PCI DSS řešení

V poslední době jsme zaregistrovali zvyšující se počet vašich dotazů na téma novinek v oblasti přijímání platebních karet a s tím souvisejících požadavků na bezpečnost ze strany karetních asociací a regulatorních orgánů vystupujících v platebním styku. Věříme, že úniky karetních údajů z hotelových řetězců, ale i u retailových obchodníků ve vás vyvolaly otázky, zda se toto nemůže přihodit také vám a jaké případné dopady z toho pro vás mohou vyplývat. Rádi bychom vám přiblížili informace o datové bezpečnosti.

Aby vaše prostředí bylo schopno čelit pokusům o odcizení citlivých dat, rozhodli jsme se uzavřít strategické partnerství se společností, jež je uznávanou firmou v oboru testování zranitelnosti IT prostředí, a toto řešení vám společně nabídnout.

Pomocí efektivních nástrojů vám otestujeme vaše systémy a vyhodnotíme potenciální zranitelnosti, které by mohly mít za následek odcizení citlivých údajů, s čímž je vždy bohužel spojena výrazná ztráta jak finanční, tak reputační.

Dle společností, zabývajících se bezpečností dat, bude v následujících letech přibývat nových způsobů hackerských útoků, jenž budou ohrožovat firmy, osobní údaje a soukromí lidí a útočit na počítače i mobilní zařízení. Závěr z tohoto sdělení bohužel vyznívá jednoznačně - krádeže firemních i soukromých dat budou stále běžnější.

V současnosti jsme rovněž svědky zvyšujícího se dohledu na ochranu osobních údajů, jako je nařízení Evropské unie, v podobě Obecného nařízení o ochraně osobních údajů (známé jako GDPR, či Mezinárodní standard v oblasti platebních karet PCI DSS (Payment Card Industry Data Security Standard), jehož dodržováním jsou povinny všechny subjekty vystupující v odvětví přijímání platebních karet (vyjma držitelů platebních

karet). Pokud využijete těchto služeb, máte jistotu, že vaše systémy budou kontrolovat lidé s nejvyššími znalostmi na trhu v oblasti PCI DSS auditu s certifikací QSA (Qualified Security Assessor).

POPIS NABÍZENÝCH SLUŽEB:

ASV skeny Externích IP adres

Analýza zabezpečení a nastavení správné konfigurace IP adres, identifikace zranitelnosti, návrh řešení a pravidelné kvartální skenování potvrzené od ASV auditora (oprávněný skenovací auditor dle standardu PCI DSS).

Skenování čísel karet

Skenování prostředí zákazníka, kde by se mohli nacházet údaje o platebních kartách pomocí specializovaného nástroje.

Asistence při vyplňování SAQ (sebehodnotících) dotazníků

Analýza prostředí zákazníka ke standardu PCI DSS, identifikace nesouladu s požadavky.

Bezpečnostní Konzultace

Identifikace a analýza IT prostředí – konzultace při implementaci konkrétních změn (například na základě výsledku ASV skenování).

Výhody služby:

- Dostupná cena: začínající na 1800 Kč měsíčně
- Komunikace v českém jazyce
- Výsledkem je oficiální certifikát, jenž můžete použít jako průkazný oficiální dokument vůči jiným institucím a zároveň vůči vašim zákazníkům, že jejich data jsou u vás v bezpečí
- Testování prostředí probíhá průběžně
- Služby je možno využít jednotlivě, nebo jako celek

NAŠE ODPOVĚDI NA VAŠE ČASTÉ DOTAZY:

Jako obchodník očekávám, že toto řeší poskytovatel platebních služeb?

Hardware i software dodávaný společností Global Payments je v souladu s PCI standardem. Nemáme dohled nad vaším IT prostředím, ani nad tím, jak nakládáte s daty. Proto je nezbytné toto řešit i ze strany každého obchodníka. Nejedná se o přímý požadavek nás či banky, ale o nařízení karetních asociací.

Co se stane, když toto řešit nebudu?

Je naší povinností vás informovat, že v tomto případě budou veškeré případné pokuty ze strany karetních asociací přeúčtovány na vás a na vyžádání karetní asociace jsme povinni vás označit jako obchodníka, který není v souladu s PCI DSS.

Jaké navrhujete řešení?

Využijte exkluzivní nabídku našeho certifikovaného auditora, který prověří váš systém a najde potenciální slabiny systému a navrhne příslušná opatření. Služba, jejíž cena začíná na částce 1800 Kč měsíčně je v porovnání s případnými následky zanedbatelná.

Pokud byste se rádi dozvěděli více informací, obraťte se prosím na nás přes emailovou adresu: pci@globalpayments.cz

VZOROVÝ PŘÍKLAD DATOVÉHO ÚNIKU

1. Hotel používá interní hotelový management systém (HMS).
2. Smlouva o přijímání platebních karet je podepsána s acquiringovou společností, jenž dodala hardware a software v souladu s PCI DSS.
3. Hotel čelí hackerskému útoku, který je veden přes hotelové IP adresy, a z rezervačního systému stáhne údaje o platebních kartách.
4. Karetní asociace identifikuje datový únik a kontaktuje acquiringovou společnost, aby tuto záležitost okamžitě řešila s obchodníkem.
5. Na vyšetření celé záležitosti je najatá nezávislá auditorská společnost.
6. Rozsah poškození je definován na celkový únik 2000 karetních údajů, které se povedlo útočníkům ze systému odcizit. Obchodník není schopen doložit řešení standardu PCI DSS – v kategorii 4 se jedná o sebehodnotící dotazník (SAQ) a zátěžové ASV skeny systému, jenž nebyly nikdy provedeny a dle tohoto zjištění stanovuje karetní asociace výši pokuty.
7. Výše pokuty byla stanovena na 18 $ za jednotlivý odcizený karetní údaj.
8. Výše pokuty za nedoložení souladu s PCI standardem – 20 000 $.
9. Výše nákladů na vyšetření datového úniku auditorskou společností – 10 000 $.
10. Celkové náklady vyčísleny na 66 000 $ (cca 1,4 milionu korun).
11. Tato částka je požadována od obchodníka, jelikož jeho prostředí nebylo v souladu s PCI DSS.