

PCI DSS 4.0, a che punto siamo?

L'attuale versione 3.2.1 del famoso Payment Card Industry Data Security Standard (PCI DSS) è formalmente datata maggio 2018, anche se in realtà incorpora solo modifiche editoriali rispetto alla versione 3.2 di aprile 2016, ormai già ben oltre le intenzioni del PCI Council (www.pcisecuritystandards.org) di avere un aggiornamento triennale dello schema.

Lo sviluppo della prossima versione 4.0, che è stato al centro dei riflettori del recente “*community meeting*” europeo promosso dal PCI Council, è ormai attivo da un paio d'anni e ha già dato luogo a una prima bozza nell'ottobre 2019 e a una più recente seconda bozza esattamente un anno dopo.

Questi documenti, indicati come “*Request For Comments*” (RFC), vengono fatti circolare alle organizzazioni che partecipano al PCI Council e agli *auditor* da esso accreditati per coinvolgere un pubblico più ampio nel processo di **aggiornamento dello schema**, nello stile, anche se più ristretto, delle consultazioni pubbliche degli enti di normazione. Non essendo possibile rendere pubblico questo documento né i dettagli al suo interno, si cercherà di dare una prospettiva di alto livello sugli elementi principali che, per quanto ne sappiamo oggi, riteniamo che potrebbero più probabilmente essere presenti nella versione finale dello schema, attesa nel corso del 2021.

L'obiettivo della prossima versione 4.0 del PCI DSS è sia di mantenere i 12 requisiti fondamentali già presenti in quella attuale, che corrispondono ai **punti cardine per la sicurezza dei dati** relativi alle carte di pagamento, sia di far evolvere lo standard per adattarlo ai cambiamenti in ambito tecnologico, di tecniche di mitigazione del rischio e relativi al panorama di minacce ed incidenti. Inoltre, un altro obiettivo fondamentale consiste nell'introdurre maggiore

flessibilità per le organizzazioni nel raggiungere e mantenere nel tempo gli obiettivi di sicurezza, facendo evolvere i metodi e le procedure di validazione.

Tra gli elementi di **novità** che hanno catalizzato maggiore attenzione fino a questo momento merita certamente una menzione di primo livello il tema del cambiamento dei controlli compensativi, meccanismo presente fin dalla prima versione dello schema e che permette di sostituire un requisito con altre misure di sicurezza purché equivalenti nel mitigare il rischio e non già richieste dal PCI DSS. L'idea è di dare ancora più libertà nella definizione e nell'uso di controlli alternativi a quelli espressi nello schema, lasciando la possibilità all'organizzazione di sceglierli usando un approccio *risk-based* strutturato e all'*auditor* di definire le proprie procedure di test per esse.

La conferma dello *scope* della certificazione, debolmente presente nella versione attuale del PCI DSS e poi rinforzata da un supplemento dedicato, è un altro elemento su cui c'è un aumento di attenzione tanto da includere tale supplemento sia in una prima fase formale dello schema sia come requisito. Si pone inoltre esplicitamente l'attenzione, in ognuna delle famiglie di requisiti del PCI DSS, sui ruoli e sulle responsabilità relativi alle attività in essa prescritte. Si introduce anche il concetto di **analisi dei rischi mirata**, che – contrariamente all'attività di *risk assessment* aziendale tradizionale – si focalizza su un determinato numero di requisiti PCI DSS che permetteranno flessibilità sulla frequenza con cui svolgere alcuni controlli. Risulterà quindi possibile definire la periodicità di alcuni controlli, ora fissa, in funzione dell'attività di analisi dei rischi mirata svolta.

Si pone maggiore attenzione anche agli attacchi di *phishing* e, più in generale, di *social engineering*, che risultano essere sempre più frequenti e sempre più una minaccia per la sicurezza aziendale, sfruttando il fattore umano e non solo le

debolezze tecnologiche dei sistemi. Essendo l'**autenticazione** un concetto importante per la protezione dei sistemi informativi, con la prossima versione del PCI DSS viene rafforzato questo concetto, incoraggiando l'estensione dell'utilizzo di meccanismi di autenticazione a più fattori. Si rafforza anche la gestione di tecnologie software e hardware non più supportate dal produttore, e quindi in "*end-of-life*", sottolineando l'importanza dell'analisi e il monitoraggio periodici di tutte le tecnologie utilizzate e i relativi tempi di aggiornamento e dismissione.

Punti di accresciuta attenzione risultano essere anche l'utilizzo e la gestione di certificati e chiavi *trusted*, nonché l'implementazione di **algoritmi di crittografia** e protocolli di sicurezza forti. Inoltre, rispetto alla versione precedente, si pone maggiore attenzione all'analisi dei "*cipher suite*" crittografici e dei protocolli utilizzati per la criptazione dei dati di account, sia in fase di memorizzazione sia in fase di trasmissione, in modo tale da garantire l'utilizzo di funzioni crittografiche robuste e in linea con le *best practice* di settore. Verosimilmente vi saranno anche cambiamenti ad alcune definizioni importanti, come ad esempio cosa si intende per "*significant change*", evento che dovrebbe poi scatenare attività aggiuntive rispetto a quelle già previste periodicamente, come ad esempio i *vulnerability assessment*.

La pubblicazione della versione 4.0 del PCI DSS è attualmente prevista, in modo generico, per "metà 2021". Come già avvenuto con gli aggiornamenti precedenti, a partire da alcuni mesi dopo il rilascio – necessari per pubblicare i documenti ancillari – ci si attende un periodo di transizione di circa 18 mesi in cui sarà possibile certificare sia utilizzando la versione 4.0 sia utilizzando l'attuale 3.2.1, alla fine del quale la vecchia versione sarà ritirata lasciando del tempo aggiuntivo per adottare tutti i nuovi requisiti, i più onerosi dei quali potrebbero anche avere delle date che ne regolano

l'entrata in vigore dilazionate di 2 o 3 anni. Uno schema riassuntivo di questi passaggi è stato oggetto di pubblicazione sul blog del PCI Council (<https://blog.pcisecuritystandards.org/pci-dss-v4-0-anticipated-timelines-and-latest-updates>).

Al momento si può dire che nel suo complesso la struttura e i requisiti “core” del PCI DSS saranno mantenuti, non introducendo quindi cambiamenti rivoluzionari. Per le organizzazioni che si dovranno conformare alla versione 4.0 del PCI DSS sarà sicuramente necessario allocare risorse per l'adeguamento ai nuovi requisiti, ma i cambiamenti prevedono contestualmente una maggiore libertà e una **maggiore attenzione al concetto di rischio** che potrà aiutare a rendere più efficaci tali investimenti.

Grazie anche alla più ampia apertura verso i feedback del mercato, i cambiamenti in corso di introduzione possono essere finora considerati positivi e potenzialmente utili da un punto di vista del miglioramento della sicurezza dei dati di pagamento e, più in generale, dell'intera organizzazione. Lo stesso PCI Council raccomanda nel frattempo di continuare a mantenere tutti i requisiti applicabili della versione 3.2.1 e di non utilizzare le RFC per alcuna attività implementativa.

La strada per la tanto sospirata e commentata versione 4.0 del PCI DSS, insomma, è ancora decisamente aperta e da percorrere.

Articolo a cura di **Fabio Guasconi** e **Beatrice Ridolfi**



Laureato in Informatica, opera dal 2003 nella consulenza su sicurezza delle informazioni e protezione dei dati personali, con focus sui temi di analisi del rischio, di governance e di conformità a norme internazionali, cui contribuisce direttamente. Certificato CISA, CISM, PRINCE2, ITIL e ISFS, è auditor ISO 9001 e ISO/IEC 27001, di cui è anche lead implementer. Ha maturato esperienze anche come DPO esterno.

Coautore del quaderno CLUSIT sulle certificazioni professionali e sullo standard PCI-DSS, è un PCI QSA / QPA attivo e partecipa regolarmente ad eventi e pubblicazioni sulla sicurezza. Ha coordinato la stesura delle norme UNI 11621, 11679 e PdR 43.2 sui profili professionali per la sicurezza delle informazioni e per la protezione dei dati personali.

Presiede il comitato italiano mirror di ISO/IEC JTC 1 SC 27 in UNINFO dal 2008 ed è membro del direttivo dell'associazione italiana per la sicurezza informatica CLUSIT dal 2012. Partecipa attivamente alle attività di SBS e della European Digital SME Alliance per lo sviluppo nel settore delle PMI.

È co-fondatore e presidente dell'azienda di consulenza BL4CKSWAN S.r.l.



Consulente in ambito sicurezza informatica, dopo una Laurea in Matematica ed esperienze di progetti di data analysis e system integration, si è dedicata maggiormente ai temi in ambito sicurezza delle informazioni, tra cui analisi del rischio, governance, conformità e cybersecurity awareness.

E' lead auditor ISO/IEC 27001, di cui è anche lead implementer, e PCI QSA.

Senior Information Security Consultant presso Bl4ckswan dal 2019.

<https://www.ictsecuritymagazine.com/articoli/pci-dss-4-0-a-che-punto-siamo/>