Auditing della conformità della sicurezza dei dati PII

Derek Mohammed, Ph.D., CISA, CISM, è un ricercatore universitario che tiene corsi di garanzia e sicurezza delle informazioni a studenti universitari e specializzandi presso un'università di discipline umanistiche privata con sede in Texas, Stati Uniti. Prima di entrare nel mondo accademico, Mohammed ha lavorato a lungo nei settori sia pubblico che privato per migliorare la sicurezza dei sistemi informativi critici. La sua attività di ricerca è incentrata sull'auditing e sulla conformità della sicurezza nel settore IT.

Le aziende e le persone si affidano sempre di più alla tecnologia delle informazioni, pertanto la quantità di dati che le identificano all'interno di diversi sistemi informativi è in continuo aumento. Alcuni dati sono strettamente personali e l'accesso ad essi da parte di persone non autorizzate potrebbe avere conseguenze molto negative. Questi dati sono chiamati informazioni per l'identificazione personale (PII, Personally Identifiable Information). Il Government Accountability Office degli Stati Uniti definisce i dati PII come "qualsiasi informazione riguardante un individuo conservata da un ente, inclusa (1) ogni informazione che possa essere usata per distinguere o scoprire l'identità di un individuo, come nome, codice fiscale, luogo e data di nascita, cognome della madre e dati biometrici; e (2) qualsiasi altra informazione correlata o correlabile a un individuo, come dati medici, formativi, finanziari e lavorativi".[1]

Esistono leggi e regolamenti intesi a proteggere i dati PII in formato digitale. Alcuni esempi di tali leggi sono: Family Educational Rights and Privacy Act negli Stati Uniti, Health Insurance Portability and Accountability Act (HIPAA)[2] negli Stati Uniti, Privacy Act in Australia, Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada e la Direttiva sulla tutela dei dati nell'Unione Europea.

Nonostante i regolamenti in vigore per proteggere le informazioni PII, la divulgazione non autorizzata di tali dati è molto frequente. Nella settimana dell'11-17 aprile 2011, ad esempio, Identity Finder ha segnalato nove casi di furto, perdita o diffusione di dati PII. Dei suddetti nove casi, un incidente riguardava l'intrusione nel sistema IT di una società internazionale, allo scopo di sottrarre i dati PII dei clienti per estorcere denaro alla società. Un altro incidente riguardava il furto di dati PII da parte di persone autorizzate ad accedere a tali dati. Un terzo incidente riguardava l'accesso non autorizzato a dati di carte di credito a causa di un difetto nel sistema di sicurezza. I restanti sei incidenti erano più comuni. Tre di essi riguardavano il furto o lo smarrimento di computer o altri supporti di archiviazione dati contenenti dati PII non crittografati; due incidenti riguardavano la divulgazione accidentale di informazioni PII al pubblico o a terzi; un incidente derivava dalla mancata distruzione dei dati PII da parte di un dipendente prima della dismissione del supporto.[3] Complessivamente, questi nove incidenti hanno coinvolto quattro milioni di persone e sono stati segnalati nell'arco di una sola e normale settimana.

È importante sottolineare che la maggior parte delle violazioni della sicurezza dei dati PII può essere evitata. È possibile rafforzare i sistemi per impedire accessi non autorizzati; inoltre è possibile migliorare la protezione e la formazione dei dipendenti in modo da evitare la divulgazione non autorizzata di dati PII a causa di furto, perdita o gestione inappropriata. Molto spesso, tuttavia, solo dopo il verificarsi di un incidente le organizzazioni eseguono una revisione approfondita e apportano i necessari adeguamenti alle procedure attinenti la sicurezza delle informazioni PII. Per ridurre il numero di violazioni della sicurezza dei dati PII, le organizzazioni devono adottare i principi di auditing della conformità e della sicurezza dei dati PII, in modo da mettere in atto misure preventive.

AUDITING A LIVELLO DI GOVERNANCE

Un programma di auditing attinente la conformità della tutela della privacy deve partire dall'alto. La capacità di un'organizzazione di definire un programma di governance in grado di affrontare e gestire efficacemente il rischio IT è fondamentale per garantire la sicurezza dei dati PII, nonché la sicurezza IT in generale. In mancanza di una governance adeguata, il sistema di controllo per proteggere le informazioni PII potrebbero essere incoerenti, ridondanti, carenti o assenti. Pertanto è essenziale che il senior management di un'organizzazione comprenda i fattori di rischio e i requisiti di conformità attinenti i dati PII. Per rispondere a tale esigenza, numerose organizzazioni creano una posizione a livello dirigenziale il cui titolo è Responsabile della sicurezza delle informazioni o Responsabile del trattamento dei dati personali. La persona che riveste tale ruolo ha il compito di individuare, valutare, monitorare e gestire il rischio IT.[4] Se una simile posizione esiste, il primo passo di un auditor consiste nell'incontrare tale responsabile e porre le seguenti domande di carattere generale:

- **I requisiti di conformità per i dati PII sono stati individuati e compresi?** Un auditor deve verificare che l'organizzazione abbia individuato e compreso i regolamenti

ISACA JOURNAL VOLUME 1, 2014 1

L'articolo è interessante?

- Leggere *Privacy and Big Data* e altri libri bianchi di ISACA.

www.isaca.org/ white-papers

- Discussione e collaborazione su tutela della privacy, protezione dei dati e strumenti e tecniche di audit nel Knowledge Center.

www.isaca.org/knowledgecenter

che definiscono e impongono l'adozione di misure di sicurezza per i dati PII. I singoli regolamenti prevedono modalità specifiche per quanto riguarda la definizione e il trattamento dei dati personali. Ad esempio, HIPAA si occupa della sicurezza delle informazioni sanitarie personali (PHI, Protected Health Information), ossia qualsiasi informazione atta a identificare un individuo e ad associarlo a condizioni sanitarie fisiche o mentali passate, presenti o future, alla somministrazione di cure mediche o a pagamenti passati, presenti o futuri per assistenza sanitaria.[5] Pertanto il livello di sicurezza necessario per proteggere i dati PII varia a seconda dell'ente normativo che definisce la protezione.

- **Quali sono i requisiti dell'organizzazione per la gestione dei dati PII?** Una volta ottenuto un quadro chiaro del modo in cui le informazioni PII vengono definite legalmente, l'organizzazione può esaminare *dove* le informazioni protette supportano i processi aziendali critici. I dati PII devono essere acquisiti, archiviati e conservati solo nei casi in cui ciò sia assolutamente necessario. Per quanto possibile, i dati PII devono essere eliminati dai processi aziendali oppure resi "non personali". Rendere anonimi i dati PII significa rimuovere o oscurare una quantità sufficiente di attributi in modo che le informazioni non possano più identificare un individuo.[6] Ciò consente all'organizzazione di continuare a supportare una funzione aziendale basata sui dati provenienti dalle informazioni PII, senza incorrere nel maggiore rischio associato alla conservazione e all'elaborazione delle informazioni PII nell'ambito di tale funzione. L'auditor della conformità della sicurezza dei dati PII deve verificare che l'organizzazione abbia applicato correttamente la definizione legale di PII per individuare i requisiti di trattamento dei dati PII, nonché verificare che l'organizzazione disponga di un processo consolidato per rivedere i requisiti e raccomandare l'eliminazione o il trattamento "anonimo" dei dati PII.
- **L'organizzazione ha effettuato la valutazione del rischio per i dati PII?** Le organizzazioni dovrebbero classificare i rispettivi dati PII in base all'impatto derivante dalla divulgazione delle informazioni. A seconda del settore economico di appartenenza e del tipo di dati PII trattati da un'organizzazione, è possibile valutare diversi fattori per stabilire il rischio associato alle informazioni PII. Potenziali fattori comprendono il *grado* di identificabilità delle informazioni, la *quantità* di dati PII e la *sensibilità* di tali dati (ad esempio, un codice fiscale o un numero di carta di credito sono dati più sensibili delle abitudini di acquisto o dello stato civile di una persona).[7] L'auditor deve verificare che sia stata effettuata una valutazione del rischio accurata e che i vari tipi di informazioni PII siano trattati con il giusto grado di riservatezza.
- **Tutti i controlli necessari per il trattamento dei dati PII sono previsti dalla politica di sicurezza dell'organizzazione?** L'auditor deve esaminare la politica di sicurezza dell'organizzazione per verificare che preveda le misure di sicurezza necessarie per proteggere i dati PII, in conformità con le leggi e/o i regolamenti applicabili. La politica deve indicare chiaramente gli obiettivi che supportano un livello adeguato di sicurezza dei dati PII e che rispondono ai requisiti di conformità, ai requisiti aziendali e al livello di rischio accettabile per l'organizzazione, e dai quali è possibile trarre standard, procedure e linee guida efficaci. La politica di sicurezza deve prevedere inoltre il monitoraggio della conformità, l'applicazione delle sanzioni nei confronti dei trasgressori e la verifica dell'efficacia dei meccanismi di controllo mediante monitoraggio e test di sicurezza periodici.

AUDITING A LIVELLO PROCEDURALE

Il livello successivo che l'auditor deve esaminare è il livello procedurale. Si tratta del livello in cui gli obiettivi strategici della sicurezza dei dati PII vengono tradotti in standard, procedure e linee guida. Inoltre, sempre a questo livello, vengono comunicati ai dipendenti la definizione di PII, gli obiettivi strategici e gli standard, le procedure e le linee guida. L'auditor deve verificare che standard, procedure e linee guida soddisfino e supportino gli obiettivi della policy per quanto riguarda la sicurezza dei dati PII, e che la comunicazione ai dipendenti sia adeguata ed efficace. Le domande da porre a questo livello sono le seguenti:

- **Gli standard, le procedure e le linee guida supportano gli obiettivi di sicurezza della policy?** L'auditor deve esaminare tutti gli standard, le procedure e le linee guida per accertare che supportino efficacemente gli obiettivi della politica di sicurezza

> "Ogni misura di sicurezza interessa la sicurezza dei dati PII."

dell'organizzazione. La policy di sicurezza deve prevedere tutte le problematiche attinenti la sicurezza dei dati PII inclusi, ad esempio, un adeguato controllo degli accessi, la crittografia, la classificazione dei dati e la loro distruzione Tuttavia, l'ambito della revisione non può essere limitato agli standard, alle procedure e alle linee guida specifici per i dati PII, poiché ogni misura di sicurezza interessa la sicurezza dei dati PII. Ad esempio, una procedura di reimpostazione della password poco rigorosa potrebbe consentire l'accesso non autorizzato a un terminale o a un database contenente dati PII, così come una carenza nella sicurezza fisica potrebbe permettere a qualcuno di sottrarre dati fisici o dispositivi contenenti dati PII non crittografati.

- **Tutti i dipendenti e/o gli utenti hanno ricevuto una formazione adeguata per l'individuazione e la gestione dei dati PII?** È necessario mettere in atto procedure per accertare che tutti i dipendenti ricevano una formazione adeguata prima di gestire i dati PII. Coloro che gestiscono direttamente i dati PII devono ricevere una formazione specifica; tuttavia, tutti i dipendenti dell'organizzazione dovrebbero essere in grado di individuare le informazioni PII e di avviare le specifiche procedure in caso di violazione della sicurezza di tali dati. Spetta all'auditor verificare in che modo policy, standard, procedure e linee guida vengono comunicati all'interno dell'organizzazione.[8] L'auditor deve stabilire se i metodi di comunicazione sono efficaci e se le responsabilità sono chiaramente assegnate. Ad esempio, se l'organizzazione intende applicare sanzioni nei confronti dei dipendenti che violano le procedure di gestione dei dati, la semplice affissione di un poster accanto al distributore automatico di caffè con la descrizione dei dati PII e delle modalità di gestione di tali informazioni probabilmente non costituisce un mezzo di comunicazione adeguato. E se un dipendente non beve caffè? In questo scenario, una formazione specifica seguita da una dichiarazione di comprensione firmata dall'interessato, conservata come documento ufficiale dalle Risorse Umane e comprendente le procedure di una gestione appropriata e le conseguenze derivanti dalla mancata osservanza, sarebbero molto più efficaci.
- **Esistono piani e procedure efficaci per rispondere agli incidenti riguardanti la sicurezza dei dati PII?** Generalmente una preparazione approfondita rappresenta il fattore determinante quando un incidente riguardante la sicurezza non viene gestito in modo corretto. Lo sviluppo di un piano di risposta agli incidenti obbliga le parti interessate, nell'ambito dell'organizzazione, a prendere decisioni ben ponderate sulle modalità di gestione dei numerosi aspetti degli incidenti riguardanti la sicurezza dei dati PII. Le decisioni possono vertere sulle modalità di miglioramento della situazione, segnalazione dell'incidente e compensazione delle persone interessate. Tali decisioni devono essere integrate nelle politiche e nelle procedure volti a rispondere agli incidenti riguardanti la sicurezza dei dati PII.[9] L'auditor ha il compito di verificare che tali piani siano stati sviluppati e che vengano rivisti periodicamente per garantire che ogni scenario immaginabile sia stato preso in considerazione.

AUDITING A LIVELLO OPERATIVO

Durante l'ultima fase dell'auditing, gli auditor della conformità della sicurezza dei dati PII eseguono la verifica e il monitoraggio della sicurezza per valutare l'efficacia dei sistemi di controllo. Si tratta essenzialmente di test per accertare che le misure di sicurezza dei dati PII funzionino in modo corretto. Le organizzazioni possono disporre di politiche, procedure e programmi di formazione molto validi per la protezione dei dati PII; tuttavia, se i dipendenti ai livelli più bassi non comprendono la formazione e/o non seguono le procedure, o se criticità inattese dei sistemi di sicurezza consentono l'accesso non autorizzato, l'investimento dell'organizzazione nella sicurezza dei dati PII risulterà vano. Un auditing della sicurezza delle informazioni PII non è completo senza la verifica dell'implementazione e dell'efficacia delle misure di sicurezza nelle attività giornaliere. Le domande da porre a questo livello sono le seguenti:

- **Si riscontra la presenza di dati PII al di fuori dei limiti previsti?** Il monitoraggio delle informazioni PII deve riguardare anche i dati memorizzati e i dati trattati e non deve essere limitato ai processi aziendali che prevedono l'uso di dati PII, ma deve interessare l'intera organizzazione, inclusi i confini dei sistemi informativi (IS) dell'organizzazione. L'auditor deve verificare che non si riscontrino dati PII in processi aziendali per i quali tali dati non sono necessari e che la crittografia sia utilizzata in modo efficace quando i dati PII sono comunicati ad aree a rischio, ad esempio al di fuori della rete interna dell'organizzazione oppure quando vengono archiviati in aree a rischio, come nel computer portatile di un dipendente (suscettibile di furto). L'auditor deve esaminare inoltre i processi aziendali che utilizzano i dati PII, per verificare che non vengano raccolte e archiviate più informazioni PII di quanto non sia strettamente necessario.

Durante il monitoraggio dei dati memorizzati è possibile riscontrare dati PII in situazioni inattese, quali metadati, file eliminati o contrassegnati per l'eliminazione, flussi di dati secondari, file grafici, file di spooler di stampa, file di collegamento, RAM e file di paging, hive del registro del sistema operativo. Inoltre vi sono molti modi in cui un utente

> "I dati PII possono trovarsi in situazioni inattese."

malintenzionato può oscurare i dati PII per impedirne il corretto monitoraggio, ad esempio modificando le estensioni dei file. Per tali motivi, gli strumenti migliori per monitorare i dati PII memorizzati durante un auditing sono gli strumenti di analisi forense.[10]

Al termine del monitoraggio, l'auditor può determinare l'efficacia del processo di monitoraggio interno dell'organizzazione. L'auditor deve verificare se la registrazione degli accessi è stata attivata per tutti i sistemi critici e se l'organizzazione ha assegnato in modo adeguato il compito di monitorare l'esecuzione. Inoltre l'auditor deve utilizzare i log di monitoraggio per controllare se gli utenti trattano i dati PII secondo le procedure.[11]

- **Il controllo accessi ai dati PII è efficace?** L'auditor deve verificare che il controllo accessi all'interno dell'organizzazione impedisca l'accesso non autorizzato ai dati PII. Solo gli utenti autenticati che hanno ottenuto la necessaria autorizzazione possono accedere ai dati PII. È opportuno accordare l'autorizzazione solo alle persone che devono eseguire l'accesso per gestire processi aziendali critici; spetta all'auditor verificare che le persone autorizzate abbiano superato i controlli di sicurezza previsti. La verifica deve comprendere anche il penetration testing, per accertare che i controlli siano efficaci e impediscano l'accesso non autorizzato dall'esterno. L'auditor deve verificare inoltre che i controlli impediscano attacchi privilege escalation che consentano agli utenti non autorizzati di accedere ai dati PII e che l'autenticazione degli utenti autorizzati soddisfi standard e linee guida adeguati per evitare che gli utenti non autorizzati possano accedere agli account degli utenti autorizzati.
- **La formazione è efficace? Le procedure vengono implementate e seguite?** L'auditor può ricorrere a diversi metodi per verificare se la formazione dei dipendenti è efficace. Ad esempio può semplicemente parlare con i dipendenti e chiedere loro di descrivere i dati PII, quindi passare in rassegna le procedure di sicurezza con il dipendente stesso. L'auditor deve esaminare i log e verificare che l'attività dei dipendenti corrisponda alle rispettive descrizioni e che queste, a loro volta, corrispondano alle disposizioni legali nonché ai criteri di sicurezza e agli standard, linee guida e procedure dell'organizzazione. La mancata osservanza delle procedure da parte dei dipendenti potrebbe significare che la formazione è inefficace, o che le sanzioni non sono abbastanza severe o che vengono applicate con eccessiva indulgenza, oppure entrambe le cose insieme. Qualora riscontri il mancato rispetto delle procedure appropriate, l'auditor deve impegnarsi a individuare la causa dei processi difettosi, piuttosto che cercare di risolvere ogni singolo incidente.

CONCLUSIONI

La conduzione di un auditing della conformità della sicurezza dei dati PII è un'attività impegnativa e sfidante. Un auditing efficace dei dati PII non può essere limitato a settori o processi aziendali specifici di un'organizzazione. Analogamente, non è possibile limitare l'ambito dell'auditing dei dati PII a un determinato livello per valutare l'efficacia dei controlli di sicurezza. L'uso di un approccio a tre livelli, dall'alto in basso, consente agli auditor di coprire efficientemente un'intera organizzazione ed duplicazioni e processi ridondanti a causa di carenze ai livelli più alti.

NOTE FINALI

1 US Government Accountability Office, "Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information," Report 08-536, USA, Maggio 2008, *www.gao.gov/new.items/d08536.pdf*

2 Pan, Yin; Bill Stackpole; Luther Troell; "Computer Forensics Technologies for Personally Identifiable Information Detection and Audits," *ISACA Journal*, vol. 2, 2010, *www.isaca.org/archives*

3 Identity Finder, Identity Theft News, *www.identityfinder.com/news/*

4 Rai, Sajay; Phillip Chukwuma; "Top 10 Security and Privacy Topics for IT Auditors," *ISACA Journal*, vol. 2, 2010, *www.isaca.org/archives*

5 Yale University, *HIPAA Policy 5100: Protected Health Information Security Compliance*, 20 aprile 2011, *www.yale.edu/ppdev/policy/5100/5100.pdf*

6 McCallister, Erica; Tim Grance; Karen Scarfone; Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information*, National Institute of Standards and Technology, Aprile 2010, *http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf*

7 *Ibid*.

8 *Op. cit.*, Rai

9 *Op. cit.*, McCallister

10 *Op. cit.*, Pan

11 *Op. cit.*, Rai