Quaderni Clusit

008

PCI-DSS

Payment Card Industry Data Security Standard

Jean Paul Ballerini
Fabio Guasconi

Clusit
Associazione Italiana per la Sicurezza Informatica

PCI-DSS

Payment Card Industry Data Security Standard

Jean Paul Ballerini

Fabio Guasconi

Quaderni CLUSIT – Novembre 2009

CLUSIT

Il CLUSIT - Associazione Italiana per la Sicurezza Informatica, è una associazione "no profit" con sede presso l'Università degli studi di Milano, Dipartimento di Informatica e Comunicazione, fondata nel luglio 2000.

Le principali attività del CLUSIT sono:

- la diffusione di una cultura della sicurezza informatica rivolta alle Aziende, alla Pubblica Amministrazione ed ai cittadini;
- l'elaborazione sia a livello comunitario che italiano di leggi, norme e regolamenti che coinvolgono la sicurezza informatica;
- la definizione di percorsi di formazione per la preparazione e la certificazione delle diverse figure professionali operanti nel settore della sicurezza ICT;
- la promozione dell'uso di metodologie e tecnologie che consentano di migliorare il livello di sicurezza delle varie realtà.

I soci del CLUSIT sono rappresentativi dell'intero "sistema Paese", in particolare della ricerca, dell'industria, del commercio, del settore bancario ed assicurativo, della Pubblica Amministrazione, della Sanità, dei servizi, delle telecomunicazioni e di Internet.

Copyright e Disclaimer

Presentazione

Il settore dei sistemi di pagamento, con particolare riferimento alle carte, è storicamente uno degli obiettivi prediletti dai truffatori e non solo telematici. Dall'introduzione di questi sistemi assistiamo ad una continua rincorsa, tipica di ogni ambito in cui la sicurezza gioca un ruolo importante, tra "ladri e guardie". I primi impegnati ad individuare e "exploitare" vulnerabilità del sistema i secondi a correggere "security bug" e migliorare i sistemi di protezione. Con l'avvento di Internet e di conseguenza della diverse forme di pagamento elettronico, la lotta tra buoni e cattivi sopra menzionata è diventata impari (o asimmetrica come si usa dire in alcuni contesti). Difatti, la rete Internet diventa componente integrante del sistema di pagamento e le voragini di sicurezza che dalla fine degli anni '80 l'avevano investita diventavano, per proprietà transitiva, voragini nei sistemi di pagamento. È risaputo tra gli addetti ai lavori, che solo un qualche intervento, non sappiamo ancora bene di quale natura, ha consentito sino ad oggi all'intero sistema di continuare a sostenersi.

Nell'arco di un brevissimo periodo di tempo i sistemi di pagamento on-line sono diventati il target preferito di tutto quel filone underground che finalizzava le sua attività al facile guadagno ed alla truffa. Sin dalla sua nascita (stiamo oramai parlando di una decina di anni fa) il CLUSIT ha cercato di sollevare il problema nelle sedi più opportune, ma nonostante l'evidenza che era sotto gli occhi di tutti, anche in un settore così critico il discorso della sicurezza informatica non veniva percepito o forse cosa ancora peggiore, non veniva capito.

Ci sono voluti diversi anni e diverse "botte", perché alla fine qualcuno decidesse di ricorrere ai ripari e provare a porre un freno agli attacchi in rete ai sistemi di pagamento. Il primo risultato concreto di questo lavoro è lo standard PCI-DSS (Payment Card Industry Data Security Standard), una serie di direttive, linee guida o best practice che dir si voglia, mirate alla protezione dei dati di una carta di pagamento. Visto il tema trattato il lettore si aspetterà uno standard particolarmente rigoroso e di difficile applicabilità, in realtà si tratta di uno standard, che partendo da livelli di consapevolezza e competenze che devono ancora crescere, si assesta su richieste e imposizioni più che ragionevoli e che, proprio per questo, può essere facilmente esteso ad ambiti non necessariamente legati alle carte di pagamento. Merita quindi di essere seriamente considerato non solo da chi opera nel settore di riferimento, ma da chiunque sia interessato a sviluppare approcci concreti e completi al

problema della protezione dei dati e dei sistemi. Ma non voglio togliere la suspance e rivelare il nome dell'assassino in anticipo.

La trattazione esposta in questo volume è sicuramente un ottimo punto di partenza per chi vuole non solo approfondire ma anche solo conoscere il tema in oggetto. Stiamo parlando di una trattazione molto agevole e di facile lettura ad un tema, come quello degli standard, spesso molto ostico e che mal si presta ad essere trattato in modo discorsivo. Di questo va dato merito agli autori che dimostrando una notevole padronanza della materia trattata sono riusciti a farne una rielaborazione stimolante e completa. In particolare, il lettore troverà nel testo tutte le informazioni necessarie per acquisire un buon livello di conoscenza dello standard PCI-DSS e cosa più importante troverà anche interessanti spunti critici, confronti con gli standard di mercato più diffusi e i necessari rinvii per approfondire i temi trattati e mantenere l'adeguato livello di aggiornamento richiesto da questo tipo di competenze. Insomma, non ci sono più scuse perché un socio del CLUSIT non debba conoscere questo standard.

Prof. Danilo Bruschi

Presidente del
Comitato Tecnico-Scientifico Clusit

Abstract

Il Quaderno che state leggendo è stato composto al fine di illustrare con chiarezza quanto ruota intorno allo standard PCI-DSS e alla connessa protezione dei dati delle carte di pagamento, rivolgendosi principalmente a un pubblico specialistico, come i soci CLUSIT. Si è però cercato, nel contempo, di rendere i concetti al di là dei termini specifici ad essi legati e di non entrare in trattazioni tecniche spinte, al fine di rendere i contenuti fruibili ad una platea più allargata, che è effettivamente quella coinvolta nell'applicazione di questo standard.

Nel primo capitolo del Quaderno si introduce il lettore ai soggetti e ai processi su cui PCI-DSS si concentra, di fondamentale importanza per avere un'illustrata visione d'insieme. Si passa quindi ad esaminare le origini dello standard e le altre norme ad esso vicine.

Il secondo capitolo tratta in maniera estesa la struttura e i requisiti di PCI-DSS, descrivendo il contenuto generale e andando a far luce sui punti di più difficile comprensione, applicazione e di maggiore rilevanza per il raggiungimento della conformità.

Il terzo quarto capitolo analizza lo standard PCI-DSS e le sue relazioni con altre norme e best practice assieme alle quali potrebbe trovarsi a convivere in un ambiente reale, ponendo l'accento sulle sinergie tra di esse.

Nel quarto capitolo si eviscera il processo di verifica e attestazione di conformità rispetto a PCI-DSS, i cui meccanismi sono forse uno degli aspetti meno conosciuti dello standard. Sono inoltre riportati i requisiti di validazione richiesti dai diversi brand delle carte di pagamento.

Il quinto capitolo illustra le scadenze passate e soprattutto future legate alla conformità rispetto allo standard, sia a livello locale che globale.

Nel sesto capitolo sono raccolte un insieme di domande frequenti, riprese dal materiale pubblicato ufficialmente e integrate con l'esperienza sul campo.

Gli ultimi due capitoli riportano gli indirizzi web, i contatti, e-mail utili e la nomenclatura impiegata.

Merita infine un breve accenno in questa sede la scelta della terminologia. Ove possibile si è fatto uso dei termini tradotti nel glossario ufficiale pubblicato dal PCI-SSC mentre, nei casi in cui questi potessero dare adito a dubbi sulla loro corretta interpretazione, si è deciso di mantenere i termini impiegati in lingua inglese.

Gli autori

Fabio Guasconi

Impegnato dal 2003 come consulente per la sicurezza delle informazioni, con particolare attenzione per le tematiche di analisi del rischio, gestione della sicurezza e verso le norme internazionali, a cui contribuisce attivamente tramite UNINFO e ISO, ha ottenuto le qualifiche di CISA e CISM. E' lead auditor qualificato con significativa esperienza sullo schema ISO/IEC 27001 (della cui traduzione in italiano è stato editor) e ha una conoscenza approfondita delle diverse attività di verifica e miglioramento della sicurezza. Opera attivamente in ambito PCI-DSS, per il quale è QSA (Qualified Security Assessor) riconosciuto dal PCI-SSC.

Laureatosi in Informatica a Torino, presiede attualmente il comitato italiano SC27 per la sicurezza delle informazioni di UNINFO ed è responsabile della Divisione Sicurezza Informazioni presso @ Mediaservice.net S.r.l.

Jean Paul Ballerini

Con un'esperienza quasi decennale nelle problematiche della sicurezza informatica, ricopre da gennaio 2009 il ruolo di Technical Sales Lead per IBM Internet Security Systems con un ruolo internazionale; nei sei anni precedenti aveva ricoperto il ruolo di Senior Technology Solutions Expert (per Internet Security Systems prima dell'acquisizione da parte di IBM), sempre con un ruolo internazionale. Durante il corso della propria attività nell'ambito della sicurezza ha ottenuto le qualifiche CISSP e PCI QSA; in questo ruolo, oltre ad eseguire accertamenti e certificazioni, è il coordinatore di IBM Internet Security Systems delle attività relative a PCI per la regione Europa, Medio Oriente e Africa (EMEA)

Laureatosi in Scienze dell'Informazione presso l'Università di Bologna, dove ha anche ottenuto un dottorato di ricerca in Informatica Giuridica e Diritto dell'Informatica, ha poi collaborato come ricercatore presso il Politecnico Federale di Zurigo prima di abbandonare la carriera accademica.

Ringraziamenti Speciali

Diverse persone, oltre agli autori, hanno contribuito in svariati modi a far giungere questo Quaderno CLUSIT tra le vostre mani. In particolare desideriamo ringraziare:

Il CD del CLUSIT per il caloroso supporto all'iniziativa fin dal suo primo giorno.

Il Prof. Danilo Bruschi per i precisi commenti nonché per la chiara e completa presentazione riportata in testa al Quaderno.

Il CTS del CLUSIT per l'attentissimo ed estensivo contributo alla revisione del testo.

Samuele Battistoni per la parte relativa a PA-DSS e per i numerosi e preziosi suggerimenti forniti.

INDICE

Elenco delle Figure

Elenco delle Tabelle

1 Introduzione

Il presente Quaderno è stato scritto con la precisa finalità di far luce su uno degli standard sulla sicurezza delle informazioni che hanno conosciuto una maggiore crescita nell'ultimo lustro e il cui impatto sul tessuto economico del vecchio continente si sta avvicinando rapidamente dopo aver imposto forti cambiamenti oltre oceano.

PCI-DSS interessa, come si approfondirà nei capitoli successivi, qualunque soggetto tratti una ben precisa informazione: il numero della carta di pagamento (tecnicamente noto come PAN) emessa dai brand VISA, MasterCard, American Express, JCB o Discovery. Per carte di pagamento si intendono carte sia di credito sia di debito. Negli USA, dove questo standard è già stato reso obbligatorio, la sola VISA considera lo standard applicabile a oltre 4000 organizzazioni senza contare quelle (numerosissime) che trattano meno di ventimila transazioni all'anno.

I contenuti di questo standard non hanno un carattere rivoluzionario e includono aspetti di processo descritti genericamente e aspetti dal taglio più tecnico accompagnati da una descrizione più dettagliata. In entrambi i casi ci si muove nella stessa direzione delle già note best practice del settore, senza innovare ma andando a individuare un insieme minimo di misure di protezione che devono essere applicate nella gestione dei dati delle carte di pagamento, con la finalità precisa di ridurre le violazioni sulla sicurezza che li interessano.

PCI-DSS è di carattere aperto fin dalla sua creazione ma, nonostante sia liberamente accessibile a chiunque, è ancora decisamente poco conosciuto nel nostro paese, spesso nemmeno dagli stessi addetti ai lavori. Senza voler approfondire le motivazioni di questa poca diffusione, ampliamente legate alla non obbligatorietà che fino a poco tempo fa lo standard aveva al di fuori degli USA, la volontà degli autori è di descrivere, ma soprattutto approfondire, i requisiti in esso inclusi alla luce di casi pratici della loro applicazione nonché di fare chiarezza su tutto quello che si attiene alla PCI-DSS oltre che alle tematiche che le ruotano intorno. Questo include anche i contesti in cui lo standard si può andare ad applicare, passando inevitabilmente per le relazioni con altre norme o best practice inerenti la sicurezza delle informazioni o, più generalmente, la gestione dei sistemi informativi.

1.1 Soggetti e ruoli chiave

Il primo passaggio necessario per comprendere al meglio la PCI-DSS è la precisa definizione delle entità che sono normalmente coinvolte nei flussi di informazioni inerenti le carte di pagamento.

Se si considera la vita di una carta di credito, il primo soggetto che compare è quello che emette fisicamente la carta, chiamato **Issuer**. Il cliente che ne ha fatto richiesta riceve la carta, esegue la procedura di attivazione (tipicamente attraverso un numero gratuito attraverso il quale vengono immessi i dati tramite i pulsanti del telefono) e può quindi cominciare ad effettuare acquisti. Per le carte di pagamento internazionali quali ad esempio VISA o MasterCard, l'Issuer opera normalmente appoggiandosi a una Banca (detta **Issuer Bank**), ossia emette carte per conto della banca presso cui il cliente ha un conto corrente. In questo caso la banca è "cliente" del soggetto Issuer.

I **Brand** delle carte di pagamento, noti al grande pubblico attraverso il nome a cui è legato il relativo circuito, sono fondamentalmente associazioni di soggetti Issuer.

Quando il cliente effettua acquisti interagisce con il soggetto, che la normativa definisce come **Merchant**. Esistono sostanzialmente due tipi di Merchant:

1. Il *Merchant elettronico* per acquisti effettuati online. In questo caso si parla anche di operazione con "card not present". I dati che solitamente vengono richiesti all'utente sono il nome sulla carta, il PAN, la data di scadenza e il CVV2[1] (il numero di 3 o 4 cifre stampato davanti o dietro la carta per verificarne la validità).
2. Il *Merchant fisico* (o negozio) per gli acquisti effettuati direttamente. In questo caso si parla anche di operazioni con "card present". In questo caso la carta viene strisciata o viene letto il chip e i dati raccolti sono il nome del proprietario della carta, il PAN, la data di scadenza e la banda magnetica completa.

Figura 1 – Fac-simile di carte con PAN di 16 e 15 cifre

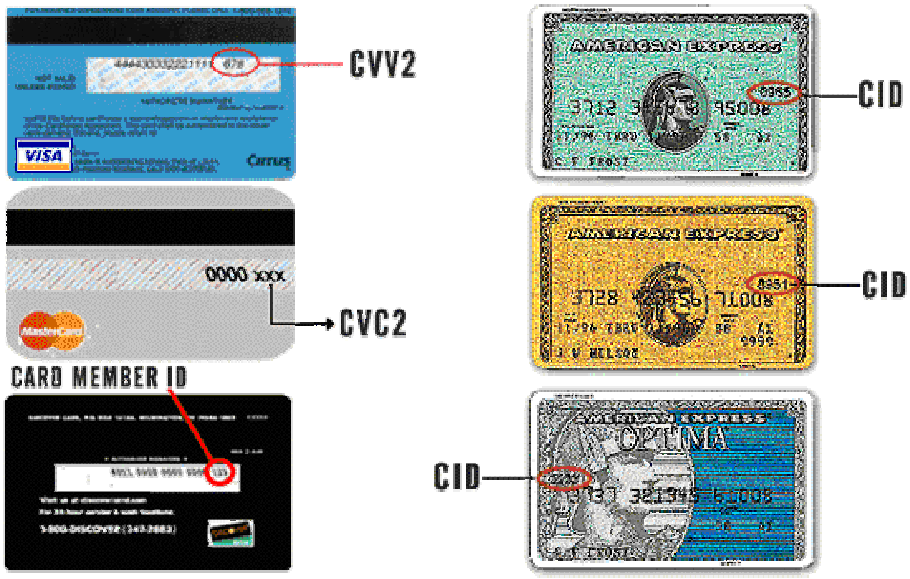

Figura 2 – Codici di sicurezza per vari brand

Quando il Merchant richiede l'autorizzazione ad accettare il pagamento si mette in collegamento con un soggetto che viene denominato **Acquirer**, il quale può procedere con l'autorizzazione oppure agire per tramite di una Banca. In questo secondo caso, la Banca,

[1] Può anche chiamarsi CAV2/CVC2/CID sulla base del brand che ha emesso la carta.

normalmente legata da un rapporto con il Merchant, è definita **Acquirer Bank** e può essere cliente di un Acquirer.

A questo schema si possono aggiungere diverse terze parti che possono essere coinvolte e tutte rientrano sotto il nome di **Service Provider**; eccone alcuni esempi:

- un soggetto che offre il servizio di pagamenti online (*Gateway*); l'online Merchant non ha questo tipo di applicazione in proprio e l'acquista da una società specializzata;
- un soggetto che offre servizio di hosting o housing dei sistemi informativi. Anche se non è direttamente coinvolta con l'attività del Merchant, i PAN fisicamente passano per questa infrastruttura e quindi diventa soggetta alla PCI-DSS;
- un soggetto che offre il servizio di deposito di backup, trasporto e/o distruzione di documenti sensibili, etc. che riceva PAN su qualunque tipo di supporto;
- un soggetto che è coinvolto in programmi di fidelizzazione del cliente finale.

Il grafo seguente riassume graficamente dei soggetti presentati hanno a che fare con quali altri. Il dettaglio delle informazioni scambiate tra di essi è espletato nel capitolo successivo.

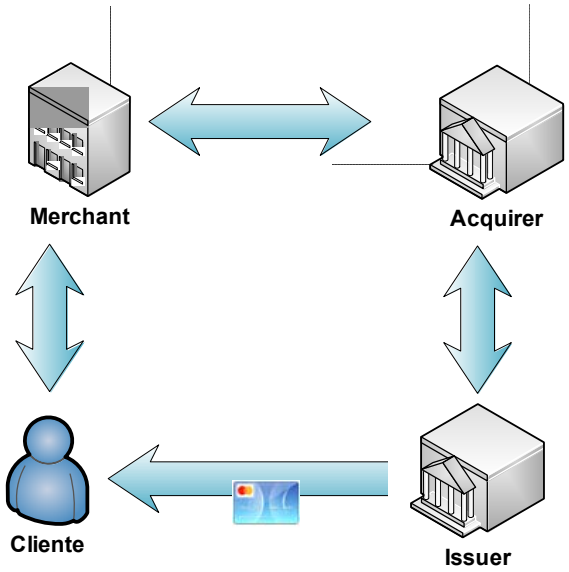

Figura 3 – Interazione tra soggetti coinvolti.

Da sottolineare che, per poter essere pienamente conformi allo standard PCI-DSS, è necessario che non solo il Merchant lo sia ma anche tutte le parti con cui questo comunica i dati delle carte di pagamento (PAN), il che produce un effetto 'domino' considerevole sul mercato.

1.2 I tre processi principali

Quando un titolare di carta effettua un acquisto viene innescato un meccanismo di interazione fra i vari soggetti al fine sia di garantire al Merchant che otterrà il pagamento, di cui ha diritto, sia di trasferire tale somma dal conto del titolare della carta a quello del Merchant. Tale meccanismo è composto da tre processi:

1. **Autorizzazione**. Attraverso l'intermediazione dell'Acquirer, il Merchant deve ottenere dall'Issuer della carta l'autorizzazione ad utilizzarla. A questo punto la transazione non è garantita. **In nessun caso è permesso ai Merchant di memorizzare il CVV2, il PIN o la banda magnetica dopo aver ricevuto il codice di autorizzazione per la transazione**[2] (vedi paragrafo 2.5.1).

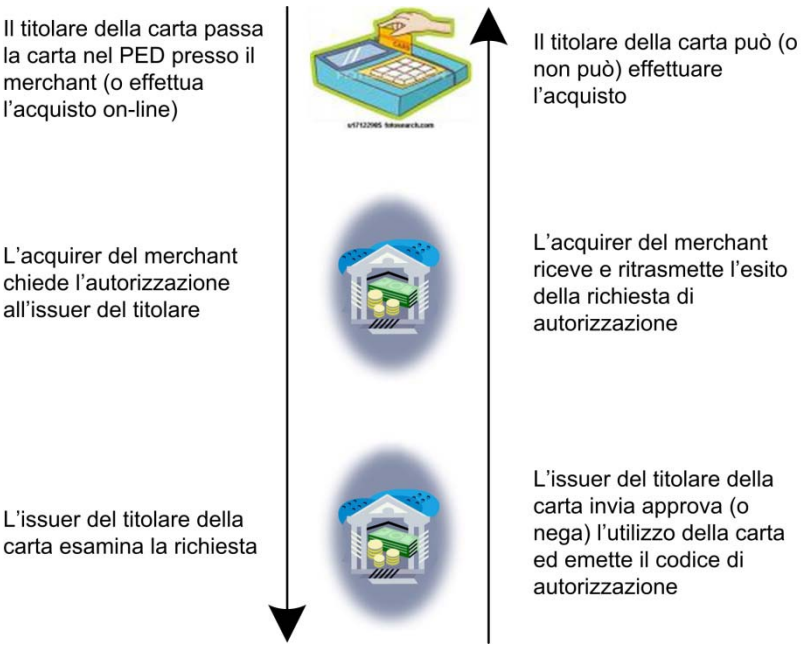

Figura 4 – Schema semplificato del processo di autorizzazione

[2] Fa eccezione a questa regola l'Issuer bank in quanto non lo memorizza al fine di autorizzare pagamenti ma come parte integrante della propria attività di emissione delle carte; esiste una FAQ al riguardo sul sito del PCI Council: *"Come possono gli Issuer essere conformi se memorizzano dati sensibili per l'autenticazione?"* (FAQ numero 9575).

2. **Clearing**. L'Acquirer ottiene i dettagli della transazione dal Merchant (quali l'importo della transazione, la data, il numero della carta, etc.); questi vengono inviati all'Issuer che li usa per l'addebito sul conto legato alla carta del titolare. A questo punto il trasferimento dell'ammontare non è ancora avvenuto.

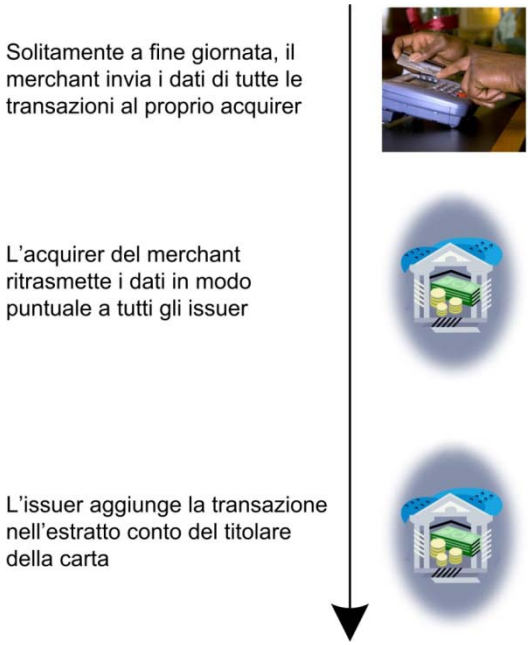

Figura 5 – Schema semplificato del processo di clearing

3. **Settlement**. I soldi a questo punto sono trasferiti dall'Issuer al conto del Merchant presso il suo Acquirer. Infine i soldi vengono prelevanti dal conto del titolare per il saldo del suo debito con l'Issuer, con una periodicità tipicamente mensile (carta di credito) oppure immediata (carta di debito).

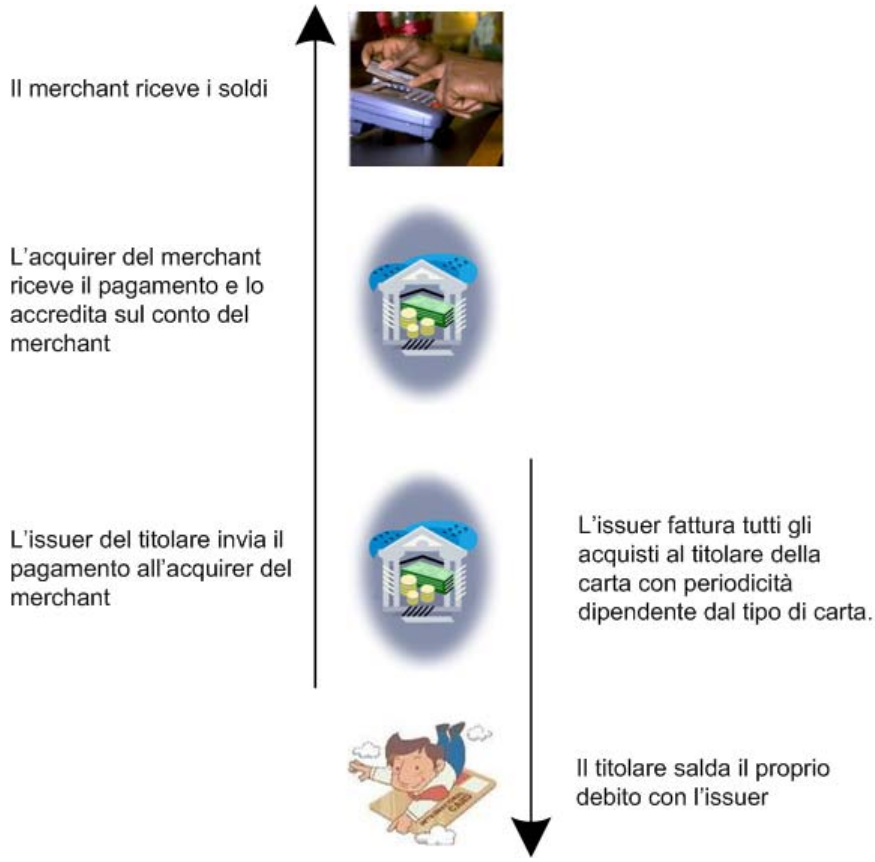

Figura 6 – Schema semplificato del processo di settlement

1.3 Genesi degli standard PCI legati alle carte

La larga quantità di frodi attraverso l'abuso delle carte di credito era stato l'elemento scatenante che aveva portato i grandi brand, in particolare VISA e MasterCard, a definire degli standard cui si dovevano attenere le società che accettavano in pagamento carte di credito dei loro circuiti. In particolare, VISA si era preoccupata principalmente di definire una politica di conformità mentre MasterCard aveva scelto piuttosto la via del monitoraggio ed eliminazione delle vulnerabilità.

Il 15 dicembre 2004, cinque brand (VISA, MasterCard, American Express, JCB e Discovery) decisero di unire le forze e definire uno standard comune. È così che fu fondato il Payment Card Industry Security Standard Council (PCI-SSC) e che venne pubblicato il primo PCI Data Security Standard (PCI-DSS). Come si può immaginare, i due elementi costituenti le richieste di conformità sono evoluti da quanto VISA e MasterCard già avevano posto in essere. La PCI-DSS quindi nasce e continua il percorso che il circuito VISA già richiedeva alle aziende. I soggetti che si certificano devono anche consegnare i rapporti delle scansioni esterne effettuate da aziende autorizzate (Approved Scanning Vendor, vedi paragrafo 4.1.2). Le procedure di scansione utilizzate da queste aziende sono definite dal PCI-SSC e sono pubblicamente disponibili.

Da un punto di vista organizzativo, il PCI Council è guidato da un Executive Committee[3], che ne determina le politiche, costituito dai cinque brand fondatori. Le decisioni operative sono prese del Management Committee[4], anch'esso costituito dai cinque brand fondatori ma da persone diverse.

Con la creazione del PCI SSC, fu anche deciso di coinvolgere enti ed aziende esterne ai brand, sia perché avrebbero dovuto implementare questa normativa, sia perché si occupano di sicurezza, tutte in qualità di Participating Organization[5] (all'8 ottobre 2009, la lista è composta da 538 aziende). Il modulo per richiedere di diventare membro si può trovare nella FAQ numero 5441). Un Comitato Consultivo, i cui membri sono selezionati tra le Organizzazioni Partecipanti, fornisce input al PCI Council e feedback sull'evoluzione del PCI-DSS. Infine esistono un Marketing Working Group, un Technical Working Group ed un Legal Committee, i cui membri sono scelti fra i brand fondatori e si occupano delle attività chiaramente definite dal loro stesso nome.

Figura 7 – PCI Security Standard Council

1.3.1 Payment Application DSS (PA-DSS)

Le aziende che sviluppano e vendono software utilizzato in ambienti che trattano i numeri delle carte di pagamento non sono soggette alla PCI-DSS perché non accettano o memorizzano direttamente tali numeri. Il software che sviluppano, invece, può essere

[3] https://www.pcisecuritystandards.org/pdfs/executive_committee.pdf

[4] https://www.pcisecuritystandards.org/pdfs/management_committee.pdf

[5] https://www.pcisecuritystandards.org/participation/member_list.html

certificato per essere utilizzato in tali ambienti; questa certificazione si chiama appunto PA-DSS, Payment Application Data Security Standard.

La prima forma di certificazione era gestita da VISA ed era nota come Payment Application Best Practice (PABP). Lo scopo della PA-DSS è quello di aiutare chi sviluppa software a farlo in modo sicuro per quanto riguarda le applicazioni destinate al trattamento di carte di pagamento, in particolare verificando e certificando che non memorizzino alcuno dei dati sensibili proibiti (ad esempio la banda magnetica, il CVV2 o il PIN) e quindi che le applicazioni supportino la conformità alla PCI-DSS da parte dell'azienda che le utilizza. In dettaglio PA-DSS verifica e certifica che le applicazioni di pagamento:

1. non memorizzino i dati sensibili delle carte di pagamento (banda magnetica, CVV2, PIN);
2. forniscano funzionalità per la gestione sicura delle password;
3. proteggano opportunamente i dati delle carte di pagamento (PAN);
4. forniscano sufficienti funzionalità di logging;
5. siano sviluppate secondo criteri e politiche di sicurezza adeguate;
6. proteggano le connessioni wireless, se utilizzate;
7. siano testate per indirizzare le vulnerabilità del codice;
8. siano progettate per essere inserite all'interno di una topologia di rete sicura;
9. che non memorizzino il PAN sulle componenti dell'applicazione esposta in Internet;
10. forniscano modalità sicure aggiornamento ed update;
11. forniscano modalità sicure di supporto da remoto;
12. implementino tecnologie di crittografia forte per la trasmissione dei dati su reti pubbliche;
13. siano accessibili da remoto (non-console) con protocolli criptati;
14. abbiano una documentazione adeguata per l'installazione (Implementation Guide) per i Merchant e i reseller.

Lo standard PA-DSS si applica ad ogni applicazione di terze parti che memorizza, processa o trasmette dati delle carte di pagamento come parte dell'autorizzazione o del settlement. Questo standard quindi impatta direttamente i software vendor di applicazioni di pagamento ed indirettamente i Merchant ed i Service Provider che acquistano ed utilizzano queste applicazioni. In particolare:

1. PA-DSS **si applica** a tutte le applicazioni di pagamento hardware o software disponibili sul mercato ("Off The Shelf") che sono vendute ed installate senza personalizzazioni da parte del vendor.
2. PA-DSS **si applica** a tutte le applicazioni di pagamento hardware o software fornite in moduli. PA-DSS si applica in questo caso a tutti i moduli che eseguono funzioni di pagamento.
3. PA-DSS **non si applica** alle applicazioni di pagamento sviluppate e vendute per un solo cliente (soluzione ad hoc) fintanto che la revisione della conformità di questa applicazione rientra nell'ambito della verifica di conformità del Merchant o Service Provider che la utilizza.
4. PA-DSS **non si applica** alle applicazioni sviluppate in casa dai Merchant e Service Provider se utilizzate internamente (non vendute a terze parti), fintanto che la revisione di questa applicazione rientra nell'ambito della verifica di conformità del Merchant o Service Provider che la utilizza.
5. PA-DSS **non si applica** ai terminali di pagamento se le seguenti condizioni sono tutte vere:
    - il terminale non ha connessioni con gli altri sistemi del Merchant;
    - il terminale è connesso solo all'Acquirer o al provider dei pagamenti;

- il vendor fornisce in modo sicuro aggiornamenti, supporto, accesso e manutenzione;
- i dati sensibili per l'autenticazione non sono mai memorizzati dopo l'autorizzazione del pagamento.

Referenze PA-DSS

- Lista di applicazioni certificate (https://www.pcisecuritystandards.org/security_standards/vpa/); è consigliabile per le aziende che necessitano acquistare una nuova applicazione di verificarne la certificazione sul sito del PCI Council.
- PA-DSS V1.2 and Supporting Documents: https://www.pcisecuritystandards.org/security_standards/pci_pa_dss.shtml

1.3.2 PIN Entry Device DSS (PCI PED)

Nelle transazioni con carta presente il cliente inserisce la propria carta ed eventualmente inserisce il PIN in un PIN Entry Device (PED). Come per le applicazioni di pagamento, esistono delle linee guida anche per i costruttori di questi dispositivi, sia per garantire che non memorizzino alcuno dei dati proibiti dallo standard sia per garantire che il PAN venga stampato mascherato sulla ricevuta.

Referenze PCI PED

- Lista dei PED approvati dal PCI Council: https://www.pcisecuritystandards.org/security_standards/ped/pedapprovallist.html
- Linee guida per il programma di test e approvazione Testing and Approval Program Guide: https://www.pcisecuritystandards.org/security_standards/ped/download.html?id=10)

- **Requisiti di Sicurezza**
  - Encrypting PIN Pad Devices v2.1 https://www.pcisecuritystandards.org/security_standards/ped/download.html?id=22 https://www.pcisecuritystandards.org/security_standards/ped/download.html?id=23
  - Point of Sale Devices v2.1 https://www.pcisecuritystandards.org/security_standards/ped/download.html?id=26 https://www.pcisecuritystandards.org/security_standards/ped/download.html?id=27
  - Hardware Security Module (HSM) v1.0 https://www.pcisecuritystandards.org/security_standards/ped/download.html?id=47 https://www.pcisecuritystandards.org/security_standards/ped/download.html?id=46
  - Unattended Payment Terminals (UPT) v1.0 https://www.pcisecuritystandards.org/security_standards/ped/download.html?id=49 https://www.pcisecuritystandards.org/security_standards/ped/download.html?id=48
- **Questionari di Valutazione dei Vendor**
  - Encrypting PIN Pad Devices v2.1 https://www.pcisecuritystandards.org/security_standards/ped/download.html?id=32

    - Point of Sale Devices v2.1
      https://www.pcisecuritystandards.org/security_standards/ped/download.html?id=36
    - Hardware Security Module (HSM) v1.0
      https://www.pcisecuritystandards.org/security_standards/ped/download.html?id=51
    - Unattended Payment Terminals (UPT) v1.0
      https://www.pcisecuritystandards.org/security_standards/ped/download.html?id=53
      https://www.pcisecuritystandards.org/security_standards/ped/download.html?id=52
- **FAQs**
    - General Frequently Asked Questions
      https://www.pcisecuritystandards.org/pdfs/PCI_PED_General_FAQs.pdf
    - Technical Frequently Asked Questions 2.0
      https://www.pcisecuritystandards.org/pdfs/pci_ped_tecnical_faqs.pdf

2 Payment Card Industry Data Security Standard (PCI-DSS)

Entreremo ora nel dettaglio della normativa PCI-DSS, preoccupandoci di trattare aspetti legati all'ambito di applicazione e al rapporto fra le entità coinvolte, di fare riferimento alla struttura dello standard anche prendendo in considerazione l'attività da svolgere per la certificazione, oltre ad approfondire alcuni dei requisiti che richiedono una maggiore attenzione perché facilmente sono sottovalutati e, infine, di fornire qualche chiarimento puntuale così come anche fa il PCI Council in merito ad alcuni requisiti molto discussi.

2.1 Ambito

A chi si applica la PCI? A qualunque società che tratta carte di pagamento per l'accettazione di trasferimenti di fondi, che trasmette o memorizza dati delle carte di pagamento dei brand fondatori. Innanzitutto è fondamentale chiarire che quando si parla di carte di pagamento, ci si riferisce sempre al Primary Account Number (PAN, in seguito anche denominato "dato di titolare di carta"[6] come indicato nello standard). Qualunque altro dato è irrilevante se non associato al PAN, qualunque altro dato diventa rilevante quando è associato al PAN. È quindi ovvio che attorno ad esso è concentrata tutta la normativa.

Prima di farsi scoraggiare da questa definizione, è fondamentale sottolineare che la normativa non si applica a tutta un'azienda in modo indiscriminato, ma che è bensì possibile limitare l'impatto attraverso una accurata delimitazione dell'applicabilità dello standard, detto anche ambito. Questo è il primo passo fondamentale da effettuare prima di avventurarsi in ulteriori analisi e, soprattutto, prima di investire denaro in operazioni di messa in conformità. I metodi principali per limitare l'ambito sono sostanzialmente due:

- segmentazione di reti attraverso l'uso di strumenti quali, Firewall o combinazioni di Access Control Lists (ACLs) e segmentazione di tipo VLAN (vedi paragrafo 2.4.1);
- crittografia di tipo punto-punto del dato in transito (vedi paragrafo 2.5.2).

2.2 Obiettivi

Come già si evince dalla storia di PCI-DSS, lo scopo primario dello standard è diminuire le frodi che coinvolgono i dati delle carte di pagamento, sia nel numero sia nell'impatto. Questo fattore è giustamente visto dai brand come strettamente legato alla fiducia che i titolari delle carte ripongono nel loro uso per effettuare transazioni monetarie quotidiane: i clienti saranno più propensi a fare un uso consistente delle carte sapendo che queste sono strumenti sicuri (e gestiti in modo sicuro), non venendo bombardati da notizie inerenti nuove compromissioni dei dati di milioni di carte ad opera di criminali più o meno organizzati, come troppo spesso ad oggi succede.
Un contesto più positivo verso l'uso delle carte di pagamento sarà ovviamente proficuo per gli stessi brand ma anche per le banche e, in ultima analisi, per gli stessi Merchant, a maggior ragione se raggiungibili prevalentemente attraverso il commercio elettronico.

2.3 Struttura

Lo standard si preoccupa di coprire tutti gli aspetti dell'attività di un'azienda definendo sia aspetti tecnici (ad esempio che cosa si intende con rete wireless) sia aspetti relativi alla

[6] Traduzione letterale della denominazione inglese "card holder data", solitamente indicata con l'acronimo CHD.

certificazione quali campionatura e controlli compensativi, che verranno trattati nel paragrafo 2.11.

In generale è importante sottolineare che la PCI-DSS richiede un certo lavoro di interpretazione al fine di determinare l'intenzione di un determinato controllo. Per questo vengono certificate delle persone (i QSA, vedi paragrafo 4.1.1) che possono aiutare a determinare la conformità con la normativa. È per questo motivo che non bisogna prendere certe terminologie alla lettera.

I sei paragrafi successivi e i rispettivi sotto-paragrafi corrispondono alle sei macro-aree che costituiscono la PCI-DSS. Nel seguito ci preoccuperemo di descrivere l'intenzione del PCI Council, più che entrare nel dettaglio ogni controllo.

- **Sviluppo e gestione di una rete sicura**, per una maggiore sicurezza dell'infrastruttura sulla quale i dati dei titolari delle carte transitano o sono memorizzati.
- **Protezione dei dati dei titolari delle carte**, per un maggior controllo su come e quali dati sono memorizzati.
- **Manutenzione di un programma per la gestione delle vulnerabilità**, perché il codice che viene sviluppato internamente sia più sicuro e affinché le applicazioni in uso vengano mantenute aggiornate al fine di proteggere i dati.
- **Implementazione di rigide misure di controllo dell'accesso**, per un miglior controllo sull'accesso a tali dati (chi, quando...) sia logico che fisico (aree sensibili).
- **Monitoraggio e test regolari delle reti**, poiché tutti i controlli si rivelano inutili se nessuno effettua un monitoraggio accurato ed una revisione dei log.
- **Gestione di una normativa per la sicurezza delle informazioni**, affinché tutto il lavoro per il raggiungimento della conformità non sia uno sforzo "occasionale" ma parte di un'attività strutturata e regolamentata.

Quando un'azienda si trova di fronte alla necessità di verificare la conformità alla normativa, deve dimostrarla rispetto a tutti i punti che la costituiscono. È alquanto frequente trovarsi in situazioni in cui non tutti questi punti sono applicabili; ad esempio sono tante le aziende in cui non c'è sviluppo di applicazioni che poi vengono utilizzate in ambiente PCI. In questo caso la conformità viene confermata dal QSA che indicherà nel proprio rapporto che l'azienda è conforme alle normative per lo sviluppo software in quanto "Non Applicabile", dovendo poi giustificare come tale conformità è stata determinata.

2.4 Sviluppo e gestione di una rete sicura

La PCI-DSS si apre trattando quelli che, storicamente, sono stati gli aspetti più trascurati nei casi accertati di frode. Si parla infatti di configurazione sicura di una rete tramite accorgimenti a livello di settaggi dei dispositivi e della rimozione forzata di valori di default facilmente attaccabili.

2.4.1 Requisito 1: Installare e gestire una configurazione firewall per proteggere i dati dei titolari delle carte

Un firewall propriamente configurato è certamente il primo passo verso una segmentazione che permetta di circoscrivere l'ambito al quale la PCI-DSS si applica, di determinare quali connessioni sono ammesse e tramite quali protocolli.

Nella maggioranza dei casi le aziende hanno delle discrete procedure per decidere se una porta e un protocollo possono essere autorizzati a passare attraverso i/il firewall, ma poi non

hanno niente per determinare quando invece porte e protocolli devono nuovamente essere disabilitati. Il risultato è una situazione di "colabrodo" che rende la funzionalità di protezione dello strumento inutile.

Lo scopo primario di questa sezione, quindi, è quello di indurre le società a strutturare i propri processi non soltanto per quanto riguarda la creazione di certe configurazioni, ma anche per il loro mantenimento ed eliminazione.

Si parla quindi di regole e di firewall e router, del mantenimento di un diagramma di rete aggiornato; la normativa entra quindi nel dettaglio di alcune configurazioni, con controlli che si potrebbero anche definire come best practice (ad esempio le regole devono avere un approccio del tipo "vieta tutto se non esplicitamente permesso" anziché il contrario).

Una prima osservazione va fatta in quanto nella normativa viene esplicitamente citato il concetto di firewall, ma nella realtà vengono accettate configurazioni combinate di Access Control Lists (ACLs) e Virtual LAN (VLAN) che permettono di implementare esattamente lo stesso livello di segmentazione della rete, separando a livello logico i sistemi che trattano dati delle carte dagli altri. Questo significa che è possibile ridurre l'ambito al quale si applica la normativa anche senza investire in ulteriori firewall per creare una segmentazione interna (è ovvio che i firewall verso il mondo esterno devono esistere comunque) ma si può semplicemente lavorare sulla configurazione dei propri switch e router al fine di raggiungere lo stesso scopo.

Un'altra osservazione va rivolta alle reti wireless. In generale il PCI Council preferisce che queste non vengano utilizzate (viene infatti esplicitamente fatto l'invito a limitare l'uso di connessioni wireless per dati non rilevanti ai fini PCI, ossia tutto tranne il PAN). Recentemente il PCI Council ha pubblicato a questo proposito un documento per i Merchant al fine di aiutarli nella corretta implementazione delle reti wireless ("PCI SSC Wireless Guidelines" - https://www.pcisecuritystandards.org/pdfs/PCI_DSS_Wireless_Guidelines.pdf). Qualora non si potesse o volesse evitare la trasmissione del PAN via wireless occorre prendere delle precauzioni principalmente sotto due aspetti:

- nei punti di connessione tra rete wireless e rete cablata occorre inserire un firewall;
- la trasmissione deve utilizzare una crittografia con chiave forte (ad esempio WPA/WPA2); si consiglia fortemente di utilizzare una crittografia punto-punto, in aggiunta a quella wireless, al fine non ultimo di ridurre ulteriormente l'ambito di applicabilità della normativa (vedi paragrafo 2.5.2).

2.4.2 Requisito 1.4

"Installazione di firewall personali (software) su tutti i computer portatili e i computer di proprietà dei dipendenti (ad esempio, i laptop dei dipendenti) che possono connettersi direttamente a Internet e che vengono utilizzati per accedere alla rete dell'organizzazione."

A prima vista questo punto non sembra particolarmente complesso; ci sono però alcuni aspetti da evidenziare al fine di comprenderne l'impatto:

- il requisito fa riferimento anche a computer di proprietà dei dipendenti. Questo significa che se per la gestione di certe situazioni critiche è stato creato un meccanismo che

permette ad un amministratore di connettersi da remoto usando un portale web, il sistema utilizzato per la connessione deve avere un personal firewall;
- le soluzioni di tipo personal firewall, AV e similari devono tutte essere protette dalla modifica e dalla disattivazione oltre che centralmente gestite. Di conseguenza se un utente è amministratore di una macchina (come normalmente lo è della propria a casa) questo tipo di configurazione non è più così semplice;
- questo tipo di configurazione non è necessariamente comune, ma il fatto che l'utente sia amministratore della propria postazione di lavoro è alquanto comune e ripropone il problema dell'immodificabilità dei meccanismi di sicurezza. Se questa casistica non può venire modificata, può essere necessario valutare l'applicazione di controlli compensativi.

2.4.3 Requisito 2: Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di protezione

Le statistiche ancora oggi ci mostrano come in molti casi chi attacca una rete abbia successo semplicemente connettendosi con account e password di default. Nel paragrafo 2.7.2 saranno trattati gli aspetti legati al concetto di non-ripudio; in questo capitolo la normativa si limita a vietare l'utilizzo di configurazioni di default nell'infrastruttura in ambito. Vengono citate esplicitamente le reti wireless, ma anche il protocollo SNMP (attraverso il quale un attaccante[7] può identificare ogni singolo sistema connesso alla rete) e all'uso di standard di hardening dei sistemi facendo riferimenti ad organizzazioni note quali SANS, NIST[8] e CIS[9].

In questo gruppo di controlli, la normativa include anche un requisito per cui tutti i servizi e protocolli insicuri e non necessari siano disabilitati. Oltre a questo è inoltre richiesto che un server abbia un solo compito primario. Questo significa che non si può certificare un'azienda che ha sullo stesso sistema DNS e Web Server, oppure Web e Database Server. La domanda che sorge spontanea è relativa al ruolo della virtualizzazione: come può un server ricoprire un solo compito quando su di esso si possono avere varie decine di sistemi virtuali? La risposta è semplice, la normativa si riferisce ad un server come ad una macchina virtuale e non ad una macchina fisica. Le macchine virtuali (così come già visto per le reti virtuali) possono quindi essere utilizzate tranquillamente con qualche accorgimento aggiuntivo:

- ogni interfaccia fisica di rete deve essere allocata al più ad una macchina virtuale in modo da evitare incidenti di percorso (in senso letterale) del traffico;
- ogni macchina virtuale svolge un solo compito primario;
- la sincronizzazione degli orologi viene fatta direttamente attraverso il protocollo NTP con dei server centrali e non attraverso l'orologio del server di virtualizzazione (vedi paragrafo 2.8.1).

Al momento della stesura del presente Quaderno, il PCI Council sta valutando l'adozione di linee guida e requisiti più dettagliati in materia di virtualizzazione.

[7] Si è in questa sede utilizzato il termine "attaccante" per definire l'azione di un soggetto malintenzionato, di ben diversa natura da quella di un "hacker".

[8] http://web.nvd.nist.gov/view/ncp/repository

[9] http://cisecurity.org/benchmarks.html

2.5 Protezione dei dati di titolari delle carte

Oltre agli aspetti legati alla normativa sulla privacy, che già obbliga le aziende a trattare i dati personali in modo particolare, la PCI-DSS si preoccupa di richiedere di proteggere con particolare cura il PAN.

2.5.1 Requisito 3: Proteggere i dati di titolari delle carte memorizzati

Il primo controllo è indubbiamente quello che le aziende dovrebbero cercare di soddisfare al più presto: ridurre al minimo la necessità di memorizzare il PAN. E' vero che a volte può tornare comodo (e talvolta anche sicuro) avere più di una copia del dato ma è fondamentale fare delle considerazioni in merito legate al rapporto tra costi e benefici in quanto ogni copia deve essere protetta adeguatamente, allargando l'ambito di applicazione di PCI-DSS ai sistemi, ai supporti e agli ambienti in cui è trattata.

Mentre per tutti i requisiti dello standard esiste la possibilità (magari non la convenienza) di utilizzare i controlli compensativi (vedi paragrafo 2.11), questo capitolo della PCI-DSS contiene l'unico requisito che non può avere controlli compensativi:

> ***3.2*** *Non conservare i dati sensibili per l'autenticazione dopo l'avvenuta autorizzazione, neppure se cifrati.*

Per quanto concerne il PAN, esistono quattro meccanismi principali utilizzabili per il suo mascheramento:

1. Funzione di hash unidirezionale. Poiché l'algoritmo è unidirezionale, il valore risultante può essere utilizzato come identificatore univoco di tutte le operazioni legate a quella carta di credito, senza però avere tutti gli oneri derivanti dall'avere un valore che si può ricondurre al PAN originale.
2. Troncatura di tipo 6/4 (e.g. 1234 56** **** 1234). In questo caso nuovamente non è possibile ricostruire il PAN originale e quindi si rimuovono tutti gli oneri associati alla gestione del PAN. Questo metodo è molto efficace perché la probabilità che una persona abbia due carte dello stesso brand con le stesse cifre dopo la troncatura che possano quindi essere confuse, è estremamente bassa, così bassa che è trascurabile ai fini operativi di un'azienda.
3. La sostituzione del PAN con dei token indicizzati (processo noto anche come "tokenizzazione"), i quali sono a loro volta associati al PAN in un database separato o, equivalentemente, l'uso di valori di one-time-pad, chiavi crittografiche ad uso unico lunghe quanto il PAN, gestite in maniera sicura.
4. La crittografia con algoritmo di cifratura forte, dove per "forte" si intende un algoritmo resistente alla crittanalisi con chiavi simmetriche da almeno 80 bit o con chiavi asimmetriche da almeno 1024 bit. In questo caso il PAN viene sì memorizzato in modo sicuro, ma è anche necessario validare il processo di gestione delle chiavi di crittografia.

	Elemento di dati	Memorizzazione Consentita	Protezione Richiesta	Req. 3.4 PCI-DSS
Dati di titolari delle carte	PAN (Primary Account Number	Sì	Sì	Sì
	Nome titolare di carta[10]	Sì	Sì[10]	No
	Codice di servizio[10]	Sì	Sì[10]	No
	Data di scadenza[10]	Sì	Sì[10]	No
Dati sensibili di autenticazione[11]	Dati completi della banda magnetica[12]	No	N/A	N/A
	CAV2/CVC2/CVV2/CID	No	N/A	N/A
	PIN/Blocco PIN	No	N/A	N/A

Tabella 1 – Dati sensibili e loro memorizzazione (sommario)

Qualora si dovesse ricorrere alla crittografia, la gestione delle chiavi è un aspetto da porre sotto dettagliata analisi; deve essere infatti implementata e documentata una gestione delle chiavi di cifratura che garantisca l'efficacia di questa tecnologia per nascondere il dato a chi non ha necessità di decifrarlo. Vi sono diversi aspetti interessanti da ricordare:

- separazione delle responsabilità: una sola persona non può avere il controllo di tutti i meccanismi di crittografia;
- si può utilizzare un meccanismo con doppia crittografia; ad esempio si può usare una chiave (key encrypting key - KEK) per crittografare la chiave di crittografia dei dati. In una situazione come questa può essere sufficiente modificare con cadenza annuale la chiave KEK e non quella di crittografia del dato, permettendo quindi una continuità di leggibilità nel tempo;
- la crittografia può essere a livello del disco. In questo caso, è necessario ricordarsi che non è accettabile l'uso di una crittografia legata al sistema o agli account locali. Quello che si vuole ottenere, sostanzialmente, è la necessità di una doppia autenticazione; di conseguenza, la situazione di un utente che effettua un login e ha direttamente accesso ai dati sensibili non è accettabile, anche se si tratta di crittografia forte.

2.5.2 Requisito 4: Cifrare i dati di titolari delle carte trasmessi su reti aperte e pubbliche

In questo paragrafo viene ribadita l'importanza di rendere sicura la trasmissione del dato su reti wireless (ricordiamo che questo fu la via d'accesso per l'attacco a TJX e che quindi il PCI Council è particolarmente sensibile a questo argomento), di renderla sicura sulle reti pubbliche e di non trasmettere mai in chiaro il PAN via email. Nella sostanza, quello che si denota in questi requisiti è la volontà di forzare la crittografia laddove il dato si trovi in zone liberamente accessibili. Da notare che lo standard considera reti pubbliche tutte le reti che possono essere accedute o "viste" dall'esterno; sono quindi considerate reti pubbliche ed

[10] Questi elementi devono essere protetti se memorizzati assieme al PAN.

[11] I dati sensibili di autenticazione non devono essere memorizzati dopo l'autorizzazione anche se cifrati.

[12] Dati della traccia completa della banda magnetica, dell'immagine della banda magnetica sul chip o in altra posizione.

aperte tutte le connessioni wireless, GPRS/UMTS, bluetooth, linee satellitari ed in genere tutte le reti che possono essere intercettate senza dover essere fisicamente presenti all'interno dell'azienda.

Nuovamente, particolare attenzione viene dedicata alle reti wireless per le quali è richiesta una forma di crittografia forte anche nel caso di reti private. In particolare:

- per le nuove implementazioni wireless, non è consentito adottare la tecnologia WEP dopo il 31 marzo 2009;
- per le implementazioni wireless già in produzione, non è consentito continuare ad utilizzare la tecnologia WEP dopo il 30 giugno 2010.

Queste indicazioni sono giustamente corroborate dalle debolezze scoperte nell'algoritmo WEP a partire dal 2001, le quali l'hanno reso facilmente aggirabile senza necessità di strumenti o capacità di alto livello. Visti i recenti sviluppi sul fronte della ricerca delle vulnerabilità[13], è probabile che il PCI Council inserisca a breve delle raccomandazioni similari in merito al WPA/PSK, suggerendo l'uso di soluzioni basate sul WPA2.

E' importante sottolineare come la crittografia possa essere utilizzata non solo per rendere illeggibile il dato su reti aperte o pubbliche, ma anche come essa possa supportare un isolamento dell'ambiente PCI dal resto dell'infrastruttura IT anche nell'ambito aziendale. Un esempio: supponiamo che il dato sensibile venga trasferito da un computer A situato nell'area dell'Help Desk a un server B situato nell'area server, il tutto all'interno della rete aziendale. Se questo dato viene trasmesso in chiaro tutti i sistemi che hanno accesso alla rete sono in ambito PCI; rientrano quindi tutti gli switch, router, firewall, e tutte le LAN non separate attraverso segmentazione opportuna. Se, invece, il dato viene crittografato sul computer A e solo il server B è in grado di riportarlo in chiaro per l'elaborazione, tutti i sistemi di supporto (switch, router...) e le LAN si possono considerare come separate e non da considerare per la conformità PCI. Si ricorda che l'ultima parola è del QSA certificante e questo esempio va inteso come linea guida di riferimento.

2.6 Manutenzione di un programma per la gestione delle vulnerabilità

Le vulnerabilità sono definite dal PCI Council come "*punti deboli in un sistema che consentono a un utente non autorizzato di sfruttare quel sistema e violarne l'integrità*" e PCI-DSS rientra nella ristretta cerchia delle norme che cercano di definire e utilizzare in pratica questo oggetto.

2.6.1 Requisito 5: Utilizzare e aggiornare regolarmente il software antivirus

Questo requisito, nonostante la sua brevità, è spesso oggetto di discussione perché esistono alcuni aspetti lasciati al giudizio del QSA e per i quali non è possibile dare una risposta sempre vera in quanto il contesto dell'azienda da certificare non è noto a priori:

1. *"5.1 Distribuire il software antivirus su tutti i sistemi comunemente colpiti da malware (in particolare PC e server)."* Praticamente ad ogni certificazione viene ridiscusso cosa vuol dire 'comunemente colpiti' da malware: un server in DMZ è potenzialmente più esposto di uno nel data center, alcuni sistemi operativi sono statisticamente più esposti di altri mentre alcuni non lo sono quasi. Tutti questi elementi devono essere presi in considerazione in modo da poter poi determinare la conformità.
2. *"5.1.1 Garantire che tutti i programmi antivirus siano in grado di rilevare e rimuovere tutti i tipi di malware nonché garantire una protezione sicura."* Anche in questo caso

[13] http://www.theregister.co.uk/2009/08/28/wpa_60sec/

troviamo argomenti di discussione: cosa significa 'tutti' i tipi di malware? E' accettabile una soluzione che previene l'installazione di malware ma che non è in grado di rimuoverlo? Come già ricordato in precedenza si deve sempre tenere a mente lo scopo del requisito più che guardare alla lettera la sua formulazione.

Vale la pena considerare che, in linea di massima, le principali suite antivirus, correttamente installate, impostate e mantenute, offrono un livello di protezione accettabile rispetto a questi requisiti. Restano in questo ambito valide le considerazioni già effettuate in merito ai firewall personali e all'impossibilità per gli utenti di disattivarli (vedi paragrafo **Errore. L'origine riferimento non è stata trovata.**).

2.6.2 Requisito 6: Sviluppare e gestire sistemi e applicazioni protette

Siccome le vulnerabilità sono la principale via di accesso per il codice malevolo e per gli attacchi, in questa sezione la PCI-DSS si occupa degli aspetti legati alla rimozione di tali vulnerabilità.

Innanzitutto viene richiesto alle aziende che tutte le patch critiche di sicurezza vengano installate entro un mese dal rilascio. Questo è un requisito che molto spesso le aziende hanno difficoltà a soddisfare. Lo standard concede esplicitamente la possibilità di distinguere fra infrastruttura critica e non critica e di estendere per quest'ultima a 3 mesi la finestra di installazione delle patch. Rimane il fatto che un mese è un tempo molto ridotto soprattutto se si prendono in considerazione le necessità di validazione delle patch, i periodi di congelamento dello status quo (solitamente in dicembre), etc. Molto spesso è necessario considerare controlli compensativi (quali l'uso di soluzioni di Intrusion Prevention) al fine di soddisfare questo requisito.

Per quanto riguarda lo sviluppo del software, questo requisito è assolutamente fondamentale per le aziende che sviluppano in casa applicazioni che vengono utilizzate per trattare dati di carte di credito. I concetti di base che vengono elencati qui sono semplici concettualmente ma non sempre di facile realizzazione. I più importanti da elencare sono:

- Separazione:
  - degli ambienti di sviluppo/test e di produzione;
  - delle responsabilità tra gli ambienti di sviluppo/test e di produzione.

  Questo è particolarmente difficile quando il team di sviluppo non è molto grande. La separazione, in particolare di responsabilità, può essere ottenuta anche con controlli compensativi.
- Nessun dato di produzione (PAN attivi) può essere usato come dato di test. Probabilmente la più antipatica delle clausole, soprattutto per gli sviluppatori che 'amano' effettuare test con i dati reali.

2.6.3 Requisito 6.4

"Seguire le procedure di controllo delle modifiche per tutte le modifiche da apportare ai componenti di sistema"

Questo requisito e quelli ad esso legati si incentrano sulla gestione dei cambiamenti, con particolare riguardo per quelli software. É richiesto che tutte le modifiche apportate al software che gestisce i dati delle carte di pagamento siano adeguatamente documentate, testate e approvate prima di passare in produzione, dove potrebbero altrimenti inserire in modo inaspettato nuove vulnerabilità di sicurezza. Da notare che anche le patch dei fornitori di software, esterne al processo di sviluppo interno, sono considerati dei cambiamenti che rientrano in questi requisiti.

2.6.4 Requisito 6.5

"Sviluppare tutte le applicazioni Web (interne, esterne e con accesso amministrativo all'applicazione tramite Web) in base alle linee guida di programmazione sicura, quali Open Web Application Security Project Guide (OWASP: http://www.owasp.org).

Nota: le vulnerabilità elencate dal punto 6.5.1 al punto 6.5.10 erano presenti nella guida OWASP al momento della pubblicazione degli standard PCI-DSS v1.2. Tuttavia, in caso di aggiornamento della guida OWASP, è necessario utilizzare la versione più recente per questi requisiti."

OWASP è un riferimento sempre più importante per quanto concerne la sicurezza delle applicazioni web ma al suo interno include numerosi sotto-progetti, una buona parte dei quali sono rivolti all'individuazione di vulnerabilità applicative. Le guide che forniscono le indicazioni più importanti per le finalità di PCI-DSS, ovvero per la scrittura di codice sicuro, sono la Development Guide (http://www.owasp.org/index.php/Category:OWASP_Guide_Project), la Top Ten Guide (http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project) e infine la CLASP (http://www.owasp.org/index.php/Category:OWASP_CLASP_Project).

Ulteriori approfondimenti in merito si possono trovare nel paragrafo 3.3.4.

I punti focali per la soddisfazione di questo requisito sono l'esistenza di processi formalizzati di sviluppo del software, inclusivi delle necessarie fasi di sicurezza, e un'adeguata formazione e sensibilizzazione in materia del personale addetto allo sviluppo.

2.6.5 Requisito 6.6

"Per le applicazioni Web rivolte al pubblico, assicurare una protezione costante da nuove minacce e vulnerabilità e garantire che queste applicazioni siano protette da attacchi noti mediante uno dei seguenti metodi:

- *Analisi delle applicazioni Web rivolte al pubblico tramite strumenti o metodi di valutazione della sicurezza delle applicazioni manuali o automatici, almeno una volta all'anno e dopo ogni modifica*
- *Installazione di un firewall per applicazioni Web davanti alle applicazioni Web rivolte al pubblico"*

Le applicazioni Web rivolte al pubblico richiedono particolare attenzione e poiché sono quelle che più spesso sono attaccate. Lo scopo di questo requisito è quello di fornire le linee guida per la protezione dei dati che vengono trattati dalle applicazioni.

- è sufficiente utilizzare uno dei due modi indicati dal requisito. Spesso le aziende hanno la sensazione di doverle soddisfare entrambe, ma non è quanto richiesto dalla norma. E' anche vero che un Web Application Firewall (WAF) potrebbe costituire una valida soluzione temporanea mentre si effettua la prima analisi delle applicazioni Web;
- "*dopo ogni modifica*" si riferisce alle modifiche relative al codice che tratta i dati di carte di credito e non ogni singola modifica (ad esempio un parametro nell'interfaccia grafica irrilevante per la PCI). Questo aspetto può essere legato al Requisito 6.4;
- "*da un'organizzazione specializzata in sicurezza delle applicazioni*" in modo da garantire una maggiore obiettività e precisione dell'analisi. Da notare che è

giustamente richiesto che ci sia una successiva valutazione della corretta chiusura delle eventuali vulnerabilità individuate;
- esistono soluzioni che combinate possono fornire la stessa (se non migliore) protezione dell'applicazione di quanto non offra un WAF. Prima di acquistare ed implementare soluzioni diverse si consiglia di analizzare con il proprio QSA le opzioni a disposizione.

Il requisito 6.6 è uno dei più dibattuti e, al fine fornire maggiore chiarezza, il PCI Council ha pubblicato un documento che può essere trovato seguendo questo link: https://www.pcisecuritystandards.org/pdfs/italian_infosupp_6_6_applicationfirewalls_codereviews.pdf.

2.7 Implementazione di rigide misure di controllo dell'accesso

Uno dei più importanti principi sul quale la PCI-DSS insiste è limitare l'accesso, sia in senso fisico che elettronico, all'informazione relativa alle carte di credito solo alle persone che ne hanno necessità sulla base delle loro mansioni. Questo accesso deve poi essere strettamente monitorato in modo da poter ricostruire ad ogni momento chi ha avuto accesso a cosa.

2.7.1 Requisito 7: Limitare l'accesso ai dati di titolari delle carte solo se effettivamente necessario

Due gli aspetti fondamentali di questa sezione. Il primo è quello di limitare l'accesso ai componenti di sistema e ai dati di titolari delle carte solo alle persone per le cui mansioni è realmente necessario. Ad esempio, mentre l'amministratore di una banca dati (DBA) sicuramente ha bisogno di avere accesso al sistema su cui la stessa è installata, e alle relative configurazioni, non ha nessuna necessità di avere accesso ai dati contenuti, in particolare a quelli relativi alle carte di credito e questo va quindi impedito.

Il secondo è quello di stabilire un sistema di controllo dell'accesso per i componenti di sistema con utenti multipli che limiti l'accesso in base all'effettiva esigenza di un utente. Non tutti gli utenti che hanno necessità di accedere ai dati hanno necessità di effettuare le stesse operazioni; ad esempio esistono situazioni in cui gli operatori di primo livello di un call center hanno soltanto diritto di accesso in lettura per verificare i dati assieme ai clienti che chiamano, mentre quelli di secondo livello hanno anche diritto di modifica per correggere gli errori che potrebbero evidenziarsi.

2.7.2 Requisito 8: Assegnare un ID univoco a chiunque abbia accesso a un computer

La gestione degli ID ha un ruolo di particolare rilevanza nella PCI-DSS poiché innumerevoli sono stati i casi accertati di aziende che non avevano un processo in essere per la loro corretta gestione.

Innanzitutto viene richiesto che ogni utente abbia un ID personale. Non è quindi accettabile che utenti utilizzino account generici come "Administrator" o "root" (comunque da evitare come richiesto dal Requisito 2: Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di protezione), ma nemmeno account di gruppo come "Helpdesk" oppure "Operatore" che non identifichino l'utente in modo univoco.

Esistono situazioni in cui questa richiesta non può essere soddisfatta: un controllo compensativo che può essere utilizzato è quello di utilizzare come login un ID generico, ma bloccare il sistema finché non ha letto un diverso identificatore univoco (ad esempio un badge, una smart card, una chiave USB, ecc). Questo tipo di soluzione è stata implementata con successo ad esempio per identificare l'operatore di cassa, l'operatore di helpdesk, etc.

Una richiesta particolare viene fatta per l'accesso remoto ai sistemi contenenti informazioni relative a carte di credito: l'autenticazione a due fattori. Esistono tre categorie di fattori:

1. qualcosa che conosco: password o passphrase;
2. qualcosa che ho: token, smart card.
3. qualcosa che sono: impronta digitale, iride.

Quando si richiedono due fattori, questi devono appartenere a due diverse categorie; non è quindi accettabile un'autenticazione in cui si devono digitare due password diverse per due ID diversi, poiché entrambi appartengono alla prima categoria.

Una lunga serie di requisiti è dedicata alla corretta autenticazione degli utenti e alla gestione delle password. Leggendo quanto richiesto dallo standard si è indotti a pensare che tutto sia naturale e ovvio; nella realtà esistono molti punti che non sono implementati correttamente nelle aziende perché non se ne vede il beneficio, o, forse, è più corretto dire che non si conoscono i rischi. Alcuni esempi:

- *"Verificare l'identità dell'utente prima di eseguire il ripristino delle password."* Spesso nelle aziende chi è all'helpdesk 'riconosce la voce', o formula sempre le stesse domande. L'identità di chi richiede il reset della password deve essere verificata in modo certo così come viene effettuato dagli istituti di credito quando si telefona per verificare i dati finanziari.
- *"Revocare immediatamente l'accesso per gli utenti non attivi."* Questo si rivolge ad utenti che non lavorano più in azienda; se la gestione non è centralizzata spesso rimangono account attivi in applicazioni che nessuno si ricorda di disabilitare.
- *"Rimuovere/disabilitare gli account utente non attivi almeno ogni 90 giorni."* Spesso le aziende non sono (o non erano) in grado di verificare quali utenti non erano attivi e per quanto tempo. Questo punto e quello precedente sono strettamente legati e sovente la soluzione dell'uno ha permesso la soluzione anche dell'altro.
- *"Abilitare gli account utilizzati dai fornitori per la gestione in remoto solo durante il periodo di tempo necessario."* I fornitori non devono poter accedere come e quando vogliono; il loro accesso deve essere programmato, giustificato e documentato. L'unico modo per ottenere questo livello di audit è mantenere gli account disabilitati in modo da forzare un processo di controllo nel momento del bisogno.
- *"Modificare le password utente almeno ogni 90 giorni."* Per molte aziende questo comporta un cambiamento importante perché impatta anche le risorse di helpdesk. E' importante ricordare e sottolineare che si tratta di tutte le password utente, anche di quelle con diritti di amministratore e anche quelle applicative.
- *"Autenticare tutti gli accessi al database contenente i dati di titolari delle carte. Sono compresi gli accessi da applicazioni, amministratori e tutti gli altri utenti."* A sottolineare che tutte le attività di accesso devono essere autenticate e tracciate; non si parla solo dell'utente 'semplice' ma anche degli amministratori e delle applicazioni.

2.7.3 Requisito 9: Limitare l'accesso fisico ai dati dei titolari delle carte

Naturalmente l'accesso ai dati elettronici non è l'unico da monitorare; l'accesso fisico ai sistemi contenenti le informazioni, o alle informazioni stesse, necessita esattamente dello stesso livello di attenzione. L'attenzione alla sicurezza fisica non giunge certo come una novità: molte aziende già hanno dei sistemi di monitoraggio ed, in alcuni casi, questi si rivelano addirittura essere già sufficienti al fine della conformità PCI. Esistono inoltre tecnologie per la sicurezza fisica che funzionano su IP e che possono contribuire validamente alla conformità rispetto a questo punto, offrendo talvolta una diretta integrazione con il database degli utenti dei sistemi informativi.

È necessario avere un sistema di monitoraggio (videocamere o altri meccanismi di controllo) dell'accesso ad aree sensibili. *Nota: per 'aree sensibili' si intendono centri elaborazione dati, aree server e aree che ospitano sistemi di memorizzazione, elaborazione o trasmissione dei dati di titolari delle carte. Ciò esclude le aree in cui vi sono i terminali dei punti vendita, ad esempio la cassa nei negozi di vendita al dettaglio e i POS. Con la versione 1.2 della PCI-DSS è stata introdotta l'opzione dei altri meccanismi di controllo che aiutano molto le aziende a raggiungere la conformità in quanto installare un sistema di videocamere può diventare un investimento economico di tutto rispetto e non sempre è consentito dalla legge.*

All'interno delle aree sensibili, deve essere possibile distinguere facilmente i dipendenti dai visitatori. Questo solitamente si ottiene attraverso l'esposizione obbligatoria di un badge. Con 'dipendenti' si intendono sia i dipendenti veri e propri sia i consulenti o collaboratori che svolgono un'attività regolare presso l'azienda. Con 'visitatori' si intendono tutte quelle persone che accedono alla struttura in modo saltuario e normalmente per non più di un giorno. Resta inteso che ogni azienda ha una propria definizione (ad esempio il QSA è solitamente un visitatore anche se può essere presso un'azienda anche due settimane consecutive) ed è sufficiente che il meccanismo di identificazione funzioni.

Deve poi essere presente la tracciabilità di tutta l'attività del visitatore: l'autorizzazione all'accesso, l'accesso stesso, un badge (o token fisico come riporta la normativa) con scadenza, la restituzione del badge all'uscita per evitare che si possa rientrare successivamente in modo non autorizzato.

Ai visitatori non deve essere infine consentito l'accesso non autorizzato alla rete, proteggendo adeguatamente i connettori o scortando i visitatori in modo costante.

Un punto su quale le aziende devono spesso lavorare è quello della classificazione ed etichettatura (labeling) delle informazioni. In particolare, ogni supporto contenente dati di titolari delle carte deve essere classificato come riservato, in modo che sia chiaro a tutti che deve essere trattato secondo particolari attenzioni, opportunamente esplicitate. Questo è importante anche perché serve ad informare i corrieri che la loro attività verrà monitorata (un po' come si fa nel passaggio di consegna di prove legali affinché non vengano manipolate). Poiché i backup devono essere riposti in luogo sicuro e, preferibilmente, in una struttura esterna, se di dovesse fare uso di una terza parte bisogna richiedere un opportuno livello di sicurezza per il dato riservato.

Un aspetto che viene dato per scontato in quanto parte della normale attività aziendale è l'approvazione del management per lo spostamento da un'area protetta di ogni supporto contenente i dati dei titolari delle carte; quest'approvazione deve essere esplicita e deve accompagnare il supporto stesso.

L'ultima richiesta della normativa è legata alla distruzione sicura dei supporti contenenti i dati di titolari delle carte; per i supporti cartacei solitamente si possono usare distruggi documenti (quelle che riducono i documenti in frammenti, le strisce non sono sufficienti per la facilità con cui si possono riassemblare) o si possono inviare a società specializzate che li bruciano o li macerano. Per i supporti elettronici si può utilizzare la cancellazione sicura (riscrittura con un minimo di 3 passaggi) oppure si può distruggere il supporto sia con macchine che effettuano procedure di degaussing con apparecchiature speciali per dischi rigidi e nastri di backup.

2.8 Monitoraggio e test regolari delle reti

Ora che tutti i meccanismi di autenticazione e controllo sono stati posti, è naturale che venga chiesto di monitorare quanto accade al fine di non rendere inutile tutto lo sforzo fatto finora.

2.8.1 Requisito 10: Registrare e monitorare tutti gli accessi a risorse di rete e dati di titolari delle carte

La regola d'oro del tracciamento è che si deve sempre poter rispondere alla domanda: **chi** ha fatto **cosa**, **quando** e da **dove** ha agito. Non sempre tutto ciò è ottenibile da un unico sistema, e non è neanche richiesto, ma la combinazione delle registrazioni e log deve portare a questo risultato.

Tutti gli utenti hanno un ID unico, tutti gli accessi a dati o aree sensibili sono registrati, è necessario avere una procedura che permetta di collegare le due cose e quindi determinare chi ha avuto accesso e quando. Devono inoltre essere registrati i tentativi di accesso non validi, per vedere se qualcuno cerca ripetutamente di accedere ad informazioni di cui non è previsto abbia visibilità.

Naturalmente queste tracce (log) vanno a loro volta monitorate e protette, affinché non vengano manipolate. Esistono varie tecniche per ottenere questo risultato; viene comunque richiesto esplicitamente di fare immediatamente un backup dei log su un registro centralizzato e, per i server con servizi rivolti al pubblico, una copia su un sistema situato nella LAN interna.

I log devono essere:

- mantenuti per almeno un anno con i tre mesi più recenti disponibili per immediata analisi (quindi possibilmente on-line o facilmente recuperabili da backup);
- analizzati giornalmente; è naturale che vista la mole di dati che vengono creati quotidianamente non ci si aspetta che tale analisi sia manuale. A tale scopo possono essere utilizzati strumenti di raccolta, analisi e generazione di avvisi che lavorano in modo automatizzato ed in tempo reale.

Un elemento sempre abbastanza delicato da trattare è quello della sincronizzazione dei sistemi. E' logico che tutti i sistemi debbano essere sincronizzati se si vuole che la correlazione ed analisi dei log abbia un senso. I requisiti che vengono posti, però, rendono questa operazione un po' più complessa di come le aziende lo vorrebbero. Ecco le condizioni richieste:

- bisogna utilizzare una versione nota e stabile di NTP (Network Time Protocol) o una tecnologia simile. Questo significa che qualunque macchina virtuale esista non si può sincronizzare con un protocollo diverso attraverso il sistema che lo ospita, ma si deve sincronizzare direttamente con il server NTP (o simile);
- non tutti i server interni ricevono segnali orari da sorgenti esterne. Bisogna avere due o tre server (*Nota: uno solo non è sufficiente in quanto costituirebbe un "single point of failure"*) di rilevamento dell'orario, centrali all'interno dell'organizzazione, che ricevono segnali orari esterni da fonti autorevoli; questi due o tre server devono comunicare tra loro per mantenere un orario esatto e quindi condividerlo con i server interni.

La situazione è più complessa quando il sistema informativo non è tutto localizzato all'interno dell'azienda ma si fa uso di terze parti che forniscono servizi (ad esempio housing, hosting). Come linea guida, sempre da verificare con il proprio QSA, si può utilizzare quanto segue:

- se il service provider è certificato PCI ed effettua tutte le attività di monitoraggio in proprio, non è probabilmente necessario sincronizzare gli orologi dei sistemi aziendali con quelli del service provider;
- se invece il service provider non fornisce il servizio di monitoraggio e l'azienda deve collezionare i log anche dai sistemi localizzati presso terzi, è necessario sincronizzare gli orologi di tutti i sistemi, in modo da mantenere la consistenza e correlabilità dei log.

2.8.2 Requisito 11: Eseguire regolarmente test di sistemi e processi di protezione

Nel Requisito 6: Sviluppare e gestire sistemi e applicazioni protette, viene richiesto di installare le patch di sicurezza entro un mese dalla loro pubblicazione. Di pari passo è necessario eseguire dei test di rete per identificarne i punti deboli.

Come già menzionato, una particolare attenzione è stata data alle reti wireless. Oggigiorno è estremamente semplice per chiunque installare una rete wireless; spesso questo succede perché si ignorano le conseguenze e i pericoli che ne conseguono. È quindi richiesto alle aziende di verificare la presenza di punti di accesso wireless utilizzando un analizzatore wireless almeno una volta ogni tre mesi. Siccome questo può rivelarsi molto difficile (pensate ad aziende con migliaia di negozi distribuiti sul territorio nazionale o internazionale), si può optare per l'identificazione di dispositivi wireless mediante dispositivi IDS/IPS wireless. IDS significa Intrusion Detection Systems mentre IPS significa Intrusion Prevention Systems; la differenza sostanziale è che i primi permettono soltanto di identificare degli attacchi mentre i secondi hanno anche la capacità di bloccare l'attacco prima che abbia effetto, e quindi prevenirlo.

Naturalmente lo stesso principio è valido anche per le reti non wireless sia interne che esterne. E' quindi necessario eseguire scansioni di vulnerabilità con frequenza trimestrale e dopo ogni cambiamento significativo apportato alla rete. Qualche appunto aggiuntivo in merito:

- esempi di cambiamenti significativi sono modifiche dell'architettura della rete, cambi degli indirizzi IP di segmenti interi (soprattutto se impattano le regole dei firewall), etc;
- per le scansioni di vulnerabilità della rete interna non ci sono richieste particolari: possono essere fatte da personale interno all'azienda con strumenti commerciali o open source;
- le scansioni esterne (i.e. di tutti gli indirizzi IP pubblici) devono essere effettuate da una azienda autorizzata (Approved Scanning Vendor, vedi paragrafo 4.1.2).

Per la sicurezza dell'infrastruttura e dei server è richiesto l'uso di sistemi IDS/IPS per tutto il traffico nell'ambiente dei dati di titolari delle carte, dando l'opzione di scegliere fra soluzioni di rete (Network-based IDS/IPS) e soluzioni per server (Host-based IDS/IPS).

Nel precedente paragrafo è stato richiesto di garantire l'integrità dei log; non ci si può però dimenticare l'integrità dei sistemi su cui si trovano, o vengono trattati, dati dei titolari di carte di credito. Al fine di monitorare tale integrità, un sistema di File Integrity Monitoring viene richiesto sui server in modo da essere allertati in maniera tempestiva. Esistono sistemi che effettuano i controlli in tempo reale, che sono quindi più tempestivi, ma possono avere un impatto sulle performance del sistema su cui sono in esecuzione; esistono altri sistemi che effettuano il controllo in maniera schedulata che quindi hanno un minore impatto sulle performance, ma sono ovviamente meno tempestivi. Entrambi gli approcci sono accettabili per la conformità alla PCI-DSS.

2.8.3 Requisito 11.3

"Eseguire test di penetrazione esterna ed interna almeno una volta all'anno e dopo ogni aggiornamento o modifica significativa dell'infrastruttura o dell'applicazione (quale un aggiornamento del sistema operativo, l'aggiunta all'ambiente di una subnet o di un server Web)."

Lo scopo è relativamente chiaro: occorre verificare se è possibile accedere ai dati di titolari delle carte in maniera non autorizzata. Poiché solitamente ciò si verifica attraverso attività di attacco ai sistemi e alle reti, viene richiesto alle aziende di verificare (personalmente se vi sono figure professionali adeguatamente preparate o attraverso aziende specializzate in caso contrario) l'impossibilità di tali eventi con frequenza almeno annua oppure dopo ogni modifica significativa dell'infrastruttura (rete e/o sistemi) o dell'applicazione.

I test devono essere condotti sia sulla rete sia sulle applicazioni coinvolte nel trattamento dei dati relativi alle carte di pagamento.

Ci sono state molte richieste di chiarimento rivolte al PCI Council stesso concernenti questo argomento; le risposte sono state raccolte ed un documento è stato pubblicato dal PCI Council (https://www.pcisecuritystandards.org/pdfs/italian_infosupp_11_3_penetration_testing.pdf).

È importante sottolineare come queste attività sono tanto più utili e confrontabili nel tempo quanto più seguono una metodologia strutturata, quali ad esempio la open source OSSTMM[14] per i test di rete e di sistema, oltre alla già precedentemente citata OWASP, con riferimento alla testing guide[15], per quelli applicativi.

2.9 Gestione di una politica di sicurezza delle informazioni

La politica di sicurezza deve essere la colonna vertebrale per la sicurezza di qualunque azienda. Tutte le decisioni concernenti la sicurezza devono essere allineate con quanto detta la politica di sicurezza ed è per questo motivo che PCI-DSS richiede alle aziende di prevedere determinate clausole specifiche al suo interno.

2.9.1 Requisito 12: Gestire una politica che garantisca la sicurezza delle informazioni per dipendenti e collaboratori

Ci sono aziende che a volte non capiscono perché devono modificare le loro politiche o procedure 'semplicemente' per essere conformi alla normativa. Innanzitutto queste variazioni sono fondamentali al fine di garantire continuità all'attività svolta per il raggiungimento della conformità. In secondo luogo, alcune di queste politiche e procedure possono sembrare irrilevanti al momento della loro stesura, ma diventano fondamentali dovessero esserci dei cambiamenti strategici legati a come l'azienda è organizzata e svolge la propria attività. Ad esempio se venisse deciso di utilizzare una società terza per certe attività (i.e. outsourcing), la politica già definisce quali sono i requisiti di conformità della società terza, quali sono i requisiti contrattuali, come devono essere trasferite le informazioni etc. (punto 12.8 della normativa). Se invece venisse presa la decisione contraria (i.e. insourcing), politiche e procedure già definiscono quali sono i principi da seguire per la configurazione delle reti, dei sistemi, degli utenti e di tutti gli altri elementi relativi a sistemi ed aree sensibili.

Occorre anche sottolineare che la conformità al requisito 12 non si ottiene semplicemente avendo le corrette politiche e procedure; deve anche esistere un meccanismo di distribuzione e verifica, affinché gli aggiornamenti siano resi noti a tutte le parti interessate. Devono inoltre essere in uso presso l'azienda; questo significa che quando il QSA effettua le interviste al personale, quest'ultimo deve essere in grado di rispondere correttamente, secondo quanto dettato dalla politica e/o procedura, sapere dove questa si trova, quali sono le proprie

[14] http://www.isecom.org/osstmm

[15] http://www.owasp.org/index.php/Category:OWASP_Testing_Project

responsabilità, e non, invece, dare risposte del tipo "*Mhmm… abbiamo sempre fatto così...*", che denotano una mancata conoscenza e distribuzione dell'informazione.

La regola d'oro per le aziende è assicurarsi che la loro politica di sicurezza soddisfi tutti i requisiti PCI-DSS. Questo può essere banale, ma, se viene rispettata come si deve, aiuta a mantenere la certificazione nel tempo in modo quasi naturale. È infatti richiesto di sviluppare procedure di sicurezza operativa che prevedono attività quotidiane, politiche di uso per le tecnologie sotto tutti gli aspetti (dall'approvazione manageriale all'etichettatura, dalla connettività alla disconnessione, ecc), l'assegnazione esplicita delle responsabilità legate alla sicurezza ad un utente o ad un gruppo di persone (dalla documentazione e distribuzione di politiche e procedure al monitoraggio degli eventi).

È richiesto per tutti i dipendenti un programma formale di consapevolezza della sicurezza con particolare attenzione, naturalmente, all'importanza della sicurezza dei dati dei titolari delle carte. Non ci si aspetta che ogni dipendente diventi un esperto di sicurezza, ma almeno che all'atto dell'assunzione e successivamente una volta all'anno, vengano effettuate delle sessioni di consapevolezza; queste possono essere sotto forma di seminario, corso elettronico, ecc. e deve essere possibile verificare l'effettiva partecipazione dei singoli dipendenti.

È richiesto di sottoporre i potenziali dipendenti a screening prima di assumerli. Ovviamente la richiesta si riferisce a quelli che hanno la possibilità di accedere ai dati di titolari delle carte, ma non per quei dipendenti che hanno accesso a un solo dato alla volta, come ad esempio cassieri ed operatori help desk.

La PCI-DSS è una normativa internazionale, e, in quanto tale, non è sempre applicabile alla lettera; in Italia infatti esistono dei forti limiti legali ai quali le aziende devono attenersi quando effettuano uno screening del personale ed esistono nazioni dove è illegale effettuare uno screening. In generale, qualora la legge vieti di soddisfare un requisito, questo viene accettato come conforme dal QSA che giustificherà l'azienda presso il PCI Council, brand e/o Acquirer bank sulla base della legislazione esistente nel paese nel quale questa opera.

Deve esistere un piano di risposta agli incidenti; la maggior parte dei requisiti legati a questo punto sono assolutamente diretti (nomine di personale disponibile 24x7, distribuzione delle responsabilità, procedure di ripristino, formazione del personale, etc.). Occorre evidenziare che le aziende, nella stragrande maggioranza dei casi, cercano di evitare uno di questi requisiti: *"12.9.2 Eseguire un test del piano almeno una volta all'anno."* Questo è normalmente legato ad un aspetto emotivo: "Se non funziona?". Non si può sottolineare a sufficienza l'importanza di sapere se un piano di risposta ad un incident non funziona durante un test ,anziché al momento del bisogno. Gli effetti collaterali possono essere catastrofici e vivere nella speranza che tutto andrà bene è assolutamente inutile. I piani di emergenza vanno testati in modo da essere ragionevolmente sicuri che funzioneranno correttamente e secondo i tempi previsti quando ce ne sarà bisogno.

2.10 Requisiti PCI-DSS aggiuntivi per provider di hosting condiviso

Quando ci si rivolge ad un provider ci si aspetta che i propri dati non vengano visti da nessun altro suo cliente; è proprio questo che viene richiesto attraverso questa appendice rivolta a quei soggetti che offrono i propri servizi a più aziende.

2.10.1 Requisito A.1: I provider di hosting condiviso devono proteggere l'ambiente dei dati di titolari delle carte

La prima garanzia che i provider devono fornire concerne gli accessi: ogni entità ospitata dall'azienda deve eseguire processi con accesso esclusivo al proprio ambiente dei dati titolari

delle carte. Al fine di ottenere questa separazione è fondamentale che non esistano ID condivisi a nessun livello, né di utente né di applicazione. Un ulteriore livello di sicurezza deriva dal garantire che tutti gli ID utente dei processi non corrispondano ad un utente privilegiato (e.g. utente amministrativo nei componenti per IIS) e che gli utenti non abbiano accesso in scrittura a file su sistemi condivisi.

Questo tipo di separazione, nella sostanza, vuole garantire che i dati di due aziende non vengano mai mischiati, che una non legga i dati dell'altra, che una non danneggi i dati dell'altra, sia a livello di applicazione sia a livello di utente.

Anche i log devono essere separati e devono ovviamente essere coerenti con il Requisito 10: Registrare e monitorare tutti gli accessi a risorse di rete e dati di titolari di carte.

2.11 I Controlli Compensativi

Quando un'azienda non è in grado di soddisfare un requisito esattamente come richiesto dallo standard, può ricorrere a quello che viene definito un controllo compensativo, ovvero un modo diverso di soddisfare il requisito.

Innanzitutto deve essere chiaro alle aziende che "non essere in grado" non è la stessa cosa di "non avere l'intenzione". Il QSA che fa la valutazione deve essere il primo ad accettare il fatto che ci siano delle ragioni tecniche precise, oggettive e valide per cui l'azienda deve optare per una soluzione alternativa. E' fortemente consigliabile verificare prima presso la propria banca Acquirer, il brand o il PCI Council se questa soluzione è accettabile. Il QSA qui gioca un ruolo fondamentale poiché tocca a lui essere convinto che la soluzione adottata soddisfi i requisiti necessari; questo non è però sufficiente per ottenere un parere favorevole ogni volta e quindi è bene verificare prima di investire tempo e denaro.

I requisiti dei controlli compensativi sono principalmente quattro:

1. Rispondere allo scopo e alla severità del requisito originale. Per questo motivo nella documentazione viene chiesto al QSA di descrivere questi elementi in modo che non ci siano delle incomprensioni.
2. Offrire un livello di protezione simile al requisito originale. Non è quindi possibile offrire un livello di protezione inferiore mentre è ovviamente accettabile un livello superiore.
3. Superare e integrare altri requisiti. Questo significa che garantire la conformità ad altri requisiti non può costituire un controllo compensativo. Ad esempio è richiesto un controllo fisico all'ingresso delle aree sensibili (videocamera o altro) che permetta di tracciare chi entra ed esce. Non è possibile utilizzare come controllo compensativo un sistema avanzato di tracciamento degli accessi ai sistemi (superiore a quanto richiesto) solo perché non si vuole investire in un controllo fisico degli accessi.
4. Essere adeguato al rischio provocato dalla mancata adesione al requisito. L'aumentato rischio deve essere completamente annullato dalla soluzione scelta.

Spesso viene naturale chiedersi se alcuni requisiti PCI-DSS non possano sostituirne altri proprio nel senso di controllo compensativo. Esistono delle regole ben precise da seguire (gli esempi qui sotto sono generici e intendono essere linee guida; occorre sempre verificare il caso specifico con il proprio QSA):

1. *"I requisiti PCI-DSS esistenti NON POSSONO essere considerati controlli compensativi se sono già richiesti per l'elemento sottoposto a revisione*." Ad esempio, non si può utilizzare l'elevata complessità delle password per compensare il fatto che queste vengano trasmesse in chiaro.
2. *"I requisiti PCI-DSS esistenti POSSONO essere considerati controlli compensativi se sono richiesti per un'altra area, ma non sono richiesti per l'elemento sottoposto a*

revisione." Ad esempio esistono meccanismi di sicurezza di rete (e.g. IPS) che bloccano qualunque traffico contenente i dati titolari di carte in chiaro; in base all'architettura di rete, questi strumenti possono essere utilizzati per garantire che i dati non vengano trasmessi in chiaro per posta elettronica.

3. *"I requisiti PCI-DSS esistenti possono essere combinati con nuovi controlli per diventare un controllo compensativo."* Ad esempio una banca dati contenente dati dei titolari di carte; al fine di isolarla da tutti gli altri sistemi nello stesso segmento (e quindi escludere questi ultimi dall'ambito) si può utilizzare una combinazione di controlli che (a) attivi tutti i livelli di auditing e sicurezza della banca dati, che (b) non accetti una connessione remota con livelli di DBA (database administrator), che (c) l'amministratore non abbia accesso ai dati stessi.

3 Legami con altre best practice

La PCI-DSS è stata concepita tenendo in considerazione il contesto normativo e, più in generale, di best practice di settore che, al momento della sua prima stesura, era già discretamente ricco anche se non ancora sviluppato come attualmente. Questo fattore rende la norma integrabile in contesti ove la gestione della sicurezza o dell'IT è stata già improntata secondo le principali best practice quali ad esempio ISO/IEC 27001 e COBIT, permettendone una gestione consistente con il paradigma adottato e quindi sia di minore impatto sia di più immediata efficacia.

Il panorama normativo della sicurezza può essere sintetizzato visualmente come segue, ordinando le varie norme e best practice inerenti la sicurezza a seconda del livello di dettaglio dei contenuti e della genericità della trattazione. Come si può osservare PCI-DSS si colloca ad un livello di mezzo secondo ciascuno dei due fattori considerati.

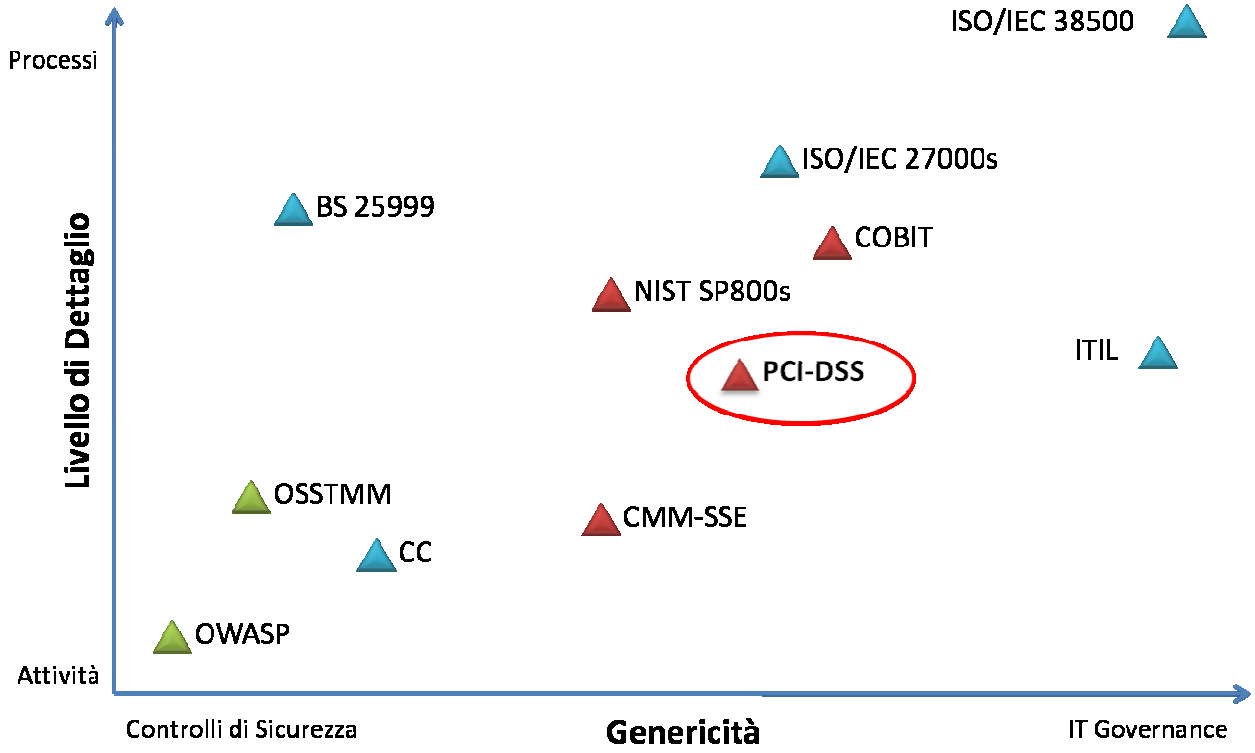

Figura 8 – Principali norme e best practice in ambito IT.

Le best practice considerate, come anche i requisiti della PCI-DSS, spesso escono da quello che è strettamente inerente a una contromisura di sicurezza. Questo aspetto fa sì che norme improntate alla gestione della sicurezza delle informazioni o alla gestione dell'IT si rapportino in modalità e porzioni profondamente diverse con la norma sulle carte di pagamento.

Nei successivi paragrafi si esaminano i punti di contatto e le possibili sinergie tra PCI-DSS e le principali best practice adottate dal mercato, senza scendere in esercizi di pura mappatura tra singoli requisiti, dando per assodata una loro conoscenza di massima da parte del lettore.

3.1 ISO/IEC 27001

3.1.1 Approccio

Questa norma internazionale si basa sull'impostazione e sulla documentazione di una serie di processi (indicati come "sistema") per la gestione della sicurezza delle informazioni. Tale sistema segue un paradigma ciclico in cui le attività si ripetono e si migliorano nel tempo, coerentemente con gli eventi interni ed esterni. L'approccio è quello di indicare la necessità di questi processi, non il loro dettaglio. L'esecuzione di questi processi è volta all'individuazione delle contromisure necessarie a mantenere un adeguato, e mai assoluto, livello di sicurezza.

La PCI-DSS, d'altro canto, considera le criticità tipiche di chi gestisce transazioni con carte di pagamento, andando direttamente a indicare le contromisure minime necessarie e il dettaglio dei processi da adottare. La ciclicità delle attività risulta in questo caso slegata dal concetto di miglioramento continuo ed è molto più vicina al mantenimento di una soglia di guardia.

In questo modo PCI-DSS permette, con uno sforzo analitico minore per chi la implementa, di raggiungere un livello di sicurezza accettabile per quanto riguarda il trattamento di informazioni legate alle carte di pagamento e l'ambiente ad esse relativo (*cardholder environment*). Questo ambiente costituisce chiaramente solo un preciso sottoinsieme della realtà aziendale mentre invece la ISO/IEC 27001 permette di definire un perimetro grande a piacimento che può anche includere tutta l'azienda e la completezza delle sue informazioni.

Entrambe le norme richiedono una verifica esterna e periodica di conformità, che convalidi la bontà delle azioni intraprese effettuando un processo di audit a campione sui requisiti.

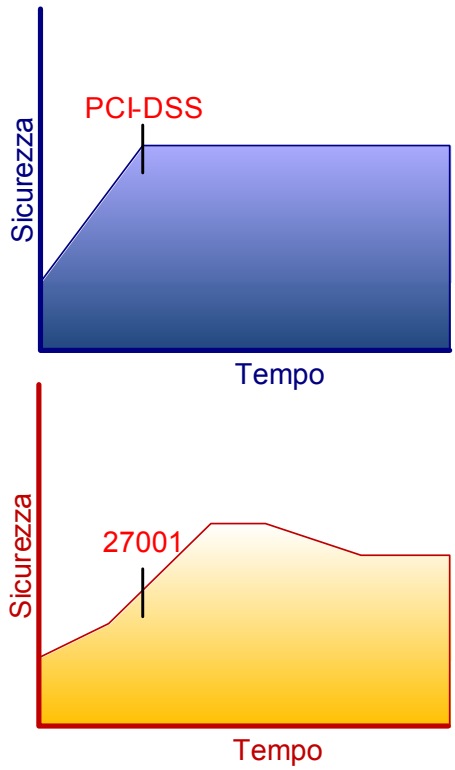

Figura 9 – Cambiamenti del livello di sicurezza nel tempo.

Risulta evidente come la PCI-DSS sia volta effettivamente a impostare, dal momento della sua applicazione, un determinato livello di sicurezza che deve rimanere costante nel tempo. La norma ISO sposta questo livello con il crescere della maturità del sistema per la gestione della sicurezza e in base alle mutate esigenze, definendo un livello di rischio "accettabile" il quale resta modificabile dall'organizzazione in base agli eventi interni ed esterni. Va sottolineato che questa caratteristica non è un fattore positivo o negativo ma costituisce una differenza non trascurabile nelle prospettive e negli intenti con cui gli standard sono stati scritti.

3.1.2 Contromisure

Un'attenta comparazione dei requisiti della PCI-DSS e della ISO/IEC 27002, dove sono specificate le contromisure (*controls*) per la sicurezza delle informazioni a cui la 27001 fa riferimento (riportandole nell'*Annex A*), permette di constatare come tutti i requisiti dello standard sulle carte di pagamento abbiano effettivamente un corrispondente nella norma ISO. Questa forte relazione permette di stabilire un nesso importante tra i due approcci, in quanto la ISO/IEC 27001 include completamente i requisiti della PCI-DSS, mentre quest'ultima presenta in diversi casi un livello di dettaglio maggiore, come riassunto visivamente di seguito.

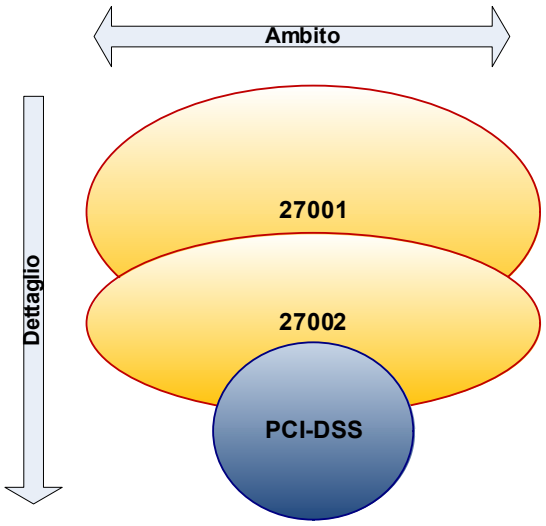

Figura 10 – Diversità di impostazione delle norme.

Guardando questo rapporto a parti invertite, determinate aree di controllo ISO (che costituiscono insiemi logici di contromisure) hanno una numerosità di requisiti PCI-DSS ad esse collegate molto superiore alle altre. Non rientra negli obiettivi del presente articolo fornire una discutibile mappatura tra contromisura 27001 e requisito PCI ma, al fine di mostrare la forza del legame tra le due norme, si è elaborato un grafo funzionale a questa rappresentazione. In esso sono evidenziate le in arancione le aree di controllo della norma ISO dove vi sono maggiori interazioni norme con PCI.

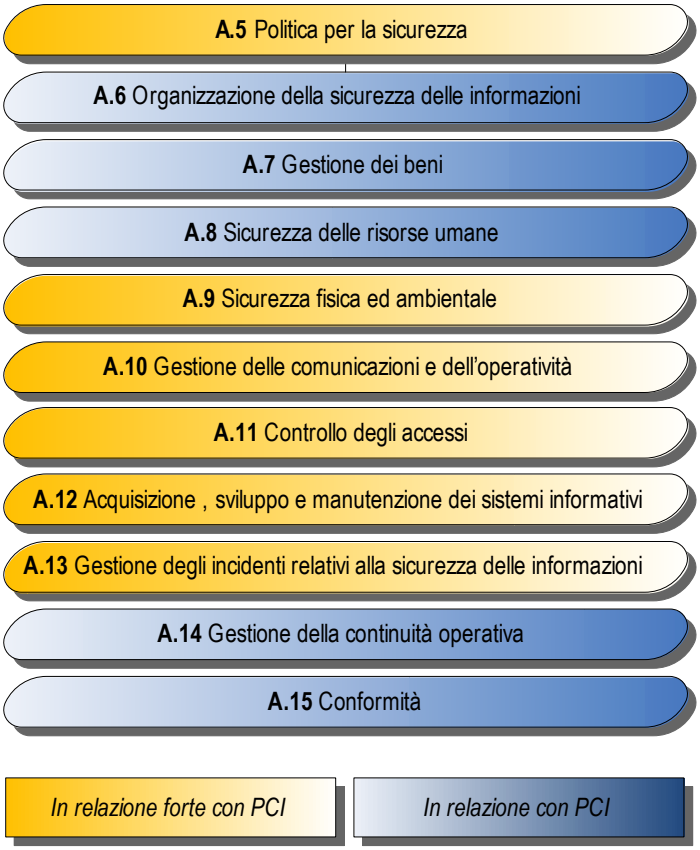

Figura 11 – Aree di Controllo ISO e legame con PCI-DSS.

In particolare le aree di più forte legame sono rispettivamente la A.11, inerente al controllo degli accessi, e la A.12, incentrata su acquisizione, sviluppo e manutenzione dei sistemi informativi.

Le aree di controllo colorate in blu hanno comunque un numero significativo di relazioni e non esiste alcuna parte della norma ISO priva di affinità con PCI-DSS.

3.1.3 Sinergie sul Campo

In pratica si possono delineare tre principali scenari all'interno dei quali si possono utilmente creare delle interazioni produttive tra le due norme:

1. PCI-DSS e 27001 sono impostate ex novo contemporaneamente.
2. Si aggiunge la PCI-DSS ad un contesto già 27001.
3. Si aggiunge la 27001 ad un contesto già PCI-DSS.

In un contesto come quello italiano, in cui sono già attivi oltre 130 certificati ISO/IEC 27001[16] e dove questa norma è da anni ampiamente impiegata come *best practice* di riferimento (a differenza di quanto avviene per PCI-DSS che si sta diffondendo solo

[16] Fonte Accredia, Luglio 2009.

recentemente), è molto più probabile assistere a scenari del secondo tipo, ma nemmeno quelli del primo o del terzo mancano. Esaminiamo con ordine i tre punti:

1. PCI-DSS e 27001 sono impostate ex-novo contemporaneamente: un'organizzazione rileva la necessità di intraprendere un percorso PCI-DSS, avvedendosi però che nel farlo potrebbe cogliere l'opportunità per migliorare tutto il proprio sistema di gestione per la sicurezza delle informazioni. In questo caso i requisiti di sicurezza e il livello di rischio accettabile per il *cardholder environment* sono già impostati partendo da PCI-DSS, mentre vengono decisi quelli per gli altri ambienti nel perimetro dell'attività. A questo punto il *risk assessment* richiesto dalla 27001 comprende entrambi gli ambiti, andando però a generare un piano di trattamento comprensivo di contromisure funzionali ai diversi requisiti di sicurezza, come è prassi comune per siti e ambienti differenti. Il piano può essere quindi implementato e, se correttamente formulato, può portare ad una doppia conformità con notevoli benefici di economia di scala. Questi benefici sono connessi principalmente all'applicazione di processi e contromisure valevoli per entrambi gli ambiti. Il *risk assessment* è un buon esempio in questo senso ma anche elementi più tecnici, come la crittografia dei numeri delle carte (PAN) e il relativo processo di gestione delle chiavi, possono nello specifico venire facilmente applicati anche ai dati personali sensibili, e così via …

2. Si aggiunge la PCI-DSS ad un contesto già 27001: un'organizzazione può trovarsi a promuovere una parte del suo perimetro già certificato 27001 anche a conformità PCI-DSS. In linea di principio se l'SGSI è stato impostato correttamente le discrepanze dovrebbero essere minime e l'effort ridotto a poche azioni al di fuori delle nuove attività di verifica formale richieste da PCI-DSS, quali le scansioni di vulnerabilità trimestrali e l'audit annuale. Nel caso il *carholder environment* non fosse già parte del perimetro 27001, si tratterebbe di esportare, similmente ma con molta più facilità rispetto allo scenario numero 1, le prassi di sicurezza già in uso (e quindi già vissute e accettate dall'organizzazione) mutuandole dove necessario con i requisiti PCI-DSS.

3. Si aggiunge la 27001 ad un contesto già PCI-DSS: per dare maggiore valenza e risalto alla propria gestione della sicurezza, un'organizzazione decide di far nascere un sistema 27001 da un nucleo di conformità PCI-DSS. In quest'ottica tutto il lavoro fatto precedentemente torna a vantaggio dell'approccio ISO, che a questo punto necessita un non oneroso allineamento strutturale e un'analisi con conseguente estensione delle misure di sicurezza già sottolineate nello scenario 1 al resto del perimetro. Parlando di allineamento strutturale si fa riferimento all'assegnazione formale di ruoli e responsabilità per la sicurezza, alla preparazione o documentazione specifica richiesta dalla 27001 (SoA, procedure documentate obbligatorie etc.) e alla messa in opera di alcuni processi specifici, quali ad esempio l'audit interno.

Come si può vedere, in qualunque modo le due norme si rapportino tra loro, restano evidenti punti di contatto e consistenti benefici nel legare i due ambiti in un approccio "parlante", ulteriormente rafforzato dal paradigma di gestione formalizzato e volto alla produzione di documentazione e reportistica per le operazioni richieste.

Non è da escludere che future integrazioni normative potranno anche tenere in considerazione processi di verifica della conformità in modo combinato (un team e un solo audit valido per più schemi) che aumenteranno ulteriormente l'efficacia della sinergia.

3.2 CobIT

3.2.1 Approccio

Il focus di questo diffuso framework di controllo americano è di abilitare una vera e propria governance dell'IT nel suo senso più lato, con un campo d'applicazione che risulta quindi molto più esteso rispetto alla ISO/IEC 27001:2005 appena trattata e, in definitiva, anche della PCI-DSS. Questa maggiore ampiezza deriva sia da una comprensione di tutto l'ambiente IT e non solo del cosiddetto *cardholder environment* sia dal fatto che si considerano tutti i processi legati a questo ambiente, una buona parte dei quali non ha un impatto diretto sulla sicurezza e quindi non è presente nella PCI-DSS.

In sostanza CobIT fornisce un framework strutturato per l'attuazione di una serie di processi legati alla gestione dell'IT, l'applicazione dei quali in un contesto dove sono trattati i dati delle carte di pagamento può effettivamente essere integrata contestualizzando in modo opportuno gli elementi costituenti del framework.

3.2.2 Attività

CobIT include una serie di processi legati all'IT, ognuno dei quali prevede delle attività specifiche ed è legato a degli obiettivi di controllo. Questi processi si collocano mediamente ad un livello di dettaglio più elevato rispetto a quello considerato da PCI-DSS che invece si allineano più facilmente con le attività. E' ad ogni modo possibile effettuare una mappatura completa dei requisiti di PCI-DSS rispetto a processi e attività di CobIT il che è esemplificativo di quanto possano essere compatibili. Di seguito è espanso il grafo già riportato nel paragrafo precedente, indicativo di dettaglio e ambito delle norme anche in relazione al CobIT.

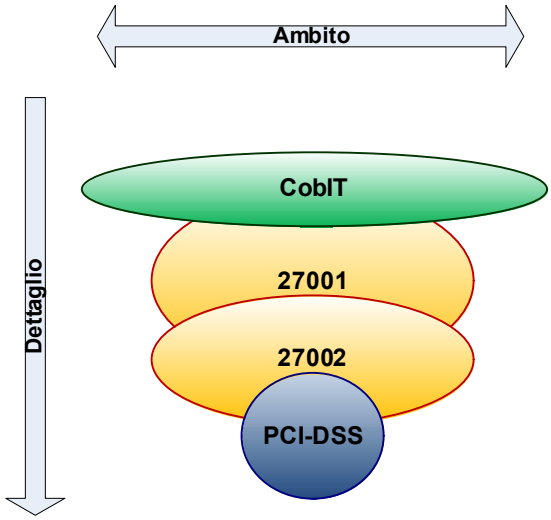

Figura 12 – Diversità di impostazione delle norme.

Vista la già citata non uniformità di livello di dettaglio dei requisiti riportati in PCI-DSS, non deve sorprendere che alcuni di essi coincidano con attività, altri con processi e che altri ancora andrebbero invece incasellati in opportune "sotto-attività" o attività aggiuntive di taglio più operativo, non contemplate da CobIT anche in quanto fortemente orientate agli aspetti di sicurezza.

Come evidenziato dalla figura precedente, la distanza tra CobIT e PCI-DSS è maggiore rispetto a quanto rilevato con la ISO/IEC 27001 e una mappatura completa tra i due standard rimane meno immediata e richiede una quantità maggiore di accorgimenti, pur potendo far fulcro sul rapporto attività-requisiti.

Entrando maggiormente nel merito, dei quattro domini in cui si divide CobIT, quello in cui la maggior parte dei requisiti di PCI-DSS rientrano è il "Delivery and Support" e, in particolare, il suo processo intitolato "ensure systems security" (DS5).

Questo fatto, oltre a sottolineare ulteriormente il dichiarato orientamento di PCI-DSS verso la fase di mantenimento nel ciclo di vita dei sistemi, è emblematico del focus su cui questo standard si orienta rispetto al più esteso ambito di gestione dell'IT.

3.2.3 Sinergie sul Campo

Pur restando validi anche in questo caso gli scenari di implementazione combinata prefigurati per il rapporto tra ISO/IEC 27001 e PCI-DSS, la sinergia tra quest'ultima norma e CobIT non è così pronunciata e il significato degli scenari è di minore portata.

Una sinergia tra le due norme si può declinare in modo più produttivo spingendola verso un'ottica di impiego dei meccanismi interni a CobIT quali l'applicazione di metriche e la valutazione della maturità delle attività legate a PCI-DSS.

Questo tipo di impiego va certamente oltre alla semplice conformità allo standard PCI-DSS ma, soprattutto in ambiti complessi, permette di gestirne al meglio la fase iniziale, monitorando progressivamente il miglioramento della maturità delle attività ad esso legate, di tenere sotto controllo le performance dei sistemi informativi e dei processi inerenti la gestione dei pagamenti legandole al meglio ai requisiti di business e infine agevola l'esecuzione delle operazioni formalizzate e documentate richieste.

3.3 Altri

I punti di contatto con altre norme e best practice, oltre alle due esaminate in precedenza, sono comunque occasionalmente forti e degni di nota, anche solo per determinati requisiti o parti specifiche. Nel seguito del capitolo sono esaminati in sintesi quelli più significativi, senza pretese di esaustività.

3.3.1 ISO/IEC 20000 e ITIL

E' doveroso premettere che per semplicità non si farà in questa sede una distinzione esplicita tra ISO/IEC 20000 e ITIL, in virtù della loro pronunciata affinità e complementarietà oltre che dell'obiettivo del presente documento.

Queste due best practice sono, come già visto per CobIT, più inerenti ad una gestione generale dell'IT (più precisamente dell'erogazione dei servizi IT) che non a quella della sicurezza. Una differenza però interessante è che in questo caso si ha un legame consistente e dichiarato con la ISO/IEC 27001 tanto che questa può considerarsi completamente inclusa nelle due best practice. Applicarle ad un processo (o servizio) che include operazioni tramite carte di pagamento può catalizzare in un unico contesto tutti i benefici derivanti dalla già esaminata sinergia con ISO/IEC 27001 e con CobIT, potendo in più vantare sul mercato una triplice conformità.

I legami con PCI-DSS si estendono tuttavia anche al di fuori della parte espressamente dedicata alla gestione della sicurezza delle due best practice che resta però l'elemento di sinergia e contatto principale. I processi di gestione dei cambiamenti e delle configurazioni, di importanza centrale per ISO/IEC 20000 e ITIL e i processi legati alla gestione di incidenti e

problemi, sono richiamati in modo consistente da PCI-DSS (rispettivamente nelle sezioni 6 e 12).

Queste relazioni sono segnalate in maniera esplicita nel grafo successivo, legato alla struttura di ISO/IEC 20000-1:2005.

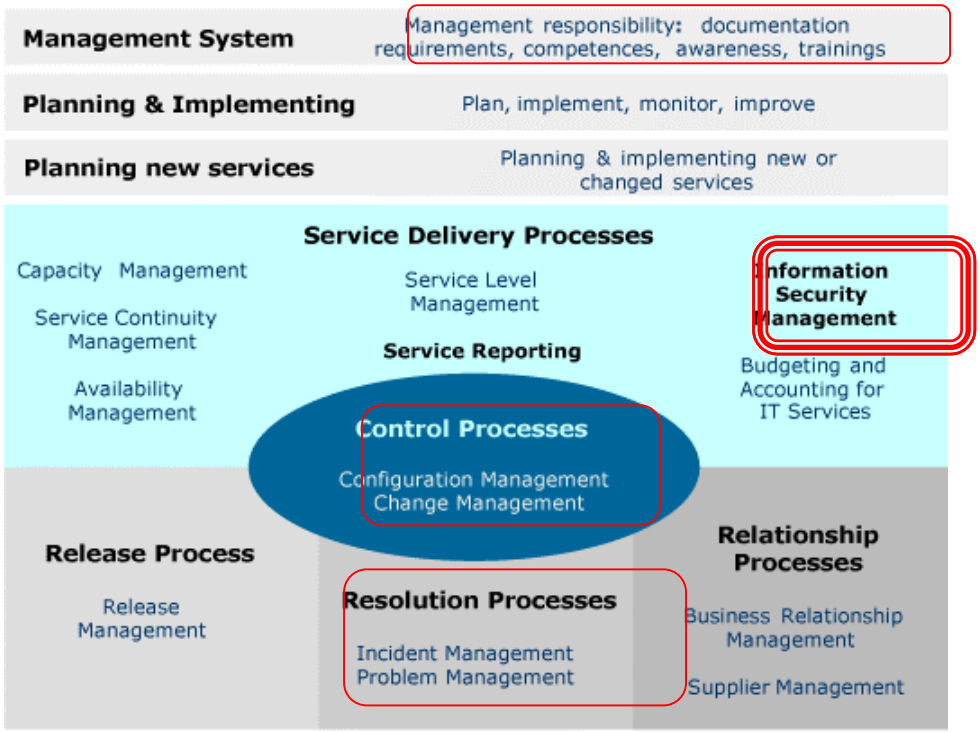

Figura 13 – Legami con ISO/IEC 20000-1:2005.

3.3.2 Basilea2

Applicato in modo consistente nel settore finanziario, questo importante framework ha dei forti punti di contatto con la sicurezza dei sistemi informativi in quanto questi ultimi sono da considerare compresi nelle possibili fonti di rischio per le organizzazioni chiamate ad osservare i dettami di Basilea2.

Per quanto PCI-DSS si leghi limitatamente al concetto di gestione del rischio, confinandolo in un solo requisito, questo può essere soddisfatto impiegando gli strumenti già in essere per il monitoraggio del *rischio operativo* di Basilea2 Si ricorda che per rischio operativo si intende *"il rischio di perdite derivanti dalla inadeguatezza o dalla disfunzione di procedure, risorse umane e sistemi interni, oppure da eventi esogeni. Tale definizione include il rischio legale, ma non quelli strategico e di reputazione"*.

3.3.3 OSSTMM

PCI-DSS ha il merito, non comune tra gli standard che si occupano di sicurezza, di prescrivere esplicitamente l'esecuzione di test di sicurezza periodici sui sistemi informativi, volti a individuarne e chiuderne le vulnerabilità. D'altro canto però non sono definiti né riferimenti né le modalità con cui questi test devono essere effettuati, limitandosi all'uso di termini diffusi sul mercato quali "vulnerabilty scan", "vulnerability assessment" e "penetration test". Il documento che regola le "scanning procedures" definite dal PCI-SSC,

applicabile solo ai "vulnerabilty scan", fornisce guida sul cosa deve essere sottoposto a test e sul come le vulnerabilità devono essere classificate.

OSSTMM (acronimo per Open-Source Security Testing Methodology Manual) è la principale metodologia di riferimento sul mercato per l'esecuzione di test di sicurezza sui sistemi informativi e

definisce cinque canali da analizzare in modo accurato e scientifico, corrispondenti alle differenti sezioni del manuale. I canali sono:

- **Personale** (HUMSEC). Comprende l'interazione con l'elemento umano, nell'ambito del quale le persone custodiscono le informazioni e la proprietà fisica.
- **Accesso Fisico** (PHYSSEC/OCOKA). Comprende l'elemento tangibile della sicurezza, nell'ambito del quale l'interazione richiede uno sforzo fisico.
- **Telecomunicazioni** (COMSEC). Comprende tutte le interazioni con reti di telecomunicazione digitali o analogiche, utilizzabili senza assistenza umana.
- **Reti di Dati** (COMSEC). Comprende tutte le interazioni non-umane che hanno luogo all'interno delle reti di comunicazione attraverso interconnessioni fisiche.
- **Wireless** (SIGSEC/ELSEC). Comprende tutte le interazioni non-umane che hanno luogo senza l'ausilio di interconnessioni fisiche.

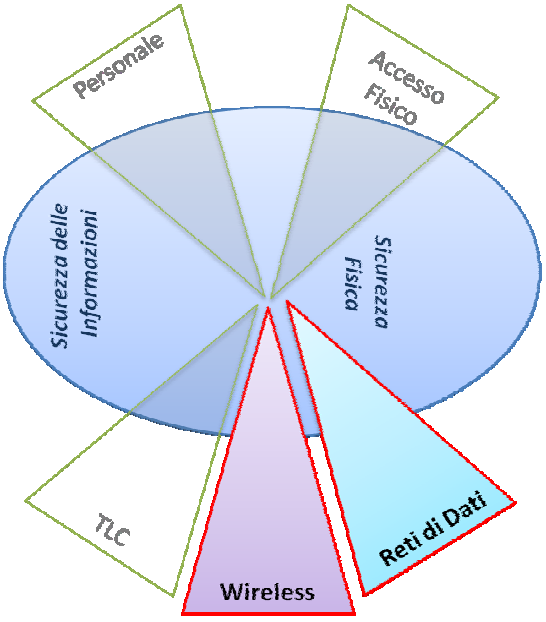

Figura 14 – Canali di OSSTMM relativi a PCI-DSS.

Di interesse per i requisiti di PCI-DSS sono i due canali evidenziati in basso a destra nella figura, tutti richiamati espressamente nella sezione 11, con un peso decisamente più consistente nelle attività di "penetration test". Per ognuno di questi canali OSSTMM riporta i passaggi che devono essere effettuati e le modalità d'azione ad essi relative, di fondamentale

importanza per poter ottenere dei risultati significativi e, cosa decisamente importante in questo ambito, ripetibili.

I professionisti che effettuano test di sicurezza possono inoltre ottenere una certificazione riconosciuta a livello internazionale chiamata OPST (OSSTMM Professional Security Tester) dopo il superamento di un esame pratico.

La versione 3 di OSSTMM, di imminente uscita al momento della stesura del Quaderno, include inoltre rimandi specifici e puntuali alla PCI-DSS.

Le sinergie con PCI-DSS sono in questo caso concretamente evidenti in quanto i test di sicurezza, uno dei requisiti più noti e importanti dello standard, possono essere in questo modo condotti con importanti miglioramenti di efficacia e offrendo maggiori garanzie, tra cui un'immediata confrontabilità tra lavori eseguiti da tester diversi e il rispetto di solidi principi etici, entrambi non strettamente richiesti ma nei desiderata di ogni organizzazione che si sottopone a test (tanto più se si parla di 'penetration test').

Degno di nota infine il fatto che OSSTMM non comprende i test applicativi, per i quali rimanda espressamente a OWASP, prossimo e ultimo elemento trattato in questo capitolo.

3.3.4 OWASP

Unico tra gli standard e le best practice menzionati ad essere espressamente richiamato da PCI-DSS, l'Open Web Application Security Project (OWASP) è una comunità di ricerca aperta creata allo scopo di consentire alle aziende lo sviluppo, l'acquisto ed il mantenimento di applicazioni web sicure. Questa comunità produce e mantiene aggiornati una serie considerevole documenti di supporto, tra cui quelli maggiormente degni di nota sono:

OWASP Testing Guide
(http://www.owasp.org/index.php/Category:OWASP_Testing_Project) , la Top Ten Guide e infine la CLASP, che non mira a fornire a chi deve testare la sicurezza delle applicazioni una banale *checklist*, bensì a definire gli strumenti per comprendere che cosa, quando, dove ed in che modo testare le applicazioni web.

OWASP Development Guide
(http://www.owasp.org/index.php/Category:OWASP_Guide_Project), inclusiva di numerosi richiami alle tecniche per la programmazione sicura contestualizzate ai principali processi applicativi (autenticazione, gestione delle credenziali, gestione dei dati delle carte di credito etc.), è il punto di riferimento per chi vuole scrivere in modo sicuro le applicazioni web.

OWASP Code Review Guide
(http://www.owasp.org/index.php/Category:OWASP_Code_Review_Project) imposta un metodo e descrive le tecniche manuali e automatizzate per la revisione del codice applicativo

OWASP Clasp
(http://www.owasp.org/index.php/Category:OWASP_CLASP_Project) definisce un processo flessibile per la programmazione sicura, utilizzabile per le applicazioni web ma facilmente generalizzabile.

Gli elementi sopra citati, liberamente scaricabili, sono indicati per soddisfare due tipologie di requisiti della PCI-DSS: principalmente quelli inerenti lo sviluppo sicuro delle applicazioni (sezione 6) e secondariamente quelli inerenti al loro testing (sezione 11). Le vulnerabilità applicative sono attualmente tra le più diffuse e insidiose, superando molto spesso in numero e complessità quelle a livello di rete. Per questo motivo una loro individuazione esaustiva richiede intense sessioni di testing ma riveste un'importanza fondamentale.

4 Certificazione

Un'azienda che tratta o memorizza dati di titolari delle carte deve certificare la propria compliance. Questo processo viene solitamente iniziato dall'Acquirer bank, che poi chiuderà il processo accettando la documentazione che ha ricevuto.

4.1 Certificante

Ai Merchant e ai Service Provider con un elevato numero di transazioni (o dati memorizzati) viene richiesto di fare uso di società esterne per effettuare la verifica di conformità. Esistono due tipi di società esterne di cui parleremo in maniera più approfondita:

- Qualified Security Assessor Company (QSAC)
- Approved Scanning Vendor (ASV)

Alcune aziende QSAC sono anche Qualified Payment Application Security Company (QPASC) che vengono utilizzate per certificare la conformità delle applicazioni alla PA-DSS.

Nell'ambito del trattamento dei dati dei titolari delle carte esistono poi società che si occupano della gestione dei casi di furto dei dati; si tratta delle Qualified Incident Response Company (QIRC) che i brand chiamano in causa per andare a svolgere attività forense soprattutto orientata a verificare che l'azienda colpita sia conforme alla PCI-DSS.

4.1.1 Qualified Security Assessor Company (QSAC)

Le QSAC sono aziende che hanno deciso di operare nell'ambito della PCI-DSS e di certificare membri del proprio staff al fine di poter offrire il servizio di analisi di conformità e di certificazione ai Merchant, ai Service Provider e anche ad Acquirer ed Issuer.

Il personale che viene certificato viene denominato QSA: Qualified Security Assessor. Questo titolo è riconosciuto solamente a personale dipendente di una QSAC; questo significa che qualora l'azienda per cui il dipendente lavora non rinnovasse l'accordo con il PCI Council, il QSA perderebbe il suo titolo. Questo vale anche, ovviamente, se questi cambiasse datore di lavoro e cominciasse un'attività o in proprio o con un'azienda non QSAC.

Il QSA è una figura fondamentale attorno alla quale girano molte attività legate alla certificazione; il motivo principale è legato al fatto che in conseguenza della sua formazione gli Acquirer si fidano del suo giudizio per la conformità alla normativa; un fatto che molto spesso non è completamente oggettivo, in particolare quando si tratta di analizzare e descrivere controlli compensativi.

Durante la sua attività presso le aziende, il QSA compila due documenti che saranno fondamentali per la validazione della conformità, il ROC e l'AOC.

- Report on Compliance (ROC). Questo documento è composto di varie parti, tutte rivolte a dimostrare la conformità con PCI-DSS e a testimoniare come questa sia stata determinata; fanno parte integrante del documento non solo tutte le risposte di conformità, ma anche la lista delle persone intervistate, la lista dei sistemi analizzati, la lista della documentazione ottenuta in supporto, la lista dei controlli compensativi e, di fondamentale importanza, i criteri di campionatura che sono stati utilizzati.
- Attestation of Compliance (AOC). Fa parte del ROC; ne esiste uno specifico per i Merchant ed uno specifico per i Service Provider. Sono tre semplici pagine riassuntive che attestano la conformità (come lo dice il nome stesso); questa sezione va compilata sulla base dei risultati dettagliati che compongono il ROC.

Il QSA, durante la propria attività di certificazione, rappresenta il PCI Council e non solamente se stesso e la propria azienda. Al termine di ogni assessment quindi, il QSA è obbligato a dare all'azienda cliente un modulo di feedback; questo è il meccanismo che il PCI Council ha inserito per permettere ai Merchant e fornitori di servizi soggetti a PCI di esprimere il loro parere sulla qualità del lavoro svolto e del supporto ottenuto.

4.1.2 Approved Scanning Vendor (ASV)

Tutti gli IP esterni delle aziende soggette a PCI devono essere analizzati trimestralmente al fine di determinare la loro conformità ai livelli i sicurezza minimi richiesti dal PCI SSC. A tale scopo esistono delle aziende che vengono identificate come Approved Scanning Vendor (ASV), le quali hanno dimostrato al PCI Council di essere in grado di effettuare tali assessment e di fornire i risultati che il PCI Council si aspetta.

La procedura di scansione viene determinata dal PCI Council che la rende pubblica; non è quindi modificabile da altre entità. Esistono due possibilità:

- ricorrere ad un ASV che effettuerà le scansioni nei tempi concordati con l'azienda;
- ricorrere ad un ASV che mette a disposizione un portale che permette all'azienda di gestire autonomamente i tempi delle scansioni.

In entrambi i casi, sarà necessario l'intervento dell'ASV per analizzare i risultati e determinare quali vulnerabilità sono emerse che necessitano una correzione (solitamente l'installazione di una patch) e quali sono i falsi positivi che si possono quindi 'eliminare' dalla lista delle pendenze. Il report finale è quello da tenere a disposizione poiché uno dei requisiti della conformità è mostrare che l'azienda ha effettuato l'analisi trimestrale degli indirizzi esterni e che il risultato è sempre stato conforme o rimediato.

4.2 I livelli

L'introduzione dei livelli ha spesso confuso le idee perché molte aziende ancor oggi pensano che i differenti livelli rappresentano diversi tipi di conformità; assolutamente no. **La conformità è uguale per tutti**, i diversi livelli influenzano solamente il modo in cui si deve dimostrare di essere conformi. (vedi paragrafo successivo). Questo meccanismo è stato introdotto per poter fare maggiore pressione alle aziende che hanno milioni di carte di credito memorizzate o in transito nella propria infrastruttura rispetto a quelle che ne hanno solo migliaia. Queste ultime devono rispettare le stesse normative, ma rappresentano un obiettivo meno interessante anche per chi vuole rubare i dati ad esempio per rivenderli sul mercato nero.

Ogni brand definisce in modo leggermente differente i livelli, come indicato nelle tabelle successive. Poiché i livelli sono legati al volume di transazioni, gli Acquirer sono i soggetti destinati a determinare il livello assegnato al Merchant o al Service Provider.

Esiste un'ulteriore flessibilità dovuta al volume di transazioni; ad esempio, esistono nazioni dove nessun Merchant o service provider arriva a 6 milioni di transazioni annue e quindi nessun Merchant sarebbe di livello 1; di conseguenze viene preso come valore di riferimento uno che sia significativo per quella nazione anche se più piccolo di quello delle tabelle ufficiali.

4.2.1 I livelli dei Merchant

Livello	VISA Europe	VISA Inc.
1	• Oltre 6 milioni di transazioni VISA all'anno • E' stato attaccato con successo durante l'anno precedente • Già livello 1 in un altra regione VISA	• Oltre 6 milioni di transazioni VISA all'anno • Già livello 1 in un altra regione VISA
2	• Fra 1 e 6 milioni di transazioni VISA all'anno	• Fra 1 e 6 milioni di transazioni VISA all'anno
3	• Fra 20'000 e 1 milione di transazioni e-commerce VISA all'anno	• Fra 20'000 e 1 milione di transazioni e-commerce VISA all'anno
4	• Meno 20'000 transazioni e-commerce VISA • Tutti gli altri Merchant che processano fino ad 1 milione di transazioni VISA all'anno	• Meno 20'000 transazioni e-commerce VISA • Tutti gli altri Merchant che processano fino ad 1 milione di transazioni VISA all'anno

Tabella 2 – Livelli VISA per Merchant aggiornata al 2009

Livello	MasterCard	American Express
1	• Oltre 6 milioni di transazioni MasterCard all'anno • E' stato attaccato con successo durante l'anno precedente	• Oltre 2,5 milioni di transazioni American Express all'anno • Altrimenti reputato di livello 1 da American Express
2	• Fra 1 e 6 milioni di transazioni MasterCard all'anno • Fra 50'000 e 2,5 milioni di transazioni American Express all'anno	• Altrimenti reputato di livello 2 da American Express
3	• Fra 20'000 e 1 milione di transazioni e-commerce MasterCard all'anno	• Meno di 50'000 transazioni American Express all'anno
4	• Tutti gli altri Merchant MasterCard	• N/A

Tabella 3 – Livelli MasterCard e American Express per Merchant aggiornata al 2009

Livello	Discover	JCB
1	• Oltre 6 milioni di transazioni Discover Network all'anno • Altrimenti reputato di livello 1 da Discover Network • Definito di livello 1 da un altro brand	• Oltre 1 milione di transazioni JCB all'anno • E' stato attaccato con successo durante l'anno precedente
2	• Fra 1 e 6 milioni di transazioni Discover Network all'anno • Definito di livello 2 da un altro brand	• Meno di 1 milione di transazioni JCB all'anno

3	• Fra 20’000 e 1 milione di transazioni e-commerce Discover Network all’anno • Definito di livello 3 da un altro brand	• N/A
4	• Tutti gli altri	• N/A

Tabella 4 – Livelli Discover e JCB per Merchant aggiornata al 2009

4.2.2 I livelli servizi dei Service Provider

Prima di parlare di livelli, occorre elencare le quattro categorie principali all’interno delle quali vengono classificati i fornitori di servizi:

1. Third Party Processor (TPP). Questa categoria identifica quei service provider che elaborano dati di titolari delle carte per conto terzi. Per American Express e JCB questa è l’unica categoria esistente.
2. Payment Service Provider (PSP). Questa categoria è solo riconosciuta da Discover ed identifica quelle aziende che facilitano il processo di pagamento; da queste sono ad esempio escluse quelle che offrono servizio di hosting.
3. Data Storage Entity (DSE). Questa categoria è solo riconosciuta da MasterCard ed identifica quelle aziende che offrono servizio anche di storage.
4. VISA Net Processor (VNP). Questa categoria è ovviamente solo di VISA ed include tutte le tipologie di service provider.

Livello	VISA	MasterCard	American Express & JCB	Discover
1	• Tutti i VNP che memorizzano, trasmettono o processano più di 300’000 transazioni all’anno	• Tutti i TPP • Tutti i DSE che memorizzano, trasmettono o processano più di 300’000 transazioni MasterCard e/o Maestro all’anno • Tutti i TPP e DSE che sono stati attaccati con successo durante l’anno precedente	• Tutti i TPP	• Tutti i service provider
2	• Tutti i VNP che memorizzano, trasmettono o processano meno di 300’000 transazioni all’anno	• Tutti i DSE che memorizzano, trasmettono o processano meno di 300’000 transazioni MasterCard e/o Maestro all’anno	• N/A	• N/A

Tabella 5 – Livelli Service Provider aggiornata al 2009

4.3 Requisiti necessari per la validazione

Come si diceva in precedenza la conformità è uguale per tutti, quello che cambia sono il tipo di attività e documenti richiesti ai Merchant e ai Service Provider sulla base del livello che è stato loro assegnato.

4.3.1 Self-Assessment Questionaire – SAQ

Un documento che molte aziende si troveranno a compilare è il Self Assessment Questionaire (noto come SAQ). Esistono ben 5 tipi diversi di SAQ:

1. **Tipo 1 / SAQ A: Card-not-present, All Cardholder Data Functions Outsourced**.
   Questo tipo è adatto per quei Merchant che non hanno nella propria infrastruttura nessun tipo di dato in forma elettronica né per il trattamento, né per la trasmissione e nemmeno per la memorizzazione; solamente (e non necessariamente) documentazione cartacea.
   Questo tipo è valido solo per Merchant che hanno solamente e-commerce: non è possibile usarlo per le aziende che hanno dei negozi "classici".
2. **Tipo 2 / SAQ B: Imprint Merchant Only, No Electronic Cardholder Data Storage**.
   Questo è il SAQ per quei Merchant che non memorizzano nessun dato di titolari delle carte in formato elettronico. I Merchant che rientrano nel Tipo 2 utilizzano solamente lo scratch-pad (noto in gergo anche come 'ferro da stiro'). Statisticamente, questo tipo di Merchant sta scomparendo.
3. **Tipo 3 / SAQ B: Standalone, Dial-out Terminal Merchant, no Electronic Cardholder Data Storage**.
   Questo è il SAQ per quei Merchant che non memorizzano nessun dato di titolari delle carte in formato elettronico. I Merchant che rientrano nel Tipo 3 utilizzano solamente terminali stand-alone fanno con connessioni dial-up. Tipici esempi sono Merchant relativamente piccoli che non hanno una rete aziendale ma che per ogni pagamento effettuano 'una chiamata' al proprio Acquirer.
4. **Tipo 4 / SAQ C: Merchants with Payment Application Systems Connected to the Internet**.
   Nel Tipo 4 rientrano tutti quei Merchant che hanno un servizio di pagamento connesso a internet per qualunque motivo; ad esempio per il suo funzionamento (e.g. e-commerce) oppure perché il fornitore dell'applicazione offre un servizio di assistenza remota. Rimane condizione fondamentale per rientrare in questo tipo non memorizzare nessun dato in forma elettronica.
5. **Tipo 5 / SAQ D: All Other Merchants and All Service Providers Defined by a Payment Brand as Eligible to Complete an SAQ**.
   Per esclusione tutti gli altri Merchant ricadono in questo tipo come anche tutti i fornitori di servizi.

Per ulteriori informazioni su quale e come compilare il proprio SAQ, si può fare riferimento alla documentazione disponibile sul portale del PCI Council (da cui è tratta la prossima Figura) https://www.pcisecuritystandards.org/pdfs/instructions_guidelines_v1-1.pdf:

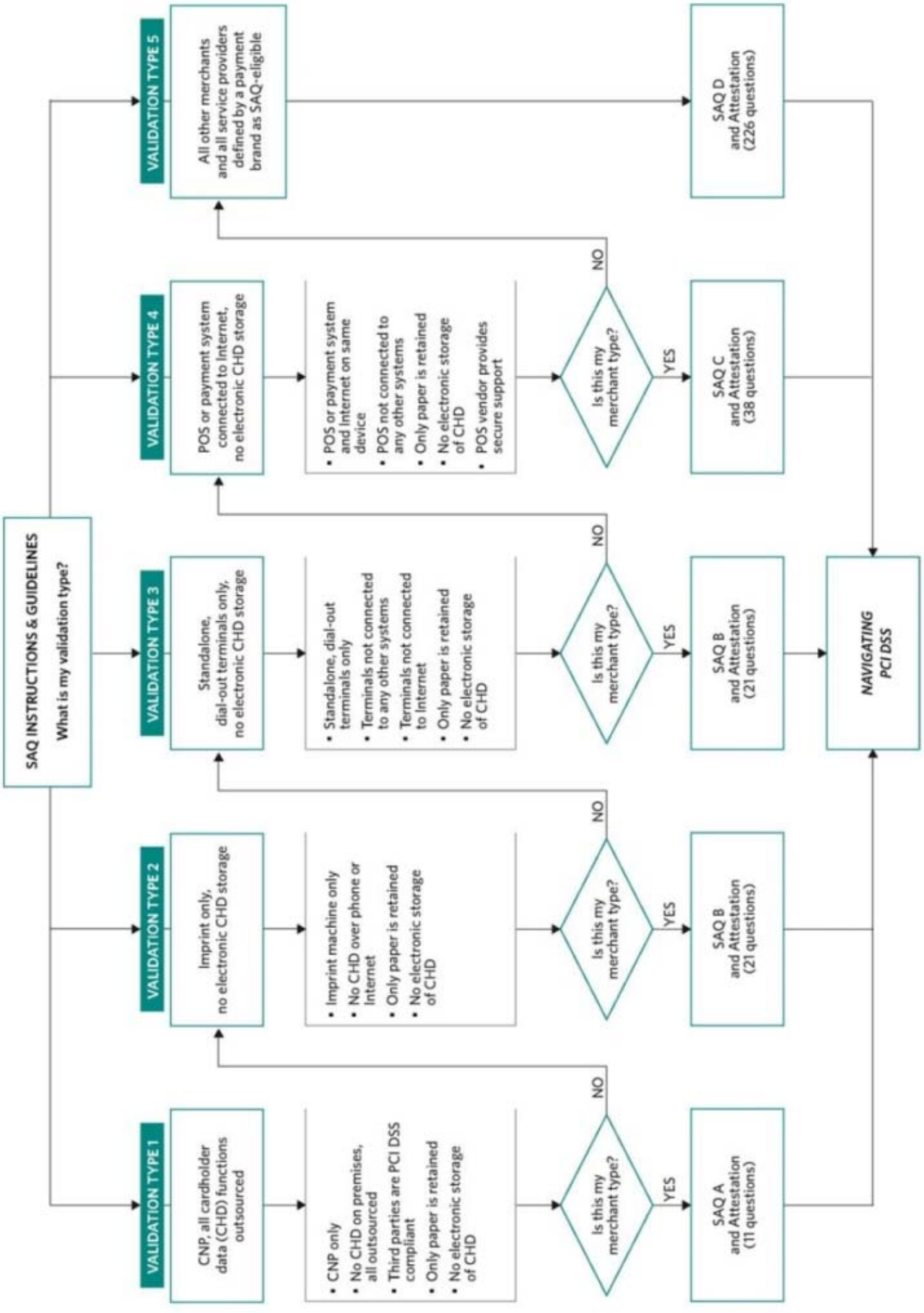
SAQ INSTRUCTIONS & GUIDELINES
What is my validation type?
VALIDATION TYPE 1
CNP, all cardholder data (CHD) functions outsourced
• CNP only
• No CHD on premises, all outsourced
• Third parties are PCI DSS compliant
• Only paper is retained
• No electronic storage of CHD
Is this my merchant type?
NO
YES
SAQ A and Attestation (11 questions)
VALIDATION TYPE 2
Imprint only, no electronic CHD storage
• Imprint machine only
• No CHD over phone or Internet
• Only paper is retained
• No electronic storage of CHD
Is this my merchant type?
NO
YES
SAQ B and Attestation (21 questions)
VALIDATION TYPE 3
Standalone, dial-out terminals only, no electronic CHD storage
• Standalone, dial-out terminals only
• Terminals not connected to any other systems
• Terminals not connected to Internet
• Only paper is retained
• No electronic storage of CHD
Is this my merchant type?
NO
YES
SAQ B and Attestation (21 questions)
VALIDATION TYPE 4
POS or payment system connected to Internet, no electronic CHD storage
• POS or payment system and Internet on same device
• POS not connected to any other systems
• Only paper is retained
• No electronic storage of CHD
• POS vendor provides secure support
Is this my merchant type?
NO
YES
SAQ C and Attestation (38 questions)
VALIDATION TYPE 5
All other merchants and all service providers defined by a payment brand as SAQ-eligible
SAQ D and Attestation (226 questions)
NAVIGATING PCI DSS

Figura 15 – Guida alla selezione del SAQ da compilare.

4.3.2 Requisiti necessari per la validazione dei Merchant

Livello	VISA	MasterCard	American Express	JCB	Discover
1	• Assessment on-site annuale da parte di un QSA[17] • Scan trimestrali della rete esposta (IP pubblici) da parte di un ASV • AoC	• Assessment on-site annuale da parte di un QSA o audit interno firmato da un manager di alto livello[18] • Scan trimestrali della rete esposta (IP pubblici) da parte di un ASV	• Assessment on-site annuale da parte di un QSA o audit interno firmato da un manager di alto livello • Scan trimestrali della rete esposta (IP pubblici) da parte di un ASV	• Assessment on-site annuale da parte di un QSA • Scan trimestrali della rete esposta (IP pubblici) da parte di un ASV	• Assessment on-site annuale da parte di un QSA o audit interno firmato da un manager di alto livello • Scan trimestrali della rete esposta (IP pubblici) da parte di un ASV
2	• SAQ annuale[19] • Scan trimestrali della rete esposta (IP pubblici) da parte di un ASV • AoC	• SAQ annuale[20] • Scan trimestrali della rete esposta (IP pubblici) da parte di un ASV	• **Solo in Europa:** SAQ annuale • Scan trimestrali della rete esposta (IP pubblici) da parte di un ASV	• SAQ annuale • Scan trimestrali della rete esposta (IP pubblici) da parte di un ASV	• SAQ annuale • Scan trimestrali della rete esposta (IP pubblici) da parte di un ASV

[17] Alcune regioni possono decidere di autorizzare la validazione attraverso un audit interno.

[18] Deve essere qualcuno con delega economica poiché ci sono delle obbligazioni/sanzioni che possono derivare dalla mancata conformità in caso di incidente in cui i dati di titolari delle carte vengano rubati.

[19] In Canada tutti i SAQ devono essere esaminati da un QSA.

[20] A partire dal **31/12/2009** verrà richiesto un assessment on-site da parte di un QSA.

Livello	VISA	MasterCard	American Express	JCB	Discover
3	• SAQ annuale[21] • Scan trimestrali della rete esposta (IP pubblici) da parte di un ASV • **VISA Europe:** in alternativa usare uno o più VNP certificati PCI-DSS per tutte le attività relative ai dati di titolari delle carte	• SAQ annuale • Scan trimestrali della rete esposta (IP pubblici) da parte di un ASV	• **Solo Europa:** Consigliato un SAQ annuale • Consigliato Scan trimestrale della rete esposta (IP pubblici) da parte di un ASV	N/A	• SAQ annuale • Scan trimestrali della rete esposta (IP pubblici) da parte di un ASV
4	• Consigliato un SAQ annuale • Consigliato Scan trimestrale della rete esposta (IP pubblici) da parte di un ASV • L'acquirer decide i requisiti di validazione	• L'acquirer decide i requisiti di validazione; consigliati: • un SAQ annuale • Scan trimestrale della rete esposta (IP pubblici) da parte di un ASV	• N/A	N/A	• L'acquirer decide i requisiti di validazione; consigliati: • un SAQ annuale • Scan trimestrale della rete esposta (IP pubblici) da parte di un ASV

Tabella 6 – Requisiti di validazione per i Merchant aggiornata al 2009

[21] In Canada tutti i SAQ devono essere esaminati da un QSA.

4.3.3 Requisiti necessari per la validazione dei fornitori di servizi

Livello	VISA	MasterCard	American Express	JCB	Discover
1	• ROC annuale da parte di un QSA • Scan trimestrali della rete esposta (IP pubblici) da parte di un ASV • AoC	• Assessment on-site annuale da parte di un QSA • Scan trimestrali della rete esposta (IP pubblici) da parte di un ASV	• Assessment on-site annuale da parte di un QSA o audit interno firmato da un manager di alto livello • Scan trimestrali della rete esposta (IP pubblici) da parte di un ASV	• Assessment on-site annuale da parte di un QSA • Scan trimestrali della rete esposta (IP pubblici) da parte di un ASV	• Scan trimestrali della rete esposta (IP pubblici) da parte di un ASV **e uno dei due successivi:** • Assessment on-site annuale da parte di un QSA o audit interno firmato da un manager di alto livello **OPPURE** • SAQ D annuale
2	• SAQ annuale • Scan trimestrali della rete esposta (IP pubblici) da parte di un ASV • AoC	• SAQ annuale • Scan trimestrali della rete esposta (IP pubblici) da parte di un ASV	• N/A	• N/A	• N/A

Tabella 7 – Requisiti di validazione per fornitori di servizi aggiornata al 2009

Una particolare specificità di VISA è la lista dei service provider conformi e certificati PCI: questa lista contiene tutti e soli i fornitori di servizi di livello 1. Questo significa che i fornitori di servizi di livello 2 devono certificarsi con le modalità di quelle di livello 1 per essere inseriti nella lista.

In questa lista viene fatto uso di una codifica colorata al fine di evidenziare lo stato dei service provider:

- Nero: in regola con la conformità PCI.
- Giallo: fino a 60 giorni di ritardo con il rinnovo della certificazione alla conformità PCI.
- Rosso: fra 61 e 90 giorni ritardo con il rinnovo della certificazione alla conformità PCI.

Oltre i 90 giorni si viene rimossi dalla lista fino a quando la necessaria documentazione sarà ricevuta per ricertificarne la conformità.

4.4 I tempi di recupero

Il consiglio a tutte le aziende che devono rispettare la conformità PCI è di coinvolgere il QSA in tutte le loro decisioni che apportano delle modifiche alla gestione, memorizzazione e trasmissione dei dati delle carte. Creando un rapporto di fiducia e collaborazione è possibile trasformare certi aspetti della propria attività aziendale senza, per questo, compromettere la propria conformità.

Se, per qualunque motivo, alla scadenza annuale per la ricertificazione il QSA identifica delle inadempienze, queste emergeranno sia nel ROC sia nell'AOC. In questo caso l'azienda dovrà accordarsi con il proprio Acquirer al fine di determinare i tempi entro i quali la conformità dovrà essere 'recuperata'; solitamente le aziende hanno in questo caso tre mesi a disposizione.

5 Quadro internazionale e scadenze

Una volta pubblicata la prima versione dello standard PCI-DSS si è immediatamente palesato l'interrogativo su come fare in modo che questo schema, la cui implementazione era legata a costi spesso non indifferenti, fosse applicato.

La prima mossa, oltre al prevedibile caldeggiamento da parte dei brand, è stata quella di introdurre, negli USA, delle multe in caso di violazioni della sicurezza dei dati inerenti alle carte di pagamento. Tali sanzioni venivano comminate se il soggetto responsabile della sicurezza di tali dati non era in linea con i dettami dello standard e, indipendentemente dal suo livello, veniva posizionato a livello 1. Parallelamente a questo, in una politica molto simile al classico "bastone e carota", i brand offrivano delle condizioni economiche agevolate (sui fee per transazione ad esempio) agli Acquirer i cui clienti fossero conformi a PCI-DSS, politica spesso ribaltata da questi ultimi sui clienti.

In questo periodo, precedente al 2006, sono stati inoltre lanciati dai brand dei programmi appositi per facilitare e controllare il raggiungimento la conformità. I più noti sono il CISP di VISA e l'SDP di MasterCard.

Il passo successivo, intrapreso sempre negli USA e capitanato fortemente da VISA, è stato invece mirato a fissare una data dopo la quale la memorizzazione delle informazioni la cui archiviazione non è consentita da PCI-DSS, non fosse più accettata. Posteriormente a questa prima data ne sono state fissate altre, tutte nel 2007, indicanti questa volta il tempo limite per raggiungere la conformità a seconda del livello del soggetto interessato. Queste date hanno interessato i primi tre livelli di soggetti interessati prevedendo multe che inizialmente potevano arrivare a 5.000$ al trimestre per poi salire fino a 25.000$ al trimestre. In agosto 2009 MasterCard ha modificato e reso pubblici gli importi delle multe per la conformità, che ora prevedono importi decisamente più elevati (fino a 200K$ al trimestre) differenti a seconda del livello. L'efficacia dei programmi dei brand è stata pressoché completa. Ad oggi VISA dichiara che meno dell'1% dei soggetti a cui è stata imposta la conformità non l'hanno ancora raggiunta.

Quanto appena detto vale però solo per gli Stati Uniti, mentre il resto del mondo è stato fino a poco tempo fa marginalmente interessato da tutto ciò. In Europa ad esempio, con il mondo finanziario concentrato sull'implementazione del progetto SEPA (volto a facilitare le operazioni finanziarie tra i paesi dell'Unione), i brand hanno aspettato a spingere sull'acceleratore. Con la conclusione di questo progetto ormai all'orizzonte si stanno or ora avvertendo i primi segnali in questa direzione: VISA ha creato un programma per la conformità molto similare a quello statunitense chiamandolo AIS e, a novembre 2008, ha annunciato due scadenze, questa volta valide a livello mondiale:

30/09/2009 – Non memorizzazione delle informazioni sensibili vietate da PCI-DSS

30/09/2010 – Conformità a PCI-DSS dei Merchant di livello 1

Queste due date rappresentano un cambio di rotta importante e sono il primo passo per l'applicazione di quanto effettuato negli USA a livello globale. Con ogni probabilità il vecchio continente sarà una delle piazze che saranno interessate per prime da queste scadenze

e dalla loro verifica ad opera dei brand, assieme probabilmente ai principali mercati asiatici. E' notizia recente che i nuovi Merchant legati a VISA basati su applicazioni di terze parti dovranno affidarsi esclusivamente su prodotti certificati PA-DSS entro il 01/07/2010, scadenza estesa di due ulteriori anni per tutti i Merchant.

A livello nazionale la stessa CartaSì sta iniziando a mostrare forte sensibilità per queste tematiche.

Un'importante nota a margine su questo argomento è che, mentre i soggetti dei primi livelli, i quali sono responsabili della grande maggioranza delle transazioni (il livello 1 si stima essere attorno al 50% del transato), con conseguenti esigenze effettive di mantenere o trattare comunque direttamente i dati delle carte di pagamento e con la possibilità finanziaria di implementare un percorso di conformità a PCI-DSS, i livelli inferiori, con budget da spendere in misure di sicurezza molto limitati, sono fortemente spinti a non memorizzare tali informazioni o di affidarle a service provider esterni in grado di garantirne una sicurezza adeguata.

Domande Frequenti

1) Sono anch'io soggetto a PCI?

PCI-DSS si applica tutte le aziende che memorizzano, elaborano o trasmettono dati sensibili, ovvero il Primary Account Number (PAN), indipendente dal volume e dal metodo (elettronico o cartaceo).

2) Tutte le mie transazioni sono gestite da un fornitore di servizi, devo certificarmi anch'io?

Assolutamente sì. Il fornitore di servizi opera in nome e per conto del committente e quindi tutte le transazioni che arrivano presso le banche e i brand sono a nome di quest'ultimo. È la responsabilità dell'azienda essere a norma. Naturalmente tutti gli aspetti tecnici della normativa non avranno un impatto pratico sull'azienda, ma esiste tutta una seria di controlli organizzativi (la maggior parte dei quali si trova nel requisito 12 (vedi pag. 37) cui si deve essere conformi comunque.

3) Ho ancora tempo?

No, le date definite dai brand sono o alle porte o addirittura scadute. A questo punto diventa una gestione della conformità di comune accordo con il proprio Acquirer (o i propri Acquirer se sono utilizzati diversi Acquirer per i diversi circuiti).

4) Ho già cominciato a migliorare la sicurezza con patch e verifica delle vulnerabilità: sono in regola?

Non si è in regola perché si comincia a fare qualcosa: la conformità è raggiunta o non si ha. Inoltre, mentre da un punto di vista della sicurezza non ci sono controindicazioni, questo approccio può essere non essere il migliore da un punto di vista economico; si rischia di investire tempo e denaro in aree che si potrebbero segmentare, in soluzioni che poi non saranno accettabili. È sempre meglio coinvolgere un QSA che sulla base della propria esperienza dia delle linee guida chiare, al fine di un raggiungimento della conformità nel modo più economico e breve possibile.

5) Sono già conforme con altre normative, essere conforme a PCI sarà veloce?

È sempre molto difficile rispondere a questa domanda perché dipende dalla dimensione dell'azienda e di quale altra normativa/normative si parla. Nel capitolo 3 si parla proprio di queste relazioni; come linea guida in una situazione di questo tipo si consiglia di considerare un tempo fra 9 e 12 mesi per la conformità a PCI-DSS.

6) Sono solo un livello 3, la mia conformità è più semplice?

Non bisogna mescolare la conformità con i livelli. Questi sono stati introdotti per avere una gestione differente della metodologia di validazione (ovvero come dimostrare la conformità), ma lo standard è uguale per tutti e non esistono scorciatoie sulla base del volume delle transazioni.

7) Se rispetto le normative introdotte da EMV, sono già conforme a PCI-DSS?

Non esattamente. Ci sono aspetti di EMV che sicuramente hanno spinto molte aziende nella direzione giusta, ma ancora non garantiscono la conformità.

8) Come faccio a sapere se la mia azienda deve richiedere una certificazione esterna o può compilare un SAQ?

I Merchant che memorizzano PAN devono contattare il loro Acquirer (o i loro Acquirer) per verificare come la loro conformità debba essere validata.

I fornitori di servizi devono contattare i brand per ottenere ulteriori informazioni su come procedere.

9) Quali sono le conseguenze della non conformità alla PCI-DSS?

Il PCI Security Standards Council incoraggia tutte le aziende che memorizzano, trattano o trasmettono dati di titolari delle carte a essere conformi con la PCI-DSS al fine non ultimo di ridurre i propri rischi finanziari legati a casi di furto di tali dati. Il PCI Council non gestisce il programma di conformità e non impone nessuna conseguenza in caso di mancata conformità

Totalmente diversa è la posizione dei brand, i quali hanno inserito programmi con incentivi ed ammende (fino a 25.000$ mensili) per le aziende che non sono conformi. Per informazioni specifiche ed aggiornate sui programmi dei singoli brand si invita a verificare quanto pubblicatonei siti come suggeriti nella sezione Riferimenti.

10) Le tracce audio contenenti dati di titolari delle carte e/o dati sensibili per l'autenticazione fanno parte dell'ambito PCI-DSS?

Solitamente questo argomento emerge nella gestione dei call center o banche telefoniche che registrano la conversazione con i propri clienti, solitamente al fine sia di non-ripudio sia di controllo qualità. La risposta del PCI Council a tale riguardo è solo per i call center e si può riassumere in questo modo: i call center possono trovarsi nella situazione in cui memorizzano in forma di audio dati proibiti dopo l'autorizzazione (CAV2, CVC2, CVV2 e CID) in violazione del requisito 3.2. Il call center è, ovviamene, parte dell'ambito e deve essere conforme alla PCI-DSS. Siccome è solitamente molto difficile cancellare tale informazione dalla traccia audio, **SE** queste tracce vengono protette in modo adeguato e conforme ai requisiti PCI-DSS è accettabile che i dati proibiti non vengano cancellati. Se, però, esiste una

soluzione commercialmente ragionevole che ne permetta la cancellazione dalla traccia, allora questa soluzione deve essere adottata. Le seguenti due situazioni si possono verificare e sono chiave al fine della decisione finale:

- Se sulle tracce audio non è possibile effettuare delle ricerche puntuali, la protezione fisica e logica del dato diventa l'aspetto principale cui conformarsi, anche per quanto riguarda le copie di salvataggio (backup).
- Se le tracce audio vengono tradotte in traccia elettronica e, di conseguenza, diventa possibile effettuare delle ricerche puntuali, i dati sensibili per l'autenticazione **devono essere cancellati** subito dopo l'autorizzazione. Tutti gli altri dati devono esser protetti secondo le indicazioni date nel requisito 3.4.

11) La PCI-DSS si applica anche a carte e sistemi di debito?

Qualsiasi tipo di carta (credito, debito, prepagata...) che abbia il logo di uno dei cinque brand che ha costituito il PCI SSC ricade nell'ambito della conformità PCI-DSS.

12) Il Council mantiene una mappatura fra PCI-DSS e ISO 27002 (precedentemente ISO 17799) o altri standard?

Il PCI Council non ha un documento che mappa la PCI-DSS con alcun altro standard. Si consiglia per questo di avvalersi del supporto di un QSA. Ulteriori informazioni si possono trovare nel capitolo 3 di questo Quaderno.

13) Con quale frequenza il PCI Council aggiorna la PCI-DSS?

Il PCI SSC verifica e valuta regolarmente le tendenze emergenti e le nuove tipologie di minacce al fine di determinare i contenuti futuri e i tempi per la pubblicazione di aggiornamenti, che tengono anche in considerazione gli input e i consigli derivanti dalle organizzazioni partecipanti.

In linea di massima, è previsto che gli aggiornamenti abbiano una frequenza fra i 18 e i 24 mesi.

14) Come viene considerata una rete MPLS per la trasmissione dei dati: pubblica o privata?

In linea generale le reti MPLS sono considerate private e non richiedono crittografia. Tuttavia questo dipenda da come il provider ha implementato la rete. Se gli indirizzi IP sono pubblici e la rete MPLS espone i dati, è meglio considerarla 'non affidabile' ('untrusted'). Il QSA deve assicurarsi che questo non sia il caso prima di definire la rete come privata; se non è in grado di ottenere le garanzie di sicurezza necessarie, il QSA deve mettere tutta la rete nell'ambito PCI.

Il Council non ha una lista di soluzioni MPLS approvate e non prevede nemmeno averla. I requisiti per garantire una trasmissione sicura sono chiari e nel dubbio conviene trattare tali reti come pubbliche.

15) Cosa bisogna fare per essere conformi alla PCI-DSS quando si hanno delle partizioni logiche (LPAR) su mainframe?

Se non è possibile effettuare una segmentazione diversa, come minimo è necessario avere un sistema di controllo degli accessi che soddisfi i relativi requisiti PCI-DSS. Inoltre, occorre

implementare contromisure di sicurezza al livello di connettività al fine di limitare l'accesso al mainframe stesso.

Riferimenti

5.1 Siti Web e indirizzi email dei brand

I seguenti indirizzi sono stati verificati ad agosto 2009.

5.1.1 PCI Security Standard Council

- Web: http://www.pcisecuritystandards.org/

5.1.2 VISA

- VISA Europe – Web: http://www.visaeurope.com/aboutvisa/security/ais
- VISA Europe – Email: datasecuritystandards@visa.com
- VISA Inc. US – Web: http://www.visa.com/cisp
- VISA Inc. US – Email: cisp@visa.com
- VISA Inc. CEMEA – Web: http://www.visacemea.com/ac/ais/data_security.jsp
- VISA Inc. CEMEA – Email: CemeaAIS@visa.com
- VISA Inc. Canada – Web: http://www.visa.ca/ais
- VISA Inc. Asia Pacific – Web: http://www.visa-asia.com/ap/sea/merchants/riskmgmt/ais.shtml
- VISA Inc. Latin America & Caribbean – Web: http://www.visalatam.com/ais
- VISA Inc. Latin America & Caribbean – Email: aislac@visa.com

5.1.3 MasterCard

- Web: http://www.mastercard.com/sdp
- Email: sdp@mastercard.com

5.1.4 American Express

- Web: http://www.americanexpress.com/datasecurity
- Email EMEA: AmericanExpressDataSecurityEMEA@aexp.com
- Email North America: AmericanExpressDataSecurity@aexp.com
- Email LAC: AmericanExpressDataSecurityLAC@aexp.com
- Email JAPA: AmericanExpressDataSecurityJAPA@aexp.com

5.1.5 Discover

- Web: http://www.discovernetwork.com/fraudsecurity/disc.html
- For questions about the DISC Program: https://servicecenter.discovernetwork.com/msc/exec/dataSecForm.do

5.1.6 JCB

- Web: http://www.jcb-global.com/english/pci/index.html
- Email: riskmanagement@jcbati.com

5.2 Link utili, forum e FAQ

- PCI Italia: http://www.pciitalia.org
- PCI Answers: http://pcianswers.com

- PCI Knowledgebase: http://www.pciknowledgebase.com

5.3 Siti Web esterni

- OWASP: http://www.owasp.org
- OSSTMM: http://www.isecom.org/osstmm
- ISO: http://www.iso.org

6 Nomenclatura

ACL:	Access Control List
ASV:	Approved Scanning Vendor
AV:	Anti-Virus
CAV2:	Card Authentication Value 2
CID:	Card Identification Number
CISA:	Certified Information System Auditor
CISM:	Certified Information Security Manager
CISSP:	Certified Information Systems Security Professional
COBIT:	Control Objectives for Information and related Technology
CVC:	Card Validation Code
CVV:	Card Validation Value
FW:	Firewall
ISO/IEC:	International Standards Organization/International Electrotechnical Commission
OSSTMM:	Open-Source Security Testing Methodology Manual
OWASP:	Open Web Application Security Project
PAN:	Primary Account Number
PCI-DSS:	Payment Card Industry Data Security Standard
PCI-SSC:	Payment Card Industry Security Standard Council
QSA:	Qualified Security Assessor
QSAC:	Qualified Security Assessor Company
VLAN:	Virtual Local Area Network
WPA:	Wi-Fi Protected Access
SANS:	System Administration Network and Security Institute
NIST:	National Institute of Standards Technology
CIS:	Center for Internet Security
DNS:	Domain Name Server
SNMP:	Simple Network Management Protocol

In generale per la consultazione degli acronimi, delle sigle e dei termini utilizzati all'interno dello standard PCI si consiglia di far riferimento al Glossario pubblicato dal PCI Council, consultabile su https://www.pcisecuritystandards.org/pdfs/pci_dss_glossary.pdf.

CLUSIT
Associazione Italiana per la Sicurezza Informatica
Sede legale presso:
Dipartimento di Informatica e Comunicazione
Università degli Studi di Milano
Via Comelico 39 - 20135 MILANO

www.clusit.it – info@clusit.it
tel. 347 23 19 285