НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Лабораторна робота 3

Дослідження криптографічних протоколів
систем WebMoney, PayPal

Виконали:

Галіца О.О.

Литвиненко Ю.С.

Паршин О.Ю.

ФІ-22мн

Перевірила:

Байденко П.В.

Київ 2023

Історія електронних гаманців

Електронні гаманці створені для зручності платежів за товари та послуги онлайн в інтернет-просторі. До рейтингу кращих електронних гаманців включають цілу низку сервісів для роботи з фіатними засобами та криптовалютою: Qiwi, PayPal, WebMoney, AdvCash, Skrill та інші. Але так було не завжди.

На початку 2000-х електронна комерція ще не була звичайною частиною нашого життя — покупки з онлайн-оплатою були рідкістю, банківські картки були далеко не у всіх, та й використовували їх здебільшого для зняття зарплати.

Зі зростанням кількості інтернет-сервісів зріс попит і на нові фінансові інструменти для фрілансерів та індивідуальних підприємців, які працюють онлайн та у сфері електронної комерції. Так з'явилися перші електронні гаманці, що дозволяють зберігати кошти та проводити транзакції у будь-якій валюті.

Однак із виведенням грошей з електронних гаманців виникли складнощі. Здебільшого через те, що інтернет-аудиторія не мала рахунків у банках, та й процес проведення подібних транзакцій виявився дорогим і непростим заняттям. Тоді й назріла потреба у прийомі оплати за товари та послуги за допомогою коштів, які розміщені в електронних гаманцях. Цей варіант зацікавив торгові та сервісні компанії, що займалися онлайн-бізнесом, і вони почали активно підключати таку можливість.

Держава практично повністю ігнорувала існування систем, що дозволяють користуватися електронними гаманцями, але вони активно розвивалися. Згодом з'явилися Webmoney, QIWI, PayPal та інші бренди, що належать спеціальним компаніям-операторам. Вони дозволили реєструвати особисті електронні гаманці та поповнювати їх — наприклад, переводити на них кошти за допомогою банківської картки та рахунки, та за бажання — виводити їх назад на картку. Якоїсь миті навіть мобільні оператори перетворили рахунки своїх абонентів на електронні гаманці, з яких теж можна було оплачувати товари чи послуги.

Взагалі електронний гаманець — це інструмент онлайн-платежів, що дозволяє користувачам здійснювати швидкі цифрові транзакції по всьому світу. Клієнти вносять гроші у гаманець безпосередньо або підключають до нього свої банківські рахунки. Активи можуть зберігатися в одній або кількох валютах. Оборот коштів у таких платіжних системах відбувається віртуально. Клієнт здатний у будь-який момент вивести свої гроші на банківську картку або отримати їх готівкою у пунктах видачі.

Переваги використання електронних гаманців:

1. доступ до гаманця з будь-якої точки світу - електронні системи переважно не прив'язані до певної країни;

2. управління гаманцями відбувається онлайн - для його створення, верифікації, поповнення, відправлення та виведення грошей не потрібно відвідувати офіси або шукати банкомати;

3. зарахування коштів під час виведення або переведення на інший гаманець займає лічені хвилини;

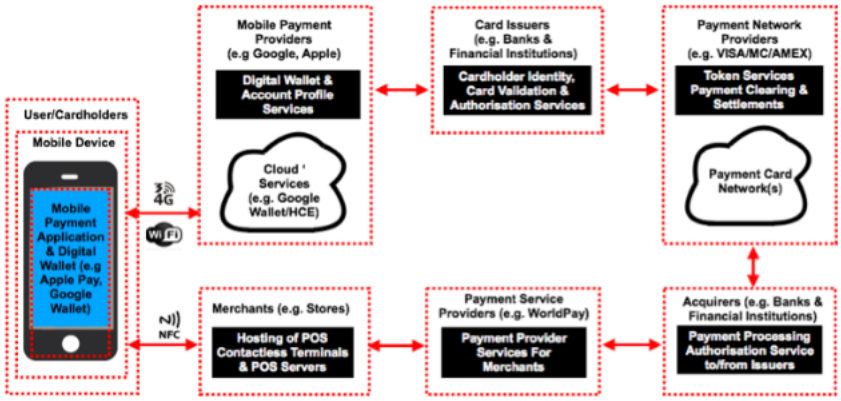
4. можливість розрахунку за товари та послуги з бізнесом та громадянами з інших країн;

5. мінімальна комісія за перекази та виведення коштів.

Загрози

Модель загроз мобільної платіжної програми повинна враховувати загрози основним компонентам екосистеми мобільної програми, виділяючи «межі довіри» (зображені нижче червоними пунктирними лініями), які є точками розмежування між частинами мобільної платіжної програми, де загрози є найімовірнішими. Загальна модель загроз екосистеми мобільних платежів показана на малюнку нижче.

Ми проаналізуємо загрози та вектори атак основних компонентів екосистеми мобільних платежів, на які вони впливають.



1. Загрози користувачів (Payment Application Users)

- **Фішинг і соціальна інженерія**

  Мобільні телефони поєднують особисте та корпоративне використання. Мобільні пристрої збирають все більше і більше інформації від клієнта, яка може допомогти здійснити складні атаки. Ці атаки спрямовані на користувача шляхом фішингових електронних листів і соціальної інженерії, використовуючи різні канали зв'язку (наприклад, телефон, електронна пошта, SMS) і дані про користувача, доступні у відкритому доступі (наприклад, сайти соціальних мереж, пошукові системи).

- **Встановлення шахрайських додатків і шкідливих програм**

  Шахраї знайдуть способи встановити зловмисне програмне забезпечення на мобільний пристрій шляхом фішингу/соціальної інженерії, щоб жертва відкрила зловмисне вкладення в електронному листі та перенаправляла користувача на шкідливу URL-адресу. Іншим можливим каналом зараження зловмисним програмним забезпеченням є незахищені точки доступу Wi-Fi (наприклад, інтернет-кафе), які можуть дозволити зловмиснику атакувати мобільний пристрій за допомогою Man-in-The-Middle. Також існує ймовірність атаки підробки мережі. Це коли зловмисник встановлює підроблену точку доступу з такою ж мережевою назвою,

як і та, яка вже існує, наприклад, назва популярного кафе чи торгової мережі. Вони можуть налаштувати фальшивий веб-сайт для «автентифікації» користувачів і таким чином збирати дані, а потім використовувати ці дані для наступних кроків у своїй атаці.

2. Загрози мобільних пристроїв (Mobile Devices Threats)

- **Несанкціонований доступ до втраченого або вкраденого мобільного пристрою**

  Припускається, що зловмисник володіє пристроєм, який або випадково втрачений користувачем, або викрадений і потрапив в руки зловмисників. Заволодівши пристроєм, зловмисник може спробувати отримати до нього доступ. Швидше за все, атаки полягають у спробах обійти будь-які блокування PIN-кодом або відбитками пальців. Коли пристрій захищено за допомогою автентифікації за відбитками пальців, зловмисник також може використовувати відбитки пальців, викрадені з інших джерел, наприклад, знімаючи приховані відбитки пальців із поверхонь.

- **Установка шкідливого програмного забезпечення на пристрій**

3. Загрози для програм мобільних платежів і цифрових гаманців (Mobile Payment & Digital Wallet Applications)

- **Зворотне проектування вихідного коду програми**

  Часто зворотне проектування самого двійкового файлу є першим портом для зловмисників, які прагнуть отримати вроджене розуміння платіжної програми, щоб використовувати вразливості, такі як жорстко закодовані паролі та ключі шифрування, а також для створення векторів атак для конкретних програм.

- **Втручання в мобільну платіжну програму**

  Зловмисник може вибрати бекдор мобільної платіжної програми, щоб отримати дані для входу та надіслати їх на контрольований зловмисником сервер. Це можна зробити, якщо завантажитии законну програму з магазину, розпакувати її, виправити відповідні процедури, а потім перепакувати та завантажити в магазин.

- **Експлуатація вразливостей програми мобільних платежів**

  Використання вразливостей мобільних програм може дозволити зловмисникам викрасти будь-які конфіденційні дані, які зберігає програма (наприклад, дані особистого облікового запису користувача та дані кредитної картки). Використання таких вразливостей, як слабка автентифікація, може дозволити зловмиснику отримати неавторизований доступ до пристрою. Крім того, можливе шахрайство з викраденими банківськими рахунками та рахунками кредитних карток, пов'язаними з програмою мобільних платежів. Шахрай також може скористатися слабкими місцями в процесі реєстрації, щоб додати інший мобільний пристрій до профілю користувача для здійснення шахрайських покупок.

- **Встановлення руткітів/шкідливих програм**

- **Права доступу до мобільної операційної системи**

  Мобільна ОС може надавати доступ до певних ресурсів з дозволу користувача. Навіть якщо певна програма не є зловмисною, наявність певних дозволів потенційно може надати доступ до конфіденційних даних або використовуватися іншою програмою для розширення доступу.

4. Загрози торговців (Merchants Threats)

- **Завантаження шкідливого програмного забезпечення на термінал безконтактних платежів**
- **Атаки MiTM на безконтактний POS-термінал і підключення до POS-сервера**

  Атаки MiTM можливі, наприклад, якщо SSL/TLS або наскрізне шифрування не використовується між POS-терміналом і POS-сервером (POS = Point Of Sale).

  Зловмисники також можуть спробувати використати слабкі місця в безпеці мережі, такі як відсутність брандмауерів для захисту внутрішньої мережі продавця, а також спробувати використати уразливості програмного забезпечення POS і неправильні конфігурації POS.

- **Естафетні атаки на безконтактний термінал POS із підтримкою NFC**

  Відомою атакою на інтерфейс NFC POS є релейна атака. Програмне забезпечення ретрансляції, встановлене на телефоні жертви, може передавати команди та відповіді між захищеним елементом і емулятором картки через бездротову мережу. Наприклад, за допомогою дистанційної ретрансляційної атаки зловмисне програмне забезпечення Android, встановлене на мобільному пристрої, може дозволити шахраю здійснювати неавторизовані платежі, направляючи зв'язок до віддаленого зловмисника, дозволяючи йому/їй робити покупки без фізичного володіння цільовим пристроєм.

5. Загрози постачальників платіжних послуг (Payment Service Providers)

- **Компрометація платіжних систем**

  Постачальники платіжних послуг (PSP) надають безконтактні POS-термінали для мобільних платежів, а також сукупні платіжні послуги для продавців, обробляючи дані з різних каналів, включаючи особисті платежі (за наявності картки), онлайн-платежі та мобільні/ безконтактні платежі. Платіжні шлюзи PSP є цікавою мішенню для зловмисників, які прагнуть скомпрометувати платіжні дані під час передачі від продавців до різних банків-еквайрів.

- **Компрометація підключення даних (атаки MiTM)**

6. Загрози еквайєрів (Acquirers Threats)

- **Компрометація систем обробки платежів**

  Оскільки еквайери надсилають запити на авторизацію платежів за допомогою токенів і криптограм і отримують авторизації від емітента через платіжну мережу, служби обробки платежів, ймовірно, є основними цілями для зловмисників, які прагнуть отримати великі обсяги

даних власників карток. Зловмисники можуть спробувати скомпрометувати сервери обробки платежів банку-еквайера зсередини мережі, наприклад, використовуючи неавторизований доступ до платіжних шлюзів і слабкі місця у забезпеченні внутрішнього контролю та заходів безпеки, а також віддалено через встановлення бекдорів і інструментів віддаленого доступу.

- **Відмова від авторизації платежу**

  Атаки відмови, такі як відхилення авторизації платежу від емітента, можуть сприяти використанням недоліків конструкції під час реалізації послуг обробки платежів еквайерами. Наприклад, не використовувати взаємну автентифікацію з'єднань «точка-точка», а також цифрові підписи для підтвердження схвалення авторизації та процесу перевірки платежу через незалежний канал від каналу платіжної мережі, з якого отримані ці авторизації.

- **Компрометація підключення даних (атаки MiTM)**

7. Загрози постачальників платіжних мереж (Payment Network Providers Threats)

- **Компрометація служб і серверів постачальників токенів**

  Постачальники послуг (TSP) надають такі послуги керування токенами, як токенізація, детокенізація і перевірка цілісності даних токенів і їх походження та перевірка за допомогою криптограми. Якщо постачальника послуг було зламано, зловмисники, ймовірно, спробують отримати інформацію типу CVV і терміну дії. Це була б ціль високого значення для зловмисників, оскільки цю інформацію легко використовувати. Інші можливі атаки на процес токенізації та детокенізації можуть включати використання вразливостей програмного забезпечення для вилучення PAN, який використовується для авторизації транзакцій, ідентифікації та перевірки даних кредитної картки, а також для розрахунків.

- **Відмова в платіжних розрахункових послугах**

8. Загрози емітентів (Issuers Threats)

- **Порушення процесу авторизації платежу**

  Однією з головних загроз для емітентів карток є процеси, які перевіряють дані власника картки та видають платіжну авторизацію еквайеру. Внутрішній зловмисник у банку-емітенті картки або зовнішній зловмисник, який отримав доступ до критично важливих серверів, може спробувати обійти засоби контролю шахрайства (наприклад, змінити ліміти платежів за карткою для авторизованих скомпрометованих кредитних карток, зареєстрованих для транзакцій мобільних платежів).

- **Компрометація конфіденційних даних власника картки**

  Кредитні та дебетові рахунки, включно з даними банківських рахунків, що зберігаються в банках-емітентах, є ціллю шахраїв і кіберзлочинців, які намагаються вчинити шахрайство

з викраденими даними кредитної картки за допомогою підроблених карток і шахрайства з відсутністю картки, а також шляхом перепродажу викрадених даних кредитної картки на чорному ринку. Це можливо, наприклад, якщо внутрішні працівники банку займаються соціальною інженерією і мають доступ до цих баз даних для отримання облікових даних користувача, включаючи дані дво факторної автентифікації (2FA) для доступу до цих систем.

- **Шахрайство з оплатою**

  Виявлення платіжного шахрайства повинно відбуватися на різних рівнях і в системах, залучених до обробки транзакцій мобільних платежів. Емітенти несуть відповідальність за забезпечення контролю, щоб запобігти використанню викрадених даних кредитної картки користувачами мобільних платежів для проведення шахрайських транзакцій чи зміни лімітів кредитної картки.

- **Компрометація даних токенів**

  Оскільки емітенти можуть використовувати послугу токенізації з платіжних мереж або запровадити власну службу токенів і самі стати постачальниками послуг (PSP), вони будуть піддаватися підвищеному ризику загроз щодо конфіденційності, цілісності та доступності даних токенів.

9. Загрози постачальників мобільних платіжних програм (Mobile Payment Applications Providers)

- **Компрометація конфіденційних даних власника картки**

  Зловмисники можуть спрямувати свої зусилля на дані власника картки та особисті дані користувача, які зберігаються постачальником послуг мобільних платежів. Основною мотивацією цих атак є викрадення даних кредитної картки, як обговорювалося раніше. Така компрометація даних також може статися під час передачі конфіденційних даних власника картки з мобільного пристрою на сервери, наприклад під час реєстрації мобільної платіжної програми в емітента картки.

- **Злом профілю користувача, яким керує постачальник послуг мобільних платежів**

  Оскільки мобільна програма має доступ до серверів мобільних платежів, наприклад під час реєстрації картки, зловмисник може спробувати скомпрометувати цей доступ, щоб вчинити шахрайство. Тоді він може зловживати неавторизованим доступом до профілю користувача і, наприклад, змінити контактні дані профілю облікового запису, електронні адреси, номери телефонів тощо.

- **DDoS атаки**

  Сервіси цифрових гаманців, у тому числі хмарні сервіси, які використовуються постачальниками мобільних платежів, можуть піддаватися DDoS-атакам з боку зловмисників, які прагнуть порушити роботу послуг мобільних платежів. Ці DDoS-атаки можуть вплинути на

транзакції, які вимагають доступу програми мобільних платежів у реальному часі до платіжних служб, розміщених у хмарі, наприклад для початкової реєстрації мобільних платіжних карток.

Особливості реалізації криптографічних механізмів і протоколів системи WebMoney

WebMoney (WebMoney Transfer) - це система онлайн-платежів, яка поєднує в собі комплексні інструменти з функціями безпечного обміну повідомленнями та спілкування між зареєстрованими користувачами. Процес реєстрації також передбачає заповнення користувачем реєстраційної форми, надання своїх персональних даних та їх верифікацію за допомогою сервісу Центру верифікації (WebMoney Passport). Після реєстрації користувач отримає WM-ідентифікатор (WMID) - унікальний номер, а також WM-паспорт – цифровий документ, що будується, відштовхуючись від персональних даних користувача.

WMID – це унікальне 12-цифрове число, яке є "адресою"користувача в системі WebMoney (наприклад, 464889785562 – це ідентифікатор сервісу Webmoney Passport). WMID не є чимось конфіденційним та не містить інформації про користувача, тому його можна повідомляти під час запиту, хоча, через сервіс WebMoney Passport можна витягнути цю інформацію, тому не варто вказуваи свій WMID в якості реквізитів для отримання платежу. Кошти можуть передані лише на WM-гаманці, які прив'язуються до WMID користувача.

WM-гаманець – це атрибут, зареєстрований під WMID, який використовується для зберігання коштів. Кожен гаманець складається з 12 цифр (схоже до WMID), але також має префікс, який вказує, в якій саме валюті зберігаються гроші на даному гаманці (Z238479008342, E9282374987384, U034873236762 – гаманці для доларів, євро та гривень відповідно).

WM-паспорт (атестат) – це цифровий документ, що посвідчує особу, завірений аналогом власноручного цифрового підпису учасника WebMoney. В атестаті записані особисті дані користувача: ПІБ, паспортні дані та контактна інформація. Процедура атестації відкриває додаткові можливості для роботи з системою, а також показує, наскільки користувач серйозно відноситься до неї. Деякі з переваг:

- збільшена довіра до власника атестату з боку інших користувачів;
- збільшений ліміт на зняття коштів на банківський рахунок;
- можливість використання автоматичних способів прийому платежів на сайті учасника;
- можливість роботи з кредитними гаманцями.

Існує декілька видів атестатів, що залежать від кількості наданої інформації системі учасником:

- Атестат псевдоніму – видається автоматично при реєстрації в системі; піходить для невеликих переказів та покупок.

– Формальний атестат – видається після введення свої паспортних даних, завантаження скан-копії та проходження VideoID ідентифікації; все те ж саме, що і в більш слабкій модифікації, але в даному - збільшено ліміти та довіру, оскільки це є, свого роду, ознакою активності.

– Початковий атестат – видається платно після перевірки паспортних даних Персоналізатором (спеціальний учасник системи, член центру атестації); рекомендується для малого бізнесу і працівників інтернет компаній.

– Персональний атестат – видається платно після перевірки паспортних даних Реєстратором (ультраспеціальний учасник системи); рекомендується для серйозного бізнесу, і просунутих користувачів, які хочуть використовувати весь доступний арсенал, що може бути наданий системою.

WebMoney надає 3 способи для автентифікації особи:

1. За допомогою логіну та пароля, де в якості логіну можуть виступати WMID, телефон, або електронна адреса, що були вказані при реєстрації. Строго рекомендується використовувати при цьому ще додаткове підтвердження (SMS, E-num тощо).
2. За допомогою файлу з секретним ключем (має фіксований розмір в 164 байти, містить зашифровану експоненту, модуль а також геш для перевірки цілісності), формат файлу – kwm, і без пароля він не відкриється (використовується не лише для ідентифікації, а й для створення ЕЦП для транзакцій).
3. За допомогою особистих цифрових сертифікатів (спочатку на стороні користувача генерується секретний ключ, і створюється запит на отримання сертифікат, система його створює та підписує та відправляє його назад користувачу). Після отримання рекомендується одразу зробити копії, бо він ніде не зберігатиметься, окрім як на стороні клієнта.

Для безпечного проведення транзакцій необхідні електронні цифрові підписи, створенням яких займається спеціальний модуль – WMSigner, що генерує ЕЦП на основі RSA (майже напевно) для кожної транзакції за допомогою секретного ключа користувача.

Для того, щоб користуватися системою, користувачу, так чи інакше, потрібен секретний ключ, тоді він зможе користуватись модулем WMSigner. Транзакції, в свою чергу, зазвичай передаються у вигляді спеціальних XML-інтерфейсів, що дозволяє уникнути ручного керування й виконати все автоматично. Всі транзакції в системі є миттєвими, відкликати їх не можна.

XML interfaces – це заздалегідь домовлений формат даних, який відправником надсилається отримувачу в текстовому форматі через HTTPS протокол.

```
<w3s.request>
  <reqn></reqn> - request number
  <wmid></wmid> - WMID of the signer
  <sign></sign> - signature created using WMSigner
  <request_type>
    ... - request parameters
  </request_type>
</w3s.request>
```

Лістинг 1: Приклад XML-інтерфейсу

Всього є 23 різні інтерфейси:

- Інтерфейс X1 – Відправлення інвойсу від продавця до покупця.
- Інтерфейс X2 – переказ коштів з одного гаманця на інший.
- Інтерфейс X3 – отримання історії транзакцій; перевірка статусу транзакції.
- Інтерфейс X4 – Отримання історії виставлених рахунків. Перевірка оплати рахунків.
- Інтерфейс X5 – Завершення транзакції, захищеної кодом. Введення коду захисту.
- Інтерфейс X6 – Відправлення повідомлення на випадковий WM-ідентифікатор через внутрішню пошту.
- Інтерфейс X7 – Перевірка власноручного підпису клієнта - власника WM Keeper WinPro.
- Інтерфейс X8 – Отримання інформації про власника гаманця. Пошук користувача системи за його ідентифікатором або гаманцем.
- Інтерфейс X9 – Отримання інформації про баланс гаманця.
- Інтерфейс X10 – Отримання списку рахунків до оплати.
- Інтерфейс X11 – Отримання інформації з паспорта клієнта за WM-ідентифікатором.
- Інтерфейс X12 – Імпорт виписки по гаманцю в документ 1С.
- Інтерфейс X13 – Відкликання незавершеної захищеної транзакції.
- Інтерфейс X14 – Повернення коштів без комісії.
- Інтерфейс X15 – Перегляд та зміна налаштувань довірчого управління.
- Інтерфейс X16 – Створення гаманця.
- Інтерфейс X17 – Операції з арбітражними контрактами.
- Інтерфейс X18 – Отримання деталізації транзакцій через merchant.webmoney.
- Інтерфейс X19 – Верифікація персональної інформації для власника WM ідентифікатора.
- Interface X20 – Здійснення транзакцій через сервіс merchant.webmoney, не покидаючи сайт продавця (ресурс, сервіс, додаток).
- Interface X21 – Встановлення довіри для платежів продавця за допомогою SMS.
- Interface X22 – Отримання квитанції форми попереднього запиту на оплату в merchant.webmoney.
- Interface X23 – Відхилення отриманих рахунків/скасування виставлених рахунків.

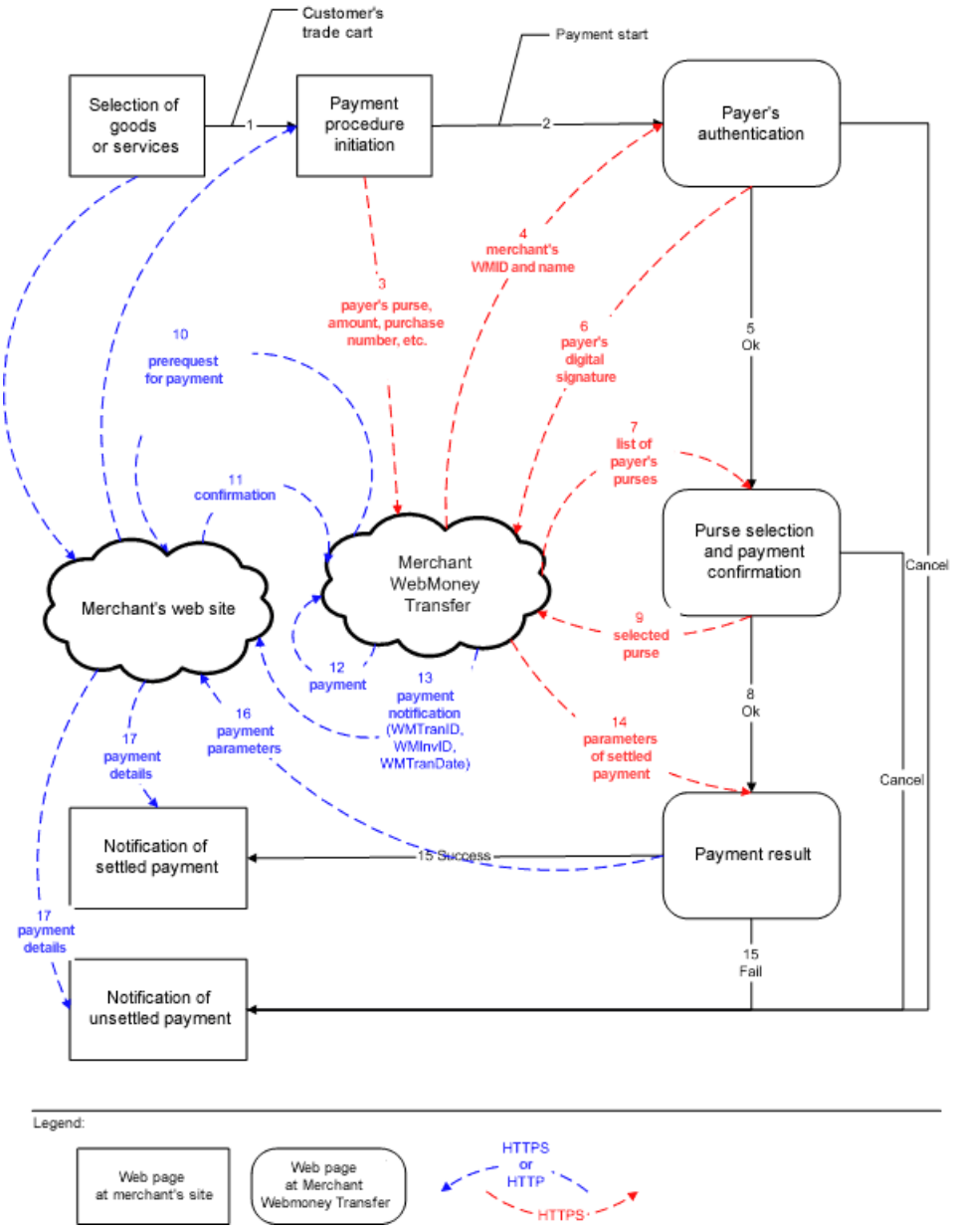


Рис. 1: Процес оплати

Особливості реалізації криптографічних механізмів і протоколів системи PayPal

Встановити точні алгоритми захисту, які використовуються системою PayPal, представилось досить складною задачею, оскільки ця система є пропрієтарною. Але ми сфокусуємось на одному з стандартів, яким ця система відповідає (принаймні, вони так вказують на своєму офіційному веб-сайті).

Цей стандарт носить офіційну (і пафосну!) назву Payment Card Industry Data Security Standard (PCI DSS). Це є набір правил та вимог, яким має відповідати будь-яка пристойна платіжна система. Почнемо ж огляд.

Даний стандарт складається з 12 пунктів. Оцінювати степінь їх виконання в компанії назначається певний орган, так званий Кваліфікований оцінювач безпеки (QSA) - це фірма з безпеки

даних, яка має відповідність від Консорціуму стандартів безпеки PCI для проведення аудитів PCI DSS на місці. QSA буде:

1. Перевіряти всю технічну інформацію, надану торговцем або постачальником послуг.
2. Використовувати незалежні судження для підтвердження того, що стандарт було виконано.
3. Надавати підтримку та керівництво під час процесу виконання вимог.
4. Перебувати на місці протягом всього аудиту за необхідності.
5. Дотримуватися процедур оцінки безпеки PCI DSS.
6. Підтверджувати обсяг аудиту.
7. Оцінювати компенсаційні засоби управління ризиками.
8. Складати заключний звіт.

Пройдемося по цих магічних 12 пунктах:

Розберемо, що ж воно таке - кожний з цих пунктів.

Вимога 1. Встановлюйте та підтримуйте конфігурацію брандмауера для захисту даних власника карти.

Брандмауери - це пристрої, які контролюють комп'ютерний трафік, що входить і виходить з мережі організації, а також в чутливі зони в її внутрішній мережі. Функціональність брандмауера також може виявлятися в інших компонентах системи. Роутери - це апаратне чи програмне забезпечення, яке з'єднує дві або більше мережі. Всі такі пристрої мережі підлягають оцінці в рамках Вимоги 1, якщо вони використовуються в межах середовища даних власника карти.

1. Встановлюйте та реалізовуйте стандарти конфігурації брандмауера та роутера, які формалізують тестування при зміні конфігурацій; визначте всі з'єднання між середовищем даних власника карти та іншими мережами (включаючи бездротові) за допомогою документації та діаграм; документуйте бізнес-обґрунтування та різні технічні параметри для кожної реалізації; складайте всі потоки даних власника карти через системи та мережі на діаграмах; та визначте перегляд наборів правил конфігурації щонайменше кожні шість місяців.

2. Створюйте конфігурації брандмауера та роутера, які обмежують весь трафік, який входить і виходить, з "ненадійних"мереж (включаючи бездротові) та хостів, та специфічно відхиляють весь інший трафік, крім протоколів, необхідних для середовища даних власника карти.

3. Встановлюйте програмне забезпечення брандмауера або еквівалентну функціональність на будь-яких пристроях (включаючи службові та/або власні пристрої працівників), які підключаються до Інтернету за межами мережі (наприклад, ноутбуки, які використовуються працівниками), і які також використовуються для доступу до середовища даних власника карти.

4. Переконайтеся, що пов'язані політики безпеки та експлуатаційні процедури задокументовані, використовуються і відомі всім зацікавленим сторонам.

Вимога 2: Не використовуйте заводські значення для системних паролів та інших параметрів безпеки

Найлегший спосіб для хакера отримати доступ до вашої внутрішньої мережі - це спробувати заводські паролі або використовувати експлойти, що базуються на заводських налаштуваннях програмного забезпечення у вашій інфраструктурі оплати кредитних карт. Занадто часто торговці не змінюють заводські паролі чи налаштування під час встановлення. Це подібно до того, якщо ви залишаєте свій магазин незачиненим фізично, коли йдете додому на ніч. Заводські паролі та налаштування для більшості мережевих пристроїв добре відомі. Ця інформація, разом із засобами хакера, які вказують, які пристрої є на вашій мережі, може спростити несанкціонований вхід, якщо ви не змінили заводські налаштування.

1. Завжди змінюйте ВСІ заводські значення та вилучайте або вимикаєте непотрібні заводські облікові записи перед встановленням системи в мережу. Це включає бездротові пристрої, які

підключені до середовища даних власника картки або використовуються для передачі даних власника картки.

2. Розробляйте стандарти конфігурації для всіх компонентів системи, які враховують всі відомі уразливості та відповідають прийнятим у галузі визначенням. Оновлюйте стандарти конфігурації системи при виявленні нових питань з уразливості.

3. Використовуйте міцне шифрування для всіх адміністративних доступів, окрім консольних.

4. Підтримуйте інвентар компонентів системи, які входять в обсяг PCI DSS.

5. Переконайтеся, що пов'язані політики безпеки та експлуатаційні процедури задокументовані, використовуються та відомі всім зацікавленим сторонам.

6. Постачальники спільного хостингу повинні захищати кожне спільне середовище та дані власника картки (деталі наведені в додатку A1 до PCI DSS: "Додаткові вимоги PCI DSS для постачальників спільного хостингу").

Вимога 3: Захищати збережені дані власника карти

Дані власника картки не повинні зберігатися, якщо це необхідно для вирішення бізнес-потреб. Чутлива інформація на магнітній смузі або чіпі ніколи не повинна зберігатися після авторизації. Якщо ваша організація зберігає PAN, важливо зробити його нечитабельним (див. 3.4 та таблицю нижче для вказівок).

1. Обмежте зберігання даних власника картки та час зберігання лише тим, що необхідно для бізнесу, юридичних або регуляторних цілей, як визначено в вашій політиці зберігання даних. Позбавляйтеся від непотрібних збережених даних щонайменше щокварталу.

2. Не зберігайте чутливі дані для аутентифікації після авторизації (навіть якщо вони зашифровані). Див. таблицю нижче. Зробіть всі чутливі дані для аутентифікації нерековерсійними після завершення процесу авторизації. Видавці та пов'язані сутності можуть зберігати чутливі дані для аутентифікації за наявності обґрунтування бізнесу та безпечного зберігання цих даних.

3. Замаскуйте PAN при відображенні (максимальна кількість цифр для відображення - перші шість та останні чотири), так що лише уповноважені особи з легітимною бізнес-потребою можуть бачити більше, ніж перші шість/останні чотири цифри PAN. Це не суперечить більш суворим вимогам, які можуть існувати для відображення даних власника картки, наприклад, на квитанції точки продажу.

4. Зробіть PAN нечитабельним, де б він не зберігався - включаючи на портативних цифрових носіях, резервних носіях, в журналах та даних, що надходять або зберігаються бездротовими мережами. Технологічні рішення для цієї вимоги можуть включати міцні однобічні хеш-функції для всього PAN, обрізання, індексні токени із безпечно збереженими криптоключами або міцну криптографію. (Див. Глосарій PCI DSS для визначення міцної криптографії.)

5. Документуйте та реалізуйте процедури для захисту будь-яких ключів, використовуваних для шифрування даних власника картки від розголошення та недопустимого використання.

6. Повністю задокументуйте та реалізуйте процеси та процедури управління ключами для криптографічних ключів, використовуваних для шифрування даних власника картки.

7. Переконайтеся, що пов'язані політики безпеки та експлуатаційні процедури задокументовані, використовуються та відомі всім зацікавленим сторонам.

Вимога 4: Шифрувати передачу даних власника карти через відкриті, загальнодоступні мережі

Кіберзлочинці можуть здатні перехоплювати передачі даних власника картки через відкриті, загальнодоступні мережі, тому важливо запобігти їх здатності переглядати ці дані. Шифрування - це одна з технологій, яку можна використовувати для того, щоб зробити передані дані нерозбірливими для будь-якої неуповноваженої особи.

1. Використовуйте міцну криптографію та протоколи безпеки для захисту чутливих даних власника картки під час передачі через відкриті, загальнодоступні мережі (наприклад, Інтернет, бездротові технології, клітинні технології, служба загальних пакетів радіозв'язку [GPRS], супутникові зв'язки). Забезпечте, щоб бездротові мережі, які передають дані власника картки або підключені до середовища даних власника картки, використовували передові практики галузі для реалізації міцного шифрування для аутентифікації та передачі.

2. Ніколи не відсилайте незахищені PAN за допомогою технологій обміну інформацією для кінцевих користувачів (наприклад, електронною поштою, миттєвими повідомленнями, SMS, чатом тощо).

3. Переконайтеся, що пов'язані політики безпеки та експлуатаційні процедури задокументовані, використовуються та відомі всім зацікавленим сторонам.

Вимога 5: Захищати всі системи від шкідливих програм та регулярно оновлювати антивірусне програмне забезпечення чи програми

Зловмисне програмне забезпечення (відоме як "шкідливе програмне забезпечення") використовує вразливості систем після проникнення в мережу через електронну пошту користувачів та інші онлайн-бізнес-активності. Антивірусне програмне забезпечення повинно бути встановлене на всіх системах, які часто стають об'єктом впливу шкідливого програмного забезпечення, щоб захистити системи від поточних та розвиваючихся загроз шкідливого програмного забезпечення. Додаткові рішення проти шкідливого програмного забезпечення можуть доповнювати (але не заміняти) антивірусне програмне забезпечення.

1. Розгортайте антивірусне програмне забезпечення на всіх системах, які часто стають об'єктом впливу шкідливого програмного забезпечення (зокрема, на персональних комп'ютерах та

серверах). Для систем, які не часто стають об'єктом впливу шкідливого програмного забезпечення, регулярно проводьте оцінки для визначення розвиваючихся загроз шкідливого програмного забезпечення та підтвердження того, чи таким системам далі не потрібне антивірусне програмне забезпечення.

2. Переконайтеся, що всі механізми антивірусного програмного забезпечення є актуальними, виконуйте періодичні сканування, генеруйте журнали аудиту, які зберігаються відповідно до Вимоги 10.7 PCI DSS.

3. Переконайтеся, що механізми антивірусного програмного забезпечення активно працюють та не можуть бути вимкнуті або змінені користувачами, якщо це не було специфічно схвалено управлінням у кожному випадку на обмежений час.

4. Переконайтеся, що пов'язані політики безпеки та експлуатаційні процедури задокументовані, використовуються та відомі всім зацікавленим сторонам.

Вимога 6: Розробляти та підтримувати безпечні системи та додатки

Вразливості в системах та програмах можуть дозволити злочинцям отримати доступ до PAN та інших даних власника картки. Багато з цих вразливостей можна усунути, встановивши відповідні патчі з безпеки, які виконують швидкі ремонтні роботи для конкретного фрагмента програмного коду. Усі критичні системи повинні мати найновіші патчі програмного забезпечення для запобігання експлуатації. Сутності повинні застосовувати патчі для менш критичних систем якнайшвидше, на основі програми управління вразливістю на основі ризику. Завжди слід дотримуватися безпечних практик розробки програм, процедур зміни та інших безпечних практик розробки програмного забезпечення.

1. Запровадьте процес ідентифікації вразливостей безпеки за допомогою надійних зовнішніх джерел та визначте рівень ризику (наприклад, "високий "середній"чи "низький") для недавно виявлених вразливостей безпеки.

2. Захищайте всі компоненти системи та програмне забезпечення від відомих вразливостей, встановлюючи відповідні патчі безпеки від постачальника. Встановлюйте критичні патчі безпеки протягом одного місяця з моменту їх випуску.

3. Розробляйте внутрішні та зовнішні програмні додатки, включаючи веб-засоби адміністративного доступу до програм відповідно до PCI DSS та на основі найкращих практик галузі. Вбудовуйте інформаційну безпеку в увесь життєвий цикл розробки програмного забезпечення. Це стосується всього програмного забезпечення, яке розробляється внутрішньо, а також спеціальної або замовленої програми, розробленої третьою стороною..

4. Дотримуйтеся процесів та процедур управління змінами для всіх змін до компонентів систем. Забезпечте виконання всіх відповідних вимог PCI DSS для нових чи змінених систем та мереж після суттєвих змін.

5. Запобігайте поширеним вразливостям коду в процесах розробки програм за допомогою навчання розробників безпечним технікам кодування та розробки програм на основі настанов з безпечного кодування, включаючи обробку чутливих даних в пам'яті.

6. Забезпечте захист всіх веб-застосунків, що взаємодіють з громадськістю, від відомих атак, або проведення оцінки вразливостей програм принаймні один раз на рік та після будь-яких змін, або встановіть автоматизоване технічне рішення, яке виявляє та запобігає веб-атакам (наприклад, брандмауер для веб-застосунків) перед публікацією веб-застосунків для постійного контролю весь трафік.

7. Переконайтеся, що пов'язані політики безпеки та експлуатаційні процедури задокументовані, використовуються та відомі всім зацікавленим сторонам.

Вимога 7: Обмежувати доступ до даних власника карти відповідно до бізнес-потреб

Щоб забезпечити можливість доступу до критичних даних лише авторизованому персоналу, системи та процеси повинні бути впроваджені для обмеження доступу відповідно до принципу "потрібно знати"і згідно з обов'язками по роботі. Принцип "потрібно знати"означає, що права доступу надаються лише на мінімальний обсяг даних та привілеїв, необхідних для виконання завдань.

1. Обмежте доступ до компонентів системи та даних власника картки лише тим особам, чия робота вимагає такого доступу.

2. Засновуйте систему (системи) контролю доступу для компонентів системи, яка обмежує доступ на основі потреб користувача і налаштована на "відмовити усе якщо це не специфічно дозволено.

3. Переконайтеся, що пов'язані політики безпеки та експлуатаційні процедури задокументовані, використовуються та відомі всім зацікавленим сторонам.

Вимога 8: Визначати та аутентифікувати доступ до компонентів системи

Привласнення унікального ідентифікаційного (ID) для кожної особи з доступом гарантує, що дії, виконані з критичними даними та системами, виконуються відомими та авторизованими користувачами і можуть бути прослідковані. Вимоги стосуються всіх облікових записів, включаючи облікові записи точок продажу з адміністративними можливостями, і всі облікові записи з доступом до збережених даних власника картки. Вимоги не застосовуються до облікових записів, які використовуються споживачами (наприклад, власниками карток).

1. Сформуйте та впровадьте політики та процедури для забезпечення належного управління ідентифікацією користувачів та адміністраторів на всіх компонентах системи. Присвойте

кожному користувачеві унікальне ім'я користувача, перш ніж дозволити їм отримати доступ до компонентів системи або даних власника картки..

2. Використовуйте принаймні один із наступних методів аутентифікації для всіх користувачів: щось, що ви знаєте, таке як пароль або фраза; щось, що ви маєте, таке як токен-пристрій чи смарт-карта; або щось, що ви є, таке як біометрика. Використовуйте надійні методи аутентифікації та робіть всі паролі/фрази нерозбірливими під час передачі та зберігання за допомогою надійного шифрування.

3. Захистіть всі індивідуальні адміністративні доступи без консолі та всі віддалені доступи до середовища для даних власника картки за допомогою багаторівневої аутентифікації. Це передбачає використання принаймні двох з трьох методів аутентифікації, описаних у 8.2. Використання одного фактору двічі (наприклад, використання двох окремих паролів) не вважається багаторівневою аутентифікацією. Ця вимога стосується адміністративного персоналу із неконсольним доступом до середовища для даних власника картки з власної мережі сутності, а також всіх віддалених мережевих доступів (включаючи користувачів, адміністраторів та сторонніх осіб), які походять ззовні мережі сутності.

4. Розробіть, впровадьте та розповсюджуйте політики та процедури аутентифікації для всіх користувачів.

5. Не використовуйте групові, спільні або загальні ідентифікатори або інші методи аутентифікації. Постачальники послуг з доступом до середовищ користувачів повинні використовувати унікальний ідентифікаційний засіб (такий як пароль/фраза) для кожного середовища користувача.

6. Використання інших механізмів аутентифікації, таких як фізичні токени безпеки, смарт-карти та сертифікати, повинно бути призначено для індивідуального облікового запису.

7. Всім доступом до будь-якої бази даних, що містить дані власника картки, повинно бути обмежено: всім користувацьким доступом повинні керувати програмні методи; прямий чи запит доступ мають лише адміністратори баз даних; та ідентифікатори додатків для додатків баз даних можуть використовувати лише додатки (і не користувачі чи не додатки відсутні).

8. Переконайтеся, що пов'язані політики безпеки та експлуатаційні процедури задокументовані, використовуються та відомі всім зацікавленим сторонам.

Вимога 9: Обмежувати фізичний доступ до даних власника карти

Будь-який фізичний доступ до даних або систем, які містять дані власника картки, створює можливість для осіб отримати доступ та/або вилучити пристрої, дані, системи чи паперові копії і повинен бути належним чином обмежений. "Персонал, присутній на місці це повно- та частково-зайняті працівники, тимчасові працівники, підрядники та консультанти, які фізично присутні на

території сутності. "Відвідувачі це постачальники та гості, які входять до приміщення на короткий період - зазвичай до одного дня. "Медіа це всі паперові та електронні носії, що містять дані власника картки.

1. Використовуйте відповідні засоби контролю входу в приміщення для обмеження та моніторингу фізичного доступу до систем у середовищі для даних власника картки.

2. Розробіть процедури для легкого розрізнення між персоналом, присутнім на місці, та відвідувачами, такими як видача ідентифікаційних значків.

3. Контролюйте фізичний доступ персоналу, присутнього на місці, до чутливих зон. Доступ повинен бути санкціонований та базуватися на конкретних обов'язках кожної особи; доступ повинен бути негайно відкликаний після закінчення терміну дії та всі фізичні засоби доступу, такі як ключі, картки доступу і т.д., повинні бути повернуті або вимкнені.

4. Забезпечте авторизацію всіх відвідувачів перед входженням в зони обробки чи зберігання даних власника картки, видаючи їм фізичний значок чи іншу ідентифікацію, яка закінчується та вказує на те, що вони не є персоналом, присутнім на місці, і просите їх повернути фізичний значок перед виходом з приміщення або на дату закінчення терміну дії. Використовуйте журнал відвідувачів для підтримання фізичного журналу відомостей та дій відвідувачів, включаючи ім'я відвідувача, компанію та персонал, який санкціонує фізичний доступ. Зберігайте журнал протягом щонайменше трьох місяців, якщо інше не обмежено законом.

5. Підтримуйте жорсткий контроль над внутрішньою чи зовнішньою розсилкою будь-якого виду носіїв.

6. Знищуйте носії, коли вони більше не потрібні з бізнесових чи юридичних причин.

7. Всім доступом до будь-якої бази даних, що містить дані власника картки, повинно бути обмежено: всім користувацьким доступом повинні керувати програмні методи; прямий чи запит доступ мають лише адміністратори баз даних; та ідентифікатори додатків для додатків баз даних можуть використовувати лише додатки (і не користувачі чи не додатки відсутні).

8. Захищайте пристрої, які захоплюють дані власника картки шляхом прямого фізичного взаємодії з карткою від втручання та заміни. Це включає періодичні огляди поверхонь пристроїв точки продажу для виявлення втручання та навчання персоналу виявляти підозрілу діяльність.

9. Переконайтеся, що пов'язані політики безпеки та експлуатаційні процедури задокументовані, використовуються та відомі всім зацікавленим сторонам.

Вимога 10: Відстежувати та моніторити всі доступи до ресурсів мережі та даних власника карти

Механізми ведення журналів та можливість відстеження дій користувачів є критичними для ефективної форензіки та управління вразливостями. Наявність журналів у всіх середовищах до-

зволяє докладно відстежувати та аналізувати події, якщо щось піде не так. Визначення причини компрометації є дуже складним завданням без системних журналів активності.

1. Впровадити сліди аудиту для зв'язування всіх доступів до компонентів системи з кожним окремим користувачем.

2. Впровадити автоматизовані сліди аудиту для всіх компонентів системи для відновлення цих подій: всі індивідуальні доступи користувачів до даних власника картки; всі дії, виконані будь-яким індивідуумом з привілеями root чи адміністратора; доступ до всіх слідів аудиту; невірні логічні спроби доступу; використання та зміни механізмів ідентифікації та аутентифікації (включаючи створення нових облікових записів, підняття привілеїв) та всі зміни, додавання, видалення облікових записів з привілеями root чи адміністратора; ініціалізацію, зупинку чи паузування журналів аудиту; створення та видалення об'єктів на рівні системи.

3. Записувати записи аудиту для всіх компонентів системи для кожної події, включаючи, як мінімум: ідентифікацію користувача, тип події, дату та час, позначку про успішність чи невдачу, походження події та ідентифікацію чи ім'я затронутого об'єкта даних, компоненту системи чи ресурсу.

4. За допомогою технології синхронізації часу синхронізувати всі критичні годинники та часи систем і впровадити засоби для отримання, розподілу та зберігання часу.

5. Захищати журнали аудиту, щоб їх не можна було змінити.

6. Переглядати журнали та події безпеки для всіх компонентів системи для виявлення аномалій чи підозрілої діяльності. Виконувати критичні перегляди журналів щодня як мінімум.

7. Зберігати історію сліду аудиту протягом принаймні одного року; принаймні три місяці історії повинні бути негайно доступні для аналізу.

8. Постачальники послуг повинні впроваджувати процес для своєчасного виявлення та повідомлення про відмови в роботі критичних систем управління безпекою.

9. Забезпечте, щоб пов'язані політики безпеки та експлуатаційні процедури були задокументовані, використовувалися та були відомі всім зацікавленим сторонам.

Вимога 11: Регулярно тестувати системи та процеси безпеки

Вразливості постійно виявляються зловживальниками та дослідниками, і вони вводяться новим програмним забезпеченням. Компоненти системи, процеси та власне програмне забезпечення повинні часто піддаватися тестуванню для забезпечення довгострокової безпеки. Тестування засобів контролю безпеки особливо важливе для будь-яких змін у середовищі, таких як впровадження нового програмного забезпечення чи зміни конфігурації системи.

1. Впровадити процеси для перевірки наявності точок доступу до бездротових мереж (802.11) та виявлення та ідентифікації всіх авторизованих та неавторизованих точок доступу до бездротових мереж квартально. Вести інвентар авторизованих точок доступу до бездротових мереж та впроваджувати процедури реагування на інциденти в разі виявлення неавторизованих точок доступу до бездротових мереж.

2. Виконувати внутрішні та зовнішні скани вразливостей мережі принаймні кожен квартал і після будь-якої значущої зміни в мережі. Виправляти вразливості та проводити повторні скани за необхідності, доки не буде досягнуто успішних сканів. Після успішного скану для вихідної відповідності до PCI DSS сутність повинна протягом наступних років завершити чотири послідовні квартали успішних сканів. Зовнішні скани щокварталу повинні виконуватися Постачальником Сканування, затвердженим вендором (ASV). Скани, проведені після змін в мережі та внутрішні скани, можуть виконуватися внутрішнім персоналом.

3. Розробити та впровадити методологію для пенетраційного тестування, яка включає зовнішнє та внутрішнє пенетраційне тестування принаймні один раз на рік та після будь-якого значущого оновлення чи модифікації. Якщо використовується сегментація для зменшення обсягу PCI DSS, виконуйте пенетраційні тести принаймні один раз на рік, щоб перевірити, що методи сегментації є операційними та ефективними. Постачальники послуг, що використовують сегментацію, повинні підтверджувати обсяг PCI DSS, виконуючи пенетраційні тести контролів сегментації принаймні кожні шість місяців та після внесення змін до цих контролів.

4. Використовуйте засоби виявлення вторгнень в мережу та/або засоби запобігання вторгненням для виявлення та/або запобігання вторгненням в мережу. Моніторте весь трафік на периметрі середовища даних власника картки, а також в критичних точках всередині середовища даних власника картки, і сповіщайте персонал про підозрілі компрометації. Двигуни IDS/IPS, базові лінії та сигнатури повинні бути завжди актуальними.

5. Впровадити механізм виявлення змін (наприклад, засоби моніторингу цілісності файлів) для сповіщення персоналу про несанкційовані модифікації (включаючи зміни, додавання та видалення) критичних файлів системи, конфігураційних файлів або файлів змісту. Налаштувати програмне забезпечення для виконання критичних порівнянь файлів принаймні щотижня. Здійснити процес реагування на будь-які сповіщення, що генеруються рішенням щодо виявлення змін.

6. Забезпечити, щоб пов'язані політики безпеки та експлуатаційні процедури були задокументовані, використовувалися та були відомі всім зацікавленим сторонам.

Вимога 12: Підтримувати політику, яка враховує інформаційну безпеку для всього персоналу

Міцна політика безпеки визначає тон для забезпечення безпеки в усій компанії організації і інформує працівників про їхні очікувані обов'язки щодо безпеки. Всі працівники повинні бути обізнані з конфіденційністю даних власника картки і своїми обов'язками щодо їхнього захисту.

1. Засновуйте, публікуйте, підтримуйте та поширюйте політику безпеки; регулярно переглядайте політику безпеки принаймні раз на рік і оновлюйте її при змінах в середовищі.

2. Впроваджуйте процес оцінки ризиків, який виконується принаймні один раз на рік та при значущих змінах в середовищі, що визначає критичні активи, загрози та вразливості, і призводить до формальної оцінки.

3. Розробляйте політики використання для критичних технологій, щоб визначити їх правильне використання всіма працівниками. Сюди входять віддалений доступ, бездротові технології, знімні електронні носії, ноутбуки, планшети, кишенькові пристрої, електронна пошта та Інтернет.

4. Забезпечуйте, щоб політика та процедури безпеки чітко визначали відповідальність за інформаційну безпеку для всього персоналу. Постачальники послуг також повинні встановлювати відповідальність за захист даних власника картки та програму відповідності PCI DSS для свого виконавчого управління.

5. Призначте індивідууму чи команді відповідальності згідно з 12.5 підпунктами.

6. Впроваджуйте формальну програму підвищення обізнаності щодо безпеки, щоб всі працівники були обізнані з політикою та процедурами безпеки даних власника картки.

7. Перед прийняттям на роботу перевіряйте можливих працівників з метою мінімізації ризику атак зсередини. До прикладу, така перевірка може включати попередній трудовий досвід, кримінальну історію, кредитну історію та перевірку рекомендацій.

8. Зберігайте та впроваджуйте політики та процедури для управління постачальниками послуг, які мають спільний доступ до даних власника картки або можуть впливати на їх безпеку.

9. Постачальники послуг письмово підтверджують перед клієнтами, що вони відповідають за безпеку даних власника картки, які вони володіють або інакше зберігають, обробляють чи передають від імені клієнта, або в тому випадку, якщо вони можуть впливати на безпеку середовища даних власника картки клієнта.

10. Впроваджуйте план реагування на інциденти. Будьте готові негайно реагувати на порушення системи.

11. Постачальники послуг повинні проводити та документувати регулярні перевірки принаймні щокварталу, щоб підтвердити, що персонал дотримується політик та експлуатаційних процедур з безпеки.