PCI DSS: Standard zabezpečení plateb

PCI DSS je soubor požadavků vytvořený velkými karetními asociacemi (Visa, Mastercard, American Express, Discover a JCB). Nejedná se o zákon, ale o smluvní závazek – pokud chce obchodník přijímat platby kartou, musí tyto standardy splňovat.

1. 12 hlavních požadavků

Standard je rozdělen do šesti logických skupin, které obsahují 12 specifických požadavků:

Budování a údržba bezpečné sítě

```
1. Instalace a údržba [[it:sw:security_web|firewallu]] pro ochranu dat
držitelů karet.
2. Nepoužívat výchozí hesla od výrobců pro systémová hesla a další
bezpečnostní parametry.
```

Ochrana dat držitelů karet

```
3. Ochrana uložených dat (šifrování dat na discích).
4. Šifrování přenosu dat držitelů karet přes otevřené, veřejné sítě.
```

Program správy zranitelností

```
5. Používání a pravidelná aktualizace antivirového softwaru.
6. Vývoj a údržba bezpečných systémů a aplikací (pravidelné patchování).
```

Silná opatření pro řízení přístupu

```
7. Omezení přístupu k datům pouze na ty osoby, které je nezbytně potřebují
znát.
8. Přidělení unikátního ID každé osobě s přístupem k počítači.
9. Omezení fyzického přístupu k datům držitelů karet (zabezpečení
serveroven).
```

Pravidelné monitorování a testování sítí

```
10. Sledování a monitorování veškerého přístupu k síťovým zdrojům a datům o
kartách.
11. Pravidelné testování bezpečnostních systémů a procesů (penetrační
```

```
testy).
```

Politika informační bezpečnosti

```
12. Udržování politiky, která řeší informační bezpečnost pro všechny
zaměstnance.
```

—

2. Úrovně shody (Compliance Levels)

Obchodníci jsou rozděleni do 4 úrovní podle objemu transakcí, které ročně zpracují:

Úroveň	Počet transakcí za rok	Požadavek na audit
Level 1	Nad 6 milionů	Každoroční audit na místě (ROC) kvalifikovaným auditorem (QSA).
Level 2	1 až 6 milionů	Každoroční sebehodnotící dotazník (SAQ).
Level 3	20 000 až 1 milion	Každoroční sebehodnotící dotazník (SAQ).
Level 4	Méně než 20 000	Každoroční sebehodnotící dotazník (SAQ).

—

3. PCI DSS v modelu SaaS (Příklad Shopify)

Jednou z největších výhod modelů SaaS jako Shopify je přenesení odpovědnosti za PCI DSS na poskytovatele.

- **U vlastního řešení:** Musíte zabezpečit jádro Linuxu, databázi, aplikaci i síť. Každý rok podstupujete složitý audit.
- **U SaaS (Shopify):** Platforma je certifikována jako **PCI DSS Level 1 compliant**. Obchodník používá jejich šifrovanou pokladnu (Checkout), takže data karet vůbec neprocházejí jeho servery. Tím se drasticky snižuje rozsah auditu pro samotného obchodníka.

—

4. Co se stane při porušení?

Nedodržení standardů může mít pro firmu fatální následky:

- **Vysoké pokuty:** Od karetních asociací (tisíce až miliony dolarů).
- **Ztráta možnosti přijímat karty:** Banky mohou vypovědět smlouvu o zpracování plateb.
- **Poškození reputace:** Únik dat zákazníků často vede ke krachu e-shopu.

Související články:

- Zabezpečení webových serverů
- Shopify a bezpečnost v cloudu
- Základy kryptografie a šifrování

Tagy: it security pci-dsx compliance finance e-commerce privacy