Polityka bezpieczeństwa informacji

Colderro Ewa Zimna

(Nazwa firmy)

07.04.2017

Data

Spis treści

Wprowadzenie....3

Polityka bezpieczeństwa informacji....3

1. Bezpieczeństwo sieci....4
2. Polityka dozwolonego użytku....4
3. Ochrona przechowywanych danych....5
4. Klasyfikacja informacji....5
5. Dostęp do poufnych danych właścicieli kart....6
6. Bezpieczeństwo fizyczne....6
7. Ochrona danych podczas przesyłania....7
8. Usuwanie przechowywanych danych....7
9. Świadomość i procedury bezpieczeństwa....8
10. Plan reagowania na incydenty dotyczące bezpieczeństwa danych kart kredytowych (PCI)....9
11. Polityka transferu informacji poufnych....13
12. Zarządzanie dostępem użytkowników....14
13. Polityka kontroli dostępu....14

Dodatek A – Formularz zobowiązania do przestrzegania– Zobowiązanie do przestrzegania zasad zabezpieczania informacji....17

Dodatek B – Lista urządzeń....18

Wprowadzenie

Niniejszy dokument dotyczący polityki bezpieczeństwa informacji obejmuje wszelkie aspekty bezpieczeństwa dotyczące informacji poufnych o firmie i musi zostać przekazany wszystkim pracownikom firmy. Wszyscy pracownicy firmy muszą zapoznać się w całości z tym dokumentem i podpisać oświadczenie potwierdzające zapoznanie się z niniejszą polityką i całkowite jej zrozumienie. Niniejszy dokument będzie poddawany weryfikacji i aktualizacji przez Zarząd corocznie lub gdy jest to istotne dla włączenia nowo opracowanych standardów bezpieczeństwa do tej polityki i przekazania ich wszystkim pracownikom i odpowiednim zleceniobiorcom.

Polityka bezpieczeństwa informacji

Firma przetwarza codziennie poufne informacje właścicieli kart. Informacje poufne muszą posiadać odpowiednie zabezpieczenia w celu ochrony danych właścicieli kart, prywatności właścicieli kart, zapewnienia zgodności z różnymi przepisami, a także zabezpieczenia przyszłości organizacji.

Firma zobowiązuje się do poszanowania prywatności wszystkich swoich klientów oraz do ochrony wszelkich danych klientów przed podmiotami zewnętrznymi. Ograniczyć korzystanie z systemów informatycznych i telekomunikacyjnych Firmy w celach prywatnych oraz zapewnić, aby nie kolidowało ono z wykonywaniem obowiązków zawodowych;

Pracownicy zajmujący się przetwarzaniem poufnych danych właścicieli kart powinni zapewnić następujące środki bezpieczeństwa:

- Przetwarzać informacje o Firmie i właścicielach kart w sposób odpowiadający ich poufności i klasyfikacji;
- Ograniczyć korzystanie z systemów informatycznych i telekomunikacyjnych Firmy w celach prywatnych oraz zapewnić, aby nie kolidowało ono z wykonywaniem obowiązków zawodowych;
- Firma zastrzega sobie prawo do monitorowania, uzyskiwania dostępu, dokonywania oceny, przeprowadzania audytu, kopiowania, przechowywania i usuwania wszelkich usług łączności elektronicznej, urządzeń, systemów i ruchu sieciowego w dowolnym celu;
- Nie wykorzystywać poczty elektronicznej, Internetu ani innych zasobów Firmy do prowadzenia jakichkolwiek działań mających obraźliwy, stanowiący zagrożenie, dyskryminujący, niezgodny ze stanem faktycznym, oszczerczy, pornograficzny, obsceniczny, napastliwy lub niezgodny z prawem charakter;
- Nie ujawniać informacji o personelu bez upoważnienia;
- Chronić poufne informacje właścicieli kart;
- Przechowywać hasła i konta w bezpieczny sposób;
- Wystąpić do kierownictwa z prośbą o wyrażenie zgody przed nawiązaniem połączeń z nowym oprogramowaniem lub sprzętem, zewnętrznym podmiotem itd.;
- Nie instalować nieautoryzowanego oprogramowania ani sprzętu, w tym modemów i punktów dostępu bezprzewodowego, bez uzyskania wyraźnej zgody ze strony kierownictwa;
- Zawsze pozostawiać biurka bez poufnych danych właścicieli kart oraz ustawiać blokady ekranów komputerów w przypadku pozostawienia ich bez nadzoru;

- Incydenty związane z bezpieczeństwem informacji należy zgłaszać bezzwłocznie osobie odpowiedzialnej za lokalne reagowanie na zdarzenia — należy dowiedzieć się, kim jest ta osoba.

Każdy z nas ma obowiązek zabezpieczenia systemów i danych firmy przed nieupoważnionym dostępem i niewłaściwym wykorzystaniem. W przypadku niejasności co do zasad przedstawionych w niniejszym dokumencie należy zasięgnąć porad i wskazówek od swojego bezpośredniego przełożonego.

1. Bezpieczeństwo sieci

Prowadzony jest ogólny schemat sieci sprawdzany co roku. Schemat sieci udostępnia ogólny przegląd środowiska danych posiadaczy kart (CDE), wskazujący co najmniej połączenia przychodzące i wychodzące ze środowiska CDE. Należy także przedstawić kluczowe elementy systemu w środowisku CDE, takie jak urządzenia POS, bazy danych i serwery WWW, a także wszelkie inne niezbędne komponenty procesu płatności (jeśli dotyczy).

Ponadto, w stosownych przypadkach, zatwierdzony przez organizację PCI SSC dostawca usług skanowania powinien przeprowadzić i ukończyć skanowanie ASV. Dowody przeprowadzenia skanowań należy przechowywać przez okres 18 miesięcy.

2. Polityka dozwolonego użytku

Intencją opublikowania przez kierownictwo Polityki dozwolonego użytku nie jest nałożenie ograniczeń stojących w sprzeczności z ugruntowaną w Firmie kulturą otwartości, zaufania i uczciwości. Kierownictwo jest zobowiązane do ochrony pracowników, partnerów i Firmy przed niezgodnymi z prawem lub szkodliwymi działaniami ze strony osób — świadomymi lub nieświadomymi. Firma będzie prowadzić zatwierdzony wykaz technologii i urządzeń oraz pracowników mających dostęp do takich urządzeń wymienionych w Załączniku B.

- Pracownicy są odpowiedzialni za dokonywanie właściwej oceny co do zasadności użytku osobistego.
- Pracownicy powinni podjąć wszelkie niezbędne kroki, aby zapobiec nieupoważnionemu dostępowi do poufnych danych obejmujących dane właścicieli kart.
- Przechowywać hasła w bezpieczny sposób i nie udostępniać kont. Uprawnieni użytkownicy są odpowiedzialni za bezpieczeństwo swoich haseł i kont.
- Wszystkie komputery stacjonarne, komputery przenośne i stacje robocze powinny być zabezpieczone za pomocą wygaszacza ekranu chronionego hasłem z funkcją automatycznej aktywacji.
- Wszystkie terminale POS i urządzenia do wprowadzania kodu PIN powinny być odpowiednio chronione i zabezpieczone w taki sposób, aby nie można było przy nich manipulować ani ich modyfikować.
- Wykaz urządzeń w Dodatku B będzie regularnie aktualizowany po zmodyfikowaniu, dodaniu lub wycofaniu urządzeń z eksploatacji. Regularnie przeprowadzana będzie inwentaryzacja i kontrola urządzeń w celu identyfikacji potencjalnej manipulacji lub zamiany urządzeń.
- Użytkownicy powinni być przeszkoleni w zakresie umiejętności identyfikacji podejrzanych zachowań w przypadku gdy może dojść do manipulacji lub zamiany. Każde podejrzane zachowanie zostanie odpowiednio zgłoszone.

- Informacje zawarte na komputerach przenośnych są szczególnie podatne na zagrożenia, dlatego należy zachować szczególną ostrożność.
- Posty wysyłane przez pracowników z adresu e-mail Firmy na grupy dyskusyjne powinny zawierać zastrzeżenie o zrzeczeniu się odpowiedzialności stwierdzające, że wyrażone opinie są wyłącznie opiniami ich autorów i nie muszą stanowić opinii Firmy, chyba że zamieszczenie postu odbywa się w trakcie pełnienia obowiązków służbowych.
- Pracownicy muszą zachować szczególną ostrożność podczas otwierania załączników e-mail otrzymanych od nieznanych nadawców, które mogą zawierać wirusy, bomby pocztowe lub kod konia trojańskiego.

3. Ochrona przechowywanych danych

- Wszystkie poufne dane właścicieli kart przechowywane i przetwarzane przez Firmę i jej pracowników muszą być przez cały czas skutecznie zabezpieczone przed nieupoważnionym wykorzystaniem. Wszelkie poufne dane kart, które nie są już wymagane przez Firmę z powodów biznesowych, należy usunąć w bezpieczny i nieodwracalny sposób.
- Jeśli nie istnieje szczególna potrzeba wyświetlania pełnego numeru PAN (numer konta stałego), należy go zamaskować przy wyświetlaniu.
- Numerów PAN, które nie są chronione we wspomniany wyżej sposób, nie należy wysyłać do sieci zewnętrznej przy użyciu technologii przesyłu wiadomości do użytkownika końcowego, takich jak czaty, komunikator ICQ itd.

Zabrania się przechowywania:

1. **Zawartości paska magnetycznego karty płatniczej (dane ścieżek) na jakichkolwiek nośnikach.**
2. **Kodu CVV/CVC (3- lub 4-cyfrowy numer na pasku podpisu na odwrocie karty płatniczej) na jakichkolwiek nośnikach.**
3. **Pod żadnym pozorem kodu PIN lub szyfrowanego bloku PIN.**

4. Klasyfikacja informacji

Dane i nośniki zawierające dane muszą być zawsze oznakowane, wskazując poziom poufności.

- Poufne dane mogą obejmować zasoby informacyjne, w przypadku których istnieją wymogi prawne dotyczące zapobiegania ujawnieniu lub kar finansowych za ujawnienie, i dane, które mogłoby wyrządzić poważne szkody Firmie w przypadku ich ujawnienia lub modyfikacji. **Wszelkie obowiązki zawodowe wymagające dostępu do danych właścicieli kart powinny być wyraźnie określone.**
- Dane do użytku wewnętrznego mogą obejmować informacje, które w opinii właściciela powinny być chronione, aby zapobiec nieupoważnionemu ujawnieniu.
- Dane publiczne to informacje, które mogą być rozpowszechniane w dowolny sposób.

5. Dostęp do poufnych danych właścicieli kart

Każdy dostęp do poufnych danych właścicieli kart powinien być kontrolowany i autoryzowany. Wszelkie obowiązki zawodowe wymagające dostępu do danych właścicieli kart powinny być wyraźnie określone.

- Każdy ekran właściciela karty powinien być ograniczony do co najmniej 6 pierwszych i 4 ostatnich cyfr danych właściciela karty.
- Dostęp do poufnych informacji właścicieli kart, takich jak numer PAN, dane osobowe i dane biznesowe jest ograniczony do pracowników mających uzasadnioną potrzebę przejrzenia takich informacji.
- Żadni inni pracownicy nie mogą mieć dostępu do tych poufnych danych, chyba że mają prawdziwą potrzebę biznesową.
- W przypadku udostępnienia danych właściciela karty Dostawcy usług (podmiot zewnętrzny) prowadzony będzie wykaz takich Dostawców usług wymieniony w Załączniku C.
- Firma sporządzi pisemną umowę zawierającą potwierdzenie odpowiedzialności Dostawcy usług za dane właścicieli kart, którymi będzie dysponować.
- Firma zadba o to, aby przed skorzystaniem z usług Dostawcy usług przeprowadzona została ustalona procedura, w tym odpowiednia analiza przedinwestycyjna.
- Firma przeprowadzi procedurę monitorowania statusu zgodności Dostawcy usług ze standardem PCI DSS.

6. Bezpieczeństwo fizyczne

Dostęp do poufnych informacji w postaci nośników zarówno sprzętowych, jak i programowych należy ograniczyć fizycznie, aby uniemożliwić nieupoważnionym osobom uzyskanie poufnych danych.

- Nośniki są określane jako dowolne drukowane lub wypisane ręcznie notatki na papierze, odebrane faksy, dyskietki, taśmy z kopiami zapasowymi, komputerowy dysk twardy itd.
- Nośniki zawierające poufne informacje właścicieli kart muszą być przetwarzane i rozpowszechniane w bezpieczny sposób przez zaufane osoby.
- Odwiedzającym musi zawsze towarzyszyć zaufany pracownik podczas przebywania w miejscach, w których przechowywane są poufne informacje właścicieli kart.
- Konieczne jest wdrożenie procedur ułatwiających wszystkim pracowników odróżnienie pracowników od odwiedzających, zwłaszcza w miejscach, w których możliwy jest dostęp do danych właścicieli kart. Określenie „Pracownik" odnosi się do pracowników pełnoetatowych i niepełnoetatowych, pracowników tymczasowych i personelu tymczasowego oraz konsultantów, którzy są „gośćmi" w siedzibach Firmy. „Odwiedzający" jest określany jako sprzedawca, gość pracownika, pracownik zajmujący się utrzymaniem lub każdy, kto musi fizycznie wejść na krótki czas na teren siedziby, zwykle nie dłużej niż jeden dzień.
- Należy prowadzić wykaz urządzeń akceptujących dane kart płatniczych.
- Na wykazie tym powinny znajdować się marka, model i lokalizacja urządzenia.
- Wykaz powinien zawierać numer seryjny lub unikatowy identyfikator urządzenia.
- Wykaz powinien być aktualizowany w przypadku dodania, usunięcia lub zmiany lokalizacji urządzeń.
- Urządzenia POS mają być okresowo sprawdzane w celu wykrycia prób manipulacji lub zamiany.
- Pracownicy korzystający z tych urządzeń powinni być przeszkoleni i zdawać sobie sprawę ze

sposobu obsługi urządzeń POS.

- Pracownicy korzystający z tych urządzeń powinni sprawdzić tożsamość wszystkich pracowników zewnętrznych podających się za osoby wykonujące naprawy lub zadania związane z utrzymaniem urządzeń, instalację nowych urządzeń lub wymianę urządzeń.
- Pracownicy korzystający z tych urządzeń powinni być przeszkoleni w zakresie zgłaszania podejrzanych zachowań i śladów manipulacji przy urządzeniach odpowiednim pracownikom. Siedziby Firmy. „Odwiedzający" jest określany jako sprzedawca, gość pracownika, pracownik zajmujący się utrzymaniem lub każdy, kto musi wejść na krótki czas na teren siedziby, zwykle nie dłużej niż jeden dzień.
- Prowadzona jest ścisła kontrola nad rozpowszechnianiem wewnętrznym i zewnętrznym wszelkich nośników zawierających dane właścicieli kart, które wymaga zatwierdzenia przez kierownictwo.
- Prowadzona jest ścisła kontrola nad przechowywaniem i dostępnością nośników.
- Na wszystkich komputerach przechowujących poufne dane właścicieli kart musi być włączony wygaszacz ekranu chroniony hasłem, aby zapobiec ich nieupoważnionemu wykorzystaniu.

7. Ochrona danych podczas przesyłania

Wszystkie poufne dane właścicieli kart muszą być skutecznie zabezpieczone w przypadku przesyłania ich drogą fizyczną lub elektroniczną.

- Danych właścicieli kart (numer PAN, dane ścieżek itd.) nie wolno przesyłać przez Internet za pośrednictwem poczty elektronicznej, czatu do przesyłania wiadomości błyskawicznych ani innych technologii przesyłania wiadomości do użytkownika końcowego.
- Jeżeli przesłanie danych właścicieli kart za pośrednictwem poczty elektronicznej lub innymi sposobami jest uzasadnione biznesowo, należy go dokonać po uzyskaniu autoryzacji i przy użyciu silnego mechanizmu szyfrowania (tj. szyfrowania AES, szyfrowania z użyciem klucza PGP, protokołu IPSEC itp.).
- Transport nośników zawierających poufne dane właścicieli kart do innej lokalizacji musi zostać zatwierdzony przez kierownictwo, zarejestrowany i zinwentaryzowany przed opuszczeniem terenu siedziby. Przy transporcie takich nośników można korzystać wyłącznie z bezpiecznych usług kurierskich. Status przesyłki należy monitorować do momentu dostarczenia jej do nowej lokalizacji.

8. Usuwanie przechowywanych danych

- Wszystkie dane należy bezpiecznie usunąć, gdy nie będą już potrzebne Firmie, niezależnie od rodzaju nośników lub aplikacji, w których są przechowywane.
- Należy zapewnić automatyczny proces usuwania niepotrzebnych już danych w sieci.
- Wszystkie wydruki z danymi właścicieli kart należy zniszczyć ręcznie, gdy nie będą już potrzebne z ważnych i uzasadnionych powodów biznesowych. Konieczne jest wdrożenie procesu wykonywanego co kwartał pozwalającego potwierdzić, że wszystkie nieelektroniczne dane właścicieli kart zostały właściwie usunięte w odpowiednim czasie.
- Firma dysponuje procedurami niszczenia materiałów w postaci drukowanej (papierowej). Wymagają one, aby wszystkie materiały w postaci drukowanej były niszczone dwukierunkowo w niszczarce, palone lub przetwarzane na masę celulozową w taki sposób, aby nie można było ich odtworzyć.

- Firma będzie dysponowała udokumentowanymi procedurami niszczenia nośników elektronicznych. Będą one wymagać następujących środków bezpieczeństwa:
    - Wszystkie dane właścicieli kart na nośnikach elektronicznych muszą być kasowane w sposób nieodwracalny, np. przez rozmagnesowanie lub wymazywanie elektroniczne z zastosowaniem bezpiecznych procedur kasowania klasy wojskowej lub fizycznego niszczenia nośników;
    - W przypadku korzystania z programów do bezpiecznego wymazywania procedura ta musi określać uznane w branży standardy bezpiecznego kasowania.
- Wszystkie informacje właścicieli kart oczekujące na zniszczenie należy przechowywać w zamykanych pojemnikach do przechowywania wyraźnie oznaczonych jako „Przeznaczone do zniszczenia" — należy ograniczyć dostęp do tych pojemników.

9. Świadomość i procedury bezpieczeństwa

Opisane poniżej zasady i procedury należy uwzględnić w działalności firmy w celu zachowania wysokiego stopnia świadomości bezpieczeństwa. Ochrona poufnych danych wymaga regularnego szkolenia wszystkich pracowników i kontrahentów.

- Dokonać oceny procedur przetwarzania poufnych informacji i organizować regularne spotkania poświęcone świadomości bezpieczeństwa w celu uwzględnienia tych procedur w codziennej działalności firmy.
- Przekazać niniejszy dokument dotyczący polityki bezpieczeństwa wszystkim pracowników do przeczytania. Wymagane jest, aby wszyscy pracownicy potwierdzili zrozumienie treści niniejszego dokumentu dotyczącego polityki bezpieczeństwa, podpisując formularz potwierdzenia (patrz Dodatek A).
- Wszyscy pracownicy zajmujący się przetwarzaniem poufnych informacji zostaną poddani kontrolom przeszłości (takim jak kontrole wpisów w rejestrach kryminalnych i kredytowych, w granicach miejscowego prawa) przed rozpoczęciem zatrudnienia w Firmie.
- Wszystkie podmioty zewnętrzne mające dostęp do numerów rachunków kart kredytowych są zobowiązane umową do przestrzegania standardów bezpieczeństwa stowarzyszeń kart płatniczych (PCI/DSS).
- Polityka bezpieczeństwa Firmy musi być poddawana corocznej ocenie i aktualizowana w miarę potrzeb.

10. Plan reagowania na incydenty dotyczące bezpieczeństwa danych kart kredytowych (PCI)

- Do zespołu ds. reagowania na incydenty dotyczące bezpieczeństwa PCI Firmy (zespołu ds. reagowania na incydenty PCI) należy dyrektor ds. bezpieczeństwa informacji oraz usług akceptanta. Opracowany przez Firmę plan reagowania na incydenty dotyczące bezpieczeństwa PCI przedstawia się następująco:

  1. Każdy dział musi zgłaszać wszelkie incydenty dyrektorowi ds. bezpieczeństwa informacji (preferowane) lub innego członka zespołu ds. reagowania na incydenty PCI.
  2. Członek zespołu, który otrzyma zgłoszenie, ma obowiązek powiadomić zespół ds. reagowania na incydenty PCI o takim incydencie.
  3. Zespół ds. reagowania na incydenty PCI zbada incydent i udzieli pomocy odpowiedniemu działowi w celu ograniczenia ryzyka dla danych właścicieli kart oraz zagrożeń związanych z incydentem.
  4. Zespół ds. reagowania na incydenty PCI opracuje rozwiązanie problemu ku satysfakcji wszystkich dotkniętych nim stron, a także zgłosi incydent oraz poczynione ustalenia odpowiednim podmiotom (stowarzyszeniom operatorów kart kredytowych, operatorom kart kredytowych), jeśli zostanie to uznane za konieczne.
  5. Zespół ds. reagowania na incydenty PCI ustali, czy należy zaktualizować zasady i procesy w celu uniknięcia podobnych incydentów w przyszłości oraz czy należy wprowadzić dodatkowe zabezpieczenia w środowisku, w którym wystąpił incydent, bądź w całej instytucji.

Zespół ds. reagowania na incydenty bezpieczeństwa PCI Firmy (lub jego odpowiednik w danej organizacji):

Dyrektor ds. informatycznych	Ewa Zimna	Bartłomiej Zimny
Dyrektor ds. komunikacji		
Dyrektor ds. zgodności z przepisami		
Radca prawny		
Dyrektor ds. bezpieczeństwa informacji		
Przedstawiciel działu płatności i usług akceptanta		
Kierownik ds. ryzyka		

Procedury reagowania na incydenty PCI związane z bezpieczeństwem informacji:

- Jeśli pracownicy działu mają uzasadnione podejrzenia, że doszło do włamania na konto, do środowiska danych właścicieli kart lub systemów powiązanych z takim środowiskiem, mają obowiązek powiadomić o tym zespół ds. reagowania na incydenty PCI w Firmie. Po otrzymaniu informacji o możliwym naruszeniu zabezpieczeń zespół ds. reagowania na incydenty PCI wraz z innymi wyznaczonymi pracownikami wdrożą plan reagowania na incydenty PCI, wspierający i uzupełniający plany działania opracowane przez dział.

Powiadamianie o reagowaniu na incydenty:

Pracownicy objęci procedurą eskalacji (lub jej odpowiednikiem w firmie):

Eskalacja — pierwszy poziom:
Inspektor ds. bezpieczeństwa informacji
Dyrektor projektowy ds. płatności kredytowych i radca prawny ds. usług akceptanta
Kierownik ds. ryzyka
Dyrektor ds. komunikacji w Firmie

Eskalacja — drugi poziom:
Prezes Firmy
Zarząd
Audytorzy wewnętrzni
Dodatkowi pracownicy (jeśli jest to konieczne)

Zewnętrzne osoby kontaktowe (jeśli jest to konieczne)
Operatorzy kart obsługiwanych przez akceptanta
Dostawca usług internetowych (jeśli dotyczy)
Dostawca usług internetowych intruza (jeśli dotyczy), operatorzy telekomunikacyjni (lokalni i ogólnokrajowi), partnerzy biznesowi
Ubezpieczyciel
Zewnętrzny zespół ds. reagowania, jeśli dotyczy (Centrum koordynacyjne CERT 1 itp.), służby ochrony porządku publicznego (w zależności od lokalnych regulacji)

W odpowiedzi na możliwe naruszenie zabezpieczeń systemu zespół ds. reagowania na incydenty PCI oraz wyznaczone przezeń osoby podejmą następujące działania:

1. Zapewnienie odizolowania systemów z naruszonymi zabezpieczeniami od sieci.
2. Zgromadzenie, przejrzenie i przeanalizowanie rejestrów i powiązanych informacji z różnych lokalnych i centralnych funkcji zabezpieczeń.
3. Przeprowadzenie odpowiedniej analizy kryminalistycznej systemu z naruszonymi zabezpieczeniami.
4. Nawiązanie kontaktu z odpowiednimi wewnętrznymi i zewnętrznymi działami oraz podmiotami.
5. Udostępnienie analizy kryminalistycznej i analizy rejestrów odpowiednim służbom ochrony porządku publicznego lub pracownikom operatorów kart zajmującym się kwestiami bezpieczeństwa.
6. Służenie pomocą organom ochrony porządku publicznego oraz pracownikom operatorów kart zajmującym się kwestiami bezpieczeństwa w prowadzeniu dochodzenia, w tym również na drodze sądowej.

Poszczególni operatorzy kart kredytowych mają indywidualne wymagania, które muszą zostać spełnione przez zespół ds. reagowania na incydenty PCI w związku ze zgłaszaniem podejrzanych lub potwierdzonych naruszeń zabezpieczeń danych właścicieli kart. Informacje na temat tych wymagań znajdują się poniżej.

Powiadamianie różnych operatorów kart o reagowania na incydenty

1. W przypadku podejrzenia naruszenia zabezpieczeń należy natychmiast powiadomić o tym dyrektora ds. bezpieczeństwa informacji lub kierownika liniowego.
2. Dyrektor ds. bezpieczeństwa przeprowadzi wstępne dochodzenie dotyczące podejrzenia naruszenia zabezpieczeń.
3. Po potwierdzeniu faktycznego naruszenia zabezpieczeń dyrektor ds. bezpieczeństwa informacji powiadomi o tym kierownictwo i przystąpi do informowania wszystkich stron, których taki incydent może dotyczyć.

Działania wymagane przez firmę VISA

Jeśli naruszenie zabezpieczeń danych dotyczy numerów kont kart kredytowych, należy wdrożyć następującą procedurę:

- Wyłączyć wszelkie systemy lub procesy dotknięte naruszeniem zabezpieczeń w celu ograniczenia zakresu zagrożenia oraz zapobieżenia dalszym zagrożeniom.
- Powiadomić wszystkie strony dotknięte naruszeniem zabezpieczeń oraz odpowiednie organy, jak na przykład bank akceptanta (bank Firmy), dział zapobiegania oszustwom firmy Visa oraz służby ochrony porządku publicznego.
- W ciągu 24 godzin udostępnić wszelkie szczegóły dotyczące zagrożonych lub potencjalnie zagrożonych numerów kart działowi zapobiegania oszustwom firmy Visa.
- Więcej informacji można znaleźć pod adresem: http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_if_ compromised.html

Szablon zgłaszania incydentów firmie Visa

Opisany poniżej raport należy przekazać firmie VISA w ciągu 14 dni od wstępnego zgłoszenia incydentu. Wypełniając raport dotyczący incydentu, należy zachować treść i standardy poniższego raportu. Raport dotyczący incydentu należy dostarczyć w bezpieczny sposób firmie VISA oraz bankowi akceptanta. Firma Visa sklasyfikuje raport jako „VISA Secret" (Informacje poufne firmy VISA).*

I. Podsumowanie
   a. Należy tu zawrzeć omówienie incydentu
   b. Należy określić poziom ryzyka (wysokie, średnie, niskie)
   c. Należy określić, czy naruszenie zabezpieczeń zostało opanowane
II. Tło
III. Wstępna analiza
IV. Procedury prowadzenia dochodzenia
   a. Należy opisać narzędzia stosowane podczas dochodzenia
V. Poczynione ustalenia
   a. Liczba zagrożonych kont, należy zidentyfikować zagrożone konta
   b. Typ zagrożonych informacji o kontach
   c. Należy zidentyfikować WSZYSTKIE przeanalizowane systemy. Należy podać następujące informacje:
      - Nazwy w systemie DNS (systemie nazw domen)
      - Adresy IP (protokołu internetowego)

- Wersja systemu operacyjnego (OS)
- Funkcje systemów

d. Należy zidentyfikować WSZYSTKIE zagrożone systemy. Należy podać następujące informacje:
    - Nazwy DNS
    - Adresy IP
    - Wersja OS
    - Funkcje systemów
e. Ramy czasowe wystąpienia naruszenia zabezpieczeń
f. Dane wyeksportowane przez intruza
g. Metoda i źródło naruszenia zabezpieczeń
h. Należy sprawdzić wszystkie potencjalne lokalizacje baz danych, aby upewnić się, że dane kody CVV2, ścieżki 1 ani ścieżki 2 nie są nigdzie przechowywane, w postaci szyfrowanej lub nieszyfrowanej (np. w duplikatach lub kopiach zapasowych tabel bądź baz danych, bazach danych używanych w środowiskach opracowywania lub testowania systemów bądź środowiskach pośrednich, jako dane na komputerach programistów itp.)
i. Jeśli dotyczy, należy sprawdzić zabezpieczenia punktów końcowych VisaNet i określić poziom ryzyka

VI. Działania podjęte przez podmiot, w którym wystąpiło naruszenie zabezpieczeń
VII. Zalecenia
VIII. Osoby kontaktowe w podmiocie oraz prowadzącym dochodzenie audytorze zabezpieczeń

*Ta klasyfikacja dotyczy najbardziej wrażliwych informacji biznesowych, przeznaczonych do użytku wewnętrznego w firmie VISA. Udostępnienie ich bez upoważnienia może stanowić poważne zagrożenie dla firmy VISA, jej pracowników, współpracujących banków, partnerów biznesowych i/lub marki VISA.

Działania wymagane przez firmę MasterCard

I. W ciągu 24 godzin od wystąpienia zdarzenia naruszenia bezpieczeństwa konta zawiadomić telefonicznie zespół ds. zagrożonych kont firmy MasterCard pod numerem telefonu 1-636-722-4100.
II. Sporządzić szczegółowe pisemne zestawienie faktów dotyczących naruszenia bezpieczeństwa konta, w tym okoliczności przyczyniających się do tego, i przesłać w zabezpieczonej wiadomości e-mail: na adres compromised_account_team@mastercard.com.
III. Przekazać działowi zapobiegania oszustwom firmy MasterCard pełną listę wszystkich znanych numerów kont, zagrożonych przez naruszenie zabezpieczeń.
IV. W ciągu 72 godzin od podjęcia informacji o potencjalnym naruszeniu bezpieczeństwa konta zaangażować personel firmy zajmującej się bezpieczeństwem danych, zatwierdzonej przez firmę MasterCard, w celu dokonania oceny wrażliwości danych i powiązanych systemów, których bezpieczeństwo zostało naruszone (np. szczegółowej oceny kryminalistycznej).
V. Co tydzień przekazywać firmie MasterCard pisemne raporty statusu, uwzględniające otwarte pytania i problemy, do chwili ukończenia audytu w sposób zadowalający dla firmy MasterCard.
VI. Niezwłocznie przekazywać zaktualizowane listy numerów kont, których zabezpieczenia zostały potencjalnie lub faktycznie złamane, dodatkową dokumentację i inne informacje, o które poprosi firma MasterCard.
VII. Przekazywać wyniki wszystkich audytów i dochodzeń do działu kontroli oszustw akceptantów firmy MasterCard (MasterCard Merchant Fraud Control) w wymaganym terminie oraz stale ograniczać istniejące ryzyko i wdrażać wydane rekomendacje aż do załatwienia sprawy w

sposób zadowalający dla firmy MasterCard.

Z chwilą otrzymania szczegółów naruszenia bezpieczeństwa danych kont i listy numerów kont, których bezpieczeństwo zostało naruszone, firma MasterCard:

1. Zidentyfikuje wystawców kart, których konta były potencjalnie narażone, i pogrupuje wszystkie znane konta pod odpowiednimi identyfikatorami nadrzędnymi wystawców.

2. Przekaże dane numerów kont odpowiednim wystawcom.

Od pracowników firmy będzie oczekiwać się zgłaszania wszelkich problemów związanych z bezpieczeństwem wyznaczonemu pracownikowi ochrony. Rola takiego pracownika ochrony polega na skutecznym komunikowaniu pracownikom firmy i wykonawcom wszelkich zasad i procedur bezpieczeństwa. Oprócz tego pracownik ochrony będzie nadzorować planowanie szkoleń w zakresie bezpieczeństwa, monitorować i egzekwować zasady bezpieczeństwa omówione w niniejszym dokumencie oraz w trakcie szkoleń, i wreszcie nadzorować wdrażanie planu reagowania na incydenty na wypadek naruszenia bezpieczeństwa poufnych danych.

Procedura dotycząca kart Discover Card

I. W ciągu 24 godzin od wystąpienia zdarzenia naruszenia bezpieczeństwa konta zawiadomić dział zapobiegania oszustwom firmy Discover Card pod numerem telefonu (800) 347-3102.
II. Sporządzić szczegółowe pisemne zestawienie faktów dotyczących naruszenia bezpieczeństwa konta, w tym okoliczności przyczyniających się do tego.
III. Sporządzić listę wszystkich znanych numerów kont, których bezpieczeństwo faktycznie naruszono.
IV. Uzyskać dodatkowe wymagania właściwe firmie Discover Card.

Procedura dotycząca kart American Express

I. W ciągu 24 godzin od wystąpienia zdarzenia naruszenia bezpieczeństwa konta zawiadomić dział obsługi akceptantów firmy American Express pod numerem telefonu (800) 528-5200 w USA.
II. Sporządzić szczegółowe pisemne zestawienie faktów dotyczących naruszenia bezpieczeństwa konta, w tym okoliczności przyczyniających się do tego.
III. Sporządzić listę wszystkich znanych numerów kont, których bezpieczeństwo faktycznie naruszono. Uzyskać dodatkowe wymagania właściwe firmie American Express.

11. Polityka transferu informacji poufnych

- Wszystkie niezależne firmy świadczące na rzecz Firmy istotne usługi muszą podpisać odpowiednią umowę o poziomie usług.
- Wszystkie niezależne firmy udostępniające obiekty gościnne muszą przestrzegać polityki Firmy w zakresie zabezpieczeń fizycznych i kontroli dostępu.
- Wszystkie niezależne firmy mające dostęp do danych właścicieli kart muszą:

1. Przestrzegać wymagań bezpieczeństwa ujętych w standardzie PCI DSS.
2. Potwierdzić zobowiązanie do zabezpieczenia danych właścicieli kart.
3. Potwierdzić fakt, że dane właścicieli kart mogą być używane wyłącznie w celu ułatwienia realizacji transakcji, na potrzeby programu lojalnościowego, świadczenia usługi kontroli oszustw lub zastosowań wymaganych przez prawo.
4. Przestrzegać odpowiednich postanowień dotyczących zapewnienia ciągłości działalności na wypadek poważnych utrudnień, klęsk żywiołowych czy awarii.
5. Zapewnić pełną współpracę i dostęp na potrzeby przeprowadzenia przez przedstawiciela lub zatwierdzony niezależny podmiot branży kart płatniczych kompleksowego przeglądu zabezpieczeń po incydencie związanym z naruszeniem bezpieczeństwa.

12. Zarządzanie dostępem użytkowników

- Dostęp do Firmy jest kontrolowany poprzez formalny proces rejestracji użytkowników, zaczynający się od oficjalnego zawiadomienia przez dział kadr lub przez bezpośredniego przełożonego.
- Każdy użytkownik posiada unikatowy identyfikator, dzięki któremu można powiązać użytkowników z ich działaniami i rozliczać ich z nich. Stosowanie identyfikatorów grupowych jest dozwolone wyłącznie wówczas, gdy wymaga tego charakter wykonywanej pracy.

- Istnieje standardowy poziom dostępu; dostęp do innych usług można uzyskać na podstawie upoważnienia uzyskanego od działu kadr/bezpośredniego przełożonego.
- Poziom dostępu pracownika do danych właścicieli kart zależy od jego stanowiska.
- Wniosek o dostęp do usługi musi złożyć na piśmie (za pośrednictwem poczty e-mail lub wydruku) bezpośredni przełożony nowego pracownika lub dział kadr. Format wniosku jest dowolny, ale musi on zawierać następujące informacje:

  Imię i nazwisko osoby składającej wniosek
  Stanowisko i grupa robocza nowego pracownika
  Data początkowa
  Wymagane usługi (usługi domyślne to: MS Outlook, MS Office i dostęp do Internetu)

- Każdy użytkownik otrzyma kopię formularza nowego użytkownika, który stanowi pisemne zestawienie jego praw dostępu, podpisane przez przedstawiciela działu informatycznego po przeprowadzeniu procedury wprowadzenia. Użytkownik podpisuje formularz, wskazując, że rozumie warunki dostępu.
- Dostęp do wszystkich systemów Firmy daje dział informatyczny, po przeprowadzeniu odpowiednich procedur.

- Z chwilą odejścia użytkownika z Firmy jego wszystkie loginy muszą zostać natychmiast unieważnione.
- W ramach procesu rozwiązania umowy o pracę dział kadr (lub bezpośredni przełożeni w przypadku wykonawców) zawiadamia dział informatyczny o osobach odchodzących z firmy i o dacie odejścia.

13. Polityka kontroli dostępu

- Wdrożone systemy kontroli dostępu mają na celu ochronę interesów wszystkich użytkowników systemów komputerowych Firmy przez zapewnienie im bezpiecznego i łatwo dostępnego środowiska pracy.
- Firma będzie przekazywać wszystkim pracownikom i innym użytkownikom informacje niezbędne im do wykonywania swoich obowiązków w sposób jak najbardziej efektywny i sprawny.
- Identyfikatory ogólne lub grupowe zasadniczo nie są dozwolone, ale mogą być przyznawane w wyjątkowych okolicznościach, o ile istnieją inne sposoby kontroli dostępu.
- Przyznawanie uprawnień (np. lokalnego administratora, administratora domeny, superużytkownika, dostępu głównego) będzie ograniczone i kontrolowane, a autoryzacje będą przyznawane wspólnie przez właściciela systemu i dział informatyczny. Zespoły techniczne powinny unikać przyznawania uprawnień całym zespołom, aby zapobiec utracie poufności.
- Prawa dostępu będą przyznawane na zasadach „najmniejszego uprawnienia" i „potrzeby posiadania informacji".
- Każdy użytkownik powinien dążyć do utrzymania bezpieczeństwa danych na ich poziomie poufności, nawet w przypadku, gdy zabezpieczenia techniczne zawodzą lub nie są stosowane.
- Użytkownicy decydujący się na umieszczenie danych na nośnikach cyfrowych lub urządzeniach pamięci, albo w odrębnej bazie danych, mogą to zrobić tylko wówczas, gdy jest to zgodne z klasyfikacją danych.
- Użytkownicy mają obowiązek zgłaszania przypadków niezgodności z CISO Firmy.
- Dostęp do zasobów i usług informatycznych Firmy będzie przyznawany przez ustanowienie unikatowego konta Active Directory i złożonego hasła.
- Dostęp do zasobów i usług informatycznych Firmy nie będzie przyznawany bez wcześniejszego uwierzytelnienia i autoryzacji konta Windows Active Directory użytkownika w systemie Firmy.
- Wydawaniem haseł, wymogami dotyczącymi ich siły, zmianą i kontrolą będzie zarządzać się za pośrednictwem formalnych procesów. Długość haseł, ich złożoność i terminy ważności będą kontrolować obiekty zasad grupy Active Directory systemu Windows.
- Dostęp do informacji poufnych, zastrzeżonych i chronionych zostanie ograniczony do osób uprawnionych, których obowiązki zawodowe wymagają tego, wyznaczonych przez właściciela danych lub wskazanego przez niego przedstawiciela. Wnioski o udzielenie, zmianę lub odwołanie uprawnień dostępu muszą być składane w formie pisemnej.
- Od użytkowników oczekuje się poznania i przestrzegania zasad, standardów i wytycznych Firmy dotyczących stosownego i dopuszczalnego użytku sieci i systemów.
- Dostęp użytkowników zdalnych będzie podlegać autoryzacji przez dział informatyczny i będzie przyznawany zgodnie z polityką dostępu zdalnego oraz polityką bezpieczeństwa informacji. Nie będzie dozwolony niekontrolowany dostęp zewnętrzny do żadnych urządzeń czy systemów sieciowych.
- Dostęp do danych jest kontrolowany w sposób zależny od poziomów klasyfikacji danych opisanych w polityce zarządzania bezpieczeństwem informacji.
- Metody kontroli dostępu obejmują: prawa dostępu przez logowanie, uprawnienia udziałów i NTFS systemu Windows, uprawnienia kont użytkowników, prawa dostępu do serwerów i stacji roboczych, uprawnienia zapory, prawa uwierzytelniania IIS w sieciach intranet/extranet, prawa do baz danych SQL, sieci wydzielone i inne metody stosowne do potrzeb.

- W regularnych odstępach czasu właściciele systemów i danych, we współpracy z działem informatycznym, powinni przeprowadzać formalny proces przeglądu praw dostępu użytkowników. Przegląd należy zarejestrować w dzienniku, a dział informatyczny powinien go zatwierdzić celem utrzymania praw dostępu użytkowników.