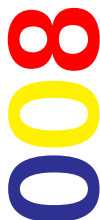


Quaderni Clusit



PCI-DSS

Payment Card Industry
Data Security Standard

Jean Paul Ballerini
Fabio Guasconi

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

Copyright © 2009 Jean Paul Ballerini, Fabio Guasconi .

Copyright © 2009 CLUSIT

Tutti i diritti sull'Opera sono riservati agli Autori e al Clusit.

Sono tuttavia attribuiti i seguenti diritti:

1. I Soci Clusit fruitori dell'Opera hanno il diritto di utilizzare l'Opera nell'ambito della propria attività professionale purchè: a) riconoscano la paternità dell'Opera in capo all'Autore e al Clusit; b) non la utilizzino per scopi commerciali; c) non creino opere derivate e/o alterino l'Opera e/o la trasformino e/o la sviluppino.
2. I diritti attribuiti ai Soci Clusit sopra riportati sono estesi a tutti i fruitori dell'Opera dopo che la stessa sarà rilasciata in forma elettronica sul sito www.clusit.it in area pubblica.

L'Autore e il Clusit non garantiscono che l'Opera sia esente da errori. Qualora vengano segnalati errori, nel limite del possibile si provvederà a correggerli nelle eventuali edizioni successive.

L'Autore e il Clusit non assumono alcuna responsabilità in relazione al contenuto dell'Opera e/o ai risultati attesi e/o ai risultati conseguenti all'uso della stessa e, pertanto, non risponderanno di eventuali e qualsivoglia danni diretti e/o indiretti che dovessero derivarne. In particolare non viene garantito che il contenuto dell'Opera sia esauriente, completo, preciso o aggiornato. Eventuali denominazioni di prodotti e/o aziende e/o i loghi e/o i marchi e/o i segni distintivi eventualmente citati nell'Opera sono di esclusiva proprietà dei rispettivi titolari.

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 suspense 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

1 INTRODUZIONE	13
1.1 SOGGETTI E RUOLI CHIAVE.....	13
1.2 I TRE PROCESSI PRINCIPALI	15
1.3 GENESI DEGLI STANDARD PCI LEGATI ALLE CARTE.....	18
1.3.1 Payment Application DSS (PA-DSS).....	19
1.3.2 PIN Entry Device DSS (PCI PED).....	21
2 PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI-DSS).....	23
2.1 AMBITO	23
2.2 OBIETTIVI.....	23
2.3 STRUTTURA	23
2.4 SVILUPPO E GESTIONE DI UNA RETE SICURA.....	24
2.4.1 Requisito 1: Installare e gestire una configurazione firewall per proteggere i dati dei titolari delle carte.....	24
2.4.2 Requisito 1.4	25
2.4.3 Requisito 2: Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di protezione	26
2.5 PROTEZIONE DEI DATI DI TITOLARI DELLE CARTE.....	27
2.5.1 Requisito 3: Proteggere i dati di titolari delle carte memorizzati.....	27
2.5.2 Requisito 4: Cifrare i dati di titolari delle carte trasmessi su reti aperte e pubbliche	28
2.6 MANUTENZIONE DI UN PROGRAMMA PER LA GESTIONE DELLE VULNERABILITÀ	29
2.6.1 Requisito 5: Utilizzare e aggiornare regolarmente il software antivirus.....	29
2.6.2 Requisito 6: Sviluppare e gestire sistemi e applicazioni protette.....	30
2.6.3 Requisito 6.4	30
2.6.4 Requisito 6.5	31
2.6.5 Requisito 6.6	31
2.7 IMPLEMENTAZIONE DI RIGIDE MISURE DI CONTROLLO DELL'ACCESSO.....	32
2.7.1 Requisito 7: Limitare l'accesso ai dati di titolari delle carte solo se effettivamente necessario.....	32
2.7.2 Requisito 8: Assegnare un ID univoco a chiunque abbia accesso a un computer	32
2.7.3 Requisito 9: Limitare l'accesso fisico ai dati dei titolari delle carte.....	33
2.8 MONITORAGGIO E TEST REGOLARI DELLE RETI	34
2.8.1 Requisito 10: Registrare e monitorare tutti gli accessi a risorse di rete e dati di titolari delle carte	35
2.8.2 Requisito 11: Eseguire regolarmente test di sistemi e processi di protezione	36
2.8.3 Requisito 11.3	36
2.9 GESTIONE DI UNA POLITICA DI SICUREZZA DELLE INFORMAZIONI	37

2.9.1	Requisito 12: Gestire una politica che garantisca la sicurezza delle informazioni per dipendenti e collaboratori	37
2.10	REQUISITI PCI-DSS AGGIUNTIVI PER PROVIDER DI HOSTING CONDIVISO.....	38
2.10.1	Requisito A.1: I provider di hosting condiviso devono proteggere l'ambiente dei dati di titolari delle carte	38
2.11	I CONTROLLI COMPENSATIVI.....	39
3	LEGAMI CON ALTRE BEST PRACTICE.....	41
3.1	ISO/IEC 27001	42
3.1.1	Approccio.....	42
3.1.2	Contromisure.....	43
3.1.3	Sinergie sul Campo	44
3.2	COBIT.....	46
3.2.1	Approccio.....	46
3.2.2	Attività	46
3.2.3	Sinergie sul Campo	47
3.3	ALTRI	47
3.3.1	ISO/IEC 20000 e ITIL	47
3.3.2	Basilea2.....	48
3.3.3	OSSTMM.....	48
3.3.4	OWASP.....	50
4	CERTIFICAZIONE.....	53
4.1	CERTIFICANTE	53
4.1.1	Qualified Security Assessor Company (QSAC)	53
4.1.2	Approved Scanning Vendor (ASV).....	54
4.2	I LIVELLI	54
4.2.1	I livelli dei Merchant.....	55
4.2.2	I livelli servizi dei Service Provider.....	56
4.3	REQUISITI NECESSARI PER LA VALIDAZIONE	57
4.3.1	Self-Assessment Questionnaire – SAQ.....	57
4.3.2	Requisiti necessari per la validazione dei Merchant.....	59
4.3.3	Requisiti necessari per la validazione dei fornitori di servizi	61
4.4	I TEMPI DI RECUPERO	62
5	QUADRO INTERNAZIONALE E SCADENZE	63
	DOMANDE FREQUENTI.....	64
	RIFERIMENTI	67

5.1	SITI WEB E INDIRIZZI EMAIL DEI BRAND	67
5.1.1	PCI Security Standard Council	67
5.1.2	VISA	67
5.1.3	MasterCard.....	67
5.1.4	American Express	67
5.1.5	Discover	67
5.1.6	JCB.....	67
5.2	LINK UTILI, FORUM E FAQ.....	67
5.3	SITI WEB ESTERNI.....	68
6	NOMENCLATURA	69

Elenco delle Figure

Figura 1 – Fac-simile di carte con PAN di 16 e 15 cifre.....	14
Figura 2 – Codici di sicurezza per vari brand	14
Figura 3 – Interazione tra soggetti coinvolti.	15
Figura 4 – Schema semplificato del processo di autorizzazione.....	16
Figura 5 – Schema semplificato del processo di clearing	17
Figura 6 – Schema semplificato del processo di settlement.....	18
Figura 7 – PCI Security Standard Council	19
Figura 8 – Principali norme e best practice in ambito IT.....	41
Figura 9 – Cambiamenti del livello di sicurezza nel tempo.....	42
Figura 10 – Diversità di impostazione delle norme.	43
Figura 11 – Aree di Controllo ISO e legame con PCI-DSS.....	44
Figura 12 – Diversità di impostazione delle norme.	46
Figura 13 – Legami con ISO/IEC 20000-1:2005.....	48
Figura 14 – Canali di OSSTMM relativi a PCI-DSS.....	49
Figura 15 – Guida alla selezione del SAQ da compilare.	59

Elenco delle Tabelle

Tabella 1 – Dati sensibili e loro memorizzazione (sommario)	28
Tabella 2 – Livelli VISA per Merchant aggiornata al 2009.....	55
Tabella 3 – Livelli MasterCard e American Express per Merchant aggiornata al 2009.....	55
Tabella 4 – Livelli Discover e JCB per Merchant aggiornata al 2009.....	56
Tabella 5 – Livelli Service Provider aggiornata al 2009.....	56
Tabella 6 – Requisiti di validazione per i Merchant aggiornata al 2009.....	60
Tabella 7 – Requisiti di validazione per fornitori di servizi aggiornata al 2009.....	61

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