

Semplificazione degli standard PCI DSS

Come affrontare le norme Payment Card Industry Data Security Standard (PCI DSS)

Le maggiori società di carte di credito hanno grosse difficoltà ad arginare gli episodi di frode che hanno colpito numerose organizzazioni e relativi consumatori. Di conseguenza, le organizzazioni che accettano operazioni di pagamento con carte sono tenute ad ottemperare agli standard PCI DSS entro la fine del 2007. Le organizzazioni che non si adeguano rischiano di non essere più autorizzate a gestire i dati dei titolari di carte di credito o debito (bancomat), nonché multe fino a 500.000 dollari USA se i dati vengono persi o derubati. Questa white paper esamina i requisiti per aderire alle norme PCI DSS, le implicazioni dell'inosservanza di tali standard e in che misura la gestione di log degli e eventi e delle vulnerabilità della rete sia in grado di ottenere questa conformità.

Introduzione

Le carte di credito sono molto diffuse e il loro utilizzo per effettuare pagamenti on line sta aumentando notevolmente. Nel 2004, circolavano negli Stati Uniti 1,3 miliardi di carte di credito, con il 76% di Americani in possesso di almeno una carta di credito. Le vendite on line al dettaglio statunitensi nel 4° trimestre del 2006 sono ammontate a 33,9 miliardi di dollari USA, pari a un incremento del 25% rispetto allo stesso trimestre del 2005.

Tuttavia, non tutte le notizie sono positive. Le frodi relative a carte di credito (25%) hanno rappresentato la forma più comune di furto d'identità del 2006. Considerando che, a causa del furto d'identità, in tale anno istituti finanziari e aziende hanno subito perdite per oltre 48 miliardi di dollari USA, mentre i privati ne hanno subite per 5 milioni di dollari USA, si può dire che le frodi relative a carte di credito stanno letteralmente frugando nelle tasche di tutti! Risultano in aumento anche le frodi on line, che hanno raggiunto nel 2006 il valore di 3 miliardi di dollari USA, con incremento del 7% rispetto al 2005. La presente white paper esamina le conseguenze del furto di dati di titolari di carte di credito/bancomat e affronta le seguenti domande chiave:

- Che cos'è la direttiva PCI?
- Perché è importante ottemperarvi?
- Quali sono le conseguenze della sua inosservanza?
- Quali soluzioni sono disponibili per affrontare la direttiva PCI?

Il furto di dati e le frodi relative a titolari di carte di credito: alcuni casi reali

- 18 febbraio 2005. La Banca d'America sostiene di aver perso oltre 1,2 milioni di registrazioni di clienti, benché affermi che non esistano prove che i dati siano finiti nelle mani di criminali.
- 16 giugno 2005. CardSystems, fornitrice commerciale di servizi di elaborazione pagamenti, è stata chiamata in giudizio in una serie di azioni legali collettive, in cui è accusata di non aver protetto in maniera adeguata le informazioni personali di 40 milioni di clienti. L'attività di CardSystems ha rischiato il collasso quando VISA e American Express hanno tagliato i loro legami con la società, vietandole di elaborare i dati delle loro carte. CardSystems è stata successivamente acquistata da un'altra società.
- 9 febbraio 2006. È stato stimato che siano stati divulgati circa 200.000 conti di carte di debito di operatori commerciali al dettaglio sconosciuti, pare OfficeMax e altri. Erano altresì inclusi conti relativi ad acquirenti di banche e cooperative in tutto il paese, quali CitiBank e Wells Fargo.

- 31 gennaio 2006. I giornali Boston Globe e The Worcester Telegram & Gazette hanno involontariamente esposto 240.000 registrazioni relative a carte di credito e debito, unitamente a informazioni di smistamento relative ad assegni personalizzati, stampate su carta riciclata adoperata per avvolgere i pacchi di giornali destinati alla distribuzione.
- 12 gennaio 2007. MoneyGram, provider di servizi di pagamento, ha riportato l'accesso illegale ad un server della società, avvenuto via internet. Il server conteneva informazioni su circa 79.000 clienti, compresi nomi, indirizzi, numeri di telefono e, in alcuni casi, numeri dei conti bancari.
- 17 gennaio 2007. TJX Companies Inc. ha dichiarato pubblicamente di aver subito un'intrusione non autorizzata nel sistema di elaborazione delle carte di credito/debito. In quella che è considerata la più prestigiosa violazione registrata finora, sono stati derubati qualcosa come 45.700.000 numeri di conti di carte di credito/debito e oltre 455.000 registrazioni di reso merci (contenenti nomi clienti e numeri di patente) dal sistema informatico della società.

Ma i grossi dettaglianti on line non sono gli unici obiettivi. La pubblica attenzione può concentrarsi sulle perdite di dati di alto profilo, ma gli esperti che studiano le frodi finanziarie dicono che gli hacker stanno mirando sempre più ai piccoli siti web commerciali. In alcuni casi, i criminali sono in grado di ottenere l'accesso in tempo reale alle informazioni sulle operazioni che avvengono sui siti web, consentendo loro di derubare numeri di carte di credito validi e di effettuare rapidamente numerosi acquisti fraudolenti. Le piccole aziende on line offrono un numero totale inferiore di vittime, ma spesso rappresentano un obiettivo più facile da raggiungere, sia per i difetti nei software utilizzati per evadere gli ordini on line sia per un eccessivo affidamento sulla protezione di siti web esterni.

Il crimine informatico e relativa minaccia del furto d'identità riducono la fiducia degli utenti e dei consumatori, rallentando l'accettazione del commercio elettronico. Di conseguenza, la sicurezza dei computer, un'attività cruciale che aiuta a proteggere questi sistemi, si è mossa giustamente verso una posizione di prominenza.

La direttiva Payment Card Industry (PCI)

La struttura di protezione dei dati *Payment Card Industry* (PCI) è stata creata da American Express, Discover Financial Services, JCB, MasterCard Worldwide e Visa International. Prima del 2004, ciascuna delle suddette associazioni disponeva di una serie proprietaria di requisiti sulla protezione delle informazioni, spesso gravosi e ripetitivi per i partecipanti di più reti di marchio. Successivamente, le associazioni hanno creato una serie di requisiti di protezione delle informazioni uniformi per tutte le marche di carte nazionali (escluse le boutique e le marche private). Tutti questi requisiti sono diventati poi noti con la denominazione di norme (o standard) PCI Data Security Standard (PCI DSS) e disciplinano tutti i canali di pagamento:

commercio al dettaglio, ordini postali, telefonici e commercio elettronico.

La struttura PCI DSS

La struttura PCI DSS è suddivisa in 12 requisiti di protezione (che VISA chiama la "Dozzina digitale") organizzati in sei categorie, nel modo che segue:

PCI DSS
Creazione e manutenzione di una rete protetta
Requisito 1: Installazione e manutenzione di una configurazione firewall per proteggere i dati dei titolari di carte di credito/debito (bancomat) Requisito 2: Non utilizzo dei valori predefiniti del fornitore per le password di sistema e altri parametri di protezione
Protezione dati dei titolari di carte di credito/debito
Requisito 3: Protezione dei dati dei titolari di carte di credito/debito memorizzati Requisito 4: Cifratura della trasmissione dei dati di titolari di carte di credito/debito su reti aperte e pubbliche
Manutenzione di un programma di gestione della vulnerabilità
Requisito 5: Utilizzo e aggiornamento regolari di software o programmi antivirus Requisito 6: Sviluppo e manutenzione della protezione di sistemi e applicazioni
Implementazione di rigide misure di controllo dell'accesso
Requisito 7: Accesso limitato ai dati dei titolari di carte di credito/debito da parte di aziende che "hanno necessità di sapere" Requisito 8: Assegnazione di un ID esclusivo a chiunque abbia accesso a un computer Requisito 9: Accesso fisico limitato ai dati dei titolari di carte di credito/debito
Monitoraggio e test regolari delle reti
Requisito 10: Individuazione e controllo di tutto l'accesso alle risorse di rete e ai dati dei titolari di carte di credito/debito Requisito 11: Regolari prove dei sistemi e processi di protezione
Manutenzione di un criterio di protezione delle informazioni
Requisito 12: Manutenzione di un criterio che si occupi della protezione delle informazioni per dipendenti e imprenditori

Tabella 1: La struttura PCI DSS

Il rispetto di questi requisiti può essere riassunto in 3 fasi principali:

- **Raccolta e memorizzazione:** raccolta protetta e memorizzazione a prova di manomissione di tutti i log dei dati affinché siano disponibili a fini di analisi.
- **Creazione di rapporti:** capacità di provare immediatamente la conformità ai requisiti in caso di verifica contabile e di presentare quindi prove dell'esistenza e applicazione di controlli ai fini della protezione dei dati.

- **Monitoraggio e avvisi:** necessità di avere in forza sistemi quali gli avvisi automatici, per aiutare gli amministratori a monitorare costantemente l'accesso e l'utilizzo dei dati. Gli amministratori sono così avvisati immediatamente in caso di problemi in modo da poterli risolvere rapidamente. Detti sistemi dovrebbero essere altresì estesi agli stessi dati di log: ci deve essere una prova che i dati di log sono raccolti e memorizzati.

Livello degli operatori commerciali e fornitori di servizi

Gli operatori commerciali e i fornitori di servizi che sono tenuti a conformarsi agli standard PCI DSS sono classificati secondo il numero di operazioni con carte di credito/debito che eseguono durante un periodo di 12 mesi. Le tabelle 2 e 3 sotto riportate descrivono i vari livelli e i requisiti di conformità sia per gli operatori commerciali sia per i fornitori di servizi.

Gli operatori commerciali costituiscono degli accettanti autorizzati di carte di credito/debito utilizzate per il pagamento di merci e servizi. Esempi di settori in cui gli operatori commerciali sono tenuti ad ottemperare ai requisiti sono, a puro titolo esemplificativo:

- commercio on line, ad esempio il dettagliante on line Amazon.com
- dettaglio, ad esempio gli sportelli al dettaglio Wal-Mart
- il settore dell'istruzione superiore, ad esempio le università
- il settore sanitario, ad esempio ospedali e cliniche
- viaggi e intrattenimenti, ad esempio alberghi e ristoranti
- energetico, ad esempio stazioni di servizio
- finanziario, ad esempio banche e compagnie di assicurazione

LIVELLO DEGLI OPERATORI COMMERCIALI	
DEFINIZIONE DI OPERATORE COMMERCIALE*	CONFORMITÀ
Livello 1	
<ul style="list-style-type: none"> Operatori commerciali i cui dati dei titolari di carte di credito/debito sono stati compromessi Operatori commerciali con oltre sei milioni di transazioni con carte di credito annue in tutti i canali, compreso il commercio elettronico (e-commerce) 	<ul style="list-style-type: none"> Accertamento annuale, in loco, della protezione dei dati PCI e scansioni trimestrali della rete
Livello 2	
<ul style="list-style-type: none"> Operatori commerciali con un numero di transazioni con carte di credito annuo compreso tra 1 e sei milioni 	<ul style="list-style-type: none"> Autoaccertamento annuale e scansioni trimestrali della rete
Livello 3	
<ul style="list-style-type: none"> Operatori commerciali con numero annuo di transazioni di commercio elettronico con carte di credito compreso tra 20.000 e 1.000.000 	<ul style="list-style-type: none"> Autoaccertamento annuale e scansioni trimestrali della rete
Livello 4**	
<ul style="list-style-type: none"> Tutti gli altri operatori commerciali 	<ul style="list-style-type: none"> Autoaccertamento annuale e scansioni trimestrali della rete

Tabella 2: Livello degli operatori commerciali

*Il livello degli operatori commerciali è basato sulle definizioni fornite da VISA (USA)

**Il protocollo PCI DSS richiede che tutti gli operatori commerciali eseguano scansioni esterne della rete per adempiere al medesimo. Gli acquirenti hanno la facoltà di richiedere la presentazione di rapporti di scansione e/o di questionari agli operatori commerciali di livello 4.

I **fornitori di servizi** sono organizzazioni che elaborano, archiviano o trasmettono i dati dei titolari di carte di credito/debito per conto di soci, operatori commerciali o altri fornitori di servizi. Esempi di fornitori di servizi tenuti ad ottemperare ai requisiti sono, a puro titolo esemplificativo:

- servizi di pagamento virtuali (on line)
- fornitori host di commercio elettronico
- fornitori di servizi gestiti
- agenzie di valutazioni di solvibilità
- società di gestione dei back-up di dati
- società di "tritadocumenti"

DEFINIZIONE DI FORNITORE DI SERVIZI	CONFORMITÀ
Livello 1	
Tutti gli incaricati del trattamento di dati (soci o non soci) e tutti i servizi di pagamento virtuali*.	Accertamento annuale, in loco, della protezione dei dati PCI e scansioni trimestrali della rete
Livello 2	
Tutti i fornitori di servizi non contemplati nel Livello 1 e che archiviano, elaborano o trasmettono oltre 1 milione di conti o operazioni con carte di credito all'anno	Accertamento annuale, in loco, della protezione dei dati PCI e scansioni trimestrali della rete
Livello 3	
Tutti i fornitori di servizi non contemplati nel Livello 1 e che archiviano, elaborano o trasmettono meno di 1 milione di conti o operazioni con carte di credito all'anno	Questionario di autoaccertamento annuale e scansioni trimestrali della rete

Tabella 3: Livello dei fornitori di servizi

*I servizi di pagamento virtuali rappresentano una categoria di agenti o servizi che archiviano, elaborano e/o trasmettono dati di titolari di carte di credito/debito nell'ambito di un'operazione di pagamento (ad esempio PayPal). Più specificamente, consentono operazioni di pagamento (ad esempio, autorizzazione o saldo) tra gli operatori commerciali e gli incaricati di trattamento dei dati (ad esempio i punti VisaNet). Gli operatori commerciali hanno la facoltà di inviare le loro operazioni di pagamento direttamente ad un punto finale (endpoint) oppure, indirettamente, a un servizio di pagamento virtuale.

Rigide scadenze di conformità

Le maggiori società di carte di credito stanno facendo forte pressione sugli operatori commerciali tenuti ad aderire al protocollo PCI DSS. Sono state fissate diverse scadenze e pesanti sanzioni e multe per le organizzazioni che non si adeguano in tempo al protocollo. Tra le scadenze più importanti, stabilite da VISA USA, figurano:

- il 31 marzo 2007: scadenza entro la quale gli operatori commerciali di livello 1 e 2 dovevano dimostrare di non memorizzare dati completi, CVV2 o PIN;

- il 30 settembre 2007: data entro la quale tutti gli operatori commerciali di livello 1 devono aver completamente ottemperato ai PCI DSS;
- il 31 dicembre 2007: data entro la quale tutti gli operatori commerciali di livello 2 devono aver completamente ottemperato ai PCI DSS;

Le scadenze di conformità possono variare a seconda delle associazioni di carte di credito e delle regioni; pertanto, gli operatori commerciali e i fornitori di servizio ancora dubbiosi dovrebbero consultare gli acquirenti o le associazioni di carte di credito per conoscere le rispettive scadenze.

Perché è importante ottemperarvi?

Sebbene si tratti di norme originate negli Stati Uniti, gli standard PCI DSS costituiscono un requisito generale per tutte quelle entità che gestiscono dati di titolari carte di credito/debito. Non tutti i paesi ne sono a conoscenza/informati. Ad esempio, una confusione diffusa nel settore bancario in Australia in merito alle nuove misure di conformità ha prodotto cinque violazioni dei PCI DSS nel 2006.

È nell'interesse delle banche acquirenti garantire che i loro clienti/operatori commerciali siano a conoscenza e ottemperino alle norme PCI DSS. Il motivo è alquanto logico: le banche acquirenti sono i principali attori che edificano la linea di fiducia tra le società di carte di credito e gli operatori commerciali. Di conseguenza, sono anche quelle che finiscono al centro del mirino delle società di carte di credito/debito quando uno o più loro clienti subiscono una violazione. Per mantenere un rapporto commerciale sano e positivo con le società di carte di credito/debito, le banche acquirenti sono tenute a garantire che i loro operatori commerciali siano tutelati in maniera adeguata, e gli standard PCI DSS costituiscono lo strumento che misura la protezione dei dati dei titolari di carte di credito/debito da parte dell'operatore commerciale.

Analogamente, gli operatori commerciali e i fornitori di servizi devono dimostrare il loro livello di conformità ai PCI DSS. In questo modo, si è in grado di mantenere un sano rapporto commerciale con le banche acquirenti e di evitare responsabilità di inosservanza.

Quali sono le conseguenze della sua inosservanza?

Le società di carte di credito/debito hanno la facoltà di imporre sanzioni agli istituti bancari loro membri quando gli operatori commerciali vengono trovati colpevoli di inosservanza degli standard PCI DSS. Le banche acquirenti possono, a loro volta, obbligare contrattualmente gli operatori commerciali a indennizzarle e rimborsare loro tali sanzioni. Le sanzioni possono raggiungere fino a 500.000 dollari USA per incidente in caso di compromissione dei dati e inosservanza da parte degli operatori commerciali. Nel peggiore dei casi, gli operatori commerciali rischiano persino di perdere la facoltà di elaborare le operazioni con carte di

credito dei clienti.

Le aziende i cui dati dei titolari di carte di credito siano stati compromessi sono obbligate a informare le autorità di legge e devono offrire servizi gratuiti di protezione delle carte di credito/debito ai soggetti potenzialmente coinvolti.

Sono altresì possibili altre conseguenze oltre alle sanzioni. La perdita dei dati dei titolari di carte di credito, accidentale o attraverso un furto, può anche comportare azioni legali da parte dei suddetti titolari. Una misura del genere produce cattiva pubblicità e, a sua volta, perdita di affari.

Quali soluzioni fornisce GFI per rispettare i requisiti PCI?

Al fine di automatizzare alcune operazioni richieste per rispettare i requisiti PCI, sono implementabili delle soluzioni tecnologiche. Queste soluzioni consentono all'utente di monitorare la conformità alle norme e di avvisarlo nell'eventualità che si verifichino eventi non autorizzati relativi ai dati dei titolari di carte di credito. GFI fornisce gli strumenti software per fare esattamente quanto appena descritto.

GFI EventsManager, GFI LANguard Network Security Scanner (N.S.S.) e GFI EndPointSecurity sono tre prodotti GFI di protezione della rete, vincitori di numerosi premi. Attraverso il controllo, monitoraggio, la creazione di rapporti e gli avvisi, questi prodotti aiutano a rispettare più sezioni di 9 dei 12 requisiti PCI, come illustrato nella successiva Tabella 4.

REQUISITI PCI DSS			
	GFI EventsManager	GFI LANguard N.S.S.	GFI EndPointSecurity
1. Installazione e manutenzione di una configurazione firewall per proteggere i dati dei titolari di carte di credito/debito (bancomat)	•	•	
2. Non utilizzo dei valori predefiniti del fornitore per le password di sistema e altri parametri di protezione	•	•	
3. Protezione dei dati dei titolari di carte di credito/debito memorizzati	•		•
4. Cifratura della trasmissione dei dati di titolari di carte di credito/debito su reti aperte e pubbliche			

5. Utilizzo e aggiornamento regolari di software o programmi antivirus		•	
6. Sviluppo e manutenzione della protezione di sistemi e applicazioni		•	
7. Accesso limitato ai dati dei titolari di carte di credito/debito da parte di aziende che "hanno necessità di sapere"	•		
8. Assegnazione di un ID esclusivo a chiunque abbia accesso a un computer	•	•	
9. Accesso fisico limitato ai dati dei titolari di carte di credito/debito			
10. Individuazione e controllo di tutto l'accesso alle risorse di rete e ai dati dei titolari di carte di credito/debito	•	•	
11. Regolari prove dei sistemi e processi di protezione	•	•	•
12. Manutenzione di un criterio che si occupi della protezione delle informazioni per dipendenti e imprenditori			

Tabella 4: Requisiti PCI DSS

GFI EventsManager

L'analisi dei dati degli eventi è indicata specificatamente nel requisito 10 (si veda la precedente Tabella 4), ma è anche buona prassi per qualsiasi organizzazione quella di controllare gli eventi.

In un ambiente di rete tipico, i dati degli eventi sono distribuiti in più locazioni, sono voluminosi ed enigmatici. Gli strumenti di analisi degli eventi forniti in modo predefinito dalla maggior parte dei sistemi operativi offre soltanto funzionalità elementari. Di conseguenza, gli amministratori non dispongono di alcun mezzo per essere avvertiti in caso di registrazione di eventi importanti o problematici, quali un accesso non autorizzato a dati dei titolari di carte di credito/debito. Gli strumenti predefiniti di esplorazione e filtraggio degli eventi forniti sono caratterizzati da capacità di ricerca e filtraggio molto limitate.

GFI EventsManager è una soluzione completa di gestione dei log che supera tutti questi ostacoli, consentendo di centralizzare gli eventi, automatizzare la loro raccolta, ricevere avvisi e rilasciare rapporti investigativi. Quando GFI EventsManager raccoglie gli eventi, i suoi set di regole interni elaborano gli eventi al fine di classificarli e attivare i conseguenti avvisi o azioni. Una delle serie di regole predefinite fornite è destinata specificatamente alla classificazione degli eventi sulla base dei requisiti PCI. L'analisi degli eventi può essere eseguita attraverso il browser di eventi interno; è anche possibile creare ed eseguire query per reperire e analizzare eventi specifici.

Grazie a GFI EventsManager le aziende possono garantire che tutti gli eventi correlati ai dati dei titolari di carte di credito/debito sono monitorati costantemente. Per maggiori informazioni e per scaricare il prodotto, visitare <http://www.gfi-italia.com/italia/eventsmanager/>.

GFI LANguard Network Security Scanner

La gestione delle vulnerabilità rappresenta il perno dei requisiti 5 e 6 (si veda la precedente Tabella 4). Tuttavia, la capacità di individuare vulnerabilità in varie aree coperte da altri requisiti è di estrema importanza.

GFI LANguard Network Security Scanner (N.S.S.) tratta i tre pilastri della gestione di vulnerabilità: scansione di sicurezza, gestione di patch e controllo della rete, in un'unica soluzione integrata. GFI LANguard N.S.S. esegue la scansione dell'intera rete alla ricerca di oltre 15.000 vulnerabilità, identifica tutti i possibili problemi di sicurezza e dota gli amministratori degli strumenti di cui hanno bisogno per individuare, valutare, produrre rapporti e rimediare a eventuali minacce prima che intervengano gli hacker.

Il dover affrontare problemi relativi a questioni di sicurezza, gestione di patch e controllo della rete in modo separato, a volte utilizzando più prodotti, costituisce motivo di grossa preoccupazione per gli amministratori. Non soltanto devono infatti installare, imparare a utilizzare e gestire più soluzioni, ma il loro tempo è impiegato prevalentemente nel cercare di capire dove siano i problemi piuttosto che occuparsi effettivamente delle minacce che

potrebbero essere presenti. Grazie all'unica consolle provvista di ampie funzionalità di creazione di rapporti, la soluzione integrata GFI LANguard N.S.S. aiuta gli amministratori ad affrontare queste problematiche in modo più rapido ed efficace.

Grazie a GFI LANguard N.S.S., le aziende possono garantire che i dati dei titolari di carte di credito/debito siano conservati in un ambiente protetto. Per maggiori informazioni e per scaricare il prodotto, visitare <http://www.gfi-italia.com/italia/lannetscan/>.

GFI EndPointSecurity

La protezione dei dati di titolari di carte di credito/debito memorizzati, cioè il requisito 3 (si veda la precedente Tabella 4), rappresenta un requisito fondamentale degli standard di protezione dei dati PCS. Garantire che tali dati non finiscano nelle mani sbagliate è vitale.

Si sa che la popolarità dei dispositivi di memoria di massa, ad esempio le chiavi USB, è cresciuta molto negli ultimi anni. Sono: facili e veloci da installare, capaci di memorizzare enormi quantità di dati e sufficientemente piccoli da poterli mettere in tasca. Se non viene applicato alcun meccanismo di protezione, è possibile effettuare facilmente e rapidamente la copia di tutti i dati dei titolari di carte di credito/debito su tali dispositivi.

GFI EndPointSecurity è la soluzione di protezione che aiuta a mantenere l'integrità dei dati impedendo il trasferimento non autorizzato di contenuto da e verso dispositivi di memoria portatili. Grazie alla sua tecnologia, GFI EndPointSecurity consente di autorizzare o negare l'accesso a un dispositivo, e di assegnare (ove possibile) privilegi "completi" o di "sola lettura" a un particolare dispositivo ovvero a un utente o gruppo locali o di Active Directory. Con GFI EndPointSecurity è possibile registrare l'attività di tutti i dispositivi portatili utilizzati sui computer della rete, compresi: data e ora di utilizzo e utenti dei dispositivi stessi.

Grazie a GFI EndPointSecurity le aziende possono garantire che i dati dei titolari di carte di credito/debito non vengano copiati su dispositivi di memoria non autorizzati. Per maggiori informazioni e per scaricare il prodotto, visitare <http://www.gfi-italia.com/italia/endpointsecurity/>.

GFI ReportCenter

GFI ReportCenter consiste in una struttura di reporting centralizzata che consente di generare vari rapporti adoperando i dati raccolti ogni prodotto GFI. GFI EventsManager, GFI LANguard N.S.S. e GFI EndPointSecurity sono tutti provvisti dei rispettivi ReportPack, che si collegano alla struttura GFI ReportCenter.

I ReportPack costituiscono dei potenti strumenti complementari, dotati di numerosi rapporti preconfigurati. Comprendono inoltre una serie completa di caratteristiche funzionali, quali la pianificazione e l'esportazione dei rapporti, nonché la loro distribuzione via email. I rapporti generati con i ReportPack sono molto preziosi per le aziende al momento di valutare l'efficacia del loro programma di conformità ai PCI. Per maggiori informazioni e per scaricare un

ReportPack, visitare <http://www.gfi-italia.com/italia/reportcenter/>.

Incentivi

È nell'interesse delle organizzazioni che trattano e conservano dati di titolari di carte di credito/debito, ottemperare agli standard di protezione dei dati PCI. È anche nell'interesse delle banche garantire che gli operatori commerciali li rispettino.

Le banche potrebbero offrire agli operatori commerciali incentivi al rispetto delle norme PCI, offrendo loro licenze dei prodotti GFI di protezione della rete nell'ambito della stipula del loro contratto. Potrebbero altresì fornire servizi aggiuntivi, quali la competenza tecnica sui prodotti GFI. Si tratterebbe di una situazione soddisfacente per tutti, poiché gli operatori commerciali raggiungerebbero la serenità di essere conformi agli standard PCI DSS, oltre ad usufruire di tutti gli altri vantaggi forniti dai prodotti GFI. Anche le banche raggiungerebbero la stessa serenità, sapendo che gli operatori commerciali che hanno autorizzato ad accettare pagamenti con carte di credito hanno adottato una misura volta alla conformità agli standard.

Conclusioni

Le società sono sempre a rischio di perdita di dati sensibili relativi a titolari di carte di credito/debito. Una tale perdita produrrebbe sanzioni, azioni legali e cattiva pubblicità, il che, a sua volta, si traduce in perdite di affari. L'ottemperanza agli Standard di Protezione dei Dati PCI dovrebbe avere la priorità nell'agenda delle organizzazioni che effettuano operazioni commerciali che prevedono l'utilizzo di carte di credito.

L'implementazione di strumenti software per la gestione dei log e delle vulnerabilità, la scansione di sicurezza e la protezione degli endpoint consentirà di fare notevoli progressi sulla strada della conformità alle norme PCI. I prodotti GFI di protezione della rete possono aiutare a raggiungere tale obiettivo.

Informazioni su GFI

GFI è una società leader nello sviluppo di software, che offre agli amministratori di rete un'unica fonte in grado di soddisfare le loro esigenze di protezione della rete, sicurezza del contenuto e messaggistica. Grazie alla tecnologia vincitrice di numerosi riconoscimenti, ad una politica tariffaria aggressiva e alla particolare attenzione rivolta alle piccole e medie aziende, GFI riesce a soddisfare le esigenze di continuità e produttività aziendali delle organizzazioni in generale. Costituita nel 1992, GFI ha uffici a Malta, Londra, Raleigh, Hong Kong, Adelaide, e Amburgo, a supporto di oltre 200.000 installazioni in tutto il mondo. GFI è orientata alla collaborazione con partner e si avvale infatti di oltre 10.000 partner in tutto il mondo. GFI è inoltre Microsoft Gold Certified Partner. Maggiori informazioni su GFI sono reperibili sul sito <http://www.gfi-italia.com>.

Fonti

CreditCards.com (2006). *Fatti relativi al settore delle carte di credito e statistiche sul debito dei privati* (documento in inglese), disponibile sul sito <http://www.creditcards.com/statistics/statistics.php> (ultima citazione: 29 dicembre 2006).

U.S. Census Bureau (2006). *Vendite al dettaglio del commercio elettronico del 2° trimestre 2006* (documento in inglese), disponibile sul sito <http://www.census.gov/mrts/www/data/html/06Q2.html> (ultima citazione: 29 dicembre 2006).

Federal Trade Commission (2006). *Dati sui reclami in materia di frodi ai danni dei consumatori e furto d'identità per il periodo gennaio-dicembre 2005* (documento in inglese).

United States Postal Service. *Furto d'identità: furto del vostro nome e del vostro denaro* (documento in inglese), disponibile sul sito: <http://www.usps.com/postalinspectors/IDtheft2.htm> (ultima citazione: 29 dicembre 2006).

Bednarz A. (2006). *Gli operatori commerciali on line perderanno 3 miliardi di dollari USA in frodi nel 2006*, Network World, Inc. (documento in inglese) sul sito <http://www.networkworld.com/news/2006/111406-online-merchants-fraud.html?nlhtsec=1113securityalert2> (ultima citazione: 29 dicembre 2006).

Marlin S. (2005). *La colpa delle perdite dei dati dei clienti addossata a operatori commerciali e software* (documento in inglese), CMP Media LLC, disponibile sul sito <http://www.informationweek.com/showArticle.jhtml?articleID=161601930> (ultima citazione: 29 dicembre 2006).

Ward M. (2005). *I negozi on line devono far fronte a misure di protezione più rigide* (documento in inglese), BBC, disponibile sul sito <http://news.bbc.co.uk/2/hi/technology/4449759.stm> (ultima citazione: 29 dicembre 2006).

Evers J. (2005). *Violazione di carte di credito espone 40 milioni di conti* (documento in inglese), CNET Networks, Inc., disponibile sul sito http://news.com.com/Credit+card+breach+exposes+40+million+accounts/2100-1029_3-5751886.html (ultima citazione: 29 dicembre 2006).

Extended Retail Solutions (2006). *Lotta allo spyware e al furto d'identità nel commercio al dettaglio* (documento in inglese), GDS Publishing Ltd., disponibile sul sito <http://www.extendedretail.com/pastissue/article.asp?art=25770&issue=147> (ultima citazione: 29 dicembre 2006).

Schneier B. (2005). *Schneier sulla protezione: Visa e Amex lasciano CardSystems* (documento in inglese), Schneier.com, disponibile sul sito http://www.schneier.com/blog/archives/2005/07/visa_and_amex_d.html (ultima citazione: 29 dicembre 2006).

dicembre 2006).

Harris Interactive (2005). *Atteggiamenti e comportamenti generali dei consumatori nei confronti della protezione dei dati* (documento in inglese), Visa International.

Krebs B. (2006). *I ladri d'identità rivolgono la loro attenzione alle aziende di e-commerce più piccole* (documento in inglese), The Washington Post, disponibile sul sito <http://www.washingtonpost.com/wp-dyn/content/article/2006/09/28/AR2006092800333.html> (ultima citazione: 29 dicembre 2006).

Cybertrust (2006). *I livelli PCI degli operatori commerciali e dei fornitori di servizi* (documento in inglese), disponibile sul sito http://www.cybertrust.com/solutions/compliance_governance/pci_compliance/pci_levels/ (ultima citazione: 29 dicembre 2006).

MasterCard. *Definiti i livelli degli operatori commerciali* (documento in inglese), disponibile sul sito http://www.mastercard.com/us/sdp/merchants/merchant_levels.html (ultima citazione: 29 dicembre 2006).

Pauli D. (2006). *La confusione australiana sulla conformità provoca violazioni della sicurezza* (documento in inglese), CXO Media Inc., disponibile sul sito http://www2.csoonline.com/blog_view.html?CID=25049 (ultima citazione: 29 dicembre 2006).

Wells Fargo. *Servizi di operatori commerciali: FAQ sulle norme Payment Card Industry (PCI) Data Security Standards* (documento in inglese), disponibile sul sito <https://www.wellsfargo.com/biz/help/merchant/faqs/pci#Q24> (ultima citazione: 29 dicembre 2006).

PCI Security Standards Council (2006). *Standard di protezione dei dati per il settore delle carte di pagamento (PCI)* (Versione 1.1 in inglese), disponibile sul sito https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf.

© 2007 GFI Software. Tutti i diritti riservati. Le informazioni contenute nel presente documento rappresentano l'attuale conoscenza della GFI, in merito agli argomenti trattati, alla data di pubblicazione. A causa di cambiamenti nelle condizioni di mercato, non deve essere considerato in alcun modo un impegno da parte di GFI, e GFI non può garantire l'esattezza delle informazioni fornite dopo la data di pubblicazione. Questa white paper deve essere considerata a puri fini informativi. GFI NON OFFRE GARANZIE, ESPLICITE O IMPLICITE, NEL PRESENTE DOCUMENTO. GFI, GFI EndPointSecurity, GFI EventsManager, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI MailArchiver, GFI LANguard, GFI Network Server Monitor, GFI WebMonitor e i rispettivi loghi sono marchi registrati o marchi di GFI Software negli Stati Uniti e/o in altri paesi. Tutti i prodotti e le aziende nominate nel presente documento sono marchi registrati dei rispettivi proprietari.