УДК 004.5:004.9

Бакай О.В.[1], Брич Т.Б.[2], Лах Ю.В.[1,2]

1. Кафедра захисту інформації, Національний університет "Львівська політехніка", 2. Кафедра управління інформаційною безпекою, Львівський державний університет безпеки життєдіяльності

ТЕХНОЛОГІЇ ЗАХИСТУ БАНКІВСЬКИХ МІЖНАРОДНИХ ПЛАТІЖНИХ КАРТОК / BANK INTERNATIONAL PAYMENT CARDS SECURITY TECHNOLIGIES

Standard PCI DSS, introduced to the required obligatory execution in 2008 for all organizations working with card systems VISA, MasterCard, American Express, Discover and JCB, has been described. Considered all the 12 requirements of the standard, proved their productivity and the main ways of these requirements implementation in automatic systems have been investigated.

Keywords – payment cards, standard, requirements, authorized staff, privileges, coding

У статті розглянуто PCI DSS стандарт, введений для обов'язкового виконання в 2008 для всіх організацій, працюючих із картковими системами VISA, MasterCard, American Express, Discover та JCB. Приймаючи до уваги всі 12 вимог стандарту, показана їх продуктивність та досліджено основні шляхи втілення цих вимог в автоматизованих системах.

Ключові слова - платіжні картки, стандарт, вимоги, авторизований персонал, привілеї, шифрування.

Вступ

За останні роки інформаційні технології не лише значно розширили можливості бізнесу, але й зробили його більш уразливим. З одного боку, налагоджуючи електронний обмін даними та документами з клієнтами або партнерами через Інтернет, компанії роблять свій бізнес ефективним, однак з іншого, ставлять під загрозу безпеку [3]. Невразливих систем не буває. І наявність уразливостей в корпоративній мережі може призвести не тільки до прямих фінансових збитків, але й до втрати репутації, втрати конкурентних переваг та інших негативних наслідків. Тому необхідно знати, наскільки захищена корпоративна інфраструктура від дій потенційного зловмисника.

Однак, останнім часом по всьому світі почастішали випадки злому й банківських інформаційних систем [2, 4], зокрема факти шахрайства та крадіжки даних утримувачів платіжних карток. Тому банки вимушені звертати значну увагу на інформаційну безпеку цих операцій. На сьогодні банківські установи вже мають відповідний досвід щодо дотримання безпеки таких операцій, який ґрунтується на комплексному підході організації їх захисту протягом усіх циклів, з яких ці операції складаються, зокрема:

- розроблення і вдосконалення нормативної бази технологій як самих платіжних карток, так і операцій з ними;
- протидія втратам банків від шахрайських дій у процесі емісії та еквайрингу;
- навчання співробітників банку та підприємств торгівлі (послуг) і складання ними кваліфікаційних іспитів на допуск до роботи з банківськими продуктами — платіжними картками.

Серед документів банку, які регулюють ті чи інші види його діяльності, відповідне місце посідають документи щодо забезпечення банківської безпеки, у тому числі й операцій з платіжними картками. Базу для формування нормативних документів з безпеки операцій з платіжними картками створює Положення НБУ "Про порядок емісії спеціальних платіжних засобів і здійснення операцій з їх використанням", затверджене Постановою Правління НБУ № 223 30 квітня 2010 р. [5].

Ураховуючи особливість роботи з платіжними картками, нормативному регулюванню підлягають такі питання:

- забезпечення безпеки роботи, пов'язаної з емісією платіжних карток;
- дії банку, спрямовані на мінімізацію ризиків від операцій з платіжними картками;
- забезпечення безпеки під час надання послуг з платіжними картками та роботи з овердрафтною заборгованістю клієнтів.

2. Призначення стандарту безпеки PCI DSS.

Тенденція зростання збитків із використанням платіжних карток стала однією з головних причин, що спонукали міжнародні платіжні системи об'єднати свої зусилля і прийняти додаткові заходи для захисту своїх клієнтів. З цією метою в 2004 році був розроблений єдиний набір вимог до безпеки даних - Payment Card Industry Data Security Standard, що об'єднав в собі вимоги ряду програм з безпеки таких платіжних систем як Visa Int., MasterCard, American Express, Discover Card і JCB.

Згодом, у вересні 2006 року, для розвитку і просування стандарту PCI DSS, була створена спеціальна Рада з безпеки - PCI Security Standards Council. Основними функції Ради з безпеки є розробка та публікація стандартів PCI і всієї супутньої документації, визначення вимог до компаній, які планують отримати сертифікацію для проведення аудитів за PCI DSS («QSA») і сканувань («ASV»), здійснення безпосередньо самої сертифікації, проведення навчальних тренінгів для майбутніх QSA-аудиторів, а також здійснюють контроль якості проведених аудиторами робіт. У свою чергу міжнародні платіжні системи приймають звітність за результатами аудитів і оцінюють роботу QSA.

Всі організації, які володіють, обробляють або передають інформацію по платіжних картках, уповноважені платіжними системами VISA, MasterCard, American Express, Discover і JCB мають відповідати стандарту безпеки PCI DSS. До них відносяться банки, постачальники платіжних послуг, інтернет-магазини і традиційні торговельні підприємства.

Відповідність не є одноразовою вимогою. Торговельні підприємства повинні підтверджувати свій статус відповідності один раз на рік, але передбачається, що підтримка відповідності буде проводитися завжди.

3. Вимоги стандарту.

Існує 12 обов'язкових вимог:

- створення і супровід конфігурації міжмережевого екрану для захисту даних тримачів карт;

Ця вимога була остаточно виправдана не так давно, і вказує на необхідність використання прикладних брандмауерів типу ISA. Сучасні брандмауери блокують атаки на рівні сесії, а також запуск шкідливого коду проти веб-сайтів і систем, які неможливо захистити за допомогою старіших рішень.

- не використовувати виставлених за замовчуванням виробниками системних паролів і інших параметрів безпеки;

Ця вимога не є надлишковою, оскільки більшість організацій – вище 60% - порушують дане правило, а постачальники послуг встановлюють і управляють рішеннями за допомогою паролів за замовчуванням [1]. І ще одною точкою доступу для зловмисника стає достовірна обчислювальна база (Trusted Computing Base), а це усе програмне і апаратне забезпечення. Операційні системи і додатки зазвичай обладнані системами автоматичного оновлення, але більшість організацій не звертають на це уваги і не оновлюють програмне забезпечення з моменту встановлення, чим і користуються зловмисники.

Також не варто нехтувати шифруванням адміністративного доступу до середовища, що також зазначається в стандарті. Технології на зразок IPSec, SSTP, SSL, SSH, SSL/TLS допомагають в забезпеченні безпечного з'єднання, що особливо важливо для віддаленого адміністративного доступу.

- забезпечення захисту даних тримачів карт в ході їх зберігання;

Вимога описує зберігання інформації про утримувача (користувача) платіжної картки (власником картки є банк-емітент). Для забезпечення конфіденційності необхідно використовувати шифрування. Будь-які дані, що записуються, також мають шифруватися. Стандарт чітко вказує: ніколи не зберігати кодів перевірки карти або PIN-кодів, але це практикується не завжди.

- забезпечення шифрування даних тримачів карт при їх передачі через загальнодоступні мережі;

Ця вимога є продовженням попередньої і має не менш велике значення в платіжному середовищі. Стандартом дані чіткі вказівки, яким чином виконувати шифрування, формувати, розподіляти, забезпечувати безпеку, зберігати, передавати, обмінюватися і розміщувати ключі шифрування.

- використання і регулярне оновлення антивірусного програмного забезпечення;

Ця вимога сама може бути стандартом, але на практиці великий відсоток організацій або не має антивірусних програм, або припускаються помилок у їх використанні. Дані організації зазвичай мають слабкі стратегії оновлення та/або неправильно налаштований антивірус, що через погану конфігурацію не оновлюється і не інформує технічний персонал про те, що оновлення не відбулося [1].

- розробка і підтримка захищених систем і додатків;

Правильна розробка додатків і подальший життєвий цикл розробки програмного забезпечення в стандарті PCI DSS з рекомендації перетворилось на вимогу. До неї також включено розділення середовищ розробки і використання. Перед тим як продукт почне працювати, мають бути видалені всі тестові елементи, якщо до цього етапу поставитись недостатньо серйозно, система отримає масу уразливостей.

- розмежування доступу до даних за принципом службової необхідності;

Лише авторизований персонал має доступ до важливих даних. Найкращий спосіб забезпечення цього – використання підходу «білих списків», або іншими словами заборонити все. Спочатку анулюються всі привілеї, після чого необхідний для роботи мінімум прав видається авторизованому персоналу.

- привласнення унікального ідентифікаційного номера кожній особі;

Ця вимога допомагає вирішити проблему, яка виникає, коли декілька користувачів мають доступ до одного ресурсу з однаковими правами. Двофакторна ідентифікація має бути реалізована для усунення послаблень в контролі доступу.

Віддалений доступ передбачає більш безпечний механізм аутентифікації, використовуючи такі технології, як RADIUS і TACACS+.

- обмеження фізичного доступу до даних тримачів карт;

Для підвищення безпеки інформація про картку має оброблятися і зберігатися в безпечному середовищі. Якщо ці умови не забезпечені, необхідно вживати заходів фізичного контролю. Класифікація даних і паперові запаси, що фізично охороняються, підпадають під це правило.

- відстеження всіх сеансів доступу до мережевих ресурсів;

Аудит є одним з ключових компонентів відповідності PCI. Це допомагає довести, що користувач отримав доступ до даних про платіжну картку і виявляти спроби неавторизованого доступу. Моніторинг і аудит доступу до інформації про картку – це вимога фіксації дати, часу доступу та результату операції.

- регулярне тестування систем і процесів забезпечення безпеки;

Регулярне тестування системи для виявлення уразливостей є частиною стандарту PCI. Для цього проводиться сканування мереж, що містять інформацію про платіжні картки. Щоквартальне сканування мережі необхідне для тих організацій, що підтримують веб-сторінки для здійснення

платежів, або ж зберігають інформацію по кредитних картках в електронному вигляді (навіть якщо це одномоментно), чи передають інформацію по платіжній картці за допомогою посилання API.

- наявність і виконання в організації політики інформаційної безпеки.

Політика безпеки стосується усіх вимог, поставлених стандартом PCI DSS. Вона має бути розроблена, опублікована, поширена і підтримувана в актуальному стані, включати правила експлуатації для критичних пристроїв, з якими безпосередньо працюють співробітники; однозначно визначати обов'язки всіх співробітників і партнерів, що мають відношення до інформаційної безпеки. Повинна бути впроваджена офіційна програма підвищення обізнаності персоналу в питаннях безпеки, щоб донести до них важливість забезпечення безпеки даних про тримачів платіжних карт.

Висновки

PCI Data Security Standard спрямований на визначення рівня забезпечення безпеки інформації про власників карт, а також на формування рекомендацій для торгово-сервісних підприємств, виробників і постачальників програмних рішень та термінального обладнання про заходи, необхідні для підвищення рівня захисту використовуваного програмного забезпечення.

Стандарт був введений для того, щоб допомогти тримачам платіжних карток, а також організаціям, що володіють інформацією про платіжні картки, вберегтися від щорічної втрати коштів через шахрайство. Він допомагає організаціям, що працюють з картками підвищити рівень безпеки, але не є єдиною причиною для реалізації відповідних рішень безпеки.

1. Ricky Magalhaes PCI DSS Security // Section: Web-page.. - http://www.windowsecurity.com. 2. Гайкович В., Першин А. Безопасность электронных банковских систем. "Единая Европа", М., 1994. 3. Голдовский И. Безопасность платежей в интернете. "Питер", СПб., 2001. 4. Задірака В.К., Олексюк О.С., Недашковський М.О. Методи захисту банківської інформації. "Вища шк.", К., 1999. 5. Постанова Правління НБУ № 223 "Про здійснення операцій з використанням спеціальних платіжних засобів" від 30 квітня 2010 р.// Сайт Верховної Ради України: Веб-сторінка. - http://zakon1.rada.gov.ua/laws/show/z0474-10.