CASE STUDY

Regione Emilia Romagna e Sinergy

Seppur dettata da esigenze normative di adeguamento al Provvedimento del Garante Privacy "Amministratori di sistema" del 27 novembre 2008, la Regione Emilia Romagna ha sin da subito voluto interpretare al meglio questa nuova esigenza. Si rendeva necessario consentire agli amministratori di sistema, l'implementazione delle policy di sicurezza e, al tempo stesso, valutarne in real-time l'attuazione attraverso avvisi di violazione e una reportistica mirata.

La risposta ad istanze puntuali di protezione dei dati personali è stata vista in Regione Emilia Romagna anche come "opportunità" per una modernizzazione del sistema IT, più efficace e funzionale. Un'attenzione al tema della sicurezza superiore alla media e molto peculiare, in virtù della quale l'ente Regione ha strutturato un team di professionisti, guidato da un Responsabile della Sicurezza. Il team si è impegnato in primis nell'analisi, valutazione dei rischi ed identificazione delle idonee procedure per una limitazione del rischio in linea con le nuove policy e successivamente, nello sviluppo e implementazione di nuove soluzioni. *"Già con l'obbligo normativo di effettuare l'analisi dei rischi abbiamo visto questi interventi con una prospettiva più ampia, ossia quella di monitorare e migliorare la sicurezza informatica,-* ***spiega Fabio Bucciarelli, responsabile delle attività inerenti la sicurezza informatica per la Giunta della Regione Emilia Romagna****. -Questi sono diventati, infatti, veri e propri strumenti di lavoro a partire dai quali si implementano le misure di sicurezza con un aggiornamento annuale anche in assenza di istanze normative, revisionando con continuità la metodologia stessa alla base dell'analisi dei rischi".*

www8.hp.com

LE FASI DI INTERVENTO

"Per un'organizzazione di oltre 4.500 utenti che opera in modo continuativo (Rete Regionale Dipendenti e Consulenti) la protezione degli utenti era diventata cruciale, così come la sicurezza perimetrale per la quale la Regione aveva già adottato un buon sistema di sicurezza: due facce di una stessa medaglia con complemen-

CASE STUDY

*tare significatività in ambito «Intrusion & Prevention»". **racconta Fabio Bucciarelli.***

*"Il primo intervento, realizzato con il supporto di Sinergy è stato l'inserimento della prima sonda inizialmente posizionata 'in frontiera' **- prosegue Bucciarelli -** perché si rendeva necessario ispezionare il traffico valutandone i rischi e innescare dei blocchi con filtri per attacchi. Successivamente, poiché la protezione esterna non era sufficiente, sono state utilizzate due sonde per proteggere la rete interna da traffico malevolo, in particolare per i Data Center".*

Anche il secondo tema (Log Management), affrontato ed integrato con il precedente è stato interpretato in Regione in modo più esteso, realizzando nel contempo un sistema di monitoraggio della sicurezza centralizzato che permettesse di fare molto di più di quanto richiesto dal Garante.

"Siamo partiti con l'installazione di un appliance HP (Logger AE7200) per la raccolta dei log, predisponendo tutte le componenti di integrazione con i diversi sistemi in uno scenario estremamente eterogeneo e distribuito al fine di normalizzare tutte le sorgenti in un unico formato. Il concentratore di log si fa carico, infatti, della conservazione in modalità sicura di tutti questi dati, consentendo la ricerca anche a posteriori".

SINERGY: UN PARTNER DI QUALITÀ

"L'information Security è per la Giunta Regionale un supporto trasversale a tutte le strutture che collaborano alla gestione e allo sviluppo del sistema informativo dell'Ente; - raccon-

Fabio Bucciarelli

*ta **Bucciarelli** -il supporto del Partner Sinergy **- evidenzia Bucciarelli -** è stato molto importante per tutti gli aspetti di implementazione, in particolare del sistema di log management, poiché ci voleva esperienza progettuale completa e competenze tecnologiche capaci di inserirsi in una realtà molto complessa come la nostra".*

UNO SGUARDO AL FUTURO

"Alcuni progetti seppure in spending rewiew sono in via di definizione anche nella componente security soprattutto in ottica razionalizzazione progetti e ottimizzazione costi. Nasce da questa necessità l'importanza di definire KPI qualitativi/quantitativi a supporto dei nuovi investimenti. In parallelo stiamo osservando aree quali la protezione dei dati non strutturati e tematiche di strong authentication".

*"Il tema della revisione metodologica **- conclude Bucciarelli -** è, inoltre, sempre molto importante quale segnale della sensibilità del nostro Ente verso la stesura di policy e loro verifica/attualizzazione nel tempo".* ■