

Automazione della gestione delle vulnerabilità ai fini della conformità alle norme PCI DSS

Un approccio pratico alla protezione della rete e alla conformità alle norme PCI DSS

La presente white paper identifica i problemi riscontrati nell'affrontare i rischi di sicurezza della rete tramite la gestione delle vulnerabilità. Descrive come la gestione automatizzata delle vulnerabilità contribuisca a rispettare gli standard del settore quali le norme Payment Card Industry Data Security Standard (PCI DSS) e aiuti a identificare attivamente i punti deboli della sicurezza prima che siano sfruttati.

Introduzione

La gestione delle vulnerabilità è una disciplina di gestione del rischio che affronta i pericoli del commercio elettronico e dei sistemi informatici. Si può definire come il controllo regolare dei componenti hardware e software delle infrastrutture informatiche, la scoperta di punti deboli e la relativa risoluzione. Considerato da molti professionisti informatici come un processo complesso e dispendioso, la gestione delle vulnerabilità è una delle operazioni più detestate e ignorate a loro assegnate.

La gestione delle vulnerabilità della rete non è però più una questione di scelta: standard del settore, come le norme PCI DSS, sottolineano regolarmente l'importanza di gestire le vulnerabilità della rete e la considerano un'operazione obbligatoria nelle procedure di conformità.

La presente white paper si occupa dell'esigenza di una gestione della vulnerabilità di rete efficace. Descrive i "dolori e acciacchi" normalmente associati a questo processo e fa luce su come l'automazione può aiutare i professionisti informatici a padroneggiare questa disciplina, a ridurre i costi e ad aumentare gli sforzi di conformità alle norme PCI DSS.

Introduzione.....	2
Cosa sono le norme PCI DSS?.....	2
Che cos'è la gestione delle vulnerabilità di rete?.....	3
Qual è la connessione tra le norme PCI DSS e la gestione delle vulnerabilità?.....	4
I "dolori e gli acciacchi" della gestione delle vulnerabilità.....	5
GFI LANguard Network Security Scanner.....	7
Conclusioni.....	7
Informazioni su GFI.....	8

Cosa sono le norme PCI DSS?

Le norme PCI DSS sono una raccolta di regole vincolanti che promuovono procedure di protezione informatica nelle organizzazioni che gestiscono informazioni su carte di credito. Le norme PCI DSS si prefiggono di ridurre le frodi finanziarie, elevando il grado delle capacità di protezione della rete di chiunque elabori informazioni relative a carte di pagamento e sono state concepite a causa di 3 fattori distintivi che alimentano tali frodi:

1. il commercio elettronico (e-commerce), che aiuta a superare i confini geografici e, spesso, le protezioni offerte dalle leggi e dai regolamenti locali;
2. l'elevata disponibilità di "denaro di plastica" per gli acquisti di beni di consumo nei paesi industrializzati;

3. una certa indifferenza alle *best practice* di protezione da parte di tutte le aziende che archiviano e/o elaborano informazioni su carte di pagamento in modo non protetto.

Per contrastare le frodi con carte di credito o di debito, le 5 maggiori società di carte di pagamento (Visa International, MasterCard Worldwide, American Express, JCB e Discover Financial Services) hanno progettato una forte struttura di protezione per rafforzare la sicurezza delle operazioni con carte di pagamento. Il risultato dei loro sforzi è stata l'emanazione delle norme Payment Card Industry Data Security Standard (PCI DSS). La conformità alle norme PCI DSS è di inconfutabile responsabilità di tutte le aziende che gestiscono dati di titolari di carte di credito o debito, compresi commercio al dettaglio, vendita per corrispondenza, vendita telefonica e commercio elettronico, indipendentemente dalla dimensione dell'azienda.

Che cos'è la gestione delle vulnerabilità di rete?

I punti deboli della sicurezza comportano un flusso continuo di aggiornamenti della protezione rilasciati periodicamente dagli sviluppatori di soluzioni software. A causa della frequenza e della quantità di aggiornamenti di sicurezza rilasciati, gli amministratori di sistema trovano difficoltoso stare al passo con questo impegnativo processo. Questa negligenza consente agli hacker di sfruttare sistemi privi di patch e lanciare attacchi alla rete, specialmente tramite worm e virus. Un caso famoso è quello del worm Mytob e dei suoi derivati. Nonostante il fatto che Mytob si diffonda attraverso vulnerabilità note, per le quali esiste una patch già dall'agosto 2004, questo worm è ancora attivo, e conserva saldamente il settimo posto dell'elenco dei primi 20 virus di aprile 2007 (Viruslist.com, [Virus Top 20 for April 2007](#)).

Anche gli attacchi mirati rappresentano una minaccia sempre crescente alla continuità aziendale che gli amministratori devono tener presente nella loro strategia di difesa. Soggetti pericolosi, a conoscenza degli aggiornamenti di sicurezza mancanti nell'infrastruttura di un'organizzazione, possono sfruttare questi punti deboli mediante software maligni che consentono loro di guadagnare l'accesso alle reti. Spesso, gli attacchi mirati non vengono notati per molto tempo e le loro ripercussioni si sono già fatte sentire.

L'espressione "protezione della rete" spesso viene erroneamente interpretata come riferirsi esclusivamente a patch e aggiornamenti di sicurezza mancanti. Invece, la protezione di una rete va molto più oltre, data l'esistenza di moltissimi veicoli di attacco e di punti deboli da prendere in considerazione. La negligenza e l'errore umano costituiscono in se stessi dei punti deboli della protezione e possono essere direttamente la causa di gravi violazioni di sicurezza. Il che solleva domande quali: "Perché, nonostante tutte le violazioni e minacce che affliggono le reti, gli amministratori di sistema lasciano funzionare i servizi con le password predefinite dei produttori? Perché, nonostante si sappia che per la protezione di una rete siano cruciali soluzioni anti-malware aggiornate, i professionisti informatici non aggiornano i software antivirus e anti-malware con le ultimissime firme? Perché le aziende permettono l'utilizzo

incontrollato di dispositivi portatili sulle loro reti? Non sanno che possono essere adoperati in modo pericoloso per impossessarsi di dati societari sensibili ovvero per introdurre e installare sulla rete applicazioni *peer-to-peer* (2P2) per contrabbandare musica piratata, per scaricare software senza licenza e altri file inaccettabili? Tutto questo conduce a interruzioni delle attività ordinarie dell'azienda ed espone le società a numerose responsabilità legali.

La gestione delle vulnerabilità è il processo che identifica tutte queste problematiche; un esercizio di autovalutazione che identifica, classifica e fornisce modi e mezzi per risolvere tali punti deboli, affrontando il discorso sicurezza da varie angolature e attaccando i veicoli che sfruttano i suddetti punti deboli. È del tutto evidente che si tratta di una parte fondamentale di qualsiasi processo di *due diligence* di protezione della rete e, pertanto, non sorprende che il Consiglio degli standard Payment Card Industry abbia incorporato la gestione delle vulnerabilità quale parte integrante dei requisiti di conformità prescritti dalle norme PCI DSS.

Qual è la connessione tra le norme PCI DSS e la gestione delle vulnerabilità?

Secondo le norme PCI DSS, la maniera di affrontare la problematica della protezione ha la forza del suo anello più debole. L'idea generale alla base delle norme PCI DSS è finalizzata a:

- creare e curare la manutenzione di una rete protetta
- proteggere i dati (del titolare di carte di credito/debito) in transito o archiviati
- curare la manutenzione di un programma di gestione della vulnerabilità
- implementare rigide misure di controllo dell'accesso
- monitorare e testare regolarmente la propria infrastruttura di rete
- mantenere una politica di protezione delle informazioni.

Per conseguire questi obiettivi, le norme PCI DSS definiscono 12 requisiti: gli amministratori di sistema sono tenuti a rispettarli e a dimostrare i loro sforzi nel rispettarli. Per esempio, il requisito n. 1 specifica che devono essere installati e curati firewall per proteggere i dati dei titolari di carte di credito da attacchi esterni. Per rispettare tale requisito, i professionisti informatici devono eseguire la scansione delle loro reti, convalidare l'installazione del firewall e garantire che le impostazioni di configurazione non compromettano la protezione della rete. Altro esempio è il requisito n. 6 che definisce lo sviluppo e la manutenzione di sistemi e applicazioni protetti, un'attività di gestione della vulnerabilità che comporta il fatto di garantire che tutti i componenti della rete siano aggiornati con le ultimissime patch di sicurezza fornite dai produttori.

La gestione delle vulnerabilità, tuttavia, si estende a tutta la gamma dei 12 requisiti PCI DSS. Va oltre i meccanismi di protezione della rete e raggiunge tutti i componenti e ambienti dell'infrastruttura informatica coinvolti nell'archiviazione, elaborazione o trasmissione dei dati relativi a carte di pagamento. Tra di loro, figurano:

- i componenti principali della protezione della rete, come i firewall, i router, i sistemi di prevenzione delle intrusioni (IPS) e i sistemi di identificazione delle intrusioni (IDS)
- i segmenti di rete come le zone demilitarizzate (DMZ)
- i server e i sistemi aziendali che ospitano servizi DNS, NTP, SMTP, POP3, IMAP e altri servizi di posta elettronica, gestione autenticazione, criteri di Active Directory, server web e server database
- applicazioni interne o interfacciate al web, compresi software prodotti in serie e software personalizzati.

I "dolori e gli acciacchi" della gestione delle vulnerabilità

La mancata implementazione di forti metodi di gestione delle vulnerabilità su tutti i componenti summenzionati pone le società in una posizione di violazione delle norme PCI DSS e le espone a minacce alla sicurezza provenienti sia dal loro esterno sia dal loro interno. Le ripercussioni dei danni provocati da tali violazioni non si limitano solo alle norme PCI DSS. Le società possono entrare in conflitto con leggi e regolamenti locali o nazionali come quelli stabiliti e imposti dalla Federal Trade Commission (autorità antitrust statunitense) o suoi equivalenti locali. Tali contrasti spesso si traducono in multe e procedure legali di gran lunga superiori a quelle imposte dalle norme PCI DSS!

Nonostante si tratti di un processo obbligatorio, i professionisti dell'informatica spesso ritengono la gestione delle vulnerabilità un'operazione scoraggiante e ripetitiva, incline a errori umani. Tutti i componenti hardware e software di una rete aziendale devono essere sottoposti a scansione; dopodiché, è necessario raccogliere le informazioni in un archivio centrale, consolidarle, capirle e agire di conseguenza. Per adempiere a tale onere, l'automazione costituisce la chiave che consente ai professionisti informatici di superare sfide come quelle sotto elencate:

Sfida n. 1: migliaia di controlli su ogni singolo computer. La famosa [violazione TJX](#) resa pubblica all'inizio di quest'anno sostiene la causa a favore della gestione delle vulnerabilità. Secondo il Vicepresidente e socio senior della Gartner John Pescatore, i punti deboli di sicurezza della rete che hanno condotto all'esposizione di registrazioni relative a oltre 45 milioni di carte di credito e debito, avrebbero potuto essere individuati con facilità tramite una semplice scansione della rete alla ricerca di possibili vulnerabilità ([SCMagazine.com](#)). Il crimine organizzato non mira solo alle grosse società. In occasione di evento sul tema della sicurezza informatica tenutosi a Londra nel novembre 2006 presso la Camera dei Lord, un ex consulente per la sicurezza presso la Casa Bianca, tale Howard Schmidt, ha sottolineato che: "Le piccole e medie imprese devono rendersi conto che il fatto che siano di piccole dimensioni non significa che non rappresentino un obiettivo. I criminali prendono di mira dovunque ci sia la possibilità di far soldi per loro ([CNET News.com](#))". Il 4 febbraio 2007, il sito web di Johnny's Selected Seeds (società di sementi relativamente piccola, con 100 dipendenti situata a Winslow, in Maine, negli Stati Uniti) è stata attaccata dagli hacker e un intruso ha rubato elettronicamente oltre 11.500

dati di carte di credito e debito (MaineToday.com). Sembra che la violazione sia stata scoperta il 18 febbraio, quando due clienti hanno chiamato la società dichiarando che le loro carte di credito erano state compromesse con addebiti fraudolenti. L'automazione delle scansioni della rete alla ricerca di vulnerabilità sostiene l'uniformità, riduce l'errore umano, semplifica l'identificazione dei punti deboli della rete e consente all'azienda di precedere le minacce.

Sfida n. 2: troppe informazioni su troppi computer. Nel marzo 2007, un lavoratore della società appaltatrice ha derubato dalla società Dai Nippon Printing Co quasi 9 milioni di dati sensibili relativi alla clientela (DarkReading.com). Le informazioni, compresi i numeri delle carte di credito, sono state derubate tramite supporti di memoria portatili. Le routine di scansione dovrebbero includere tutti gli esempi pericolosi al di là delle sole definizioni di vulnerabilità pubblicate. Le soluzioni di gestione delle vulnerabilità all'avanguardia forniscono ampie capacità di controllo di controllo della rete, che elencano l'hardware e software maligno che potrebbe costituire un pericolo per l'integrità della rete, informazione non sempre prontamente disponibile.

Sfida n. 3: la gestione delle patch è un'operazione basata sulla casualità. Con il numero di aggiornamenti di protezione critici rilasciati solo da Microsoft che ha raggiunto quota 104 nel 2006, gli amministratori di sistema hanno ottime ragioni per sentirsi sommersi dalla gestione delle patch! Attraverso le soluzioni di gestione automatizzata delle patch, le società sono in grado di garantire che le patch mancanti siano scaricate automaticamente in modo tempestivo. Non soltanto le patch possono essere automaticamente distribuite o "spacciate" sui computer target, ma possono anche essere ripristinate al fine di apportare stabilità all'infrastruttura informatica in caso di necessità.

Sfida n. 4: gli strumenti di gestione delle vulnerabilità predefiniti sono limitati. Un esempio sono i servizi Microsoft Windows Server Update Services (WSUS), una soluzione che gestisce il download degli aggiornamenti Microsoft mancanti senza alcun supporto di scansione alla ricerca di vulnerabilità, controllo della rete e operazioni di reporting. Il che crea un'ulteriore sfida da superare per gli amministratori di sistema: la correlazione dei risultati. Nel caso di soluzioni specializzate distinte, gli amministratori devono pure dare un senso ai risultati delle scansioni di vulnerabilità, a quelli del controllo della rete e alle informazioni di gestione delle patch, correlando tutto ciò manualmente. Inoltre, nella maggior parte dei casi, la generazione di rapporti è limitata; pertanto, l'amministratore dovrà sprecare altro tempo a compilare i rapporti manualmente, spesso tramite operazioni di "taglia e incolla".

Sfida n. 5: l'ottemperanza alle norme è un processo molto difficile. L'unico modo per ottenere la conformità è avvalendosi di dettagliati rapporti che delineano le modalità di attuazione della gestione delle vulnerabilità e che forniscono una prova tangibile di rispetto delle norme. I problemi sorgono con la quantità di rapporti richiesti e con l'archiviazione di tali dati. Ancora una volta, l'automazione semplifica la vita degli amministratori di sistema, attraverso funzioni che consentono la generazione pianificata di rapporti e la distribuzione automatizzata, rafforzando così gli sforzi di conformità e facendo risparmiare tempo, altrettanto

prezioso quanto il denaro!

Il superamento di tutte le sfide grazie all'automazione è solo un aspetto della soluzione completa. Anche altre caratteristiche funzionali, quali un database di definizioni delle vulnerabilità completo e autorevole e la facoltà di consolidare diverse operazioni in un unico prodotto, aiutano gli amministratori di sistema ad identificare persino altri punti deboli, mantenendo così la protezione della rete aziendale in perfetta forma. Gli amministratori di sistema richiedono strumenti che non soltanto automatizzino, ma integrino la gestione delle vulnerabilità nel loro processo quotidiano, con le procedure meno invasive possibili, ossia, una soluzione come GFI LANguard Network Security Scanner.

GFI LANguard Network Security Scanner

GFI LANguard Network Security Scanner (N.S.S.) è una soluzione, vincitrice di numerosi premi e provvista di certificazione OVAL, che individua, valuta, rilascia rapporti e corregge le vulnerabilità presenti sulla rete. Con un'unica soluzione, fornisce: scansione alla ricerca di vulnerabilità e controllo di reti eterogenee, capacità di gestione delle patch del tutto sviluppate e funzioni ineguagliate di creazione di rapporti, grazie al ReportPack dedicato.

Nella GFI PCI Suite è inclusa inoltre una versione di GFI LANguard N.S.S. personalizzata specificamente per la conformità alle norme PCI DSS. La suite comprende altresì GFI EventsManager, soluzione di gestione dei log degli eventi, insieme a un pacchetto di rapporti su misura. Per maggiori informazioni su GFI LANguard N.S.S. e sulla GFI PCI Suite, nonché su come tali prodotti aiutano la propria azienda a ottenere la conformità alle norme PCI DSS, visitare il sito: <http://www.gfi-italia.com/italia/pci/>.

Conclusioni

Oggigiorno, i professionisti informatici non possono sfuggire ai loro doveri di gestione delle vulnerabilità; questi sono radicati sia negli sforzi di *due diligence* sia nell'obbligo di conformità alle norme PCI DSS. In passato, il monitoraggio alla ricerca di vulnerabilità della rete era un'operazione difficile per qualunque amministratore di rete. Oggi, soluzioni come GFI LANguard N.S.S. introducono caratteristiche di automazione in grado di aiutare i professionisti informatici a eseguire l'estremamente importante operazione di scansione alla ricerca di vulnerabilità della rete con il minor sforzo possibile, al contempo riducendo i costi e la probabilità di errori umani.

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>.

© 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.