allegro

allegro

Norma bezpieczeństwa PCI DSS

Korzyści i problemy implementacji

Wojciech Śronek, Zespół Administratorów Sieci, Grupa Allegro Sp. z o.o.

Data Security Standards

- Payment Card Industry Security Standards Council
  - Payment Card Industry DSS
  - Payment Application DSS
  - PIN Transaction Security
- Przechowywanie, przetwarzanie, przesyłanie danych kartowych
- PCI obowiązkowy od 1 stycznia 2011
- Self-Assessment Questionnaire (SAQ)
- Qualified Security Assessor (QSA)

allegro

PCI DSS Cardholder Data Environment (CDE)

- Urządzenia sieciowe i serwery
  - Przełączniki, routery, firewalle, wifi
  - Serwery webowe, aplikacyjne, bazodanowe, mailowe
- Aplikacja
  - Wewnętrzna i zewnętrzna
- Pracownicy
  - Stacje komputerowe
- Technologie
  - Wirtualizacja
  - Proxowanie

allegro

Grupa Allegro a norma PCI DSS

- Usługi e-commerce w Grupie Allegro
- SAQ do pewnego poziomu dojrzałości serwisu
- Początek 2010 - decyzja o implementacji wymagań
- PCI w dwóch serwerowniach
- Współpraca wielu różnych zespołów
- Ilość i różnorodność urządzeń, systemów
- Za duży wolumen logów
- Wymogi proste – interpretacja i dostosowanie do konkretnej sytuacji bardzo trudne

allegro

Grupa Allegro a norma PCI DSS

- Druga połowa 2010 decyzja o oddzielnym środowisku PCI
- Zespół, który koncentrował się jedynie na wdrożeniu PCI
- Szukanie rozwiązań i zakup sprzętu zgodnego z PCI
- Spotkania przed audytem z audytorem
- Luty 2011 – Audyt przez QSA
- PCI to również planowanie następnego roku

allegro

Pierwsze wnioski

- Segmentacja sieci
  - Mniejszy zakres audytowanego środowiska
  - Mniejszy koszt wdrożenia i utrzymania
- Dobór urządzeń, systemów spełniających wymagania PCI
- Sieć bezprzewodową jedynie do transmisji jawnych danych

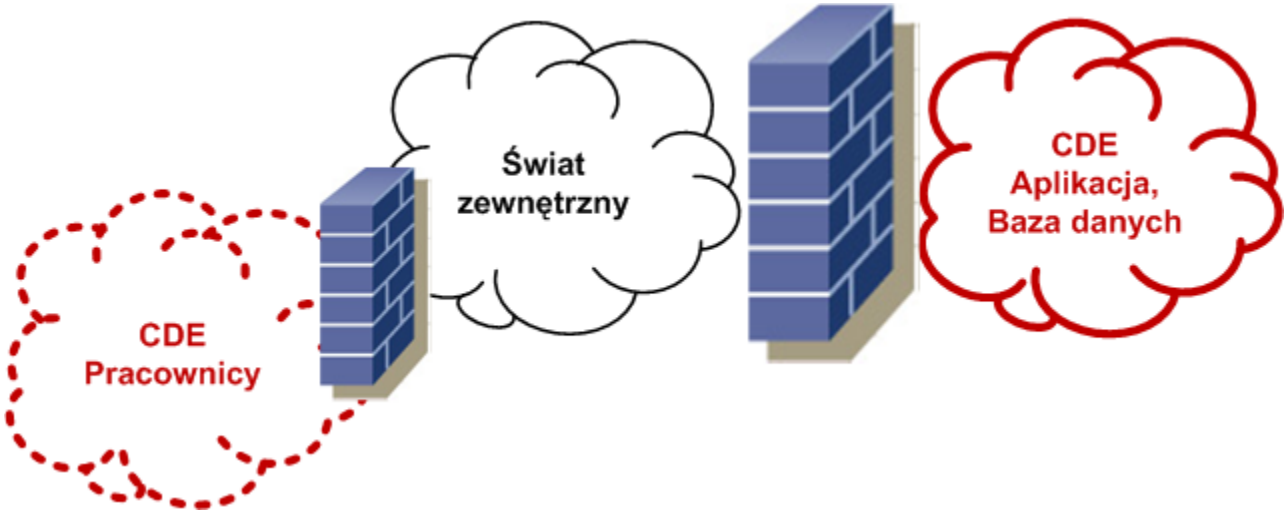
allegro

Pierwsze korzyści

- Budowa wzorcowego, bezpiecznego środowiska CDE
- Pewność użytkowników, że transakcje kartowe są bezpiecznie przetwarzane przez organizację
- Lista zaufanych organizacji Visa i Mastercard
- Uniknięcie kar finansowych
  - spełniając wymogi
  - unikając kompromitacji

allegro

Zbudowanie bezpiecznej sieci



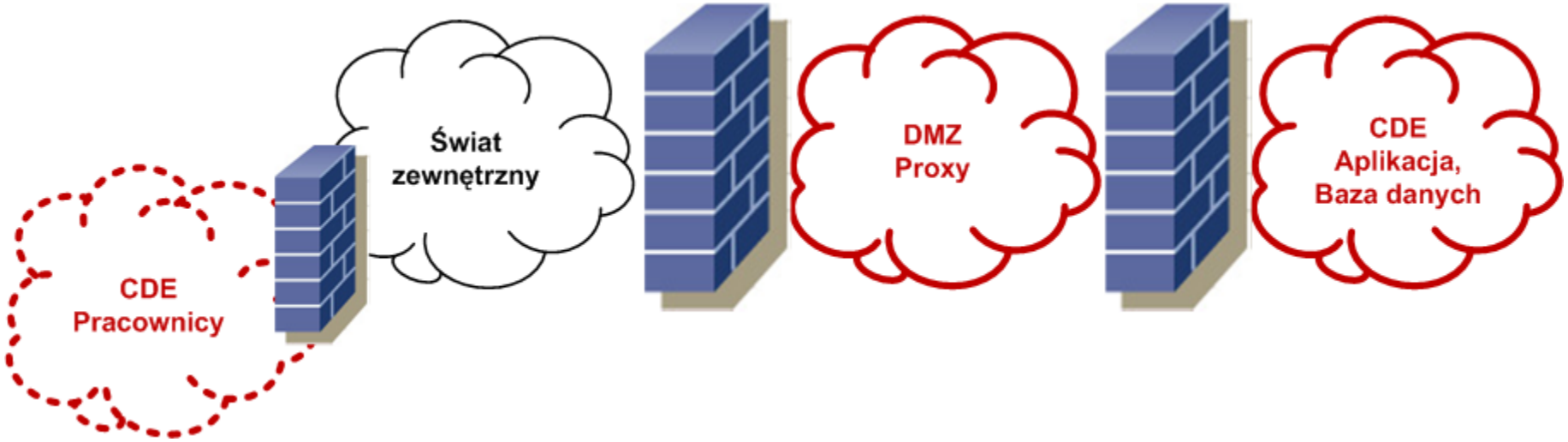
- Firewall stanowy
- NAT, adresacja CDE zgodnie z RFC1918

allegro

Zbudowanie bezpiecznej sieci

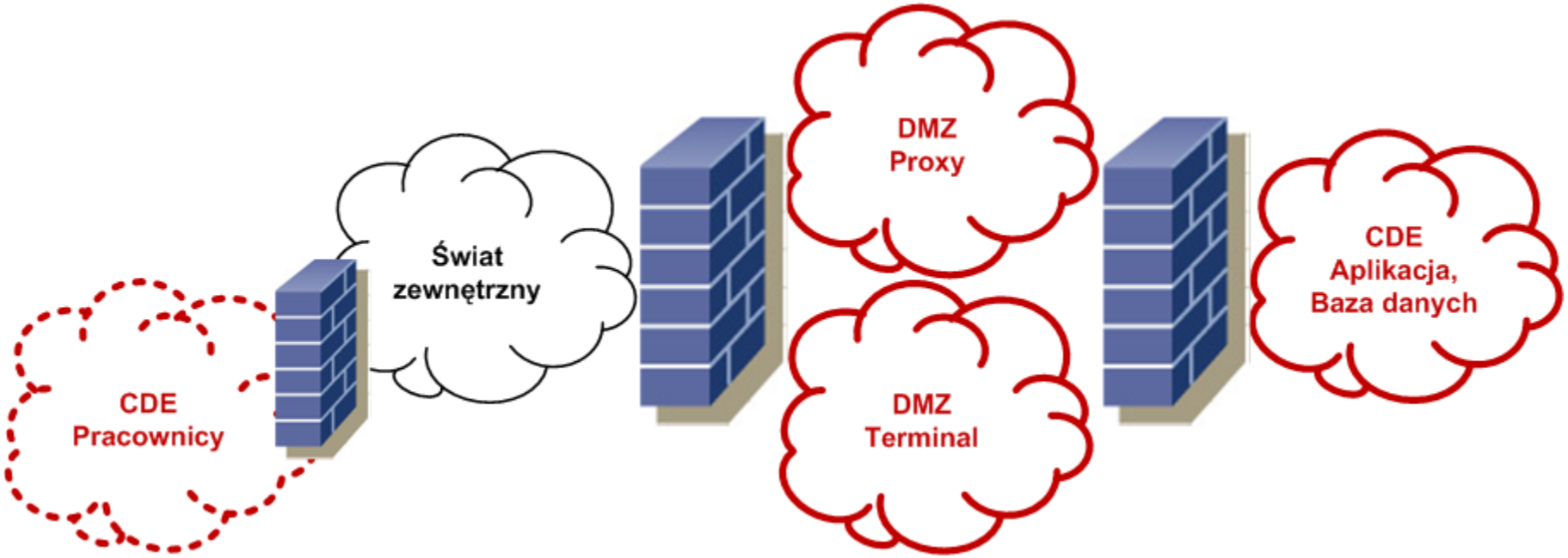
- Dokumentacja reguł firewalla
  - Źródłowy adres IP
  - Docelowy adres IP
  - Docelowy port
  - Usługa
  - Numer zmiany
  - Uzasadnienie biznesowe
- Diagram przepływu danych
- Przeglądane co 6 miesięcy
- Konfiguracja zawsze zsynchronizowana

Zbudowanie bezpiecznej sieci



- Ruch przychodzący i wychodzący przez DMZ
- DMZ Proxy

Zbudowanie bezpiecznej sieci



- SSH nie może być „proxowane”
- DMZ Terminal

allegro

Zbudowanie bezpiecznej sieci

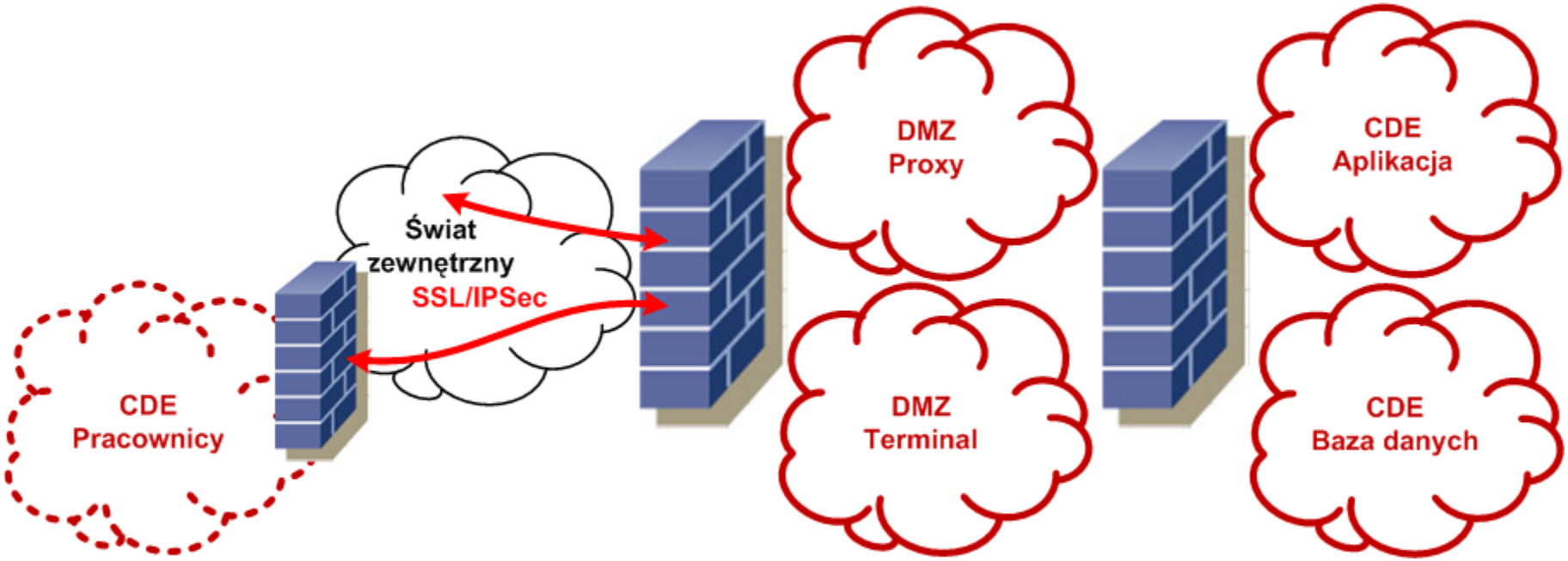
- Standardy konfiguracji urządzeń sieciowych, serwerów, systemów (NIST, CIS, ISO, SANS)
  - Do zarządzania bezpieczne protokoły SSH / HTTPS
  - Uruchom tylko usługi, skrypty, które są wymagane do poprawnej pracy urządzenia, systemu
  - Zmień wszystkie domyślne ustawienia
  - Minimalizuj ilość niezabezpieczonych protokołów, słabych algorytmów
  - Szyfruj hasła, klucze wykorzystywane przez protokoły
- Opis ról i odpowiedzialności
- Jedna funkcja per serwer/wirtualny serwer

allegro

Zabezpieczenie danych kartowych

- Bezpieczeństwo bazy danych CDE
  - Limituj ilość przechowywanych danych kartowych
  - Usuwaj systematycznie dane kartowe niewykorzystywane
  - Maskuj, obcinaj, używaj silna kryptografia dla PAN
  - Zaszyfruj hasło do bazy
- Osobna sieć dla bazy danych CDE

Zabezpieczenie danych kartowych



- Szyfrowanie połączeń SSL/IPSec
- WiFi jeśli tylko jest taka konieczność

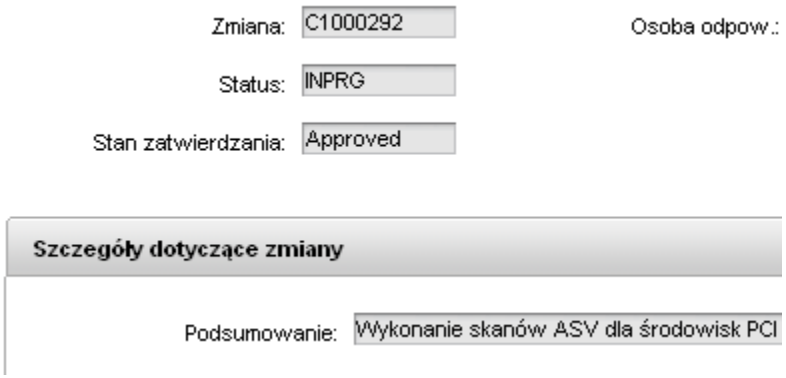
allegro

Program przeciwdziałania zagrożeniom

- Systemy wyposażone w aktualizowane na bieżąco oprogramowanie antywirusowe
- Systemy i urządzenia monitorowane pod kątem podatności na zagrożenia
- Wgrywanie łatek poddawana analizie pod kątem bezpieczeństwa

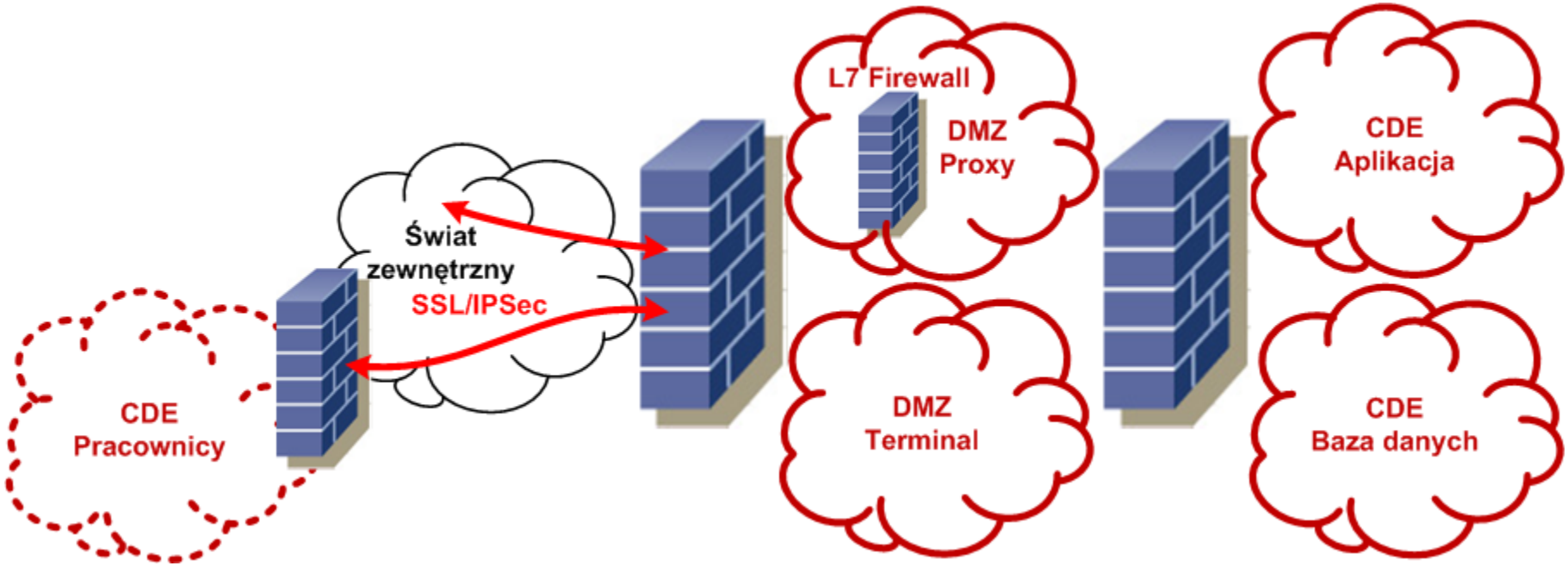
Program przeciwdziałania zagrożeniom

- Wszystkie zmiany dot. środowiska PCI kontrolowane



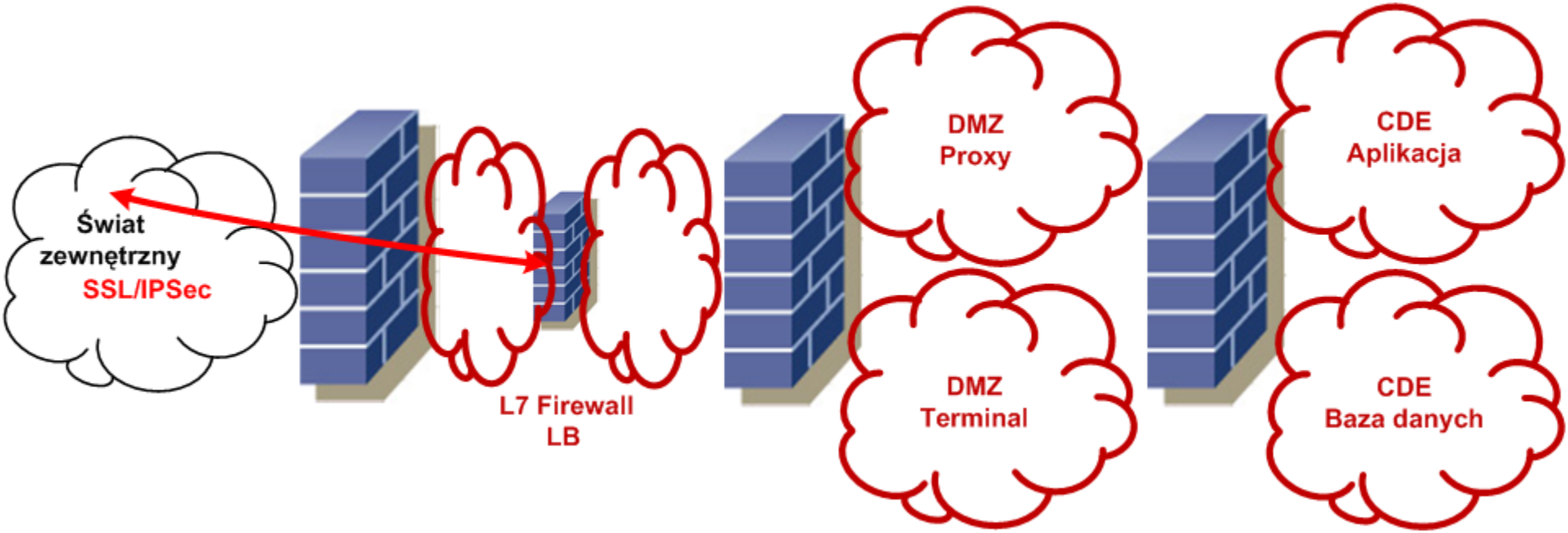
- Zakaz wstępu deweloperów na produkcje
- Oddzielne środowiska deweloperskie, testowe i produkcyjne

Program przeciwdziałania zagrożeniom



- Firewall L7
- IDS

Program przeciwdziałania zagrożeniom



allegro

Implementacja silnej kontroli dostępu

- Podwójna autoryzacja w dostępie do środowiska PCI
- Zabezpiecz dostęp do środowiska PCI tylko dla określonej grupy pracowników
- Przypisz tyle przywilejów ile jest potrzebnych danej grupie pracowników
- Każdy użytkownik ma przypisany unikalny ID
- Konta root/admin tylko w przypadku awarii
- Silna kryptografia przy transmisji haseł

allegro

Implementacja silnej kontroli dostępu

- Zmiana hasła co 90 dni (30 dni prawo obowiązujące w Polsce)
- Hasło co najmniej 7 znaków
- Nowe hasło nie może być takie samo jak poprzednie
- 6 nieudanych prób blokuje konto
- Blokada na co najmniej 30 minut

- Nieaktywne sesje terminowane po 15 minutach

allegro

Implementacja silnej kontroli dostępu

- Fizyczny dostęp do komponentów środowiska PCI
  - Autoryzowany dostęp do serwerowni
  - Monitorowanie dostępu i pobytu
  - Goście pod nadzorem
  - Ograniczanie dostępu fizycznego do urządzeń, serwerów
  - Przechowywanie logów monitoringu co najmniej 3 miesiące

allegro

Monitorowanie, testowanie sieci i systemów

- Monitorowanie
  - aktywności użytkowników
  - integralności plików systemowych i konfiguracyjnych
  - zdarzeń sieciowych i systemowych

splunk>

- Wiarygodne źródło czasu NTP
- Mechanizm śledzenia zmian w plikach logów
- Przechowywanie plików logów w bezpiecznym miejscu

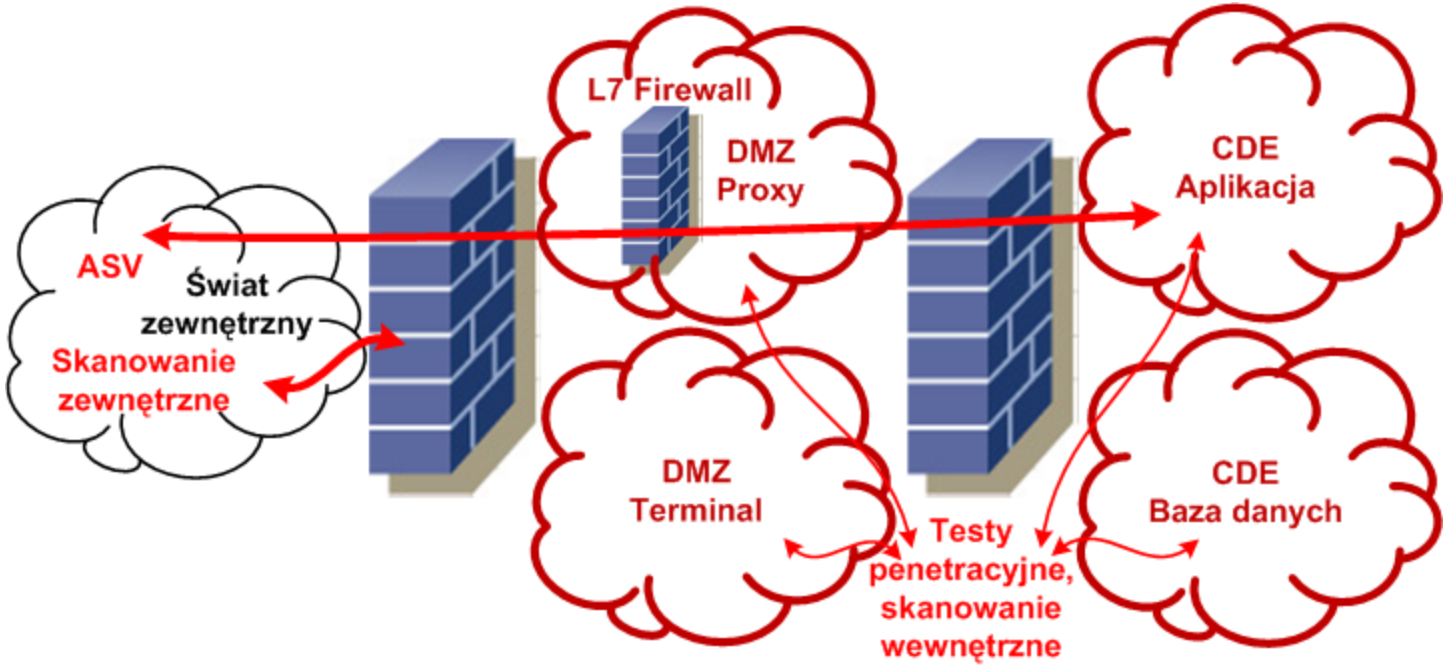
allegro

Monitorowanie, testowanie sieci i systemów

- IDS w celu monitorowania anomalii w środowisku PCI
- Przeglądy
  - logów IDS, serwerów autoryzacji przeglądane raz dziennie
  - zmian w krytycznych plikach co najmniej raz w tygodniu
- Sieć bezprzewodowa – monitorowanie niezautoryzowanych punktów dostępowych

allegro

Monitorowanie, testowanie sieci i systemów



- Testy PCI SSC Approved Security Vendor (ASV)
- Wewnętrzne/zewnętrzne skanowanie systemów i sieci

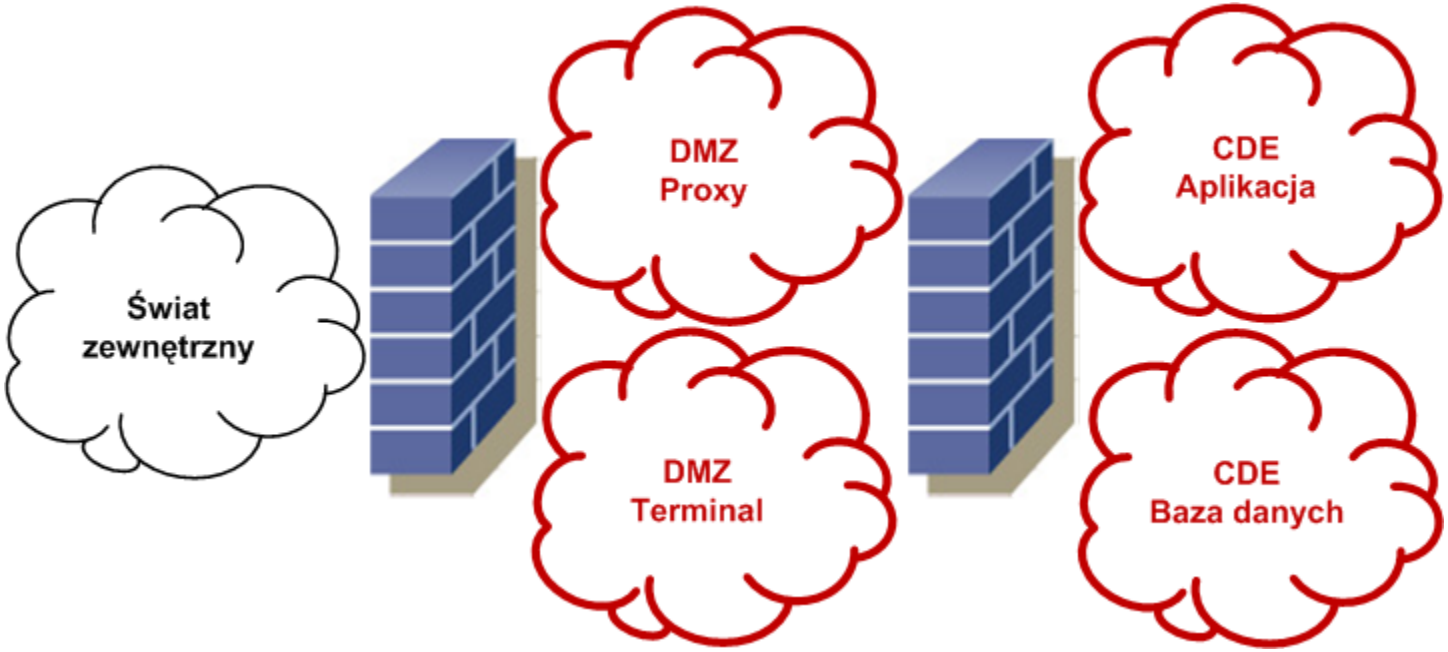
allegro

Utrzymanie polityki bezpieczeństwa informacji

- Rozpowszechnianie polityki bezpieczeństwa
  - informacje o wymaganiach PCI DSS
  - identyfikacja zagrożeń w firmie
- Program zwiększania świadomości bezpieczeństwa
- Polityki korzystania z krytycznych technologii
- Dzienne procedury operacyjne
- Plan odpowiedzi na incydenty

allegro

Komputery pracowników



- Terminal graficzny w DMZ Terminal

allegro

Metody kompensacyjne

- Kiedy nie można spełnić danego wymagania PCI
- Użyj innych metody rygorystycznych zgodnych z wymaganiami PCI
- Przykłady :
  - Brak szyfrowania kluczy
  - Hasła przesyłane jawnym tekstem
- Muszą zostać zatwierdzone przez audytora
- Procedury

allegro

Problemy

- Długi czas związany ze znalezieniem ostatecznego rozwiązania
- Nauczenie ludzi, że mamy PCI
- Brak świadomości w kwestii bezpieczeństwa
- Utrzymanie środowiska
- Utrzymanie certyfikacji

allegro

Korzyści

- Efektywne bezpieczeństwo
- Wdrożenie mechanizmów bezpieczeństwa w serwerowni
- Zwiększenie świadomości dot. bezpieczeństwa
- Prowadzenie projektów angażujących wiele osób z różnych działów

allegro

Pytania ?

- PCI Security Standards Council
  https://www.pcisecuritystandards.org

- Specyfikacja PCI DSS v2.0
  https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf