ПРИПИНІТЬ РОЗМОВУ АБО ВТРАТИТЕ ГРОШІ

Вішингова атака: припиніть розмову або втратите гроші

Сьогодні в Україні одним із найпоширеніших типів шахрайства з використанням платіжних карток є вішинг. Злочинці під час телефонної розмови намагаються ***випитати у власника секретні дані карти і банківські sms-паролі.*** Відповідно до статистики, 76% власників платіжних карт, які стали об'єктом вішингу, розголошують шахраям реквізити своїх карт.

Асоціація ЕМА (Ukrainian Interbank Payment Systems Member Association "EMA") розробила інфографіку, що містить інформацію про методи розпізнавання телефонних шахраїв, ефективні способи захисту та дії на той випадок, якщо злочинець дізнався карткові реквізити.

Серед конфіденційних платіжних даних, які ніколи і ні за яких обставин не можна розголошувати разом з номером карти:

• термін дії карти;

* тризначний код безпеки на зворотній стороні картки (код CVC2/CVV2), який потрібен для здійснення операцій з платіжною карткою в Інтернеті;

• паролі з смс-повідомлень від банку, які потрібні для підтвердження операцій з карткою (якщо карта захищена по системі 3D Secure).

Отримавши ці дані, злочинці скористаються ними для здійснення грошових переказів з картки, іноді і для здійснення покупок в Інтернеті.

Найпоширенішим в Україні способом, за допомогою якого шахраї намагаються випитати у громадян реквізити карти по телефону, є звернення під виглядом працівника банку (в 94% випадках), поліції, СБУ, НБУ, Пенсійного фонду, благодійної організації або покупця під різними приводами (перевірка служби безпеки, блокування карти, нарахування надбавки до пенсії, придбання товару).

Ніхто із перерахованих осіб та інстанцій не має права вимагати від власника картки повідомити платіжні реквізити (в тому числі НБУ). При цьому

для отримання грошового переказу на карту – достатньо надати особі, яка робитиме переказ, лише номер карти.

Основний спосіб захисту від телефонних шахраїв – негайно припинити розмову, якщо вас почали питати реквізити карти (не тільки номер, але й термін її дії, тризначний код безпеки, смс-паролі із банківських повідомлень).

Якщо в результаті вішингової атаки карткові реквізити все ж були розголошені, першочерговою дією будь-якого користувача повинно бути негайне блокування платіжної карти. Після чого необхідно повідомити про інцидент в кіберполіцію, наприклад, через форму зворотного зв'язку на сайті Департаменту кіберполіції Національної поліції України.

Додатково на сайті Асоціації ЕМА розміщена інструкція для власників карток, зокрема навчальне відео «Як правильно відповідати телефонним шахраям» та лайфхак «Вішинг: прийоми телефонних шахраїв і як їм протистояти».

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.

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.

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

. - 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 4 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.