RAPORT ZGODNOŚCI Z PRZEPISAMI PCI-DSS

Przykładowa firma inżynierska zatrudniająca 200 pracowników

safetica

Spis treści

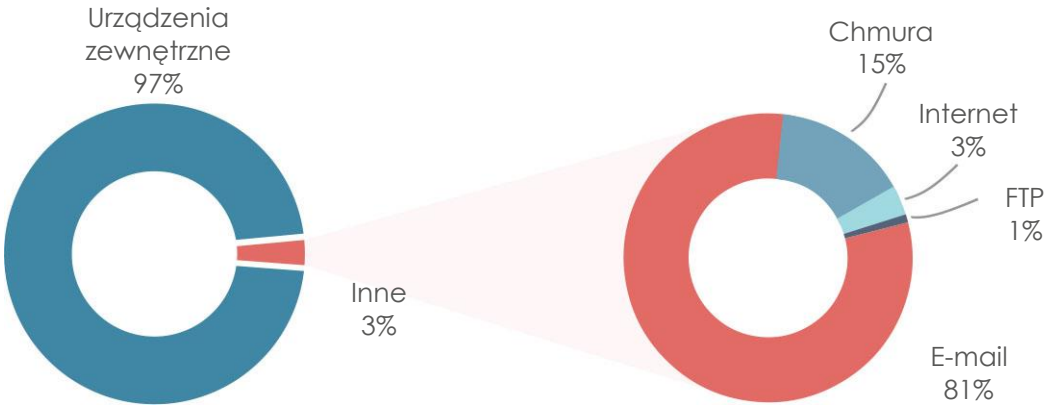
Payment Card Industry Data Security Standard

Payment Card Industry Data Security Standard (PCI-DSS) jest standardem opracowanym w celu ochrony poufnych danych związanych z kartami płatniczymi i tworzonych przy użyciu takich kart. Sam standard zawiera dwanaście wymogów, które opisywane są przez konkretne wyznaczniki. Aby osiągnąć pełną zgodność z PCI-DSS, firma musi spełnić wszystkie wymagania określone w tych wyznacznikach. Obecnie w użyciu jest wersja 3.2 PCI-DSS wydana w kwietniu 2016 roku.

Wszystkie informacje o numerach kart kredytowych, płatnościach i danych właścicieli kart są w niniejszym dokumencie nazywane „poufnymi informacjami".

Informacje zawarte w niniejszym raporcie koncentrują się głównie na wymaganiach normy PCI-DSS. Zawiera on również ogólne zalecenia, które pomogą dodatkowo zabezpieczyć środowisko i zwiększyć bezpieczeństwo w całej firmie.

Incydenty w okresie sprawozdawczym



15 Niezgodność z przepisami: przesyłanie podejrzanych plików

32 Użytkowników powiązanych z incydentami bezpieczeństwa

Incydenty według plików

company_contacts.doc ..... 10×
unit_blueprint.dwg ..... 6×
customer_data.xls ..... 2×

Główne ustalenia

⚠ 5128 plików zawierających poufne informacje

⚠ 2791 z 13 741 e-maili zawierało poufne informacje

⚠ Tylko 25 z 280 urządzeń używanych w środowisku jest zaszyfrowanych

Identyfikacja poufnych danych

Zgodnie z wymogami PCI-DSS przedsiębiorstwa są zobowiązane do ochrony przechowywanych danych posiadaczy kart.

⚠ 5128 plików zawierających poufne informacje

Skuteczną ochronę danych można zapewnić tylko wtedy, gdy wiadomo, gdzie znajdują się wrażliwe treści. Pierwszym krokiem jest odnalezienie wszystkich plików zawierających poufne informacje, sklasyfikowanie ich jako wrażliwe i ustalenie najlepszych sposobów postępowania.

Ustalenia:

- Pliki te są przechowywane zarówno na dyskach lokalnych, jak i na dyskach udostępnianych w sieci
- W sumie 12 z 200 użytkowników przechowuje te pliki na swoich lokalnych dyskach
- Przykładowe miejsca:
  - *\\192.168.91.151\operations*
  - *\\192.168.91.142\archives*
  - *C:\Users\l.baker\Desktop*

ℹ **Zalecane ustawienia w Safetica**

- Zaklasyfikować poufne dane w *Safetica Console* (Konsola Safetica) > *DLP* > *File Tagging* (Kategorie danych) > *Content rules* (Dane wrażliwe)
- Stworzyć zasady bezpieczeństwa w *Safetica Console* (Konsola Safetica) > *DLP* > *DLP rules* (Reguły DLP)

Definiowanie kanałów danych

Zgodnie z wymogami PCI-DSS istnieje potrzeba śledzenia i monitorowania wszystkich kanałów sieciowych.

⚠ W różnych kanałach znaleziono ponad 33 000 plików zawierających poufne informacje

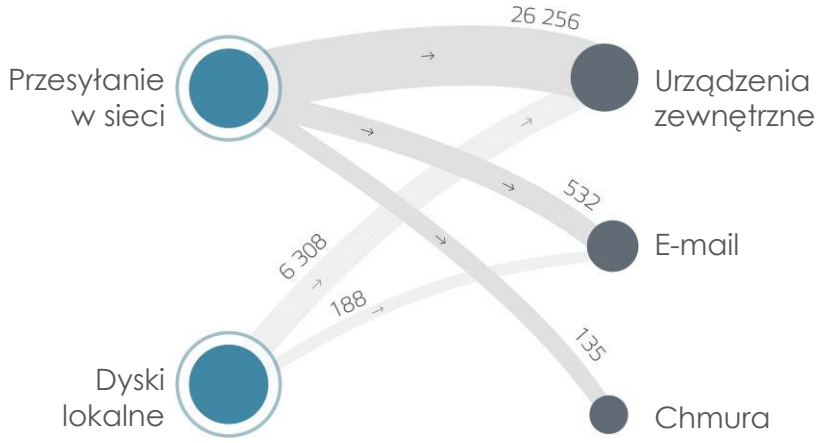
Aby móc chronić poufne dane, trzeba wiedzieć, co się z nimi dzieje. Kiedy już wiadomo, jak przepływają, można ustanowić procedury, które zatrzymają dane w środowisku firmowym.

Ustalenia:

Przegląd plików zawierających poufne informacje według kanałów:

- 32 564 pliki zostały skopiowane na urządzenia zewnętrzne
- 720 plików zostało wysłanych pocztą elektroniczną
- 135 plików zostało przesłanych do usług w chmurze, takich jak OneDrive dla Firm, OneDrive Personal, SharePoint i Dropbox
- 30 plików zostało przesłanych za pośrednictwem przeglądarek internetowych do różnych serwisów przechowywania plików i sieci społecznościowych
- 8 plików zostało przesłanych przez protokół FTP

3 główne kanały wysyłania plików zawierających poufne informacje:



Zalecane ustawienia w Safetica

- Uruchomić analizę wewnętrznego bezpieczeństwa danych

Utrzymywanie kontroli nad kanałami

Wymogi PCI-DSS nakładają obowiązek tworzenia i utrzymywania bezpiecznych systemów i aplikacji, ograniczania dostępu do danych posiadaczy kart oraz ochrony transmisji tych danych w sieci.

Przesyłanie do usług w chmurze

Przypadki korzystania z usługi przechowywania danych w chmurze zarejestrowano na 56 komputerach w firmie

Korzystanie z publicznej pamięci w chmurze, takiej jak usługi Dropbox, OneDrive lub Google Drive, zamiast z oficjalnej firmowej usługi w chmurze, to kolejna potencjalna droga wycieku poufnych informacji. Aby temu zapobiec, warto sprawdzić, czy wykorzystywana jest publiczna pamięć w chmurze, a także zabronić jej używania.

Ustalenia:

- Folder zsynchronizowany z usługą Dropbox jest używany na 12 komputerach
- Globalnie dozwolona jest usługa OneDrive Personal, mimo że dostępna jest usługa OneDrive dla Firm
- 15 plików zawierających poufne informacje przeniesiono na dyski w chmurze

Zalecane ustawienia w Safetica

- Sprawdzić wykorzystanie pamięci w chmurze publicznej w całym środowisku firmowym w *Safetica Console* (Konsola Safetica) > *DLP* > *Disk guard* (Ochrona dysku)
- Ograniczyć przesyłanie plików tylko do oficjalnej pamięci w chmurze w *Safetica Console* (Konsola Safetica) > *DLP* > *Channel control* (Kontrola kanałów) lub *Safetica Console* (Konsola Safetica) > *DLP* > *DLP rules* (Reguły DLP)

Wysyłanie poufnych danych za pośrednictwem poczty elektronicznej

⚠ 2791 z 13 741 e-maili zawierało poufne informacje

Nieograniczona możliwość wysyłania plików zawierających poufne informacje za pośrednictwem poczty elektronicznej również może prowadzić do wycieku danych.

Ustalenia:

- 17 użytkowników wysłało pocztą elektroniczną pliki z poufnymi informacjami
- Wiadomości zostały wysłane łącznie do 45 odbiorców
- 1371 z 2791 wiadomości zawierających poufne informacje wysłano poza domenę firmy

Zalecane ustawienia w Safetica

- Zabronić wysyłania plików zawierających poufne informacje poza firmę w *Safetica Console* (Konsola Safetica) > *DLP* > *DLP rules* (Reguły DLP)

Przesyłanie do publicznych stron internetowych

⚠ W firmie zarejestrowano przypadki korzystania z serwisu WeTransfer.com

Innym sposobem na udostępnienie plików zawierających poufne informacje poza firmą są strony internetowe, takie jak WeTransfer.com, MEGA.nz lub facebook.com.

Ustalenia:

- 13 użytkowników przesłało pliki z poufnymi informacjami do publicznych stron internetowych
- 30 plików zawierających dane kart kredytowych zostało umieszczonych na stronach internetowych
- W sumie użytkownicy przesłali pliki na 7 różnych publicznych stron internetowych

Zalecane ustawienia w Safetica

- Zabronić wysyłania plików zawierających poufne informacje poza dozwolone strony internetowe w lub *Safetica Console* (Konsola Safetica) > *DLP* > *DLP rules* (Reguły DLP)

Przynoszenie własnego urządzenia

⚠ Tylko 25 z 280 urządzeń używanych w środowisku jest zaszyfrowanych

Pliki zawierające poufne informacje mogą zostać przypadkowo lub celowo przeniesione na niezabezpieczone urządzenia i wyniesione poza firmę.

Ustalenia:

- Ze ścieżki sieciowej skopiowano na urządzenie zewnętrzne 5264 pliki zawierające poufne dane
- 51 użytkowników podłączyło swoje telefony komórkowe lub inne urządzenia przenośne z systemem Windows
- Tylko 173 z 213 stacji końcowych jest chronionych przez Safetica

Zalecane ustawienia w Safetica

- Ograniczyć wykorzystanie urządzeń zewnętrznych poprzez ustawienie listy dozwolonych urządzeń w *Safetica Console* (Konsola Safetica) > *DLP* > *Device Control using Zones* (Kontrola urządzeń z wykorzystaniem ~~ss~~tref)
- Rozpoznać sytuację i zabronić przenoszenia i kopiowania plików zawierających poufne informacje na niezaszyfrowane urządzenia
- Zainstalować klienta Safetica na wszystkich komputerach w sieci w *Safetica Console* (Konsola Safetica) > *Maintenance* (Ustawienia) > *Update and deploy* (Instalacja i aktualizacja)

Korzystanie z komunikatorów

⚠ W firmie zarejestrowano przypadki korzystania z komunikatorów

Korzystanie z komunikatorów internetowych, takich jak Skype czy Slack, również może być źródłem wycieku plików zawierających poufne informacje.

Ustalenia:

- Globalnie dozwolona jest aplikacja Skype, mimo że zainstalowano aplikację Skype dla firm
- 273 poufne pliki zostały wysłane przez aplikację Skype
- 23 poufne wiadomości zostały udostępnione za pomocą aplikacji Slack

Zalecane ustawienia w Safetica

- Zabronić przesyłania plików zawierających poufne informacje za pośrednictwem komunikatorów w *Safetica WebConsole* (WebSafetica) > *Policies (Polityki)* > *Applications* (Aplikacje)

Szyfrowanie dysków twardych

Zgodnie z wymaganiami PCI-DSS konieczne jest szyfrowanie danych i dysków na wszystkich platformach.

⚠ Tylko 25 z 560 dysków twardych w firmie jest zaszyfrowanych

Aby chronić poufne informacje, zalecamy szyfrowanie wszystkich używanych dysków twardych firmy.

Ustalenia:

- Tylko 25 z 560 dysków komputerowych jest zaszyfrowanych przy użyciu metody BitLocker
- 34 dyski komputerowe są zaszyfrowane inną metodą szyfrowania
- Nie ustanowiono zasad szyfrowania urządzeń zewnętrznych

Zalecane ustawienia w Safetica

- Zaszyfrować wszystkie dyski twarde tak, aby mogli je otworzyć wyłącznie upoważnieni użytkownicy w *Safetica Console* (Konsola Safetica) > *DLP* > *BitLocker disks* (Szyfrowanie Dysków)

Przegląd punktów końcowych

Zgodnie z wymogami PCI-DSS należy regularnie przeprowadzać testy procesów i bezpieczeństwa.

⚠ 13 urządzeń końcowych z systemem operacyjnym Windows XP lub Vista

Korzystanie z przestarzałego systemu operacyjnego stanowi poważne zagrożenie dla bezpieczeństwa. Takie urządzenia mogą łatwo stać się punktem wejścia dla hakerów, którzy mogą włamać się do firmowego systemu komputerowego.

Ustalenia:

- Na 8 komputerach zainstalowano system Windows XP
- Na 5 komputerach zainstalowano system Windows Vista
- Tylko 173 z 213 stacji końcowych jest chronionych przez Safetica

Zalecane ustawienia w Safetica

- Zidentyfikować urządzenia końcowe pracujące na przestarzałym lub nieobsługiwanym systemie operacyjnym w *Safetica Console* (Konsola Safetica) > *Maintenance* (Ustawienia) > *Endpoint overwiew* (Przegląd stacji roboczych)

Dostęp do krytycznych aplikacji

Zgodnie z wymaganiami PCI-DSS każdy dostęp do komponentów systemu musi być zidentyfikowany i uwierzytelniony, a także zabezpieczony przed złośliwym oprogramowaniem.

⚠ Uruchomiono 5 podejrzanych aplikacji

Zwłaszcza nieprzeszkoleni użytkownicy mogą łatwo uruchomić krytyczne aplikacje, które mogą zainfekować środowisko firmowe złośliwym oprogramowaniem lub innymi niebezpiecznymi programami.

Ustalenia:

- 2 użytkowników uruchomiło aplikację o charakterze krytycznym, np. keylogger
- Serwery hostujące pliki są globalnie dozwolone w środowisku i można z nich swobodnie korzystać
- 5 użytkowników korzystało z aplikacji typu torrent do pobierania danych

Zalecane ustawienia w Safetica

- Zablokować dostęp do podejrzanych stron internetowych w Web*Safetica* (Konsola WebSafetica) > *Polityki* > *Application control* (Aplikacje)
- Ustawić alerty informacyjne lub bezpieczeństwa w *Safetica Console* (Konsola Safetica) > *Alerts* (Alerty)
- Ustawić wysyłanie raportów ogólnych do kierownictwa w *Safetica Console* (Konsola Safetica) > *Reports* (Raporty)

Odwiedzanie krytycznych stron

Zgodnie z wymogami PCI-DSS należy zainstalować i utrzymywać konfigurację zapory, aby chronić dane posiadaczy kart i środowisko.

⚠ Odwiedzono 32 podejrzane strony internetowe

Odwiedzanie podejrzanych stron internetowych to kolejny sposób na zainfekowanie środowiska firmowego niebezpiecznym oprogramowaniem.

Ustalenia:

- 13 użytkowników weszło na strony należące do krytycznych kategorii: pornografia, nielegalne lub złośliwe oprogramowanie
- Serwery hostujące pliki są globalnie dozwolone w środowisku i można z nich swobodnie korzystać
- Usługa WeTransfer była regularnie i wielokrotnie odwiedzana

Zalecane ustawienia w Safetica

- Zablokować dostęp do podejrzanych stron internetowych w WebSafetica (Konsola WebSafetica) > *Polityki* > *Web control* (Strony internetowe)
- Ustawić alerty informacyjne lub bezpieczeństwa w Safetica Console (Konsola Safetica) > *Alerts* (Alerty)
- Ustawić wysyłanie raportów ogólnych do kierownictwa w Safetica Console (Konsola Safetica) > *Reports* (Raporty)