Sommario Rassegna Stampa

Pagina	Testata	Data	Titolo	Pag.
Rubrica	**Oracle**			
38/41	Top Trade Informatica	01/05/2012	*LA MATURITA' DELLA SICUREZZA AL TEMPO DI MOBILITY E CLOUD*	3

toptrade informatica
Mensile
PLEON
Data 05-2012
Pagina 38/41
Foglio 1 / 3

La maturità della sicurezza al tempo di mobility e cloud

La sicurezza non passa mai di moda, anzi. Questa è la sintesi della chiacchierata con gli operatori di canale specializzati in security su prospettive e opportunità del settore. Se, da un lato, il cliente è a uno stadio di consapevolezza abbastanza avanzato, dall'altra le nuove tendenze come l'enterprise mobility o il cloud richiedono nuovi approcci e nuove metodologie che non sempre l'azienda cliente è in grado di comprendere e apprezzare.
«È necessario spostare l'attenzione degli utenti - ha affermato Stefano Paganelli, line of business manager, security & network integration di Dimension Data Italia - dall'approccio alla security come un insieme di oggetti che risolvono un'esigenza temporanea a una visione più ampia basata sul concetto di infrastruttura di sicurezza. Ancora oggi si fa troppa attenzione al firewall di nuova generazione senza avere le idee chiare sull'esigenza specifica che si vuole risolvere».
Il system integrator, allora, deve tentare un timido approccio innovativo senza però mostrarsi impreparato di fronte all'esigenza tradizionale di application e di end-point security.
«Lutech punta all'innovazione - ha dichiarato Bernardino Grignaffini, practice manager, security & IT governance del system integrator lombardo - monitorando e supportando le aziende contro le nuove minacce, senza dimenticare la security classica. È un approccio su due piani: il fulfillment del mainstream e l'allineamento alle nuove esigenze del mercato».
La responsabilità di questa situazione transitoria è in parte dei vendor che, a detta di molti, hanno spinto per troppi anni sulla singola soluzione, software o hardware, per risolvere il problema immediato. La situazione, però, va tutto a vantaggio del system integrator che, onorando la propria missione, è in grado di integrare i singoli pezzi scegliendo il best of breed delle diverse proposte modulando l'offerta alla specifica esigenza. Un approccio corretto prevede, come sempre, una completa analisi dei rischi e mai come oggi l'offerta in quest'ambito è corposa: ci sono gli standard procedurali, ci sono i tool e le best practice.

Nonostante il mercato rincorra ancora la tecnologia sulla prevenzione sul perimetro è ora di agire all'esterno dell'azienda con nuovi tool di monitoraggio

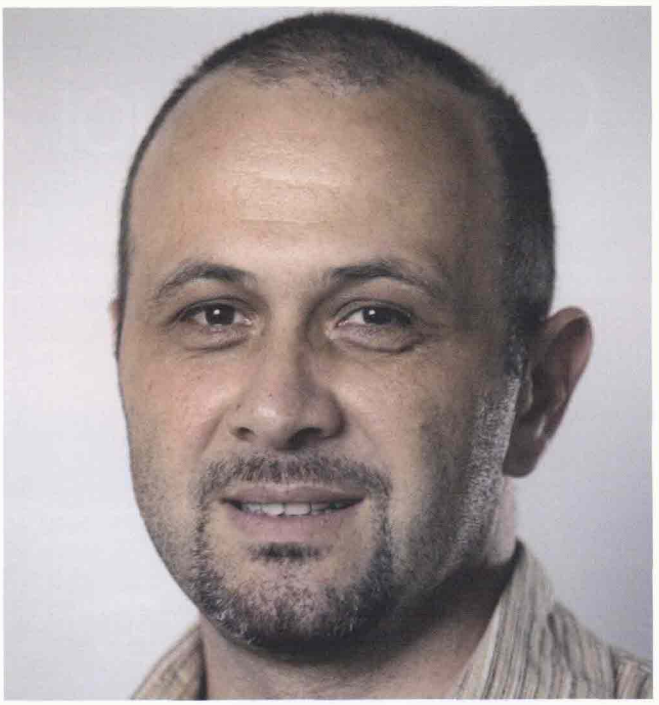
NON È SOLO HARDWARE

«Oggi - ha osservato Sergio Fumagalli, vice presidente di Zeropiù, partner storico di Oracle in ambito security - l'offerta si basa su forti componenti non espressamente tecnologiche e questo è un vantaggio che il mercato apprezza poiché i riscontri sono più immediati rispetto all'approccio con gli strumenti classici di qualche anno fa».
Signori si cambia, dunque: «Rispetto al passato in cui ci si focalizzava sulla prevenzione del rischio - ha proseguito Grignaffini - ora momenti come il rilevamento e la riposta diventano centrali. Le nuove modalità di attacco e i nuovi

trend riducono le capacità di difesa in prevenzione tipiche di antivirus e firewall e richiedono di proteggersi anche all'esterno dell'azienda. È giunto il momento di focalizzarsi sul rilevamento e sulla risposta».
Per questo cresce il gradimento per soluzioni di tipo Siem (Security information and event management) di Arcsight (acquisita da HP nel 2010), Rsa, Novell, Ibm o per soluzioni di monitoraggio dei dati e reportistica come quelle di Splunk, Symantec, Cisco e Airwatch. Si fanno largo, così, piccoli ma potenti tool realizzati con lo scopo specifico di risolvere le nuove minacce legate all'enterprise mobility e al Byod (Bring your own device). Si tratta di scenari completamente nuovi che richiedono che i Cio si pongano altri interrogativi, correndo ai ripari con una certa rapidità: «Per esempio, di chi è la responsabilità di un danno subito fuori dall'azienda? - Si è chiesto Paganelli - e, ancora, chi è il proprietario del terminale mobile in uso al dipendente?».
Nel momento in cui il manager lavora con il suo smartphone o con il tablet fuori dall'ufficio, si collega a reti di cui poco si sa, espone se stesso e l'azienda a pericoli nuovi capaci di minare l'integrità aziendale e su cui poco può fare la protezione classica sul perimetro.

COMPLIANCE E SICUREZZA IT SI FONDONO

L'enterprise mobility, e anche la cloud, richiedono uno sforzo intellettuale all'azienda cliente per considerare la sicurezza come un tema articolato in cui la governance non è più un argomento troppo distinto dalla security più propriamente IT.
Tutti gli operatori interpellati hanno distinto i due argomenti, perché generalmente gli interlocutori aziendali sono distinti e, soprattutto, perché gli approcci sfruttano strumenti e metodologie diverse. Ciò nonostante, non appena non è più sufficiente la protezione del perimetro, i due ambiti si avvicinano grazie al paradigma comune delle policy aziendali. Purtroppo, questa convergenza non è ancora realtà in azienda. «Sul mercato spesso sono presenti un responsabile della sicurezza, che si occupa di policy e di compliance - ha aggiunto Paganelli - poco tecnico e uno di estrazione più tecnica, spesso il Cio stesso. Il canale si trova a dialogare con due persone, una attenta alla tecnologia e l'altra alla compliance che non dialogano tra loro».
Eppure è proprio la compliance che, suo malgrado, fa da driver al settore dato il suo carattere di urgenza obbligata dalla normativa. I vincoli posti dalle leggi, soprattutto nel caso di aziende internazionali, rappresentano la maggior leva per il business e fortunatamente l'esperienza fatta finora ha portato a una maturazione dell'azienda cliente che evita gli abusi e gli eccessi degli ultimi anni.
«Molto spesso - ha continuato Grignaffini - accade che la nuova figura aziendale responsabile della compliance provenga dalla divisione IT».
Se, da una parte, il soggetto parla la stessa lingua del canale, dall'altra, però, è ancora troppo lontano da un approccio analitico e di progettazione.
Posto di trovarsi di fronte a un'azienda recettiva in questo senso, il canale lavora prima di tutto su un'analisi dei rischi e poi corre ai ripari con strumenti di protezione software, spesso realizzati appositamente, che veicolano il flusso di dati dall'azienda al terminale mobile e viceversa su Vpn monitorate puntualmente e che richiedono potenti autenticazioni.



Stefano Paganelli, line of business manager, security & network integration di Dimension Data Italia

BANCHE E FINANCE TIRANO LA VOLATA

«La nuova prospettiva è l'intelligence sulla governance - ha affermato Giacomo

DUE STUDI ILLUMINANTI

Al Security Summit 2012, la Oracle community for security ha presentato i due studi Privacy nel cloud e Mobile privacy che, ha detta di Sergio Fumagalli, hanno registrato un discreto successo (un totale di circa 5mila download poco tempo la pubblicazione sul sito della community).
«Abbiamo voluto dare un taglio specifico ai due documenti - ha spiegato Fumagalli - trattando il tema security dal punto di vista del titolare del trattamento dei dati personali di una tipica azienda italiana nella fase di passaggio verso il cloud e l'enterprise mobility».
Lo studio sul cloud ha evidenziato, in particolare, che le aziende si sentono ancora poco garantite a proposito di sicurezza anche e soprattutto a causa dell'estrema differenziazione dei servizi, dalla diversificazione delle tipologie di fornitori e dai diversi quadri normativi di riferimento dovuti alla "internazionalizzazione silenziosa" del dato. Sembra che, ancora una volta, la tecnologia superi la normativa risultando arduo far rientrare le relazioni tra i protagonisti di un'offerta cloud nel classico rapporto titolare-responsabile.
Sempre secondo lo studio, è fondamentale che le varie funzioni coinvolte operino in sinergia per rivedere i processi interni, operativi e di controllo, valutando l'impatto del cloud sull'organizzazione interna. Dall'altro lato, i fornitori dovrebbero adottare tecnologie e processi che garantiscano standard di interoperabilità e di sicurezza superiori agli attuali. Lo studio sulla Mobile privacy ha evidenziato, invece, le criticità correlate ad aspetti di natura tecnologica (per esempio, l'eterogeneità dei terminali e l'esistenza di vulnerabilità intrinseche delle piattaforme mobili). Ancora, il gruppo di lavoro della community Oracle sostiene che è necessario rivedere le misure minime di conformità alle normative dei terminali in particolare per quanto riguarda il controllo degli accessi logici, il salvataggio dei dati e l'adozione di soluzioni anti-malware. Lo studio è entrato molto nello specifico del tema segnalando, per esempio, aspetti come la dismissione dei terminali. Secondo il gruppo di lavoro, infatti, è importante prestare particolare attenzione alla corretta eliminazione dei dati presenti su tutte le componenti del dispositivo, Sim esterna e memoria interna, come richiede il provvedimento del Garante della Privacy del 13/10/2008.