

PCI-DSS: la norma e la tecnologia

Sicurezza dei dati nelle carte di pagamento

Autori: Alberto Perrone
Alfredo Valenza

Oracle Community For Security

The Clusit logo features a stylized 'C' composed of a circle of stars, with the word 'Clusit' in a bold, blue, sans-serif font to its right.

Clusit
Education

Programma

1. Introduzione

- ◆ Frodi e SSC
- ◆ Soggetti coinvolti
- ◆ Carte e processi

2. PCI-DSS

- ◆ Famiglia di standard
- ◆ Applicabilità
- ◆ Conformità
- ◆ Requisiti
- ◆ Audit e scansione
- ◆ Statistiche e sanzioni
- ◆ Materiale a disposizione
- ◆ Rapporto con altri standard
- ◆ Snapshot del Mercato
- ◆ Pro e Contro

3. Alcune soluzioni tecnologiche

- ◆ Cifratura dati in transito e nel database
- ◆ Separazione dei ruoli
- ◆ Accesso ai dati per classificazione degli utenti
- ◆ Funzionalità di auditing
- ◆ Mascheramento dei dati
- ◆ Gestione delle identità e controllo accessi
- ◆ Gestione della sicurezza dei documenti

Prima di iniziare

Alberto Perrone

(in sostituzione di Fabio Guasconi)

Lead Auditor qualificato ISO/IEC 27001:2005

OSSTMM Professional Security Tester

Divisione Sicurezza Informazioni

@ Mediaservice.net S.r.l.



Prima Parte:

INTRODUZIONE

Frodi sulle carte

In risposta al preoccupante fenomeno delle frodi, i principali Brand delle carte di pagamento hanno deciso di unire le forze.

- Furto della carta
- Skimming
- Furto d'identità
- Phishing
- Attacchi informatici

Tutte le tipologie di frodi sono basate sull'acquisizione non autorizzata di dati relativi alle carte.

Il dato di una carta singola non è rilevante, i DB di dati o i sistemi che ne trattano numerose (siti internet, POS, ATM) sono l'obiettivo preferenziale.



Soggetti coinvolti: chi

| | |
|-------------------------|--|
| Titolare | <ul style="list-style-type: none">• Intestatario della carta di pagamento, può usarla fisicamente o via elettronica• Riceve gli estratti conti dall'Issuer |
| Merchant | <ul style="list-style-type: none">• Soggetto a favore del quale il cliente effettua una transazione |
| Acquirer | <ul style="list-style-type: none">• Soggetto che elabora la transazione per conto del Merchant• Dialoga con l'Issuer, direttamente o tramite reti proprietarie• Amex, Discover e JCB possono essere acquirer |
| Issuer* | <ul style="list-style-type: none">• Soggetto che emette la carta di pagamento:<ul style="list-style-type: none">- presso cui il titolare ha un conto (Banca)- a cui il titolare ha richiesto una carta (Amex, Discovery, JCB) |
| Service Provider | <ul style="list-style-type: none">• Soggetto coinvolto nel trattamento dei dati delle carte• Può essere legato al Merchant, all'Acquirer o all'Issuer |

*i Brand delle carte sono associazioni di soggetti Issuer.

Soggetti coinvolti: cosa

PCI-SSC

- Gestisce gli standard creando un punto di convergenza unico
- Gestisce l'accreditamento e la QA di QSA, PA-QSA, ASV e i PED Labs nonché le liste di prodotti conformi

Merchant

- Deve dimostrare la conformità all'Acquirer

Acquirer

- E' responsabile della conformità dei Merchant
- Come l'Issuer deve essere conforme a PCI-DSS senza dover però dimostrarlo come un Merchant

Service Provider

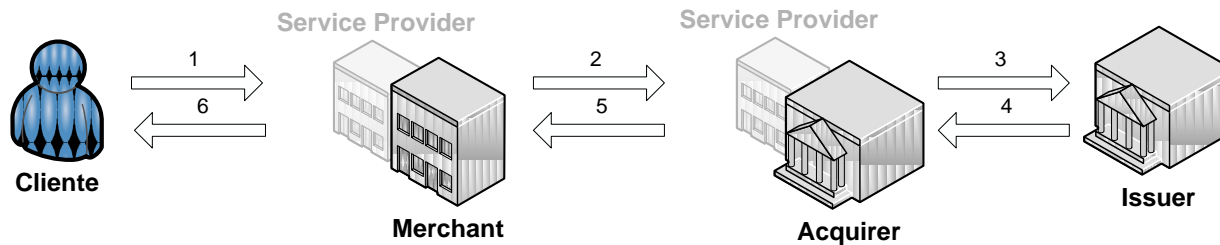
- E' coinvolto nella conformità del Merchant a seconda del servizio fornito
- Può essere escluso (e.g. storage senza chiave crittografica)

Brand

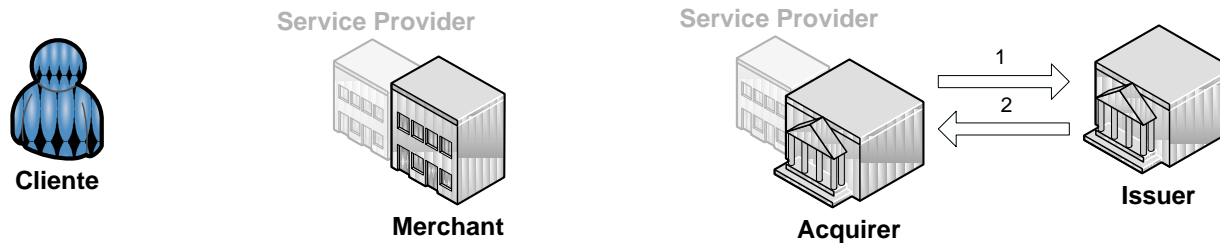
- Gestisce il proprio programma di conformità ricevendone adeguata documentazione
- Effettua le indagini forensi a valle degli incidenti per stabilire cause e responsabilità

Transazioni con carta

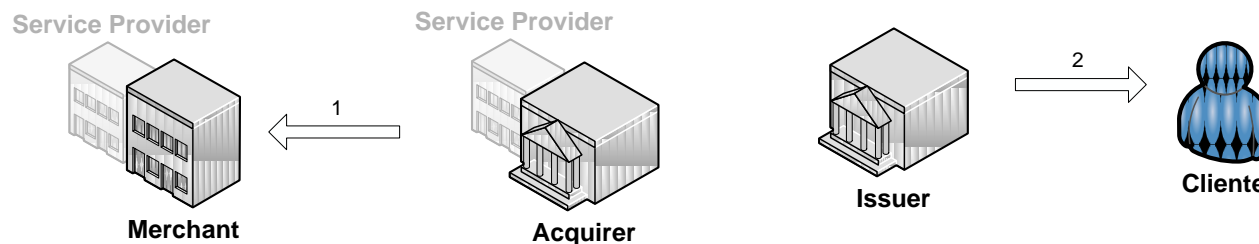
Authorization (secondi): Il Merchant richiede l'autorizzazione all'Issuer



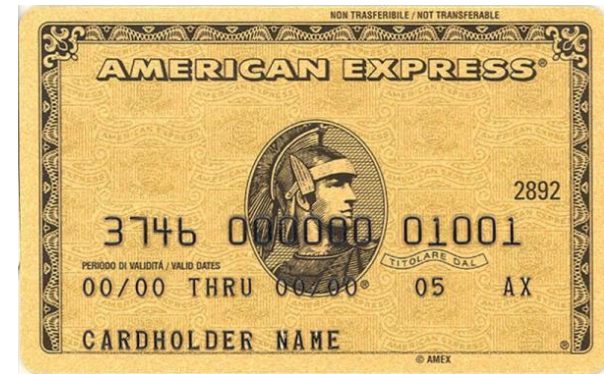
Clearance (un giorno): Acquirer e Issuer si scambiano i dati della transazione



Settlement (due giorni): L'Acquirer accredita la somma transata al Merchant e l'Issuer la addebita al Titolare della carta



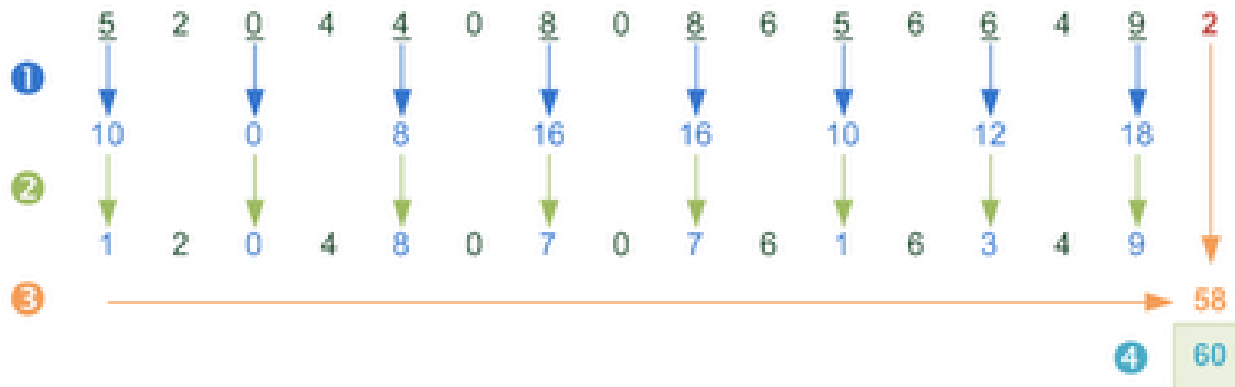
Carte



Il PAN (Primary Account Number) è il dato singolo più importante della carta, ed è costituito da 13, 14, 15 o 16 caratteri.

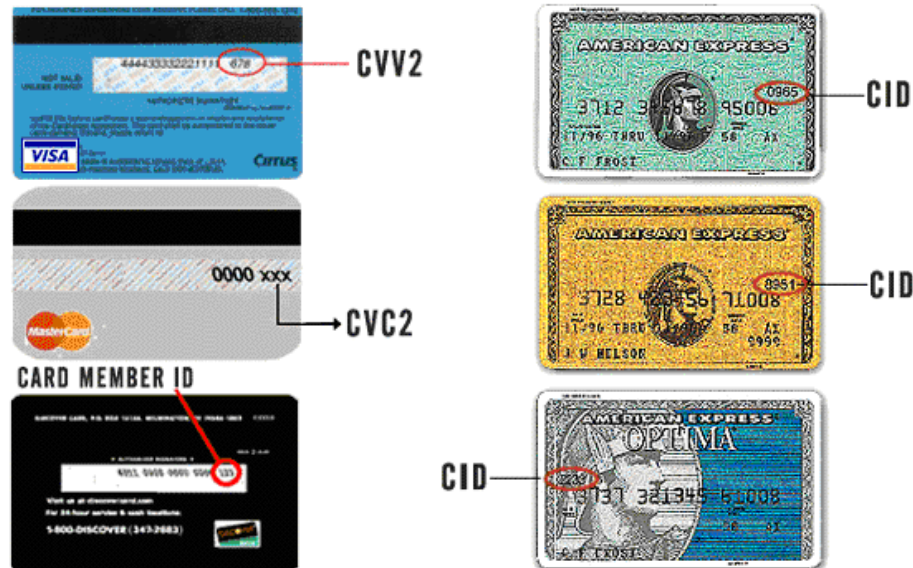
I PAN non sono casuali e la loro validità può facilmente essere verificata.

Formula di Luhn



Carte

Come misura anti frode sono stati aggiunti dei codici di sicurezza, denominati e formattati in modo diverso da ogni Brand.



La differenza fondamentale tra di essi è che possono essere a 3 o 4 caratteri. CVV e CVC sono memorizzati nelle tracce magnetiche, uso se card-present.

Dati dei Titolari delle Carte

La tabella seguente riassume quali sono i dati considerati dallo standard.

| | 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* | Sì | Sì | No |
| | Codice di servizio* | Sì | Sì | No |
| | Data di scadenza* | Sì | Sì | No |
| Dati sensibili di autenticazione | Dati completi della banda magnetica | No | N/A | N/A |
| | CAV2/CVC2/CVV2/CID | No | N/A | N/A |
| | PIN/Blocco PIN | No | N/A | N/A |

* Questi elementi devono essere protetti se memorizzati assieme al PAN.

Memorizzazione e protezione si riferiscono ai momenti **successivi all'autorizzazione**.



Seconda Parte:

PCI-DSS

Applicabilità

Qualsiasi soggetto effettui un trattamento di dati delle carte (PAN)

Principalmente (98%):

Merchant fisici (negozi, catene)

Merchant elettronici (e-commerce via web o telefono)

Service Provider dei Merchant (hosting, fornitori di DR, stampatori delle carte, agenti di vendita, call center, payment gateway)

Alcune operazioni oltre ai pagamenti:

Programmi di fedeltà

Annullamento di transazioni

Pagamento di rimborsi

Backup

Applicabilità

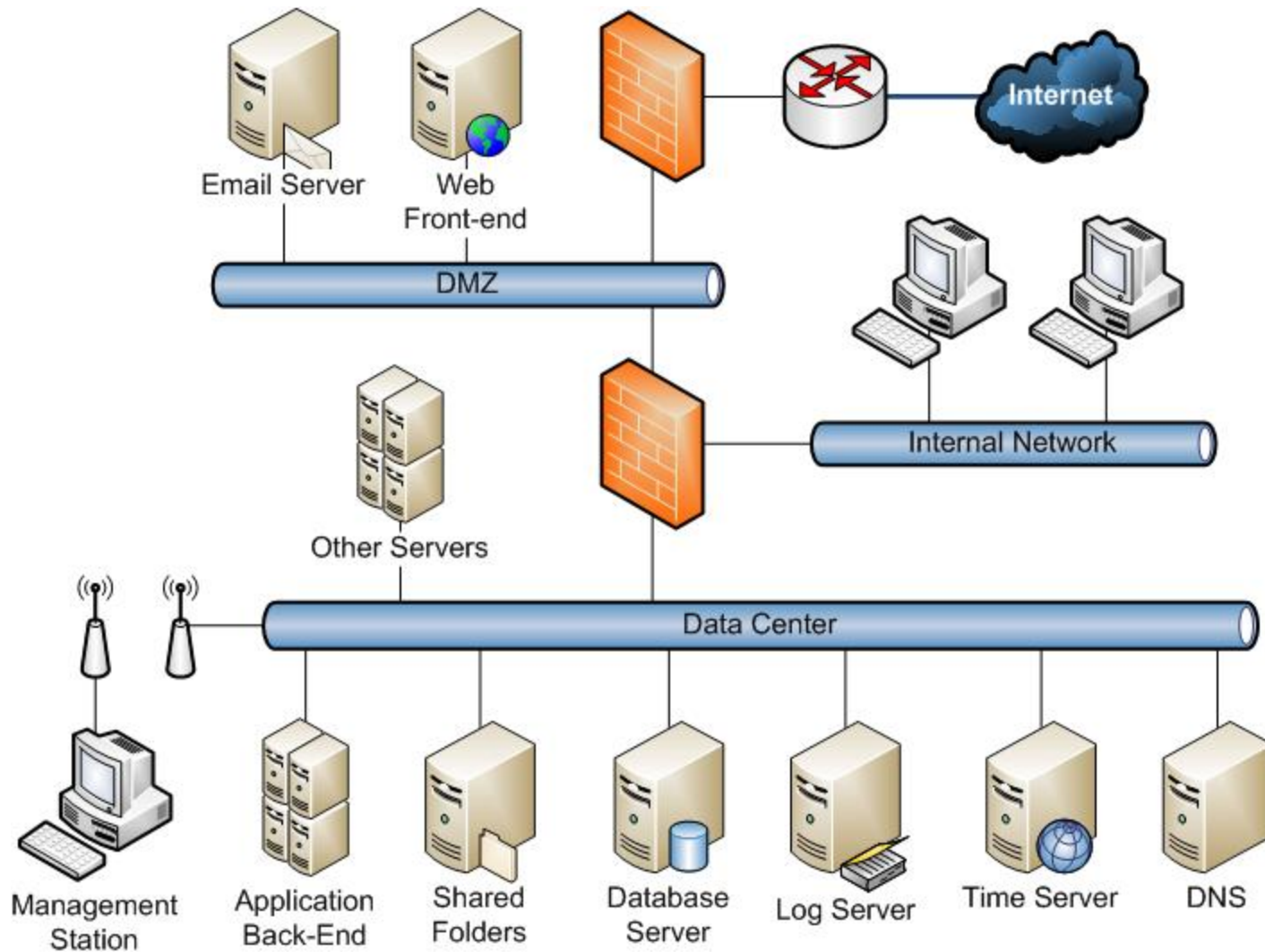
PCI-DSS si applica in modo diverso a **tutti i componenti di sistema** inclusi o connessi nell'ambiente in cui sono trattati i dati delle carte di pagamento.

Il primo passo necessario è definire i flussi di tali dati attraverso:

- Sistemi informatici
- Apparecchiature
- Applicazioni
- Database
- Dispositivi di rete
- Personale
- Terze parti

Nota: attenzione ai metodi meno facilmente individuabili, come registrazioni vocali e log, ma anche al cartaceo.

Applicabilità: esempio di rete



Conformità a PCI-DSS

Per raggiungere la conformità allo standard ci sono una serie di passaggi propedeutici:



La prima validazione può avere diverse caratteristiche da quelle successive, tecnicamente denominate **rivalidazioni**.

Normalmente questo succede per i Service Provider,

Definizione del livello: merchant

Il livello non è legato al rispetto dei requisiti!

L'Acquirer stabilisce il livello del Merchant o del Service Provider, partendo da quanto definito dai Brand. Per i Merchant:

| | VISA | Mastercard | Amex | Discover | JCB |
|------------------|---|---|---|--|---|
| Livello 1 | >6M Transazioni Violazione subita l'anno precedente | >6M Transazioni Violazione subita l'anno precedente | >2,5M Transazioni Così definito da Amex | >6M Transazioni Livello 1 per altro Brand | >1M Transazioni Violazione subita l'anno precedente |
| Livello 2 | Tra 1M e 6M Transazioni | Tra 1M e 6M Transazioni | Tra 50K e 2,5M Transazioni Così definito da Amex | Tra 1M e 6M Transazioni Livello 2 per altro Brand | <1M Transazioni |
| Livello 3 | >20K Transazioni e-commerce | >20K Transazioni e-commerce o Maestro | Meno di 50K Transazioni | >20K Transazioni e-commerce Livello 3 per altro Brand | N/A |
| Livello 4 | Tutti i merchant non compresi nei precedenti | Tutti i merchant non compresi nei precedenti | N/A | Tutti i merchant non compresi nei precedenti | N/A |

Altri soggetti?

Acquirer

- Sono tenuti a raggiungere la conformità esattamente come i Merchant
- Devono assicurarsi della conformità dei Merchant e dei fornitori
- Non sono obbligati ad avvalersi di QSA

Issuer

- Sono tenuti a raggiungere la conformità esattamente come i Merchant, con l'eccezione che possono memorizzare i dati sensibili

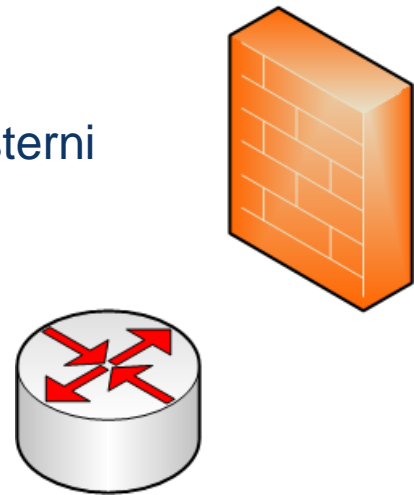
Requisiti

La versione 1.2 della PCI-DSS comprende **210 + 4** requisiti divisi in 13 sezioni:

- 1: Configurazione dei firewall
- 2: Valori di default
- 3: Protezione dei dati archiviati
- 4: Protezione dei dati trasmessi
- 5: Antivirus
- 6: Sviluppo e manutenzione
- 7: Controllo degli accessi
- 8: Identificazione, autenticazione
- 9: Sicurezza fisica
- 10: Log
- 11: Testing
- 12: Policy
- A: Service Providers

1: Configurazione dei firewall

- Configurazione sicura di firewall e router
- Adozione di standard di configurazione
- Controllo del traffico in entrata e in uscita
- Individuazione di servizi e protocolli in uso e loro giustificazione
- Revisione semestrale delle regole
- Approccio “deny all”
- Installazione di firewall davanti alle reti wireless
- Creazione di DMZ tra carte e Internet
- Uso di tecnologie di stateful inspection e NAT
- Installazione di personal firewall su sistemi portatili/esterni



2: Valori di default

- Rimozione di account e password di default su componenti di sistema
- Cambio di chiavi, communities SNMP, password su AP wireless
- Adozione di standard di configurazione sicuri
- Impostazione di una sola funzione primaria per server
- Rimozione di servizi, protocolli e demoni inutili
- Impostazione di parametri di configurazione sicuri
- Crittografia degli accessi amministrativi non da console



- *Separazione totale degli ambienti dei vari clienti da parte dei service provider di hosting condiviso*

3: Protezione dei dati archiviati

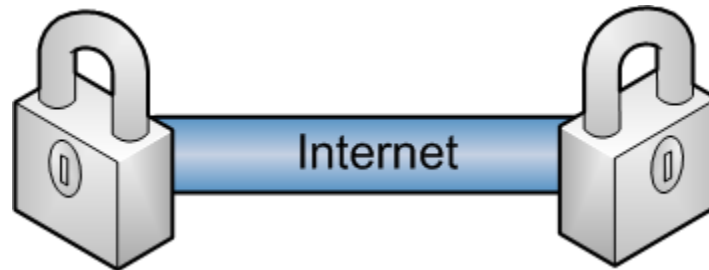
- Politiche di mantenimento dei dati e di loro dismissione (tempi)
- Rimozione trimestrale automatica dei dati che superano la soglia
- Non memorizzazione di dati sensibili oltre all'autorizzazione
- Mascheramento del PAN visualizzato ove possibile
- Troncamento, hashing, indicizzazione o crittografia del PAN, **ovunque**
- Uso di tecniche di crittografia del file system non legate agli utenti
- Separazione di DEK e di KEK, controllo degli accessi alle chiavi
- Impiego di split-knowledge e/o dual control per le chiavi
- Sostituzione almeno annuale delle chiavi o in caso di compromissione
- Assegnazione del ruolo di custode delle chiavi



Algoritmi crittografici accettati: standard di mercato, non compromessi. L'uso di hashing non sicuri è permesso tramite salting.

4: Protezione dei dati trasmessi

- Uso di SSLv3+, TLS o IPSEC per trasmissione dei dati su **reti pubbliche**
- Non trasmissione di dati su reti pubbliche se non protetti con crittografia
- Impiego di tecniche di protezione WPA o superiori per trasmissione dei dati su reti wireless



Il WEP è tollerato fino al 30 Giugno 2010 ma solo per le installazioni già esistenti al 31 Marzo 2009.

5: Antivirus

- Installazione di software antivirus sui sistemi affetti da malware
- Adozione di prodotti in grado di individuare, rimuovere e proteggere contro tutti i tipi di malware
- Aggiornamento costante delle definizioni
- Impostazione di scansioni periodiche
- Impossibilità di disattivazione del software
- Generazione e conservazione dei log



6: Sviluppo e manutenzione

- Aggiornamento dei sistemi e del software
- Individuazione e installazione delle patch critiche di sicurezza entro 30 giorni
- Allineamento degli standard di configurazione (2) in base alle patch
- Adozione di un processo di sviluppo sicuro del software
- Testing dei cambiamenti prima del rilascio
- Separazione degli ambienti di sviluppo (no PAN attivi) e produzione, in termini sistemistici e di personale
- Rimozione di account e dati di test prima dei passaggi in produzione
- Revisione automatica/manuale del nuovo codice scritto, non fatta dall'autore
- Adozione di procedure di controllo dei cambiamenti inclusive di documentazione degli impatti, approvazione, testing e roll-back
- Uso di tecniche di programmazione sicura
- Revisione annuale o dopo ogni cambiamento significativo delle applicazioni web aperte al pubblico / adozione di un WAF

7: Controllo degli accessi

- Approccio del minimo privilegio
- Impiego di sistemi RBAC
- Autorizzazione necessaria da parte del management
- Controllo automatizzato su tutti i componenti di sistema



8: Identificazione, autenticazione

- Tutti gli utenti hanno un ID unico per l'accesso ai componenti di sistema
- Le password relative agli ID non sono salvate o trasmesse in chiaro
- Uso di due fattori di autenticazione per gli accessi remoti
- Verifica dell'identità del richiedente per il reset della password
- Impostazioni di password iniziali univoche
- Rimozione degli account inattivi da 90 giorni
- Attivazione e disattivazione degli account esterni in base all'uso
- Le password devono essere cambiate ogni 90 giorni e devono essere lunghe almeno 7 caratteri, con vincoli di complessità e senza poter riutilizzare le 4 precedenti
- Divieto di utilizzo di account di gruppo e di condivisione delle password
- Attivazione di lockout di almeno 30 minuti dopo 6 tentativi di autenticazione
- Attivazione di screen-saver dopo un massimo di 15 minuti di inattività
- Limitazione dell'accesso diretto ai DB ai DBA e delle application ID alle sole applicazioni

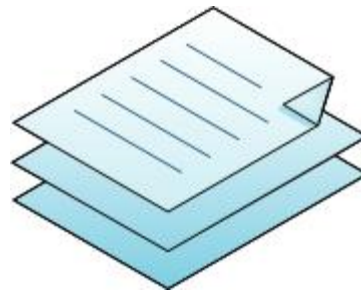
9: Sicurezza fisica

- Installazione di videocamere all'ingresso delle aree sensibili e mantenimento delle registrazioni
- Controllo delle prese di rete
- Limitazione dell'accesso fisico ai dispositivi di rete (AP, chioschi etc.)
- Assegnazione di badge distintivi
- Associazione dei badge ad un periodo di validità e controllo della restituzione
- Adozione di un registro degli accessi esterno e alle aree sensibili
- Ispezione annuale delle località di conservazione dei supporti
- Classificazione, tracciatura, etichettatura ed inventario dei supporti
- Dismissione sicura dei supporti



10: Log

- Logging centralizzato di tutte le attività amministrative
- Controllo degli accessi e dell'integrità dei log
- Mantenimento di informazioni di logging complete
- Logging derivanti da tutti i componenti di sistema (OS, applicazioni, dispositivi, antivirus, DNS etc.)
- Mantenimento di riferimenti temporali attendibili con due o più server interni
- Retention dei log per 1 anno, di cui almeno 3 mesi consultabili online
- Revisione giornaliera (automatica) dei log



11: Testing

- Analisi della presenza di reti wireless trimestrale o adozione di WIDS/WIPS
- Esecuzione di vulnerability assessment esterne (ASV) e interne trimestrali o a valle di cambiamenti significativi
- Effettuazione di penetration test annuali o a valle di cambiamenti significativi sia a livello di rete sia a livello applicativo
- Implementazione e mantenimento della funzionalità di sistemi IDS o IPS per monitorare tutto il traffico
- Adozione di sistemi per il monitoraggio dell'integrità dei file di configurazione e loro controllo settimanale



12: Policy

- Diffusione e revisione annuale di una Policy di Sicurezza
- Sviluppo di procedure inerenti le attività giornaliere di sicurezza
- Diffusione di una Politica per l'Uso Accettabile della strumentazione
- Definizione e assegnazione delle responsabilità per la sicurezza
- Adozione di un programma di formazione annuale sulla sicurezza
- Screening preventivo all'assunzione per posizioni critiche
- *Gestione dei Service Provider e della loro conformità*
- Diffusione di un Piano di Risposta agli Incidenti comprensivo di procedure di reazione per le violazioni di sicurezza e testato annualmente



A: Service Provider

Se si tratta di fornitori di hosting condiviso:

- Impossibilità per i clienti di accedere ad ambienti oltre al loro o di monopolizzare le risorse dei sistemi
- Distinzione e separazione dei log dei diversi ambienti
- Adozione di procedure che permettano immediate indagini forensi in caso di compromissione



Controlli Compensativi

E se un requisito non si può applicare? Devono esserci:

- **Legittimi vincoli tecnici oppure**
- **Documentati vincoli di business**

A questo punto è possibile indicare delle contromisure che compensano la mancata soddisfazione di un particolare requisito, le quali devono

- Essere allineati con l'**intenzione** e il **rigore** del requisito originale, mitigando in modo equivalente i rischi collegati
- Essere **al di sopra** degli altri requisiti di PCI-DSS implementati sul componente di sistema e non creare rischi aggiuntivi

I controlli compensativi devono essere documentati in modo rigoroso.

Scoping dei Requisiti

| | rete | applicazioni | db | sistemi | persone | locali |
|------------------------------------|------|--------------|----|---------|---------|--------|
| 1: Configurazione dei firewall | X | | | | | |
| 2: Valori di default | X | X | X | X | | |
| 3: Protezione dei dati archiviati | | X | X | X | | |
| 4: Protezione dei dati trasmessi | X | | | | | |
| 5: Antivirus | | X | | | | |
| 6: Sviluppo e manutenzione | | X | | X | X | |
| 7: Controllo degli accessi | X | X | X | X | | |
| 8: Identificazione, autenticazione | X | X | X | X | | |
| 9: Sicurezza fisica | | | | | | X |
| 10: Log | X | X | X | X | | |
| 11: Testing | X | X | X | X | | |
| 12: Policy | | | | X | X | |
| A: Service Providers | X | X | | X | | |

Passaggi chiave

1. Analisi dei flussi dei dati

2. Esecuzione di una Gap Analysis

3. Remediation di prima e terza parte

4. Verifica di conformità

5. Documentazione e reportizzazione

Audit on-site e Scansione

Per due attività di validazione della conformità entrano in gioco degli attori riconosciuti direttamente dal PCI-SSC: i QSA e gli ASV

Approved Scanning Vendor (ASV)

Requisito 11.2: Scansioni di rete esterne e interne trimestrali o a fronte di cambiamenti significativi. Si applica a tutti.

Qualified Security Assessor (QSA)

Audit on-site per i livelli più elevati.

Entrambe le figure sono una combinazione di **persone** esperte in sicurezza e **aziende** del settore.

I requisiti includono professionalità, organizzazione, indipendenza, qualità e opportune polizze assicurative.

Sanzioni

Al momento è noto che solo un brand abbia erogato sanzioni ma un altro ha reso pubblico un listino di multe:



A valle di compromissione se non compliant tra 5.000 e 25.000 \$ a trimestre



A partire dal 2011, multe da 10.000 a 200.000 \$ per evento, a seconda del livello e della ripetizione

... e i merchant che subiscono violazioni possono essere “spostati” a **livello 1!**

Pro e Contro di PCI-DSS

Vantaggi

- Opportunità per focalizzarsi sulla sicurezza
- Allineata alle best practices di sicurezza
- Possibilità di ottenere migliori condizioni dagli Acquirer
- Ritorno di immagine verso i Clienti (finali e non)

Svantaggi

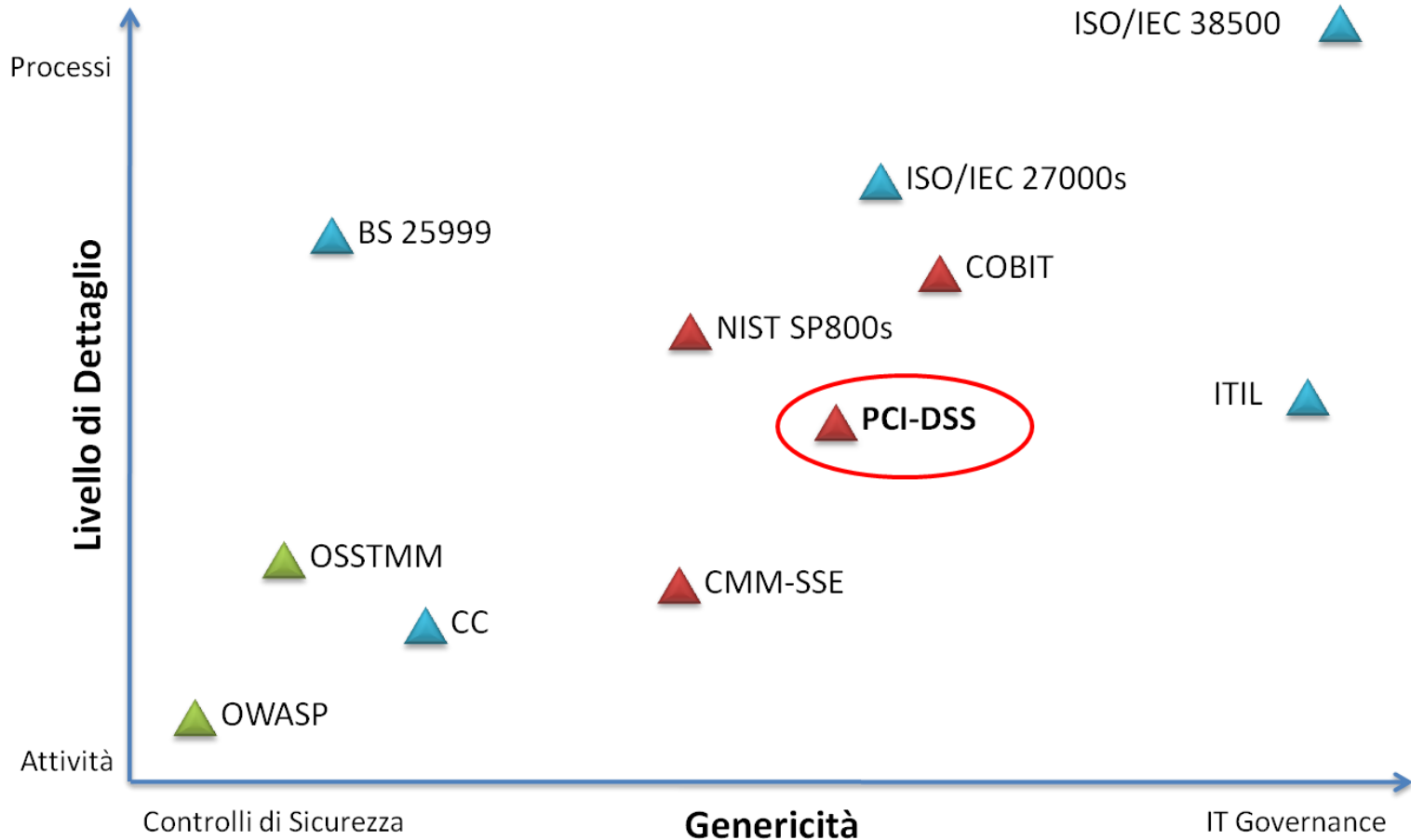
- Oneri aggiuntivi per l'azienda
- Prevede uno schema di validazione proprietario
- Possibilità di ricevere sanzioni dai Brand
- Difformità di gestione tra i diversi Brand e incertezza

Materiale disponibile

Il sito www.pcisecuritystandards.org contiene una buona quantità di documentazione online, di diversa natura e utilità. Diverse sono anche reperibili nella versione italiana.

- **TUTTI GLI STANDARD**
- Self Assessment Questionnaire (tipo A, B, C, D-Merchant, D-TPP)
- Security Scanning Procedures
- Security Audit Procedures
- Attestation of Compliance (AOC) legata a SAQ/ROC
- Glossario
- Guide (approccio prioritizzato, navigazione della norma)
- Registro di QSA e ASV
- Lista delle applicazioni validate
- Lista dei TPP validati (*prossimamente*)

Altri Standard e PCI-DSS



Riferimenti

- www.pcisecuritystandards.org
- www.visaeurope.com/aboutvisa/security/ais
- www.visa.com/cisp
- www.mastercard.com/sdp
- www.americanexpress.com/datasecurity
- www.discovernetwork.com/fraudsecurity/disc.html
- www.jcb-global.com/english/pci
- www.pciitalia.org



alberto.perrone@mediaservice.net