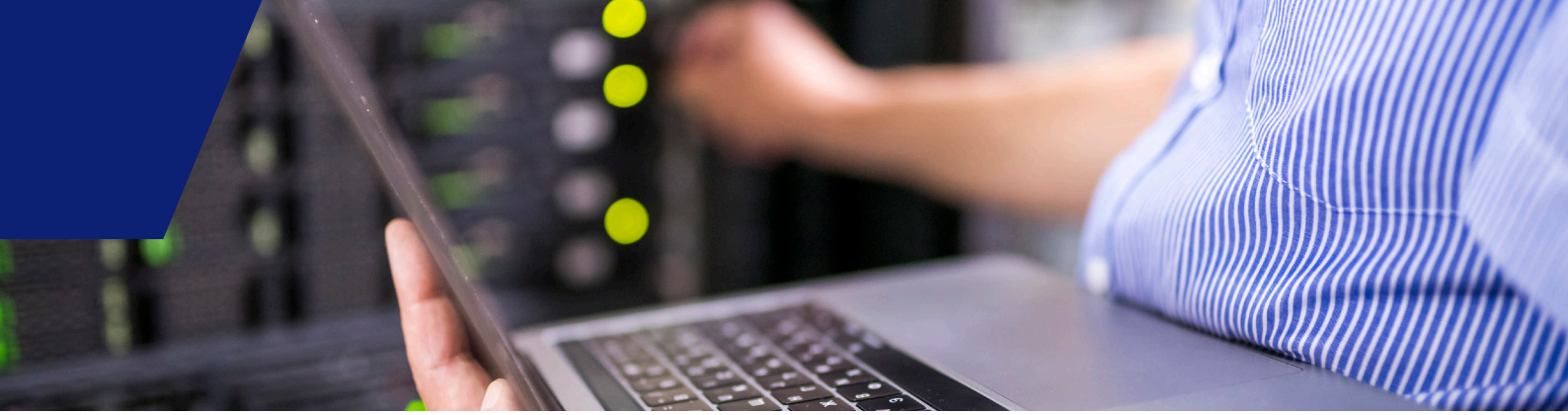
Elavon

Co należy zrobić w przypadku utraty lub kradzieży danych kartowych?

Krótki przewodnik Elavon

elavon.pl



Należy działać szybko

Organizacje obsługujące płatności kartowe są narażone na kradzież danych posiadaczy kart, w wyniku ataku hakerskiego, kradzieży typu „card skimming" lub innych metod stosowanych przez przestępców. Głośne przypadki oszustw regularnie prezentowane są w mediach.

Oszuści często upatrują sobie jako cel systemy przechowywania, przetwarzania bądź przesyłania danych posiadaczy kart. Systemy te mogą być własnością przedsiębiorstwa lub zewnętrznego dostawcy, z którym przedsiębiorstwo współpracuje.

Naruszenie bezpieczeństwa danych w terminologii branżowej określa się mianem **naruszenia ochrony danych (Account Data Compromise - ADC).**

W przypadku wystąpienia zdarzenia ADC w organizacji kluczowe znaczenie ma posiadanie wewnętrznego planu reagowania na tego typu sytuacje. Taki plan dopasowany do środowiska biznesowego firmy pozwala na podjęcie skutecznych działań. W tym przewodniku znajdują się pomocne wskazówki w tym zakresie.

Zapobieganie naruszeniom bezpieczeństwa przede wszystkim

Standard PCI DSS ma na celu wzmocnienie ochrony, jednak nie gwarantuje pełnego bezpieczeństwa danych wrażliwych. Przedsiębiorstwa muszą więc podjąć kroki służące zabezpieczaniu własnego mienia oraz danych swoich klientów. Firma Elavon opracowała w tym celu ważne wytyczne. Po prostu skontaktuj się z nami.

Zasady postępowania w przypadku naruszenia bezpieczeństwa danych

W przypadku wykrycia zdarzenia ADC lub podejrzenia jego wystąpienia należy wykonać poniższe kroki:

Krok 1

Natychmiast skontaktuj się z zespołem ds. bezpieczeństwa firmy Elavon.

Krok 2

Nie używaj i nie zmieniaj nic w zaatakowanych systemach. Najważniejsze jest tu zaniechanie działań, które mogłyby wymazać wskazówki, zanieczyścić dowody lub w inny sposób nieumyślnie pomóc hakerowi.

Krok 3

Odłącz zaatakowane urządzenia od sieci internetowej, ale ich nie wyłączaj i nie wprowadzaj na nich żadnych zmian.

Krok 4

Skorzystaj ze swojego planu reagowania na incydenty i skontaktuj się z osobami właściwymi dla tego rodzaju sytuacji, takimi jak zewnętrzni dostawcy usług, prawnicy, pracownicy działu kadr, PR, obsługi klienta i wszelkimi innymi zespołami odpowiedzialnymi za kontakty z klientami, które powinny być zaangażowane w działania związane z usuwaniem skutków naruszenia bezpieczeństwa danych.

Jak można skontaktować się z Elavon?

Prosimy o kontakt z zespołem ds. naruszenia ochrony danych Elavon. Służymy pomocą w każdej sytuacji.

Kraj	E-mail	Telefon
UK	ADCqueries-EU@elavon.com	01923 651 622
Ireland	ADCqueries-EU@elavon.com	0402 25322
Inne kraje UE	ADCqueries-EU@elavon.com	

Analiza zdarzenia

Po zgłoszeniu sprawy wprowadzona zostaje procedura zarządzania zdarzeniem ADC. Procedury te zakładają udział specjalisty ds. kryminalistyki PCI (PFI) badającego przyczyny naruszenia.

- W ciągu 5 dni musisz wyznaczyć specjalistę PFI
- W ciągu 10 dni ty i specjalista PFI musicie podpisać umowę
- W ciągu kolejnych 5 dni specjalista PFI rozpocznie pracę

Firma Elavon służy pomocą w realizacji tego procesu.

Organizacje kartowe zarządzają zdarzeniami ADC w różny sposób. Sposób postępowania w przypadku zdarzeń ADC jest dyktowany przez organizacje kartowe (Visa, Mastercard, Amex, Diners lub JCB), których dotyczy dane naruszenie.

Visa Europe realizuje dwa typy analiz w zależności od poziomu klienta oraz liczby i rodzaju przetwarzanych transakcji kartą.

Ogólna analiza PFI

Ma na celu szybką i efektywną kosztowo analizę ewentualnego zdarzenia związanego z naruszeniem ochrony danych u małych klientów oraz podjęcie działań naprawczych.

Dla kogo jest przeznaczona?

- Klienci przyjmujący do 10 000 transakcji
- Jedynie klienci poziomu 4 PCI. Do trzech urządzeń elektronicznych, np. strona internetowa, serwer i baza danych
- Klienci, którzy nie przyjmują transakcji za pomocą terminala wirtualnego

Uwaga: Jedynie organizacja Visa wykonuje ogólną analizę PFI. Jeśli nie spełniasz kryteriów ogólnej analizy PFI, musisz ukończyć szczegółową analizę PFI.

Szczegółowa analiza PFI

Podczas tej analizy zdarzenie naruszenia ochrony danych badane jest bardziej szczegółowo.

Dla kogo jest przeznaczona?

- Klienci przetwarzający ponad 10 000 transakcji
- Klienci przetwarzający transakcje za pomocą terminala wirtualnego
- Sprzedawcy, u których wcześniej wystąpiło naruszenie bezpieczeństwa i którzy nie przeszli ogólnej analizy PFI
- Klienci przetwarzający transakcje w punktach sprzedaży, narażone na naruszenie ochrony danych

Uwaga: Wszystkie organizacje kartowe otrzymają stosowne informacje od zespołu ds. naruszenia ochrony danych Elavon.

Jakie opłaty ADC nalicza organizacja Visa?

Visa stosuje różne poziomy opłat dla zdarzeń naruszenia ochrony danych. Dla wszystkich przypadków obowiązuje standardowa kara w wysokości 3000 GBP, jednak koszty mogą być wyższe w przypadku szczegółowych analiz PFI.

Visa Europe może obciążać takimi opłatami wszystkich agentów rozliczeniowych przetwarzających płatności w imieniu klienta.

Ogólna analiza PFI	Szczegółowa analiza PFI
Klienci przetwarzający do 10 000 transakcji dokonywanych za pomocą kart Visa: • Opłata 3000 GBP za przypadek • Brak naliczania dalszych kar w przypadku uzyskania zgodności w procesie ogólnej analizy PFI	**Klienci przetwarzający ponad 10 000 transakcji dokonywanych za pomocą kart Visa:** • 3 EUR za utraconą kartę – tylko długi numer karty • 18 EUR za utraconą kartę – długi numer karty i kod bezpieczeństwa • Opłata 3000 EUR za przypadek

Elavon może pomóc firmom w obniżeniu opłat nakładanych przez organizację Visa

Istnieje możliwość ograniczenia wysokości kar o 25-100% w oparciu o wcześniejsze, samodzielne zgłoszenie naruszenia i prawidłowe zgłoszenie statusu zgodności PCI organizacjom kartowym.

Kluczowe znaczenie ma w takim wypadku kontakt z Elavon natychmiast po wykryciu lub powstaniu podejrzenia ewentualnego naruszenia. W ten sposób możemy zwiększyć prawdopodobieństwo obniżenia kosztów.

W przypadku klientów zweryfikowanych przez Visa (VbV), u których wystąpiło zdarzenie naruszenia ochrony danych i którzy podlegają karze finansowej w oparciu o liczbę zagrożonych kont istnieje możliwość zredukowania kar nawet o 50%.

Klient A → 35% **zweryfikowanych transakcji VbV** → 35% **ograniczenia kosztów**

Klient B → 65% **zweryfikowanych transakcji VbV** → 50% **ograniczenia kosztów**

Opłaty za zdarzenia ADC nakładane przez Mastercard

Opłaty Mastercard za zdarzenia naruszenia ochrony danych (ADC) zwane są zwrotem operacyjnym (OR) i zwrotem z tytułu nadużycia (FR). Mastercard nakłada opłaty, jeśli zdarzenie dotyczy 30 000 kont Mastercard.

Struktura naliczania kar jest bardzo skomplikowana i zależy od tego, który wydawca wybrał model zwrotów.

Zaraz po otrzymaniu informacji o opłacie nałożonej przez Mastercard, Elavon kontaktuje się z klientem.

Obliczanie opłat po wykryciu naruszenia

W zależności od charakteru oraz skali naruszenia bierze się pod uwagę różne czynniki i ulgi.

W tym przykładzie doszło do zdarzenia ADC z udziałem klienta, który nie uzyskał certyfikatu zgodności z normami branżowymi, oraz 4 000 zagrożonych kart Visa i do 30 000 zagrożonych kart Mastercard. Na potrzeby tego przykładu główny numer rachunku (PAN) oraz numer CVV został zlokalizowany.

Visa	€	£
Główny numer konta (PAN) i numer CVV 4000 x 18 EUR	(72 000 EUR)	61 512 GBP
Obniżenie kary za zgodność 25%	-(18 000 EUR)	-15 378 GBP
	(54 000 EUR)	**46 134 GBP**
Obniżenie kary dla klientów VbV	-(27 000 EUR)	-23 067 GBP
	(27 000 EUR)	**23 067 GBP**
Opłata za przypadek ADC	(3000 EUR)	2563 GBP
Suma częściowa	**(30 000 EUR)**	**25 630 GBP**
Mastercard	(0 EUR)	0 GBP
	Suma łączna	**25 630 GBP***

*Kwoty kary są poprawne na dzień i godzinę ich naliczenia, podlegają zmianie i są określane dla konkretnych przypadków.

Na jakie inne koszty są narażone przedsiębiorstwa?

Oprócz uiszczania kar, przedsiębiorstwa muszą również podjąć kroki gwarantujące, że naruszenie nie wystąpi po raz kolejny. Zaangażowanie audytora bezpieczeństwa (Qualified Security Assessor) w celu opracowania szczegółowego raportu dotyczącego zgodności (certyfikat 1 poziomu) może kosztować ok. 9000 GBP plus VAT oraz obejmować dodatkowe koszty w zależności od złożoności systemów.

Przedsiębiorstwa mogą jednak stanąć w obliczu szeregu dodatkowych kosztów, które muszą uwzględnić:

- Migrację do rozwiązania opartego na outsourcingu
- Ponowne opracowanie strony internetowej
- Realizację bieżącego programu zgodności w ciągu 90 dni
- Koszt ryzyka utraty reputacji

Elavon służy pomocą

Współpraca z jednym z największych na świecie agentów rozliczeniowych przynosi korzyści w postaci fachowej wiedzy dotyczącej branży płatniczej.

Naszym klientom zapewniamy wsparcie na każdym etapie procesu ADC:

- Pomoc w nawiązaniu współpracy z podmiotami zewnętrznymi
- Zapewnienie bezstronnej porady i wytycznych dotyczących środków zaradczych
- Działania na rzecz ograniczenia kosztów

Aby uzyskać więcej informacji:

skontaktuj się ze swoim opiekunem handlowym Elavon

lub z zespołem ds. naruszenia ochrony danych Elavon.

Kraj	E-mail	Telefon
UK	ADCqueries-EU@elavon.com	01923 651 622
Ireland	ADCqueries-EU@elavon.com	0402 25322
Inne kraje UE	ADCqueries-EU@elavon.com	

We make it possible. You make it happen.

Elavon

terminale@elavon.com **elavon.pl**