

Voglia di STANDARD in ambito sicurezza

Le innovazioni tecnologiche che stanno avanzando sul mercato, come la virtualizzazione e il cloud computing, affiancate dalla spinta della compliance normativa e dall'aumento della criminalità sul mondo virtuale, fanno della sicurezza uno dei fronti più caldi dell'It aziendale. Ne parliamo con Marco Bresciani, responsabile security It di Accenture in Italia, per avere alcuni consigli in merito. «Una volta il perimetro dei sistemi era ben circoscritto - ha esordito - mentre oggi sta diventando sempre più elastico, per cui è più difficile da difendere, grazie anche a servizi come il SaaS e quelli erogati attraverso il cloud, che può essere articolato su più livelli, dai processi all'applicazione, dalle piattaforme all'infrastruttura. Tutto questo obbliga le aziende utenti a valutare con attenzione la scelta del fornitore di servizi, per capire se è affidabile sia dal punto di vista finanziario che normativo. In particolare, prima di mettere le applicazioni sul cloud deve essere fatta un'attenta analisi di risk management».

Un altro tema che sta complicando la vita ai security manager, ricordato da Bresciani, è quello del moltiplicarsi dei terminali, soprattutto mobili, che utilizzano i lavoratori per accedere dall'esterno al sistema aziendale, «per cui il perimetro di difesa rischia di diventare ancor più vulnerabile - ha sottolineato il manager -. Inoltre, soprattutto le nuove generazioni di dipendenti spesso non usano nemmeno il pc per interagire con i sistemi aziendali, ma i device mobili di ultima generazione. Tutti questi fenomeni vanno controllati con attenzione, tenendo presente che la sicurezza, innanzitutto, va affrontata con un approccio culturale, il che significa affrontare i processi in un certo modo, per cui la tecnologia diventa solo un fattore

abilitante». Quindi, sparando il perimetro ben delineato di una volta, la difesa deve passare dal classico firewall e controllo dell'end point, che tuttavia servono sempre, a controlli di sicurezza che sono più legati o al soggetto dell'informazione, come l'utente, oppure all'oggetto della medesima, come il dato o i device utilizzati, e questo determina uno spostamento molto significativo. «Bisogna, dunque, attivarsi per l'identificazione delle risorse, il governo e il controllo del tipo di ac-

cesso che viene consentito - ha sottolineato il manager -. E tutto questo deve essere fatto in modo dinamico, o addirittura con una valutazione probabilistica del livello di rischio, anche perché va bilanciato dal fatto di poter dare un servizio con performance accettabili. Un altro aspetto interessante è che in questi ultimi anni è cambiato profondamente il livello di servizio che le aziende offrono al mercato. Per fare un esempio, una volta il servizio delle

banche era limitato alle ore in cui la filiale era aperta, adesso con l'online il servizio è diventato attivo 24 ore su 24, per sette giorni, per cui non è detto che la struttura It sia in grado di gestirlo attraverso il proprio Security operation center, ma potrebbe essere necessario demandare a chi può garantire questo tipo di servizio di sicurezza dati, soprattutto durante la notte e i fine settimana. E questo approccio, tipico di banche e telco, sta per essere adottato anche da altri settori di mercato, in quan-

to sempre più aziende si appoggiano a Soci esterni che erogano questi servizi, per cui si assiste a una continua commistione di servizi erogati internamente e di servizi affidati all'esterno».

In quest'ottica, secondo il manager, soprattutto con il cloud, non è vero che il ruolo dell'It diminuisce ma diventa più

importante, perché oltre a essere l'esecutore di servizi interni deve anche diventare l'autorità in grado di determinare quella che deve essere la governance complessiva del servizio, quali sono le regole per scegliere i fornitori esterni, valutare la sicurezza che offrono e quindi i rischi connessi. Ma un altro fenomeno che va attentamente considerato in ambito sicurezza è quello delle minacce che possono arrivare dall'interno, in particolare dai dipendenti che vengono licenziati, un fenomeno non trascurabile in questo momento di crisi.

La spinta della compliance

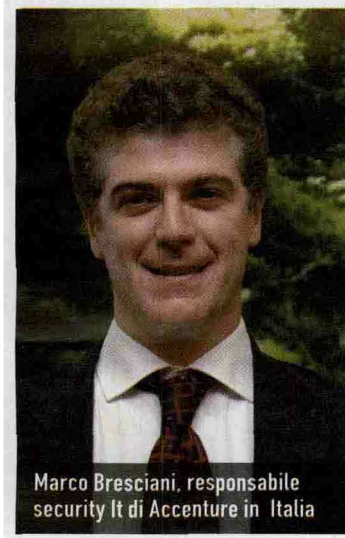
«Tuttavia, pur in un momento in cui la spesa It viene diminuita, - ha osservato Bresciani - è sintomatico che l'investimento in sicurezza continui a rimanere costante: cresce, infatti, la consapevolezza che diventando la tecnologia sempre più critica nella gestione del business e che ormai molti processi si svolgono sempre più in rete, è necessario avere un sempre

maggior governo della sicurezza. Dall'altro lato non è trascurabile la compliance normativa, proprio perché il business si diversifica, si internazionalizza, si sposta sempre più attraverso la rete, per cui vanno tenute presenti le regulation dei vari paesi esteri. Va anche detto che in questi anni c'è stata una maturazione del mercato, per cui si è affermato lo standard Itil, che

4

fa sì che quando una società prende servizi in casa propria o in outsourcing, la prima cosa che verifica è che siano industrializzati secondo quel modello. La stessa cosa vale per la sicurezza: ci sono standard, come per esempio l'Iso 27001, che prevede una serie di controlli che molti operatori del cloud rispettano e in effetti il tipo di maturazione e di industrializzazione del livello di sicurezza che viene chiesto all'It sta andando nella direzione di adeguamento agli standard. Peraltro è plausibile pensare che fra qualche anno verrà richiesto quasi da norma il fatto di avere l'identificazione fatta in un certo modo e lo stesso avverrà per l'identità delle applicazioni dei servizi in rete. Tanto più la rilevanza diventa di sistema, tanto più sarà regolamentata».

Maristella Rizzo



Marco Bresciani, responsabile security It di Accenture in Italia

sono i milioni di dollari spesi nel 2008 da **Accenture** nella formazione sulla sicurezza

UN APPROCCIO A LARGO RAGGIO

I servizi di sicurezza sono offerti da **Accenture** attraverso la Service Line Security, attiva da oltre vent'anni (fa parte della divisione Technology Consulting) che conta circa 1.650 professionisti a livello mondiale, che lavorano utilizzando metodologie collaudate e framework.

L'offerta sulla sicurezza include: Security Strategy & Risk Management (consiste in un approccio olistico, integrato e scalabile per la gestione dei rischi di sicurezza, che considera aspetti organizzativi, procedurali e tecnologici); Identity & Access Management (sviluppo di una strategia globale e fornitura di soluzioni che affrontino gli aspetti sulla gestione delle identità e accessi relativi a processi, tecnologie e persone); Enterprise Application Security (aiuta le aziende a proteggere le proprie applicazioni dalle minacce esterne, usando una combinazione di processi, tecnologie, training & awareness delle persone); Business Resilience (fornisce tecniche avanzate e innovative per il disaster recovery e la business continuity); Infrastructure Security (offre un approccio completo end-to-end per garantire la sicurezza delle infrastrutture tecnologiche e consentire un controllo granulare della sicurezza dei dati) e Data Protection & Privacy (individuazione e gestione dei flussi di dati sensibili e conduzione del risk assesment, che si fonda su due approcci: un'analisi top-down dei processi di business, focalizzata sul ciclo di vita dei dati sensibili e il loro uso legittimo, e un assesment bottom-up delle applicazioni per stabilire se i controlli chiave dell'applicazione sono adeguati per evitare la perdita dei dati sensibili).