

Október 27-28-án tartja idei második PCI DSS tanfolyamát a HOPET Informatika

2010. szeptember 3.

Összefoglaló

A hitelkártya-adatok jogtalan megszerzése, az adatokkal való visszaélés milliárdos pénzbeli veszteséget és ezzel összemérhető piacvesztést és erkölcsi károkat okoz évente a hitelkártya iparág szereplőinek. A kártyaadatok eltulajdonításával kapcsolatos visszaélések megakadályozására alakították ki a piacvezető kártyatársaságok - MasterCard, Visa, Discover, JCB, American Express - a **Payment Card Industry Data Security Standard - PCI DSS** - előírást. Ez egy sor átfogó információbiztonsági követelmény teljesítését követeli meg minden olyan szervezettől, amelyek fizetőkártyák adatainak kezelésével, feldolgozásával vagy tárolásával foglalkoznak, bankoktól, kártyaszolgáltatóktól, bolti- és Internetes kereskedőktől egyaránt. A **PCI DSS** - előírásait, és a megfelelés feltételeit oktató 2 napos, **PCI DSS Compliance Management**[®] tanfolyamának idei második, őszi kurzusát október 27-28-án tartja a HOPET Informatika Kft. A tanfolyam célja a biztonságos bankkártya rendszerek ismereteinek széleskörű elterjesztése. A részvétel mindazok számára ajánlott, akik vállalatuknál – bankok, a bankkártya elfogadók, szolgáltatók -, a bankkártya adatok biztonságáért, továbbá a **PCI DSS Compliant** szint teljesítéséért felelősek: a kártya üzletág és az IT felelős vezetőinek, compliance felelőseinek, információbiztonsági szakembereknek, adathálózati- és IT rendszergazdáknak, valamint a belső ellenőrzés és az internal audit munkatársaknak egyaránt.

Október 27-28-án tartja idei második PCI DSS szakmai tanfolyamát a HOPET Kft.

2010. szeptember 3.

A hitelkártya-adatok jogtalan megszerzése, az adatokkal való visszaélés milliárdos pénzbeli veszteséget és ezzel összemérhető piacvesztést és erkölcsi károkat okoz évente a hitelkártya iparág szereplőinek. A szervezett bűnözői körök szakmailag felkészültek, felvenni velük a versenyt nehéz. A hitelkártya-csalások, valamint a kártyaadatok eltulajdonításával kapcsolatos visszaélések megakadályozására alakították ki a piacvezető kártyatársaságok - MasterCard, Visa, Discover, JCB, American Express - a **Payment Card Industry Data Security Standard - PCI DSS** - előírást. Ez egy sor átfogó információbiztonsági követelmény teljesítését követeli meg minden olyan szervezettől, amelyek fizetőkártyák adatainak kezelésével, feldolgozásával vagy tárolásával foglalkoznak, bankoktól, kártyaszolgáltatóktól, bolti- és Internetes kereskedőktől egyaránt. Az előírás megköveteli az előírások teljesítését, amelyet a kártyatársaságok megkövetelnek, és rendszeresen ellenőriznek.

Dr. Horváth Károly, a **HOPET Informatika** ügyvezető igazgatója elmondta, hogy cégük 2008-ban indította el PCI DSS programját, és 2009-ben sikeresen lefolytatták Magyarország egyik meghatározó Level-2 vállalatának PCI DSS megfelelési projektjét. A projekt tapasztalatai, és az utóbbi időben hozzájuk

beérkezett nagyszámú technikai érdeklődés, azt mutatják, hogy Magyarországon is egyre erősebb az érdeklődés a PCI DSS iránt, viszont hazánkban még mindig nem ismert kellő mértékben a PCI DSS, sem a bankkártya kezeléssel érintett szervezetek, sem az információbiztonsági szakemberek között. A PCI DSS-sel eddig többnyire csak azok a szervezetek kerültek kapcsolatba, akik számára a megfelelőséget, azaz a Compliance szint elérését a külföldi tulajdonos vagy valamelyik elfogadó bank, illetve közvetlenül valamelyik kártyatársaság - szigorúan előírta.

„2011-ben a PCI DSS lesz az év hazai információbiztonsági „top slágere”- jósolja Dr. Horváth Károly. A PCI DSS ugyanis jóval több, mint a bankkártya kezeléssel érintett szervezetek kötelező előírása, ez egy olyan egységes, naprakész **információbiztonsági útmutató**, amelynek a bevezetését ütemezetten, a szervezet egészére is érdemes kiterjeszteni. A PCI Data Security Council (a „Tanács”) - a PCI előírásokért felelős szervezet - aktuális technikai jelentéseit figyelve, és a PCI DSS verziófrissítések nyomon követésével az **elvárható legmagasabb szintű** információbiztonságot lehet fenntartani az egész szervezet számára. Erre garanciát ad, hogy a Tanács tagjai között ott vannak az iparág olyan meghatározó technológiai cégei is, mint pl. a Cisco, a VmWare, az ArcSight vagy a LogLogic. Ezek a szervezetek biztosítják, hogy a PCI DSS tartalma mindig naprakészen igazodik a védelmi technológiák legmagasabb szintjéhez, a legkorszerűbb védelmi megoldásokhoz.

A PCI DSS ellenőrzésekkel kapcsolatosan Dr. Horváth Károly hangsúlyozta, hogy a PCI DSS esetében a megfelelőség vizsgálata nem azonos a klasszikus értelemben vett audittal. Az ellenőrzést nem auditorok, hanem **assessorok** végzik, akik magasan képzett informatikai- és hálózati szakismeretekkel rendelkező információvédelmi szakemberek. Ők, amellett, hogy a PCI DSS megfelelőség megállapítása során elvégzik a vizsgálatok hatókörének és az információbiztonsági kontrollok ellenőrzését, döntenek a kompenzációs kontrollok elfogadásáról is, valamint a szervezetek számára a megfelelőség elérésével kapcsolatban szakértői támogatást nyújtanak.

A tanfolyamra visszatérve Dr. Horváth Károly elmondta, hogy a tanfolyam első kurzusát idén januárjában tartották meg, amelyen a magyar kereskedelmi bankok, a Pénzügyi Szervezetek Állami Felügyelete mellett részt vett több „multi” hazai vállalatának a képviselője is. A tanfolyam tartalma az előzetes felkészülési követelmények alapján került összeállításra, és megadja az ahhoz szükséges ismereteket, hogy a a tanfolyam elvégzését követően a hallgatók PCI DSS Compliance hitelkártya környezeteket építhessenek ki, illetve az előírásoknak való megfelelést egy objektív, ismételhető módon ellenőrizhessék.

A tanfolyamon a hallgatók megtanulják a PCI DSS keretrendszerét, megismerkednek az előírt információbiztonsági követelményekkel, útmutatást kapnak az elfogadott technológiai megoldásokról, és elsajátítják a biztonságos üzemeltetés feltételeit.

A tanfolyam elvégzésével a hallgatók képesekké válnak arra, hogy a szervezetüknél költséghatékony PCI DSS rendszert vezessenek be, alkalmassá válnak a vállalatuk PCI DSS rendszerének belső auditálására, és arra, hogy a megfelelőségi vizsgálatokon eredményesen együtt tudjanak működni a PCI DSS assessor-okkal.

A tanfolyam minden információbiztonsággal érintett szervezetnek szól, de kiemelten hasznos a hitelkártya kezeléssel foglalkozó szervezetek üzletági- és informatikai vezetőinek, compliance felelőseinek, valamint az információbiztonsági szakembereknek, rendszergazdáknak, és az internal audit munkatársaknak.

A tanfolyamon való részvételről a résztvevők látogatási bizonyítványt kapnak, és a tanfolyam végén lehetőség van vizsga letételére. Az írásbeli vizsgát sikeresen letett hallgatók Payment Card Industry Certified Field Officer - **PCI CFO** - oklevelet kapnak.

A PCI DSS-ről és a tanfolyamról további információk a **HOPET Informatika** honlapján: www.hopet.hu találhatóak.