SECURITY 2012

20. ročník konference o bezpečnosti v ICT

Řízení rizik podle PCI DSS Prioritized Approach

Jakub Morávek

Wincor Nixdorf

Obsah přednášky

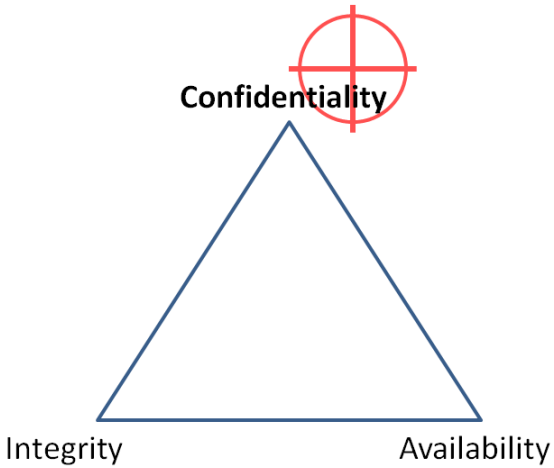
- Co je PCI DSS a jak řídí rizika?
- Jaké nástroje PCI DSS používá a nabízí?
- Jak můžeme PCI DSS využít i mimo platební systémy?

PCI DSS přesně vymezuje pravidla bezpečnosti pro specifické subjekty

- PCI DSS (**P**ayment **C**ard **I**ndustry **D**ata **S**ecurity **S**tandard) vydává PCI SSC (**S**tandard **S**ecurity **C**ounsil)
- PCI SSC založily karetní asociace Amex, Discover, JCB, MasterCard, Visa International
- Asociace specifikovaly požadavky na ochranu dat držitelů platebních karet
- Data držitelů platebních karet musí chránit každý, kdo je zpracovává, přenáší nebo ukládá

PCI DSS definuje specifický přístup k řízení rizik a ochraně přesně definovaných dat v rámci organizace

- Karetní asociace definují požadavky pro zabezpečení svých dat v prostředí jiných entit.
- Standard neřeší plánování kontinuity podnikání, plány obnovy, apod.
- Standard definuje, co všechno pokrývá a jak se vytváří scope
- Přístup zdola nahoru – od implementace firewallu k bezpečnostním politikám



Prioritizovaný přístup představuje účinný nástroj pro implementaci standardu PCI DSS

- Podrobný plán, který umožňuje eliminovat rizika podle priorit.
- Pragmatický přístup, který může pomoci rychle ochránit data.
- Podporuje finanční a provozní plánování.
- Poskytuje objektivní a měřitelné ukazatele postupu implementace.
- Umožňuje demonstrovat postup plnění souladu.
- Koncipován na základě poznatků z průniků, auditů a vyšetřování bezpečnostních incidentů.

Prioritizovaný přístup je rozdělen do 6 navazujících milníků, které zajistí implementaci PCI DSS

1. Odstraňte citlivá autentizační data, omezte výskyt a životnost ukládaných dat.
2. Zabezpečte, DMZ, interní a bezdrátové sítě.
3. Zabezpečte platební aplikace.
4. Sledujte a řiďte přístup k systémům.
5. Zabezpečte uložená data držitelů karet.
6. Dokončete zbývající požadavky, a ověřte, že všechna opatření jsou implementována.

Prioritizovaný přístup prochází neustálou kontrolou a zapracovává poznatky z účastníků platebního procesu (viz změny oproti verzi 1.2)

- Požadavek 9.1 přesunut z M5 do M2
  - Monitor physical access to systems in the CDE.
- Požadavek 10.5 přesunut z M6 do M4
  - Secure audit trails so they cannot be altered.
- Požadavek 11.1 přesunut z M6 do M4
  - Test for the presence of wireless access points.
- Požadavek 11.3 přesunut z M6 do M2
  - Perform penetration testing.
- Požadavek 12.1.2 přesunut z M6 do M1
  - Security policy includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment.
- Požadavek 12.5.3 přesunut z M6 do M4
  - Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.
- Požadavek 12.9 přesunut z M6 do M4
  - Implement an incident response plan. Be prepared to respond immediately to a system breach.

Pro účinnější implementaci všech kontrol vydává PCI SSC Informační dodatky, které se vztahují k implementaci bezpečnostních technologií

- Doporučení pro bezpečnou implementaci technologií
  - Virtualization Guidelines
  - Wireless guidelines
  - Protecting Telephone-based Payment Card Data
- Doporučení pro implementaci procesů a kontrol
  - Requirement 11.3 Penetration Testing

End–to-end šifrování a tokenizace umožní redukovat výskyt „citlivých“ dat

- Cíl
  - redukce množství systémů, které mohou ovlivnit bezpečnost chráněných dat
  - zachování úrovně zabezpečení chráněných dat
- Tokenizace
  - Nahrazení citlivých dat zástupnými údaji
- End-to-end šifrování
  - Data se šifrují ihned na vstupu
  - Data se dešifrují až když se musí zpracovávat

Shrnutí

- PCI DSS
- Prioritizovaný přístup
- Informační dodatky
- End-to-end šifrování, tokenizace

  - https://www.pcisecuritystandards.org

SECURITY 2012

20. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Jakub Morávek

Wincor Nixdorf

jakub.moravek@wincor-nixdorf.cz