткої політики безпеки. Політика безпеки повинна визначати вимоги до безпечного зберігання даних, унеможливлення зловживання цими даними та гарантування, що лише авторизовані користувачі будуть мати доступ до них. Ключовим правилом визначення чіткої політики безпеки є: "те, що явно не дозволяється, те явно забороняється." Це дасть вам змогу сконцентруватись не на загрозах вашій мережі, а на інструментах та доступі до даних, яких потребують ваші клієнти для їх нормальної роботи. Пам'ятайте, ваша політика безпеки визначає те, що ви потребуєте, а не те, як ви це зробите. Тому правила політики безпеки треба робити настільки чітко окресленими, наскільки це можливо.

Хорошу політику безпеки визначають такі критерії: *конфіденційність* – ваша інформація повинна бути конфіденційною і несанкціонований доступ до неї повинен бути унеможливлений; *цілісність* – ваша інформація повинна бути захищена від спотворення і не може бути модифікована без вашої санкції; *доступність* – ваша інформація повинна бути доступна для зареєстрованих користувачів, коли їм це потрібно.

Як правило, користувачі підприємства хотіли б мати якнайширший спектр послуг, і, наприклад, окрім наданого їм для роботи доступу до корпоративних серверів, WWW, e-mail хотіли б ще мати доступ до усіх можливих послуг Інтернету, таких, як IRC, ICQ, AOL, PointCast, RealAudio та інших, які їм не обов'язково потрібні і які можуть відкрити дірки в системі захисту. З іншого боку, роботодавці хотіли б повністю заблокувати ці послуги. Розумним виходом з цієї ситуації є компроміс, який би можна було охарактеризувати так:

– чим менше послуг надається, тим менше є шансів несанкціонованого доступу до ресурсів системи;

– надавати треба лише ті послуги, які є конче необхідні для роботи.

Взагалі чим жорсткіша політика безпеки, тим вищий рівень захищеності системи.

Наступним етапом є проектування системи, в основі якої повинен лежати багаторівневий захист. Треба пам'ятати, що ідеального захисту не буває, і тому система, в якій застосовується багаторівневий захист – біометричні засоби аутентифікації для входу в систему, пластикові картки для входу в приміщення тощо, – все-таки краще зупинить хакера, ніж звичайна система, в якій для доступу до ресурсів треба знати лише ім'я користувача та пароль.

Проектування багаторівневої системи захисту слід починати з реалізації управління доступом по мережі із аутентифікацією користувачів, контролем доступу від джерела, контролем доступу до отримувача та протокольного управління.

Аутентифікація користувачів здебільшого полягає в тому, що кожен клієнт мережі має унікальне ім'я користувача і пароль для доступу в систему. Цей тип моделі під-

тримується більшістю операційних систем, але його недоліком є залежність від користувачів, які зберігають їх паролі і необхідність вилогуватись з системи перед тим, як покинути робоче місце.

Контроль доступу від джерела та контроль доступу до отримувача діють подібно та дають змогу встановлювати з'єднання відповідно лише від та до певних довірених хостів. Використовуючи такий контроль, користувачам не треба пам'ятати ніяких паролів чи вводити будь-яку інформацію, – ця модель захисту є прозорою для користувача. Проблема з цією моделлю передбачає ідентифікацію надійного джерела (чи, відповідно, отримувача). Одним з найпоширеніших способів ідентифікації є спосіб з використанням IP-адреси. Проте відомо, що IP-адреси можна фальсифікувати. Крім того, багато мереж застосовують DHCP-протокол, який робить неможливим гарантію, що IP-адреса клієнта залишається тією самою.

Можлива ідентифікація і через інші засоби. Деякі виробники програмного та апаратного забезпечення пропонують використання *cookies*, інші застосовують власні апаратні засоби для забезпечення хосту доступу до системи. Але сьогодні не існує жодного методу контролю доступу від джерела (чи до отримувача), який би не можна було підробити.

Характеризуючи окремо контроль доступу до отримувача, треба зазначити, що хоча він і є добрим для блокування доступу до певних комп'ютерів чи мереж, він має певні недоліки. За допомогою цієї моделі практично неможливо обмежити доступ лише окремим користувачам. Контроль доступу до отримувача не захищає також від DoS-атак (атак типу "відмова від обслуговування")

DoS-атака відбувається тоді, коли хтось заповнює усю смугу пропускання вашого каналу зв'язку, наповнює ваші накопичуючі пристрої або посилає спотворену чи зловмисну інформацію до ваших серверів для виведення їх з ладу. DoS-атаки вважаються атаками проти третього критерію безпеки – доступності і застосовуються проти публічних WWW-, FTP-серверів та серверів електронної пошти. Ці атаки важко зупинити без пристрою управління доступом по мережі.

Управління протоколами часто використовується маршрутизаторами, пакетними фільтрами та анонімними публічними серверами всіх типів і дає змогу керувати доступом до мережевих ресурсів. Воно є дуже корисним для блокування трафіку, який ви не будете використовувати. Обмеження кількості протоколів, які пропускає ваш міжмережевий екран, дає змогу ефективно зменшити кількість методів, які можуть застосовувати хакери проти вашої системи, а також обмежити кількість трафіку і зберегти пропускну здатність каналу для ваших клієнтів.

Загалом зазначимо, що жодна з моделей захисту – аутентифікація користувачів, контроль доступу від джерела, контролю доступу до отримувача чи управління протоколами – не є досконалою і тому самостійно не використовується. Разом ці моделі взаємно доповнюють одна одну і забезпечують краще управління доступом по мережі.

Найпростіший метод забезпечити таке управління – інсталювати брандмауер. Звичайно, вам буде потрібно виконати його конфігурацію згідно з вашими умовами.

Часто вважають, що як тільки ваша мережа захищена брандмауером, то ви маєте 100-процентний захист. Але це далеко не так. Брандмауер є лише першою лінією оборони. Він контролює лише трафік, який проходить через нього і тому не захищає від внутрішніх зловмисників, атак з сегментів, що не є за брандмауером, але підключених до вашої мережі (таких, як RAS-сервер віддаленого доступу), а також авторизованих користувачів зі зловмисними намірами.

Ви є відповідальними за те, щоб гарантувати, що атакуючі зроблять найменшу кількість пошкоджень вашій системі. Є багато шляхів, як це можна зробити, але розглянемо ті з них, які мають відношення до наших трьох критеріїв безпеки інформації – конфіденційності, цілісності та доступності, а також дуже важливого четвертого критерію – фізичної безпеки.

Для забезпечення конфіденційності доцільно скористатись різними методами контролю доступу до важливих внутрішніх ресурсів, наприклад, використовувати не лише стандартну схему аутентифікації користувачів за їх іменами та паролем, а також схеми покращеної аутентифікації на основі продуктів третіх фірм-виробників, як, наприклад, SecureID. Другим важливим кроком із забезпечення конфіденційності є застосування методів шифрування даних, які себе добре зарекомендували і не мають слабких місць.

Цілісність даних і системних файлів важко гарантувати, оскільки кваліфікований хакер може змінити важливі дані без вашого відома і усунути усі сліди свого вторгнення в систему. Але часто цілісність є важливішою за конфіденційність. Одним з кращим засобів забезпечення цілісності є, знов-таки, шифрування. На додаток до того, що ваші дані залишаються секретними, системи шифрування здатні формувати цифровий підпис, який дає змогу однозначно встановити факт зміни файла після того, як він був підписаний.

Ще одним засобом гарантування цілісності є системи виявлення втручання (IDS-системи). Вони працюють, використовуючи комбінації контрольних сум файлів, цифрових підписів, каталогів файлової системи і вдосконаленої журналізації. Такі системи існують як для Windows-, так і для Unix-систем, зокрема, для останніх відзначимо систему Tripwire, яку, на нашу думку, обов'язково необхідно ставити на кожному відповідальному хості. Проте зазначимо, що IDS-системи не є ефективні для захисту даних, які часто змінюються, оскільки вони перевіряють поточний стан зазначених файлів із зразками, записаними в базі IDS-системи.

Для того, щоб забезпечити необхідний рівень доступності і визначити засоби, які цей рівень будуть підтримувати, необхідно проаналізувати причини, які ведуть до порушення доступності даних. Зловмисник, якого не зупинили ваші засоби захисту, може спричинити аварійну відмову ваших серверів чи заблокувати доступ до вашої системи, застосувавши DoS-атаку і заповнивши повністю ваш канал зв'язку. У такому разі для забезпечення доступності ваших даних необхідні такі заходи:

1. Зберігати повні і поточні резервні копії вашої системи. Без них ви не зможете відновити вашу систему після її злому чи інших несподіванок. На додаток до стандартних процедур резервування рекомендується раз на тиждень робити повну копію системи і зберігати її зовсім в іншому приміщенні на випадок захисту від стихійних лих чи крадіжки.

2. Не мати єдиної точки відмови системи. Коли відмовляє обладнання – брандмауер, сервер чи канал зв'язку, – система резервування повинна бути готова вступити в дію, причому бажано без втручання адміністратора і звертання уваги користувачів.

3. Гарантувати фізичний захист комп'ютера. Без нього всі інші заходи із захисту не допоможуть. Прикладом може служити система, в якій був застосований багаторівневий захист – покращена аутентифікація, системи виявлення втручання, постійний моніторинг мережі, але яка зазнала вторгнення, бо сервери з корпоративними незашифрованими даними, що зберігались в загальнодоступному неконтрольованому приміщенні, були викрадені. В іншому випадку в будинку був забезпечений належний рівень фізичного захисту системи, але оптоволоконні кабелі, які виходили з будинку, проходили через лісисту

місцевість. Це дало змогу зловмиснику знайти панель доступу до цих кабелів і вставити оптоволоконне відгалуження, внаслідок чого він отримав можливість моніторингу незашифрованого трафіку підприємства.

Наступним етапом забезпечення необхідного рівня захисту комп'ютерної системи підприємства (після планування та проектування) є реалізація архітектури безпеки – один з найважчих етапів, оскільки вона передбачає об'єднання усіх згаданих вище заходів на практиці.

Одним з найважливіших кроків гарантування того, що ваша інформація залишиться неушкодженою, є створення середовища, де всі будуть свідомі тих заходів безпеки, які слід вжити. Ваша політика безпеки повинна бути однаковою для всіх співробітників підприємства. До роботи над проектом безпеки підприємства повинні бути залучені керівники усіх підрозділів, головні менеджери, працівники підрозділу інформаційних технологій та системні адміністратори – ваш проект може містити заходи, які інші спеціалісти вважають такими, що належать до їх юрисдикції, і сприймуть його як вторгнення на їх територію.

Ви також повинні інформувати користувачів підприємства про ваш проект – вони сприймуть будь-яку незручність чи зміну в роботі, яку вони роблять, як злочин. Інформуйте користувачів про стан вашого проекту і вони будуть зацікавлені у ньому. Розсилайте їм повідомлення про необхідні поновлення програмного забезпечення, антивірусних баз тощо.

Останній і найважливіший крок роботи з користувачами – їх підготовка, – є найтривалішим і найдорожчим. Ви повинні навчити користувачів працювати з засобами безпеки, проводити з ними практичні заняття, і результати будуть варті ваших затрат.

Реалізуючи архітектуру безпеки згідно з політикою безпеки підприємства, необхідно вибрати ряд програмно-апаратних рішень, зокрема тип брандмауера і його виробника. Розрізняють три типи брандмауерів: пакетні фільтри, шлюзи прикладного рівня та брандмауери з контролем стану.

Пакетні фільтри можуть блокувати трафік, що проходить через брандмауер по інформації, яка міститься в заголовках пакетів – типі протоколу, номері порта відправника та номері порта отримувача. Цей тип брандмауерів легко конфігурується, вони вважаються досить стабільними і недорогими порівняно з двома іншими типами міжмережевих екранів. Деякі пакетні фільтри мають підтримку VPN-рішень та шифрування, але ці функції виконані в них на базовому рівні і тому не є сумісні з подібними рішеннями інших виробників. Пакетні фільтри можуть бути як програмно, так і апаратно реалізовані – останні вважаються найшвидшими серед усіх типів брандмауерів. Але, на жаль, пакетні фільтри вважаються такими, що забезпечують найменший рівень безпеки серед усіх екранів. Пакетні фільтри практично не мають засобів для управління користувачами, віддаленого управління та інших опцій, які забезпечують екрани інших типів. Оскільки пакетні фільтри виконують моніторинг лише мережевого рівня, вони є вразливими до атак з підробленими адресами відправника (IP spoofing), DoS-атак (як, наприклад, "ping of death", SYN flood-атаки тощо). Найтиповішими представниками апаратних пакетних фільтрів є серія брандмауерів Cisco PIX, а програмних пакетних фільтрів (які, до речі, можуть бути недорогими або зовсім безплатними) – FWTK та Ipchains для FreeBSD та Linux, хоча FWTK та Ipchains включають деякі функціональні можливості інших типів брандмауерів.

Шлюзи прикладного рівня реалізовані програмно і працюють на апаратному забезпеченні загального призначення з багатьма мережевими операційними системами. Вони вважаються найтиповішими представниками міжмережевих екранів і пропонують багато функціональних можливостей, зокрема, мають кращий рівень управління трафіком (вони

можуть переглядати вміст пакетів) та хороші властивості реєстрації цього трафіку. Однак і цей тип брандмауерів має ряд недоліків – вони сильно залежать від стабільності операційної системи, апаратних компонент комп'ютера, таких, як швидкості вінчестера, процесора (особливо при шифруванні трафіку), продуктивності комп'ютера та оперативної пам'яті. Шлюзи прикладного рівня вимагають значно більшої їх конфігурації, ніж пакетні фільтри, не захищають від DoS-атак на мережевому рівні. Типовими представниками шлюзів є Microsoft Proxy, Black Ice, SQUID, а представниками вдосконалених шлюзів (з додатковими функціональними можливостями, такими, як шифрування, VPN-рішення тощо) – BorderWare, Axent Eagle (колишній Raptor), та NAI Gauntlet.

Багато спеціалістів з захисту інформації вважають третій тип міжмережевих екранів – брандмауери з контролем стану – найрізностороннішими і такими, що забезпечують найвищий рівень безпеки. Вони пояснюють це тим, що останній тип брандмауерів поєднує в собі функціональні можливості як пакетних фільтрів, так і шлюзів прикладного рівня. Крім того, вони здатні додатково зберігати інформацію про стан мережевих зв'язків у так званій "таблиці станів". Зрештою, і брандмауери з контролем стану мають певні недоліки – хоча вони і швидші, ніж шлюзи прикладного рівня, але не досягають швидкості пакетних фільтрів. Як і proxy-системи, вони сильно залежать від стабільності самої операційної системи. Брандмауери з контролем стану також не забезпечують тих proxy-сервісів, які пропонують шлюзи прикладного рівня (як, наприклад, у випадку з RealAudio). І нарешті, брандмауери з контролем стану є одними з найскладніших у своєму класі продуктів, їх складно програмувати, відлагоджувати, підтримувати, конфігурувати. Тому вони є найдорожчими в своєму класі. Типовими представниками брандмауерів з контролем стану є, насамперед, CheckPoint FireWall-1, який є доступний для ряду популярних UNIX-платформ та для Windows NT-платформи, а також NetGuard Guardian.

Останнім четвертим етапом забезпечення необхідного рівня захисту комп'ютерної системи підприємства є обов'язкове дотримання усіх пунктів політики безпеки. Якщо хоча б одна з ланок системи не буде відповідати загальним вимогам захисту, то вона може вважатися найслабшою ланкою в цьому захисті. І, отже, потенційне зламування системи може трапитись саме в цьому місці.

Наведемо приклад, в якому покажемо доцільність дотримання наведених міркувань при реалізації системи захисту. На підприємстві була встановлена корпоративна комп'ютерна система, базована на домені Windows NT, в якому були прийняті жорсткі правила політики безпеки (заборона входу користувача Guest; довжина паролів не менше за 12 символів; формування лише складних паролів; унікальність паролів – не менше від п'яти; тривалість паролів – не більше ніж 30 днів; блокування входу після 5 неуспішних спроб; активізований аудит ряду важливих подій; на вході системи був встановлений брандмауер FireWall-1 фірми CheckPoint; користувачам підприємства була доступна з Інтернету лише електронна пошта). Система була зломана. Після аналізу причин, спеціалістами підприємства було встановлено, що зламування сталося зсередини – один з комп'ютерів підприємства під управлінням операційної системи Windows NT Workstation мав локальну політику безпеки, яка істотно відрізнялася від доменної політики підприємства – був, зокрема, дозволений гостьовий вхід локально на цей комп'ютер (через який і сталося зламування системи), і були неправильно встановлені права доступу файлової системи NTFS до системного каталогу Winnt та до деяких ключів системного реєстру. Це дало змогу зловмиснику встановити троянську програму і отримати пароль з адміністративними пра-

вами доступу. Оскільки за підтримку та супровід цього комп'ютера відповідав працівник, який на ньому працював, то винними були визнані цей працівник та відповідальний за безпеку інформації підприємства, оскільки було встановлено, що робота останнього з користувачами із роз'яснення заходів безпеки підприємства була незадовільною.

Підводячи підсумки, можна зазначити, що реалізація захисту системи – це захід, який вимагає багатьох комплексних рішень, відповідають за які не лише ті, хто розробляв цю систему захисту, але і усі користувачі, які беруть участь в роботі системи.

УДК 621.317.7

В.М. Засименко, В.О. Яцук
Національний університет"Львівська політехніка",
кафедра "Метрологія, стандартизація та сертифікація"

ЯКІСНА ОЦІНКА МЕТРОЛОГІЧНИХ ХАРАКТЕРИСТИК ТЕМПЕРАТУРНИХ КАНАЛІВ ІНДИВІДУАЛЬНИХ ТЕПЛОЛІЧИЛЬНИКІВ

Проаналізовано теплотехнічні аспекти побудови індивідуальних лічильників тепла в будівлях з багатоввідним теплопостачанням, запропоновані спрощені співвідношення для побудови їх температурних каналів та встановлені вимоги до технічних характеристик. Розглянуто наявні методи побудови температурних каналів індивідуальних теплових лічильників, обґрунтоване використання в них напівпровідникових перетворювачів температури та запропонована їх математична модель.

The theoretical design aspects of personal heat meters for multi introduction heat supplied system are analysed in this paper. The simplified ratio for personal heat meters construction is offered too. Also it makes choice of temperature semiconducting converters for using in personal thermal meters and creates it mathematical model for measuring current modulation mode.

Вимірювання кількості фактично використаного споживачами тепла має велике економічне значення і є досить складною не тільки технічною, але і соціальною проблемою. Основні технічні труднощі полягають в тому, що принцип побудови систем водяного теплопостачання в Україні і країнах СНД при всіх його модифікаціях такий, що тепло до кожної окремої квартири, офісу підводиться по декількох трубопроводах. Нормативними документами регламентується методика визначення спожитого тепла індивідуальним споживачем пропорційно до усередненого значення кількості тепла, що припадає на одиницю опалюваної площі в будівлях [1]. Фактично спожита індивідуальними споживачами кількість тепла визначається без нормованих метрологічних характеристик і, тому немає об`єктивного економічного стимулу для всебічної економії ним теплоспоживання, зокрема і встановлення регуляторів температури приміщень. Сьогодні поширений інший підхід до вирішення цієї проблеми, який полягає в тому, що вимірюється кількість тепла у всій споруді з наступним встановленням частки тепла, спожитого окремим споживачем.