PCI-DSS

Wprowadzenie

Robert Jaroszuk

Zimowisko TLUG 2011

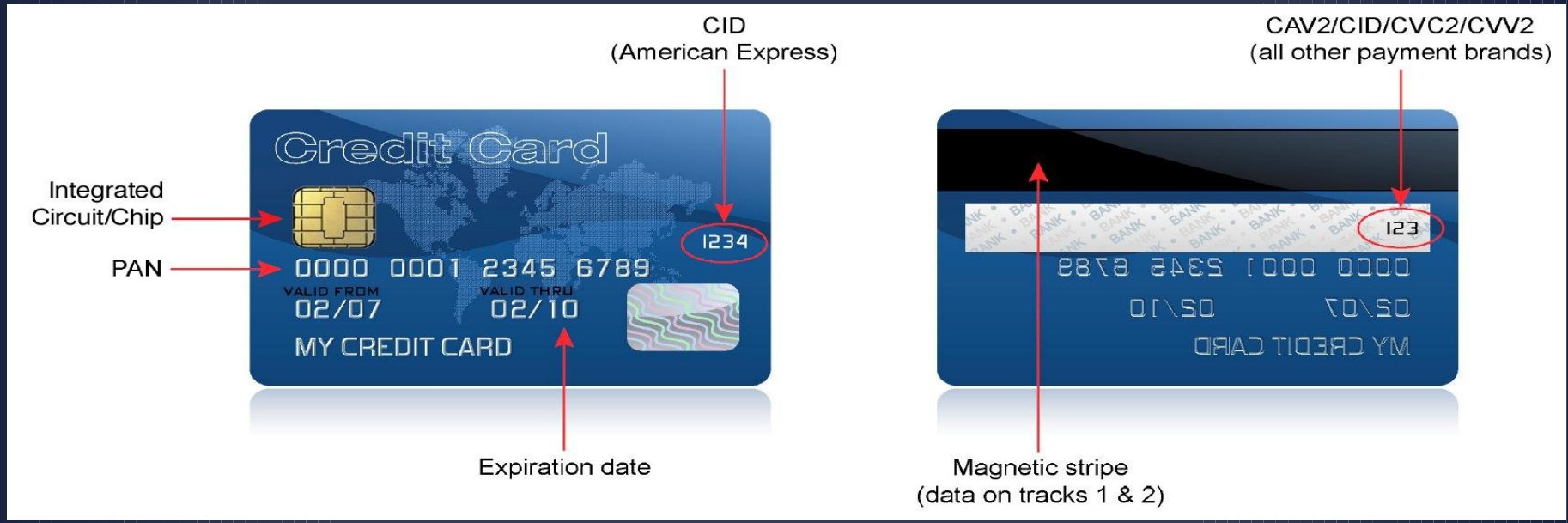
Payment Card Industry Security Standards Council

- Założony przez: American Express, Discover Financial Services, JCB International, MasterCard Worldwide, oraz Visa Inc.
- Poszczególne marki są odpowiedzialne za egzekwowanie zgodności ze standardem oraz ustalenie wysokości i zasad nakładania kar za brak zgodności.
W naszym przypadku są to VISA oraz MasterCard.

Cel

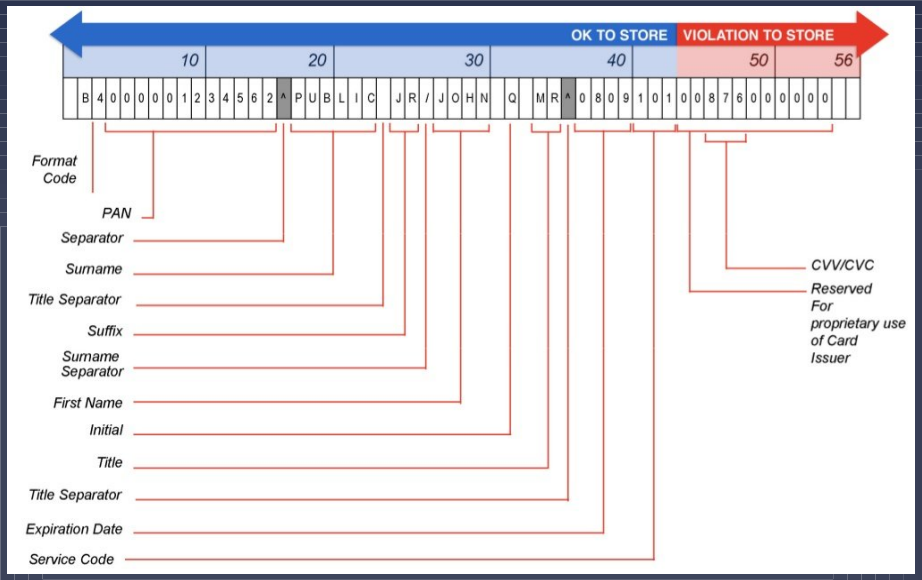
- Dostarczenie mocnych i obszernych standardów oraz materiałów pomocniczych, by wzmocnić bezpieczeństwo systemów przetwarzających CHD.
- Dane objęte standardami:
  - PAN Primary Account Number (nr karty) – 16-19 cyfrowy numer karty
  - Cardholder Name – Imię i nazwisko właściciela karty
  - Service Code – 3 cyfry
  - Expiration Date – data ważności karty
  - Full Magnetic Stripe Data – dane zapisane na pasku magnetycznym
  - CAV2/CVC2/CVV2/CID
  - PIN/PIN Block

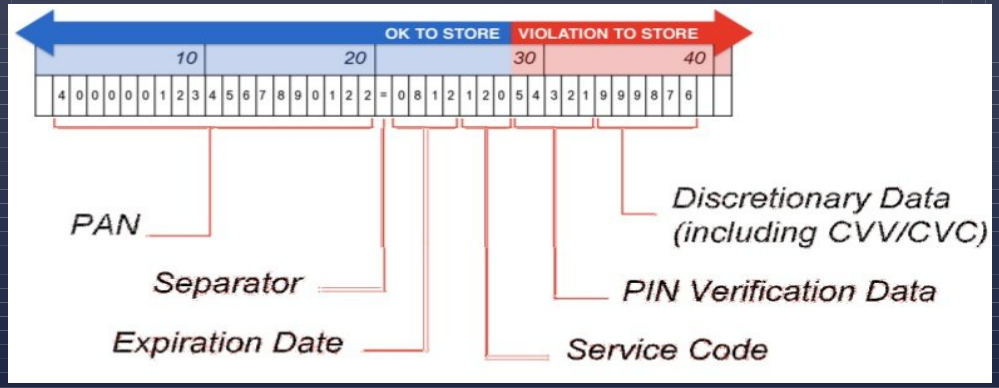
CHD



(PCI-DSS – Cardholder Data)

CHD





(PCI-DSS – Cardholder Data)

CHD

		Data Element	Storage Permitted	Render Stored Account Data Unreadable per Requirement 3.4
Account Data	Cardholder Data	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data [1]	Full Magnetic Stripe Data [2]	No	Cannot store per Requirement 3.2
		CAV2/CVC2/CVV2/CID	No	Cannot store per Requirement 3.2
		PIN/PIN Block	No	Cannot store per Requirement 3.2

(PCI-DSS – Cardholder Data)

Dlaczego stworzono PCI-DSS?

- Rozpowszechniony handel danymi kartowymi pochodzącymi z kradzieży:
  - 70% incydentów wywołali zewnętrzni intruzi
  - 48% spowodowali ludzie pracujący w danym systemie
  - 11% spowodowali partnerzy biznesowi
  - 27% przypadków jest mieszanych
  - 97% wszystkich danych zostało ujawnionych przez zewnętrzne źródła

(źródło – Verizon Business 2010 Data Breach Investigation Report)

Sposoby wykradania danych

- 40% ataki z zewnątrz
- 38% użycie malware
- 48% nadużycie uprawnień
- 28% użycie socjotechniki
- 15% ataki fizyczne
- 85% incydentów popełnionych przez grupy zorganizowane

(źródło – Verizon Business 2010 Data Breach Investigation Report)

Przykłady

- Ceny kradzionych danych:
  - Visa Classic – 35$/szt.
  - Visa Gold – 80$/szt.
  - Visa Platinum – 100$/szt.

File Edit View History Bookmarks Tools Help

sell cc & sell cvv high quality ha...

Join Date: Nov 2010
Last Online: Today @ 10:03 AM
Posts: 20
Thanks: 0
Thanked 0 Times in 0 Posts

.VN

hello everyone coming and going to work with me.
cc I'm selling cheap, and sell boat engines, hacking tools store, xfer tool,
I look forward to working with those who need to buy tools and hack cc. and I can also help you lead a lot of money. and I can only work with decent people who work and fr
sell bank login,paypal, ship laptop + iphone and i can transfer WU with error WU Bug .
My rule and i can't break up my rule, hope u read right before cotact me
- dont trust dont talk more
- send money first

- no test free
- u can buy 1test,if good u can buy more
- if not good,i will change for u
- if who dont want myrule , plz dont contact me
- i accept LR or WU but i only accept WU>50
Thanks read my thread . Hope u can read right before contact me
Additionally I can help you purchase everything you need. such as buying tickets online. payment of electricity and water debts so forth.
I look forward to cooperating with you and I promise you and I will all benefit in this.
when necessary, to contact me yhaoo: hackpro.6868
email hackpro.6868 @yah oo.com.vn
List cc i have and frice i have :
Us (vis,mas) = 2$/1cvv if buy more than 50 cc 1,5$/1cvv
Us (dis,amex) = 4$/1cvv if buy more than 50 cc 3,5$/1cvv
Uk (vis,mas) = 5$/1cvv if buy more than 50 cc 4,5$/1cvv
Uk (amex,dis) = 7$/1cvv if buy more than 50 cc 6$/1cvv
Au = 10$/1cvv if buy more than 50 cc 9$/1cvv
Ca = 12$/1cvv if buy more than 50 cc 10$/1cvv
+ Switzerland (VE) = 15.00 $
+ belgium = 12$ per 1
+ Itali = 15$/1cvv if buy more than 50 cc 23$/1cvv
+ Spain = 15$/1cvv if buy more than 50 cc 18$/1cvv
+ Denmark = 20$/1cvv if buy more than 50 cc 23$/1cvv
+ Sweden = 15$/1cvv if buy more than 50 cc 18$/1cvv
+ Germany (GE) = 15.00 $; Germany with dob : 30$/1
+ Middle East = 15$/1cvv if buy more than 50 cc 13$/1cvv
+ Asia = 15$/1cvv if buy more than 50 cc 13$/1cvv
US with bin : 4$
US fullz : 20$
Uk with bin = 15$
Uk with dob = 20$
Uk with bin + dob = 30$
Us Full = 20$/1cvv
Uk full = 30$/1cvv
Eu full = 40$/1cvv
Wu transfer :
1000$=100$
2500$=200$
7000$=500$
With Paypal Veritified :

Hello guest! It looks like you aren't a member. Get now full access and register for free!

Done

Kto jest kim?

- Visa i MasterCard zrzeszają organizacje, które mogą być Issuerami lub Acquirerami (albo zarówno tym jak i tym)
- Acquirerzy są członkami VISA/MC, którzy świadczą usługi dla Merchantów
- Issuerzy są członkami VISA/MC, którzy wydają karty dla Cardholderów.
- Merchantci to te organizacje, które „akceptują” transakcje kartowe.
- Cardholderzy to... no właśnie. To my :)
- Service Providerzy to organizacje świadczące jakikolwiek rodzaj usług, będący elementem procesu przetwarzania danych kartowych (np. przechowywanie, przetwarzanie, transport informacji kartowych)

Propagowanie

Organizacje płatnicze

Issuers/Acquirers

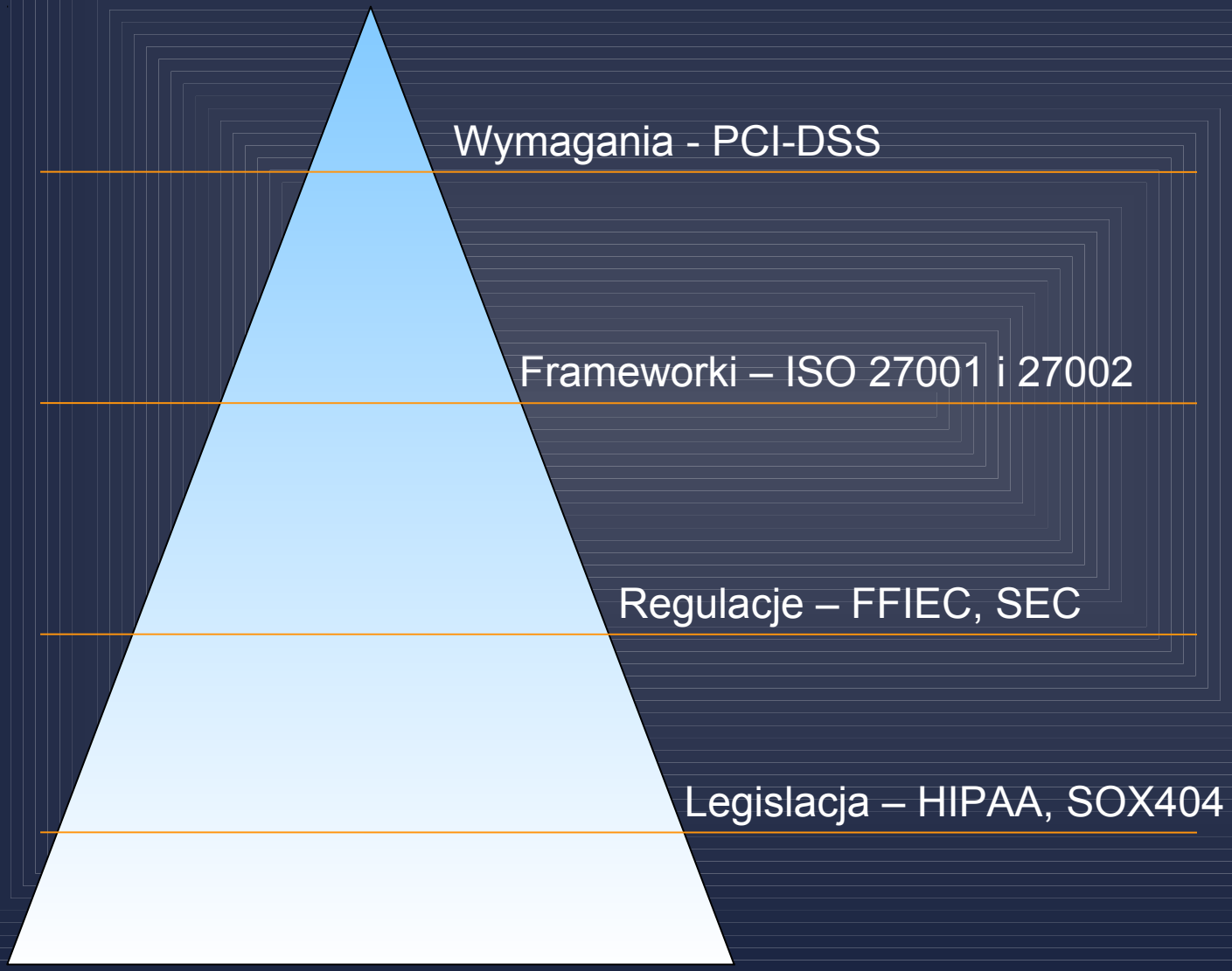
Merchants

Service Providers

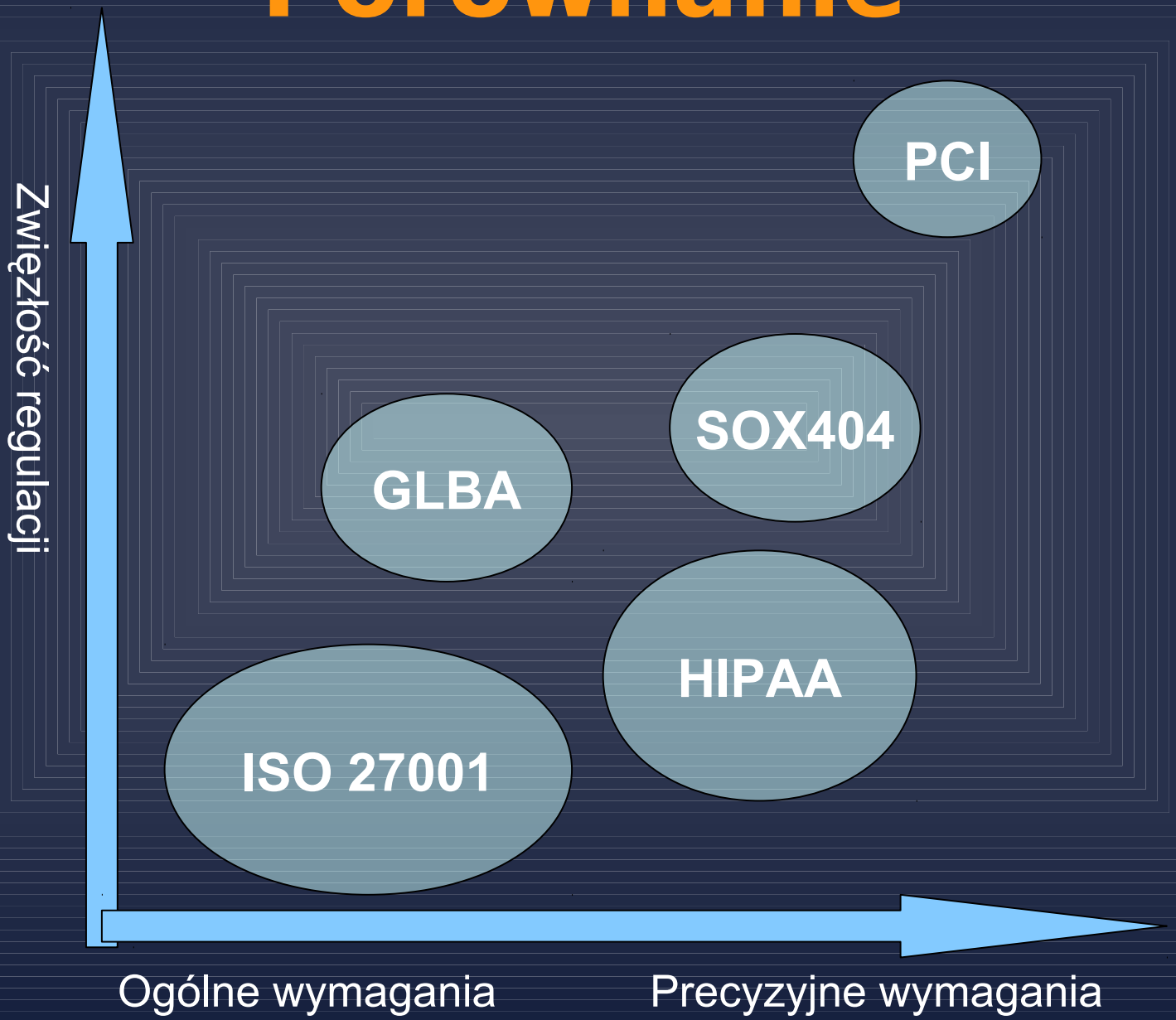
Data Storage Entities

3rd Party Processors

Kontekst PCI DSS



Porównanie


Zwięzłość regulacji
PCI
SOX404
GLBA
HIPAA
ISO 27001
Ogólne wymagania
Precyzyjne wymagania

Wymagania vs Frameworki

- ISO 27002:2005

  Appropriate, timely action should be taken in response to the identification of potential technical vulnerabilities. The following guadiance should be followed to establish an effective management process for technical vulnerabilities:

- c) **A timeline should be defined** to react to notifications of potentially relevant technical vulnerabilities;

Wymagania vs Frameworki

- ISO 27002:2005

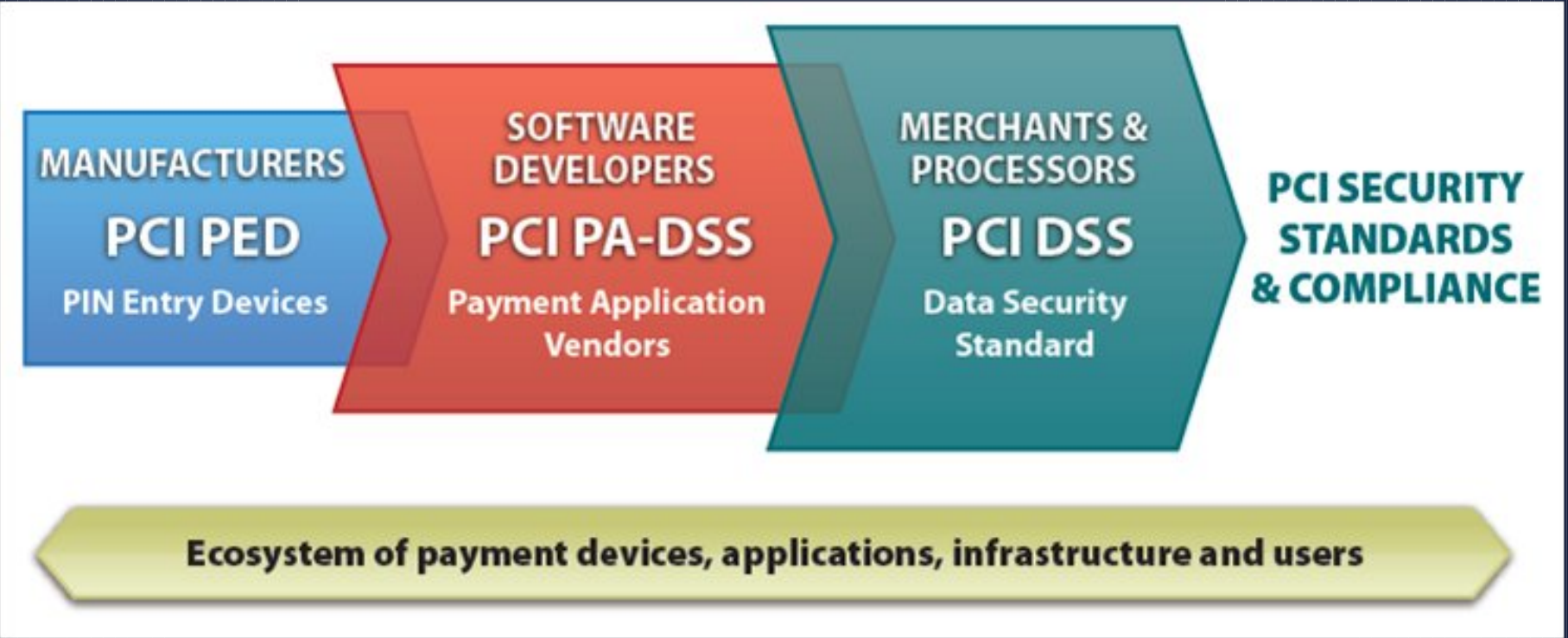
Appropriate, timely action should be taken in response to the identification of potential technical vulnerabilities. The following guadiance should be followed to establish an effective management process for technical vulnerabilities:

c) **A timeline should be defined** to react to notifications of potentially relevant technical vulnerabilities;

- PCI DSS 1.2.1

6.1. Ensure that all system components and software have the latest vendor-supplied security patches installed. **Install critical security patches within one month of release.**
Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing **less critical devices and systems within three months.**

Standardy PCI



(http://www.pcisecuritystandards.org)

PCI-DSS

„The primary account number is the defining factor in the applicability of PCI DSS requirements. PCI DSS requirements are applicable if a primary account number (PAN) is stored, processed, or transmitted. If PAN is not stored, processed or transmitted, PCI DSS requirements do not apply.”

– Payment Card Industry (PCI) Data Security Standard
Requirements and Security Assessment Procedures
Version 2.0, October 2010

PCI-DSS

Dotyczy **KAŻDEJ** organizacji, która przechowuje, przetwarza lub transmituje dane kartowe.

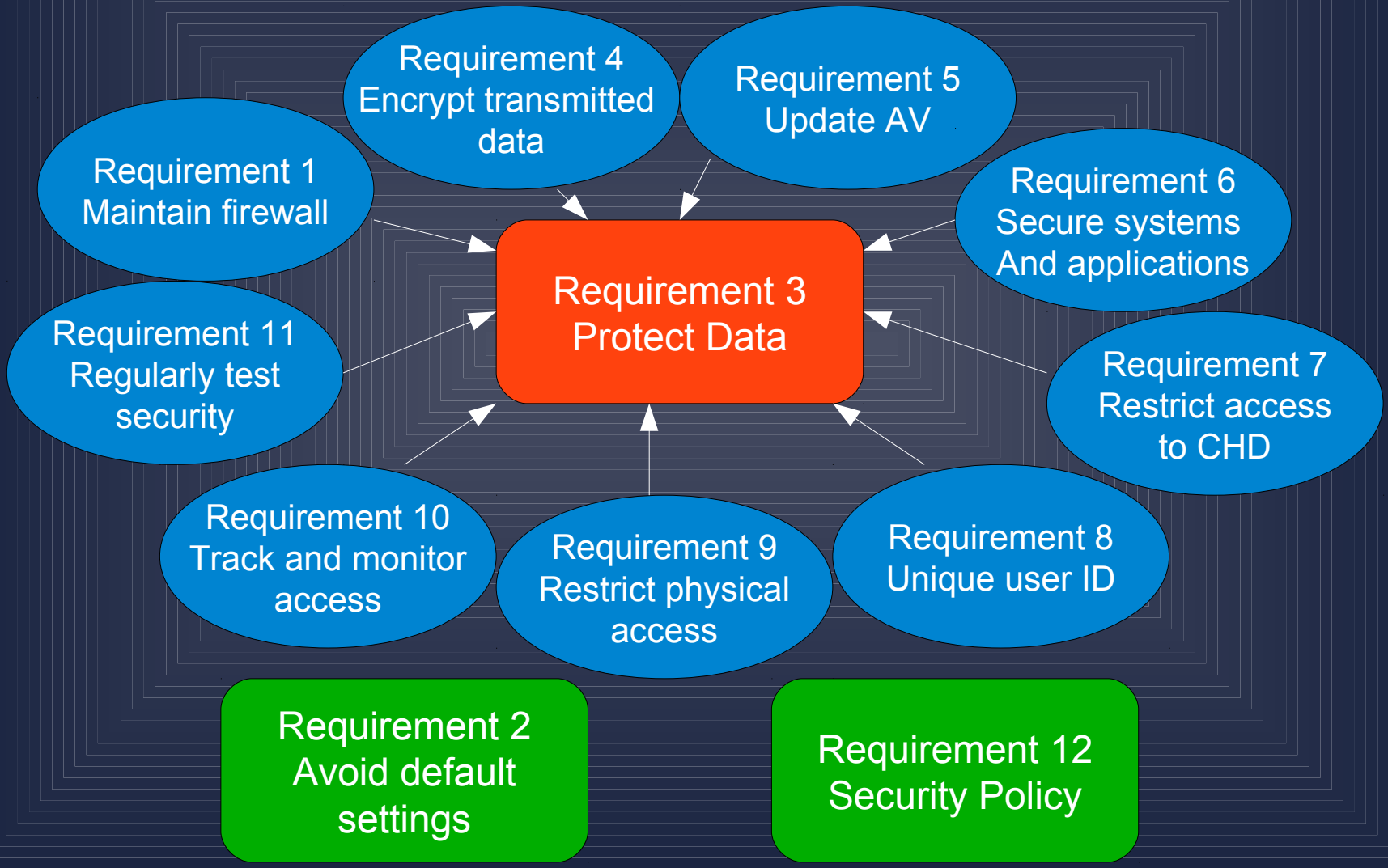
PCI-DSS obejmuje wszystkie komponenty bezpośrednio lub pośrednio związane ze środowiskiem danych kartowych.

Wymagania

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

https://www.pcisecuritystandards.org/

Wymagania


Requirement 4
Encrypt transmitted data
Requirement 5
Update AV
Requirement 1
Maintain firewall
Requirement 6
Secure systems
And applications
Requirement 3
Protect Data
Requirement 11
Regularly test security
Requirement 7
Restrict access to CHD
Requirement 10
Track and monitor access
Requirement 9
Restrict physical access
Requirement 8
Unique user ID
Requirement 2
Avoid default settings
Requirement 12
Security Policy

Wymagania - przykłady

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.
Sources of industry-accepted system hardening standards may include, but are not limited to:
- Center for Internet Security (CIS)
- International Organization for Standardization (ISO)
- SysAdmin Audit Network Security (SANS) Institute
- National Institute of Standards Technology (NIST)

2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)

Wymagania - przykłady

2.2.2 Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system.

2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.

Wymagania - przykłady

4.1 Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks.

Wymagania - przykłady

5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).

5.1.1 Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.

5.2 Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.

Wymagania - przykłady

6.2 Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities.

Notes:

- Risk rankings should be based on industry best practices. For example, criteria for ranking “High” risk vulnerabilities may include a CVSS base score of 4.0 or above, and/or a vendor-supplied patch classified by the vendor as “critical,” and/or a vulnerability affecting a critical system component.

- The ranking of vulnerabilities as defined in 6.2.a is considered a best practice until June 30, 2012, after which it becomes a requirement.

Wymagania - przykłady

8.1 Assign all users a unique ID before allowing them to access system components or cardholder data.

8.5 Ensure proper user identification and authentication management for non-consumer users and administrators on all system components as follows:
(...)
8.5.2 Verify user identity before performing password resets.
(…)
8.5.4 Immediately revoke access for any terminated users
(…)
8.5.5 Remove/disable inactive user accounts at least every 90 days.
(…)
8.5.14 Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.
(...)

Wymagania - przykłady

9.2 Develop procedures to easily distinguish between onsite personnel and visitors, especially in areas where cardholder data is accessible.

Wymagania - przykłady

10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.

10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).

Q/A ?

https://www.pcisecuritystandards.org/