



La security a misura dell'economia 2.0

Con l'esplosione di e-commerce ed e-banking le imprese e i consumatori chiedono la massima tutela dei dati. Tre aziende raccontano come la offrono

LA SICUREZZA OGGI INEVITABILMENTE SI declina anche attraverso tutte le tecnologie informatiche (IT): non soluzioni "virtuali", ma una vasta gamma di soluzioni che proteggono molte dinamiche della vita quotidiana. Basti pensare all'e-banking e a come il rapporto tra gli istituti di credito e i clienti oggi sia quasi completamente mediato dalle tecnologie. Analogamente a quanto avviene anche nell'e-commerce, con la possibilità di acquistare o vendere direttamente on line, con transazioni (anche di grande entità) gestite attraverso il proprio pc. La vita delle aziende trova nelle tecnologie non solo la soluzione più immediata a tante esigenze date dalla globalizzazione (l'e-learning e il telelavoro, che permettono di gestire anche a grande distanza il rapporto con i dipendenti): oggi più che mai è proprio il patrimonio di informazioni e di know-how a costituire la ricchezza di un'azienda, ecco perché è importante garantire la sicurezza sia nella "custodia" di queste informazioni, sia nella trasmissione e condivisione di esse

con altre aziende, con la necessità di sistemi che tutelino al massimo dalle intrusioni. Si tratta di piccoli esempi, che possono dare l'idea della vicinanza di questo tema alla vita di ogni cittadino. *Tempi* ha chiesto a tre diverse aziende che si occupano di questo settore nevralgico quali sono le ultime sfide che le coinvolgono.

Ibm

Ibm ha realizzato un'indagine approfondita, il Global IT risk study 2010, per capire come si stiano muovendo i responsabili informatici rispetto all'obiettivo della riduzione dei rischi. Tra gli obiettivi principali dello studio erano la valutazione del modo in cui innovazioni come il cloud e il mobile computing influiscono sulle strategie globali di rischio informatico e l'analisi di come il ruolo dei responsabili infor-

Secondo il Global IT risk study 2010 di Ibm, i nuovi tool di social network rappresentano la maggiore preoccupazione delle aziende. Ora li potranno integrare nella loro infrastruttura

matici stia cambiando in relazione a queste innovazioni. L'indagine ha coinvolto 556 intervistati provenienti da tutte le aree geografiche, che rappresentano aziende con ricavi da meno di 500 milioni di dollari fino a 10 miliardi di dollari, e appartenenti a diversi settori, quali finanza, assistenza sanitaria, biotecnologie, produzione, pubblica amministrazione e servizi informatici. Ebbene, i manager coinvolti prevedono un aumento delle loro responsabilità correlate al rischio.

Anche se le imprese e i loro responsabili di information technology hanno strutture e modi diversi di raggiungere i propri obiettivi, concordano sulle aree di focus per il successo di un programma di gestione del rischio IT. Primo punto: all'interno di un'impresa, la consapevolezza del rischio è responsabilità di tutti. Occorre perciò che politiche e procedure correlate al rischio siano radicate nella cultura aziendale. Perciò le aziende devono impegnarsi maggiormente a educare, comunicare e supportare le iniziative di gestione del rischio e conformità in tutta l'impresa.

Secondo punto: i dati sono un motivo di preoccupazione comune in tutti gli aspetti della gestione del rischio IT (dalla sicurezza alla business resilience e continuità, dalla disponibilità delle infrastrutture al disaster recovery, dagli attacchi degli hacker alla conformità, fino alla gestione dei dati). Le aziende dovrebbero quindi adottare un approccio unificato e olistico al rischio IT, tenendo conto di tutti gli elementi che caratterizzano il rischio, con l'obiettivo generale di realizzare maggiori ritorni ed efficienze più elevate. Un esempio è l'Ibm security framework (Isf), un modello sviluppato per ►

► definire la sicurezza in termini di risorse di business che devono essere protette. L'Isf analizza le problematiche di sicurezza secondo un approccio orientato al business, basandosi su best practices, tecnologie e servizi e suddividendo la sicurezza in cinque domini: governance e gestione del rischio; persone e identità; dati e informazioni; applicazioni e processi; reti, server ed endpoint. Il tutto per aiutare le aziende ad essere "secure by design", ovvero per fare in modo che la sicurezza sia intrinseca rispetto ai propri processi di business, allo sviluppo dei prodotti e alle attività operative quotidiane ed affrontando al contempo i concetti emergenti di conformità.

Terzo punto: tra i trend emergenti nelle soluzioni, c'è la necessità di incorporare il cloud computing, la tecnologia mobile e il social networking nell'infrastruttura esistente. I tool di social networking sono stati il principale motivo di preoccupazione, in termini di rischio, per il 64 per cento degli intervistati, per lo più in termini di accessibilità, uso e controllo dei dati, soprattutto per quanto riguarda il pericolo di un accesso non autorizzato a informazioni riservate e proprietarie. Questo perché molte organizzazioni non hanno ancora posto in essere processi e metodi per integrare tali tool nella loro infrastruttura e nel loro flusso di lavoro. Adottando un approccio proattivo, le aziende possono posizionarsi in modo da restare un passo avanti alle vulnerabilità. Un esempio di questo approccio sono i servizi di sicurezza gestiti da Ibm, (o "Ibm Managed security services") che permettono alle aziende di demandare ad Ibm l'identificazione delle vulnerabilità dei dispositivi di rete, dei server, delle applicazioni web e di posta, oltre che la gestione dei problemi di sicurezza, il tutto con l'efficienza e la flessibilità tipiche dei servizi in modalità cloud. È disponibile per le aziende di qualsiasi dimensione che desiderino affrontare in modo facile e rapido le esigenze di conformità, ed è gestito presso i Security operation center di Ibm in tutto il mondo.

T-Systems

Sotto la spinta di normative nazionali e internazionali, molte aziende hanno sviluppato un programma per la gestione del rischio e della sicurezza informatica. T-Systems si rivolge al mercato con modelli di sicurezza "end-to-end" attraverso la perfetta sinergia tra la profonda conoscenza delle diverse aree di business e l'impiego di standard tecnologici elevati, che costruiscono un valore competitivo reale.

Il brand appartenente al gruppo Deutsche Telekom conserva nel proprio



Ci sono soluzioni che consentono di rilevare la minaccia di frodi in tempo reale, con l'analisi dei movimenti sui conti correnti; o di seguire passo passo le proprie istruzioni di pagamento

Dna un approccio olistico, e al contempo pratico e modulare, alla sicurezza che consente la realizzazione di progetti sulla base delle specifiche esigenze di business dei propri clienti. In un contesto complesso come quello rappresentato da internet è necessario alzare il livello di guardia e potenziare ancor di più gli attuali sistemi di monitoraggio delle transazioni.

Il sistema di tracciabilità delle frodi "Fraud detection" di T-Systems svolge una funzione proattiva in quanto rileva, in tempo reale, le minacce di frodi attraverso l'analisi delle attività effettuate sui sistemi di pagamento e/o sui conti correnti per analizzarne i comportamenti e le modalità di accesso, confrontarle con una casistica estesa in grado di autoalimentarsi e di fornire indicazioni puntuali su quanto rilevato. Nell'ambito della funzionalità del sistema, un motore di rilevazione stima il rischio di frode di un'operazione, dall'accesso da parte del cliente fino a tutte le attività successive, quali, ad esempio, il cambio di indirizzo o il trasferimento di fondi. La soluzione è "trasparente" ai potenziali malintenzionati per non consentire loro di apprendere le regole del sistema e al tempo stesso non reca alcuna turbativa ai clienti.

TAS

La Psd (Payment service directive) è la nuova direttiva che liberalizza il settore europeo dei pagamenti e, dalla ratifica in Italia nel gennaio 2010 è una realtà per ogni operazione di incasso e pagamento. TAS, azienda che progetta e realizza soluzioni software, da anni lavora con il siste-

ma bancario in Europa ed in Sud America ed è attore principale nel trasmettere agli utilizzatori degli strumenti di pagamento (tradizionali, elettronici e con carte di pagamento) un'avanzata percezione della sicurezza delle transazioni da loro immesse nel sistema tramite Cbi, Internet, Atm e Pos. Il soggetto che istruisce un pagamento, sia esso un cittadino o un'azienda, attraverso un canale messo a disposizione dal proprio prestatore di servizi (banca o payment institution), ha la necessità del trattamento sicuro dei dati che ha trasmesso. In questo contesto i circuiti finanziari hanno predisposto dei processi adeguati per la cifratura e verifica dei dati nella tratta end-to-end e cioè dal mittente fisico al ricevente fisico.

I prestatori di servizi di pagamento hanno inoltre attivato nei loro work-flow dei processi di prevenzione e scudo contro le frodi, specialmente per le carte di pagamento, in grado di controllare i pagamenti richiesti da una carta nello spazio e nel tempo. La Psd richiede però un'ulteriore attenzione attraverso la tracciatura dell'operazione all'interno del circuito finanziario. Quest'ultimo requisito rende possibile creare una reale interazione con il cliente per personalizzare l'interazione con il prestatore di servizi di pagamento sullo stato delle proprie istruzioni di pagamento e verificare on-line eventuali richieste di addebito (su carta o conto corrente) non precedentemente autorizzate. La tecnologia è disponibile e ormai tutti siamo dotati di un terminale che può connettersi in modalità sicura. TAS ha iniziato a proporre, al fianco delle proprie soluzioni di crittografia dei dati e anti frode avanzate, una soluzione che consente ai prestatori di servizi di pagamento di offrire ai propri clienti, nel rispetto della privacy, una maggiore percezione dello stato delle istruzioni di pagamento.