

PCI-DSS e ISO/IEC 27001

Articolo pubblicato su "ICT Security" n.74, Giugno 2009

Tra gli standard di sicurezza specifici per settori di mercato, PCI-DSS sta conquistando un ruolo importante sullo scenario internazionale. Parlando di sicurezza delle informazioni il punto di riferimento è ormai indiscutibilmente costituito dalla ISO/IEC 27001 che presenta requisiti generali, applicabili a tutti i tipi di organizzazioni. Questa sua generalità lascia (volutamente) spazio a standard di settore più verticali su tematiche specifiche e PCI-DSS è la perfetta incarnazione di questo nell'area delle carte di pagamento.

Scopo del presente articolo è di fornire evidenza di come le due norme sopra citate si integrino e completino vicendevolmente, piuttosto che approfondire la struttura dell'uno o dell'altro standard, sotto gli occhi di tutti gli addetti ai lavori da anni.

Differenze di Approccio

La ISO/IEC 27001 si basa sull'impostazione e sulla documentazione di una serie di processi per la gestione della sicurezza delle informazioni. Questo 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 ma 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.

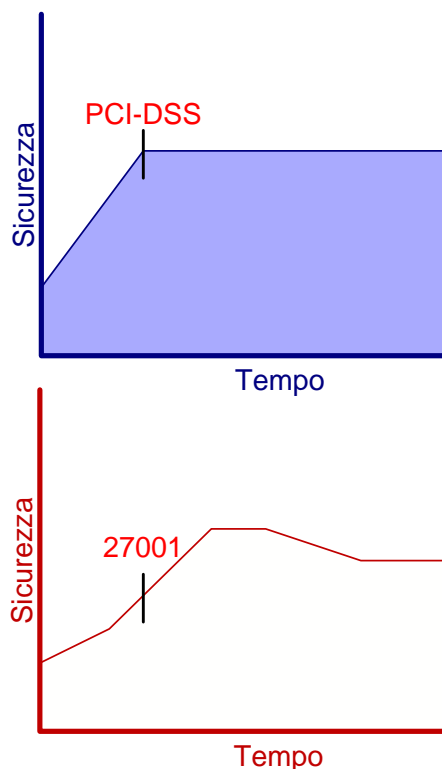


Figura 1 – Cambiamenti del livello di sicurezza nel tempo.

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.

Affinità nelle 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 (riportati 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 in figura 2.

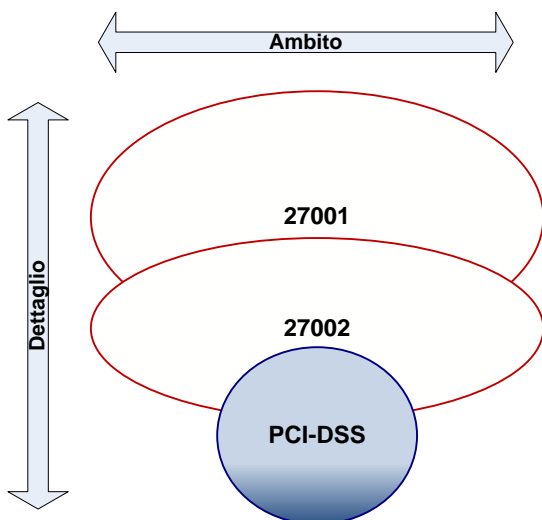


Figura 2 – Diversità di impostazione delle norme.

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 contromisure 27001 e requisito PCI ma, al fine di mostrare la forza del legame tra le due norme, si è elaborato in figura 3 un grafo funzionale a questa rappresentazione. Sono evidenziate le in arancione le aree di controllo della norma ISO dove vi sono maggiori interazioni norme con PCI.



Figura 3 - 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.

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 esistono 129 certificati ISO/IEC 27001¹ e dove questa norma è ampiamente impiegata come *best practice* di riferimento, 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 *cardholder 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". Per arrivare a ciò è assolutamente necessario che gli attori coinvolti abbiano una solida preparazione ed esperienza su entrambe le norme.

¹ Fonte Sincert, Febbraio 2009.

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.

Conclusioni

Ogni qual volta si parla di *compliance* o conformità, resta sempre in agguato lo spettro dell'adempimento pedissequo a una serie più o meno consistente di requisiti. Se la norma ha dei contenuti validi ed è interpretata in modo attivo, allora la conformità può diventare una strada che porta con sé un considerevole valore aggiunto. Nell'ambito della sicurezza delle informazioni questo si traduce principalmente in un minor costo derivante da eventi dannosi o sfavorevoli per il business o per l'immagine aziendale.

Nel caso specifico di PCI-DSS e ISO/IEC 27001 questo discorso acquista una valenza ancora più forte perché l'obiettivo delle due norme è comune e il vantaggio derivante da una loro applicazione combinata può essere significativamente più consistente rispetto a quella separata o a quella di uno standard soltanto.

Note sull'autore



Fabio Guasconi, responsabile della Divisione Sicurezza Informazioni di @ Mediaservice.net, è certificato LA27001, CISA e ITILv3.

Partecipa alle attività del SC27 della ISO/IEC incaricato della stesura delle norme serie 27001 e ha maturato esperienza sul campo nell'applicazione di PCI-DSS presso alcuni esercenti di alto livello, combinandola anche con la ISO/IEC 27001.