Tivoli Day 2009

IBM

15.10.2009 r. - Warszawa

PCI DSS

Nowe wyzwanie dla sektora finansów i dystrybucji

Robert Kępczyński
robert.kepczynski@pl.ibm.com

Agenda

- Krótkie omówienie PCI DSS
- Rola organizacji kart płatniczych i PCI Council
- Przestępstwa bazujące na danych kartowych
- Gdzie mogą wyciekać dane w systemie płatności kartowych?
- Metody weryfikacji zgodności z PCI DSS
- Obowiązki weryfikacyjne dla sprzedawców i dostawców usług
- Scenariusz wdrożenia PCI DSS wg Visa AIS
- ISS PCI Portal
- IBM ISS jako certyfikowany dostawca usług związanych z PCI

Przed 2004r.

Cardholder Information Security Program (CISP)

Site Data Protection Program (SDP)

Jak to wszystko razem spełnić?

Discover Information Security Compliance (DISC)

Data Security Standard (DSS)

Co to jest PCI DSS?

- Payment Card Industry Data Security Standard (PCI DSS) jest standardem bezpieczeństwa informacji dla kart płatniczych stworzonym przez Visa, Mastercard, American Express, Discover i JCB

- PCI DSS jest standardem pozarządowym dotyczącym wszystkich podmiotów gospodarczych, które przetwarzają, transmitują lub przechowują dane kartowe (imię i nazwisko, numer karty, data ważności, kod serwisu oraz zapis na pasku magnetycznym/chipie)

- Nadzór nad wdrożeniem standardu sprawują organizacje kart płatniczych

- Niedostosowanie się do wymogów PCI DSS grozi poważnymi konsekwencjami biznesowymi lub finansowymi, aż do wykluczenia z systemu kart płatniczych

Szczegółowe wymogi PCI DSS

Build and Maintain a Secure Network
Requirement 1: Install and maintain a firewall configuration to protect cardholder data
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data
Requirement 3: Protect stored cardholder data
Requirement 4: Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program
Requirement 5: Use and regularly update anti-virus software
Requirement 6: Develop and maintain secure systems and applications
Implement Strong Access Control Measures
Requirement 7: Restrict access to cardholder data by business need-to-know
Requirement 8: Assign a unique ID to each person with computer access
Requirement 9: Restrict physical access to cardholder data
Regularly Monitor and Test Networks
Requirement 10: Track and monitor all access to network resources and cardholder data
Requirement 11: Regularly test security systems and processes
Maintain an Information Security Policy
Requirement 12: Maintain a policy that addresses information security

Przykład konkretnego wymogu PCI DSS

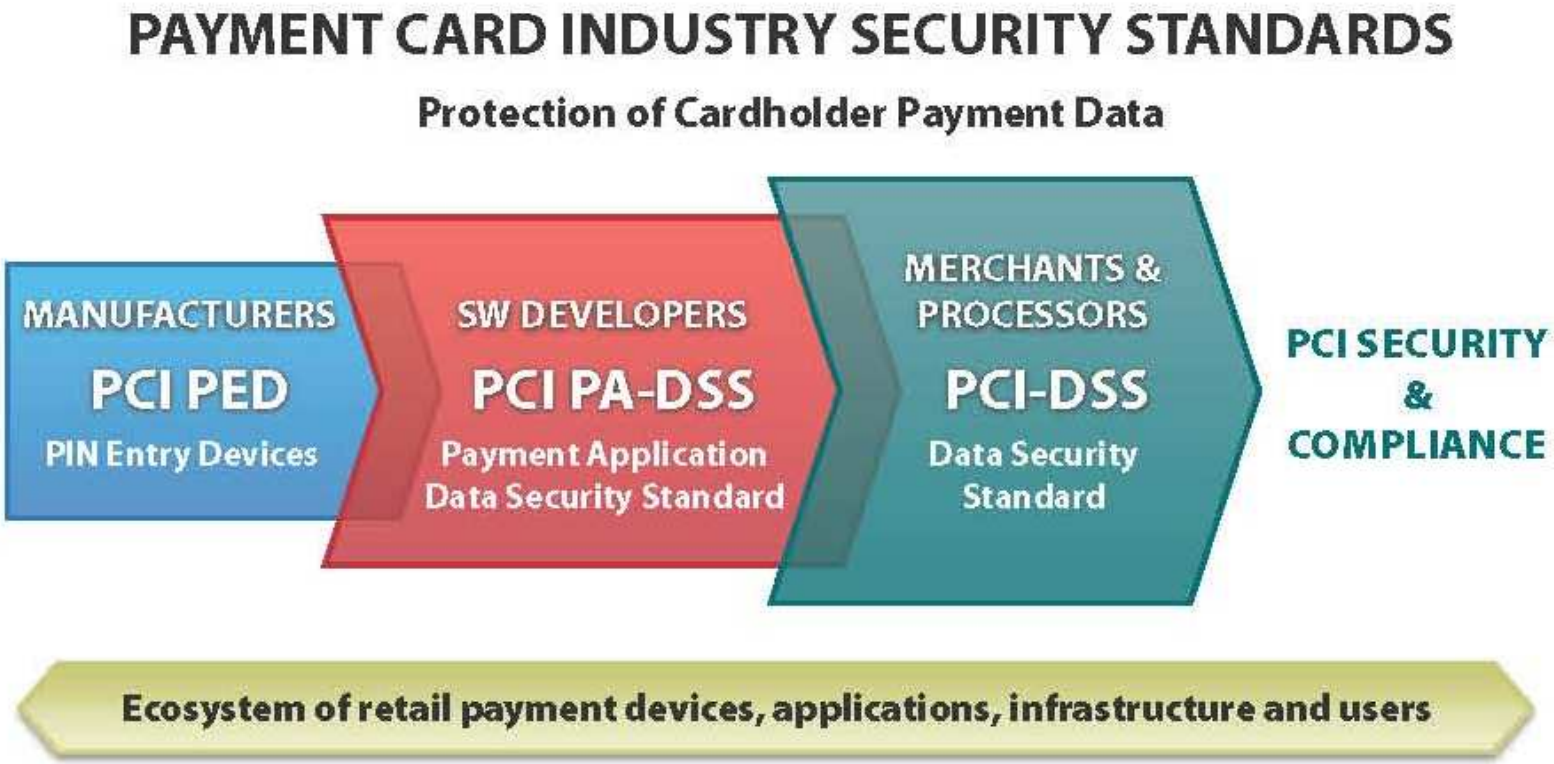
2.2. Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.

- 2.2.1 Implement only one primary function per server.
- 2.2.2 Disable all unnecessary and iinsecure services and protocols (services and protocols not directly needed to perform the device's specified function).
- 2.2.3 Configure system security parameters to prevent misuse.
- 2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.

Co to jest PCI Council?

- PCI Security Standards Council (PCI Council) została powołana w celu zarządzania standardami bezpieczeństwa kart płatniczych, w tym PCI DSS.
- PCI Council certyfikuje firmy i audytorów (nazywanych QSA) wykonujących usługi związane z weryfikacją zgodności z PCI DSS.
- PCI Council określa sposób weryfikacji wdrożenia standardu przez tworzenie narzędzi do weryfikacji zgodności.

Inne standardy zarządzane przez PCI Council



Role w systemie kart płatniczych i obowiązki wobec PCI DSS

Sprzedawca i właściciel karty

Acquirer
(centrum autoryzacyjno-rozliczeniowe)

Sieci firm kartowych

Service provider
(dostawca usług)

Issuer
(bank wydający karty)

Jak dane kartowe i dane o ich właścicielach są wykorzystywane w głównych rodzajach oszustw?

1. Klonowanie karty. Klonowanie może dotyczyć całej karty lub tylko paska z zapisem magnetycznym

2. Użycie ukradzionych danych kartowych do dokonania transakcji Card-Not-Present

3. Dokonanie transakcji kartą zgubioną lub ukradzioną przez inną osobę niż jej właściciel

4. Kradzież tożsamości właściciela karty. Dane właściciela mogą być użyte do otworzenia rachunku bankowego z kartą płatniczą, zmiany adresu właściciela karty w istniejącym rachunku, etc.

Przewidywania Interpolu i Europolu

Skala i powszechność oszustw finansowych za pomocą komputerów, do których zaliczają się oszustwa kartowe, w ciągu trzech lat będą większe niż nielegalny handel narkotykami.

Przewiduje się, że najbardziej popularnymi sposobami dokonywania oszustw finansowych będą:

- Socjotechnika (social engineering)
- Phishing
- Wykorzystywanie słabości w aplikacjach płatniczych

– *Źródło: PCI Town Meeting Brussels 22 October 2008 – Europol and Interpol, Peter Zinn Netherlands Police Agency*

Gdzie mogą wyciekać dane w systemie płatności kartowych?

Sprzedawca i właściciel karty

Acquirer
(centrum autoryzacyjno-rozliczeniowe)

Sieci firm kartowych

Service provider
(dostawca usług)

Issuer

Obowiązki weryfikacyjne

Według PCI DSS każdy podmiot gospodarczy, który przetwarza, transmituje lub przechowuje dane kartowe musi być zgodny z PCI DSS.

Obowiązkowej weryfikacji zgodności podlegają:

1. Sprzedawcy
2. Dostawcy usług
3. Centra autoryzacyjno-rozliczeniowe (acquirer).

W systemie Visa i Mastercard proces dochodzenia do zgodności nadzorują agenci autoryzacyjno-rozliczeniowi

Metody weryfikacji zgodności z PCI DSS

1. **Self-Assessment Questionnaire** (SAQ). Ankieta zawiera pytania dotyczące stanu wdrożenia PCI DSS i jest wypełniana przez przedstawiciela przedsiębiorstwa raz w roku.

2. **On-site Audit**. Audyt wdrożenia PCI DSS przeprowadza się raz w roku. W przypadku dostawcy usług audyt musi wykonać certyfikowany audytor (PCI Qualified Security Assessor).

3. **Vulnerability Network Scan**. Skanowanie sieci na podatności przeprowadza się raz na kwartał. Skanowanie musi być wykonane przez usługodawcę zatwierdzonego przez PCI Council (Approved Scanning Vendor), np. IBM ISS.

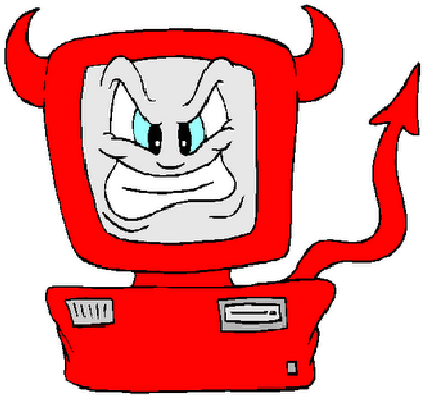
Typ kwestionariusza SAQ określa podzbiór obowiązujących wymogów PCI DSS

Rodzaj kwestionariusza zależy od sposobu przetwarzania, przesyłania i przechowywania danych kartowych (cytat z oryginalnego tekstu):

1. Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. This would never apply to face-to-face merchants. (typ A, 11 pytań)
2. Imprint-only merchants with no electronic cardholder data storage (typ B, 21 pytań)
3. Stand-alone terminal merchants, no electronic cardholder data storage (typ B, 21 pytań)
4. Merchants with POS systems connected to the Internet, no electronic cardholder data storage (typ C, 38 pytań)
5. All other merchants (not included in Types 1-4 above) and all service providers defined by a payment brand as eligible to complete an SAQ (typ D, 226 pytań)

Kogo dotyczy Vulnerability Network Scan?

- Vulnerability Network Scan dotyczy wszystkich podmiotów, których sieć wewnętrzna jest dołączona do Internetu i ma styk z podsiecią z danymi kartowymi
- Skanowane są wszystkie urządzenia i komputery z adresami IP dostępnymi od strony Internetu
- Zakres skanowania można ograniczyć przez segmentację fizyczną lub logiczną
- Aby wykonać on-site audyt musimy mieć jeden skan bez wykrytych podatności



Kryteria przypisywania poziomów obowiązkowej weryfikacji dla sprzedawców VISA

Kryteria dla poziomu 1:

- minimum 6.000.000 transakcji kartowych w ciąg roku
- każda firma, w której zdarzył się incydent bezpieczeństwa naruszający poufność danych
- każda firma bezpośrednio wskazana przez VISA

Kryteria dla poziomu 2:

- przetwarza rocznie od 1.000.000 do 6.000.000 transakcji

Kryteria dla poziomu 3:

- przetwarza rocznie od 20.000 do 1.000.000 transakcji dokonywanych przez kanał internetowy (e-commerce)

Kryteria dla poziomu 4:

- poniżej 20.000 transakcji e-commerce lub poniżej 1.000.000 innych transakcji rocznie

Poziomy weryfikacji zgodności dla sprzedawców

Poziom weryfikacji	Weryfikacja dla danego poziomu
Poziom 1	• Przeprowadzić raz w roku **On-site Audit przez QSA** • Co kwartał **Network Scan** przeprowadzony przez ASV
Poziom 2	• Przeprowadzić raz w roku **On-site Audit przez QSA** • Co kwartał **Network Scan** przeprowadzony przez ASV
Poziom 3	• Wypełnić raz w roku **Self-Assessment Questionnaire** • Co kwartał **Network Scan** przeprowadzony przez ASV
Poziom 4*	• Wypełnić raz w roku **Self-Assessment Questionnaire** • Co kwartał **Network Scan** przeprowadzony przez ASV

*) O wymogach weryfikacyjnych decyduje agent autoryzacyjno-rozliczeniowy

Poziomy weryfikacji zgodności dla sprzedawców

Poziom weryfikacji	Weryfikacja dla danego poziomu
Poziom 1	• Przeprowadzić raz w roku **On-site Audit** • Co kwartał **Network Scan** przeprowadzony przez ASV
Poziom 2	• Wypełnić raz w roku **Self-Assessment Questionnaire** • Co kwartał **Network Scan** przeprowadzony przez ASV
Poziom 3	• Wypełnić raz w roku **Self-Assessment Questionnaire** • Co kwartał **Network Scan** przeprowadzony przez ASV
Poziom 4*	• Wypełnić raz w roku **Self-Assessment Questionnaire** • Co kwartał **Network Scan** przeprowadzony przez ASV

*) O wymogach weryfikacyjnych decyduje agent autoryzacyjno-rozliczeniowy

Poziomy weryfikacji zgodności dla dostawców usług

Poziom weryfikacji	Weryfikacja dla danego poziomu
Poziom 1	• Przeprowadzić raz w roku **On-site Audit przez QSA** • Co kwartał **Network Scan** przeprowadzony przez ASV
Poziom 2	• Wypełnić raz w roku **Self-Assessment Questionnaire** • Co kwartał **Network Scan** przeprowadzony przez ASV

Koszt wycieku danych kartowych i koszty wdrożenia PCI DSS według szacunku branży (w USA)

- Według fundatorów PCI koszt wycieku danych jest od 60 do 200 razy większy niż koszt wdrożenia PCI DSS
- Przeciętny koszt wdrożenia PC DSS wynosi 3 USD na kartę w systemie
- Przeciętny koszt wycieku danych wynosi 300 USD na kartę w systemie
- Przykład: Firma ma 2000 kart w swoim systemie i wykradziono dane dotyczące 50 kart. Całkowity koszt związany z wyciekiem danych wynosi 600.000 USD

Visa AIS Program

Visa stworzyła program Account Information Security (AIS) w celu wdrożenia PCI DSS u wszystkich partnerów biznesowych Visa w Europie.

Według **Visa International Operating Regulations** agent autoryzacyjno-rozliczeniowy (acquirer) jest odpowiedzialny za doprowadzenie do zgodności z PCI DSS wszystkich swoich sprzedawców.

Według Visa International Operating Regulations ostateczna odpowiedzialność za uzyskanie zgodności z PCI DSS przez dostawców usług (także w przypadku kiedy tylko sprzedawca współpracuje z dostawcą usług) także spoczywa na agentach autoryzacyjno-rozliczeniowych.

Scenariusz wdrożenia PCI DSS według AIS

Rola agenta autoryzacyjno-rozliczeniowego w programie AIS w przypadku sprzedawców:

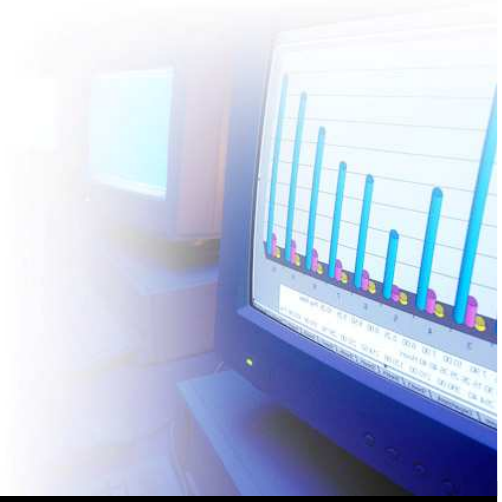
- Zapoznanie sprzedawców z PCI DSS i jego wymogami
- Pomoc w wyodrębnianiu środowiska teleinformatycznego, w którym występują dane kartowe
- Współuczestniczenie w procesie szacowania stanu zgodności z wymogami PCI DSS
- Przypisanie poziomu obowiązkowej weryfikacji
- Uzgodnienie harmonogramu działań naprawczych
- Uzyskanie certyfikatu zgodności z PCI DSS

ISS PCI Portal

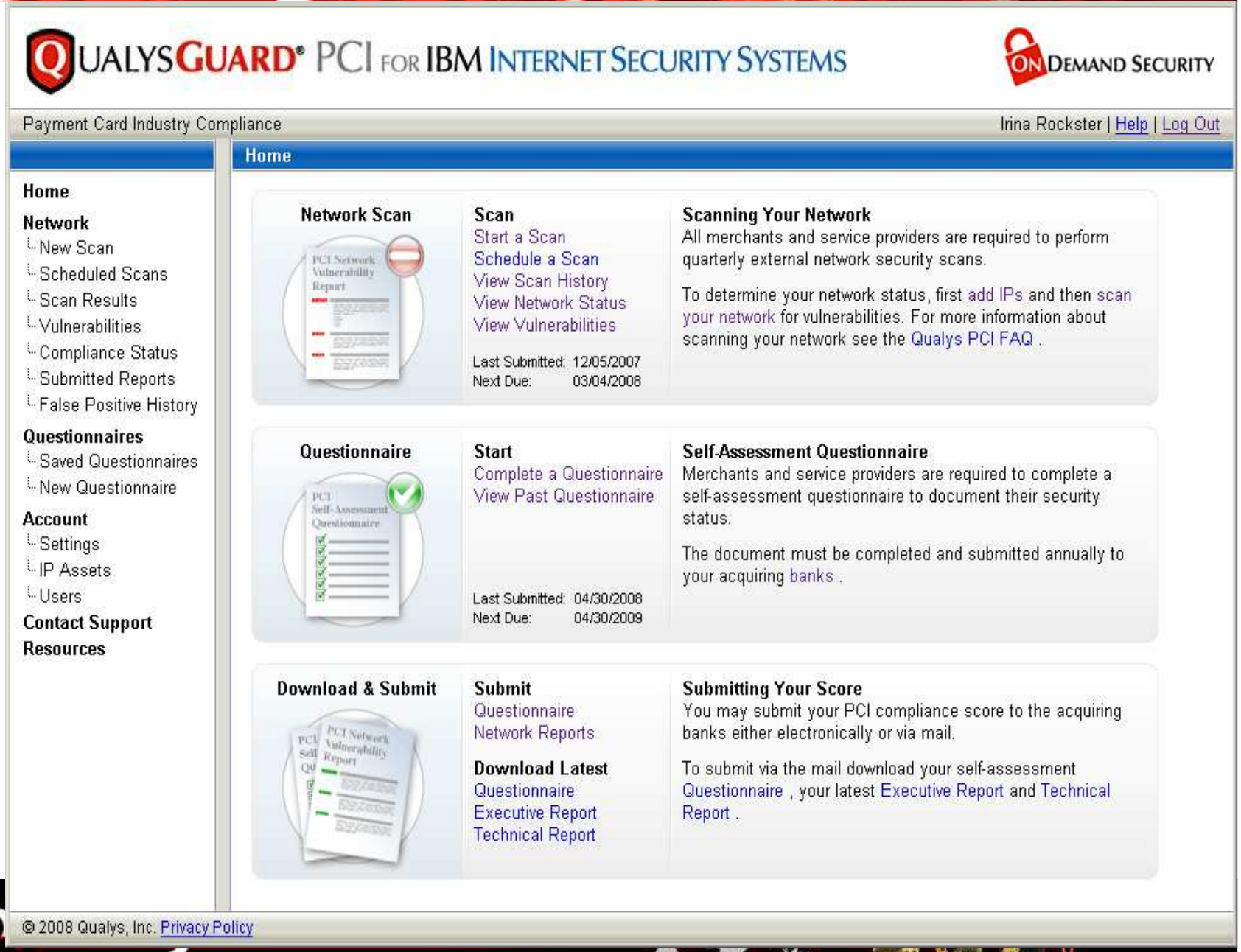
ISS PCI Portal do wypełniania obowiązków weryfikacyjnych

ISS PCI Portal to doskonałe narzędzie do wypełniania obowiązków weryfikacyjnych.

- Ułatwia wypełnić SAQ i umożliwia zadawanie pytań do specjalistów PCI DSS
- Umożliwia samodzielne wykonywanie Network Scan, sprawdzanie czy zostały usunięte podatności oraz wyłączanie podatności błędnie wykrytych
- Pomaga przygotować dokumentację wymaganą w przypadku weryfikacji zgodności z PCI DSS za pomocą SAQ i Network Scan



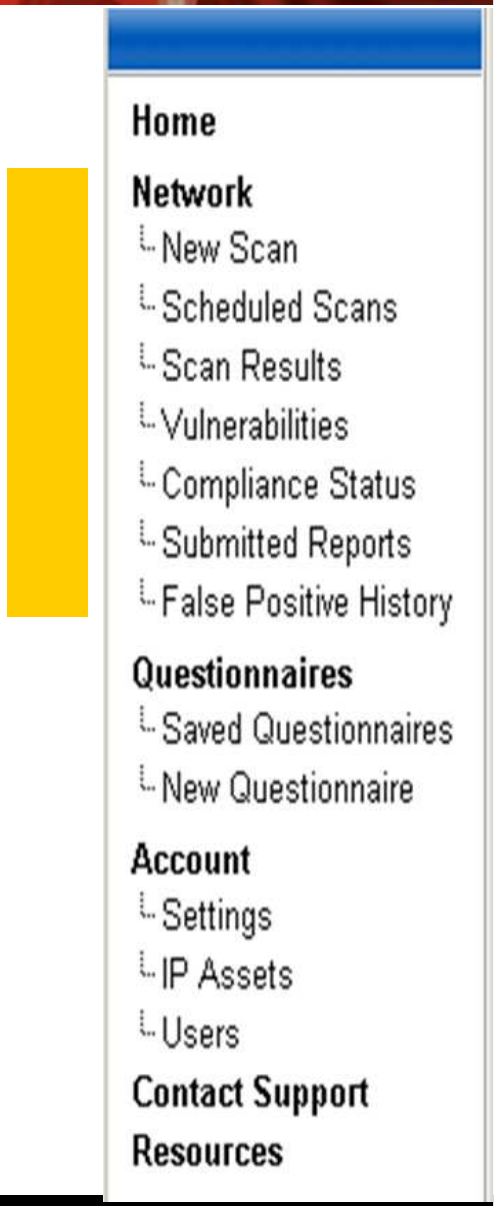
ISS PCI Portal



Wykrywanie i usuwanie podatności

Proces wykrywania i usuwania podatności:

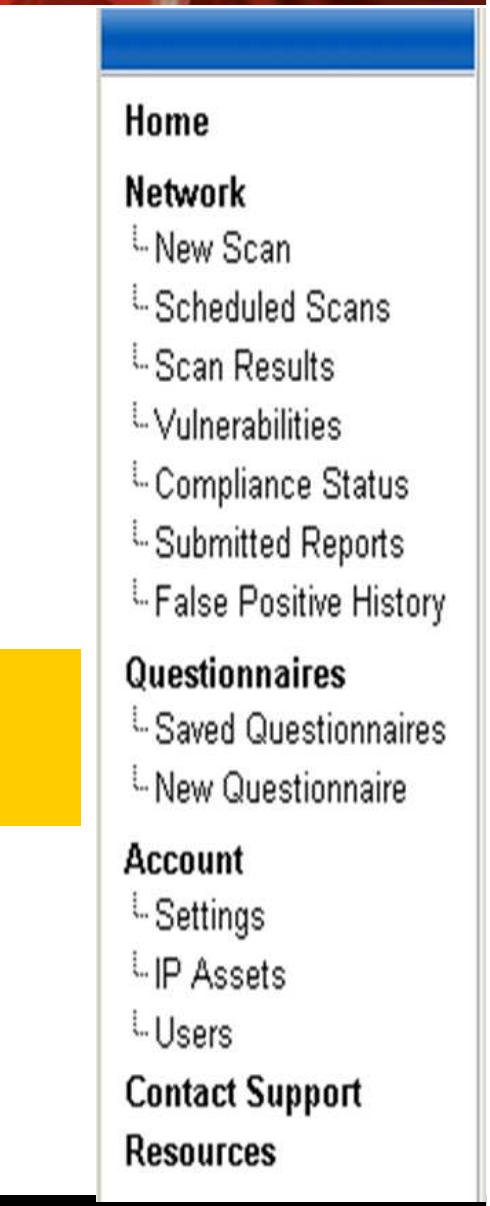
1. Rozpocznij Network Scan
2. Zapoznaj się ze znalezionymi podatnościami
3. Wyeliminuj podatności
4. (Opcjonalnie) Wyślij prośbę w celu uznania podatności za false positive



Wypełnianie SAQ na ISS PCI Portalu

Proces wypełniania PCI Self-Assessment Questionnaire:

1. Wybierz właściwy typ kwestionariusza SAQ
2. Odpowiedz na wszystkie pytania
3. Wyślij wypełniony SAQ do ISS PCI Portal
4. Potwierdź zakres zgodności z PCI DSS
   - Zadeklaruj daty zakończenia prac prowadzących do uzyskania pełnej zgodności z PCI DDS
5. Wyślij wypełniony SAQ z potwierdzonym zakresem zgodności do agenta autoryzacyjno-rozliczeniowego



ISS PCI Portal jako narzędzie monitorowania statusu zgodności sprzedawców i dostawców usług

Agent autoryzacyjno-rozliczeniowy poprzez ISS PCI Portal może na bieżąco śledzić status zgodności z PCI DSS swoich sprzedawców i dostawców usług

Specjalna funkcjonalność Portala dostępna tylko dla agenta autoryzacyjno-rozliczeniowego zapewnia dostęp do:

- Wypełnionych SAQ
- Historii raportów ze skanowania podatności
- Informacji o postępach w usuwaniu podatności wykrytych w trakcie Network Scan

Dziękuje za uwagę