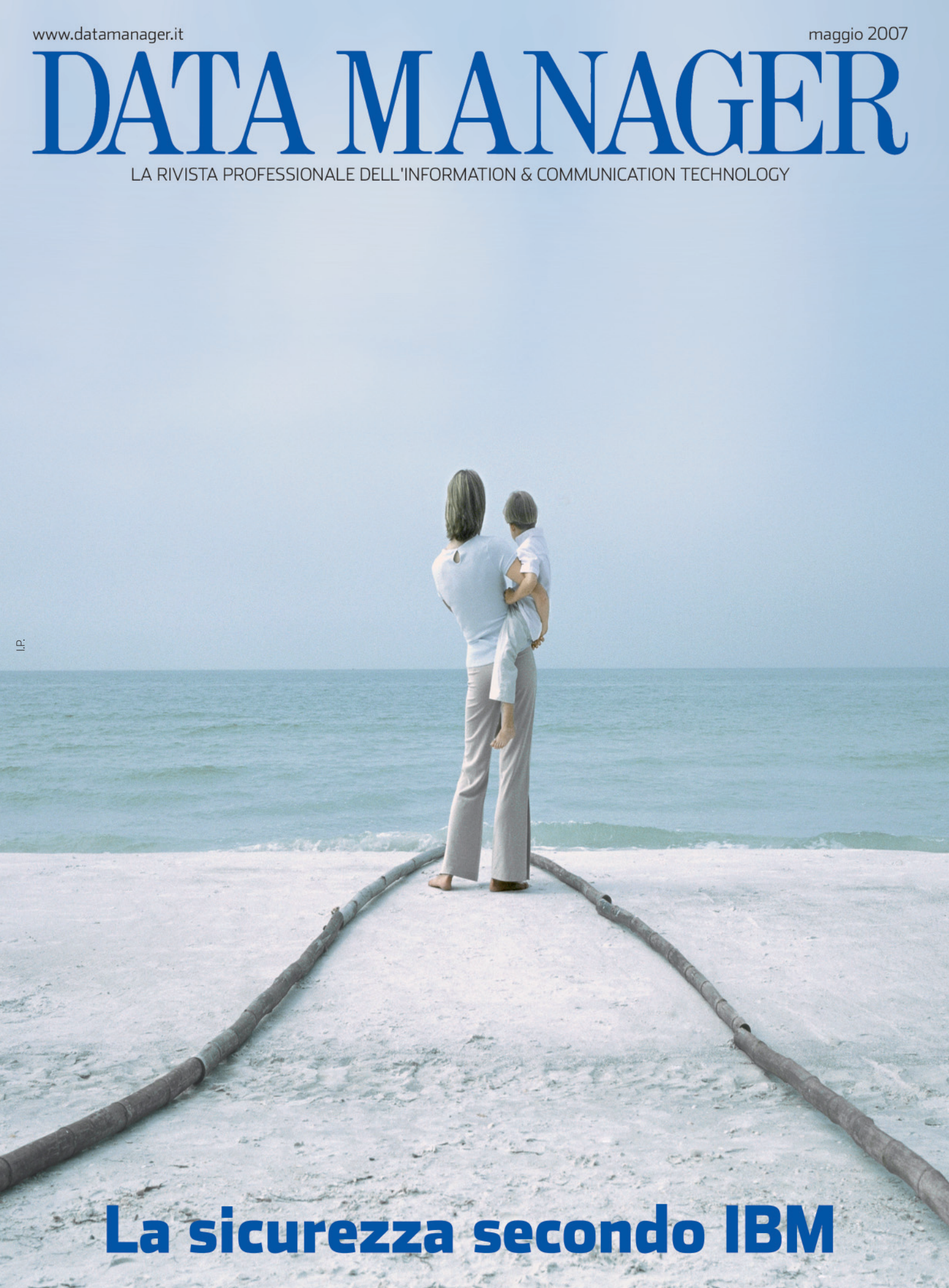
www.datamanager.it

maggio 2007

DATA MANAGER

LA RIVISTA PROFESSIONALE DELL'INFORMATION & COMMUNICATION TECHNOLOGY



I.P.

La sicurezza secondo IBM

Introduzione

CRESCERE IN SICUREZZA

L'evoluzione della security, da fenomeno tecnologico a valore strategico di componente essenziale del business

di Edoardo Bellocchi

La sicurezza è da tempo in cima alle priorità degli investimenti It da parte delle aziende. Ma non è solo l'aumento delle minacce "classiche", come virus, attacchi di hacker, oppure phishing, a far focalizzare l'attenzione sulla sicurezza. Perché una spinta rilevante è data anche dai cambiamenti avvenuti nei paradigmi di business. Gli imperativi della flessibilità, della reattività e della competitività hanno fatto sì che i processi di business vadano sempre più oltre i confini dell'azienda. L'esplosione delle reti e delle connessioni remote, con tutto il corollario di computer portatili, di palmari e di altri dispositivi wireless, ha ulteriormente complicato gli scenari, portando problematiche prima sconosciute che necessitano di soluzioni sempre nuove e sofisticate. E soprattutto di un approccio nuovo, che tenga conto dei nuovi paradigmi: oggi si parla di "data centric security", vale a dire di sicurezza basata sul valore e sull'importanza che i dati e le informazioni hanno per l'azienda, mentre perde sempre più importanza la "risk centric security", quella che basa l'approccio solo sui rischi e le minacce.

L'EVOLUZIONE DELLA SECURITY

Ed è anche per questo che il segmento della sicurezza, inteso in senso ampio, comprendente oltre alle soluzioni di sicurezza anche la business continuity e il disaster recovery, è quello che cresce di più all'interno dell'intero settore It. Perché quello della security è un processo continuo, dove nuove esigenze e nuove soluzioni si susseguono in base sia all'evoluzione dell'azienda, sia all'evoluzione del mercato e dell'ambiente esterno, per esempio al sorgere di nuove minacce o di nuove disposizioni normative. Ma anche le tecnologie più attuali hanno guidato il cambiamento verso una maggiore importanza strategica della sicurezza: un esempio illuminante a questo proposito è l'utilizzo delle reti di trasmissione su protocollo Internet (Ip) da parte degli apparati anti-intrusione, quali telecamere o altri sistemi, che ha determinato uno spostamento dell'orizzonte anche della sicurezza "fisica", ormai sempre più collegata alla rete aziendale e connessa ai "dati" della sicurezza "logica". Rendendo quindi sempre meno netta la tradizionale distinzione tra sicurezza "logica", cioè quella attinente alle reti, ai sistemi aziendali, alle infrastrutture e ai dati, e sicurezza "fisica", riguardante i beni fisici dell'azienda o il territorio.

La sicurezza secondo IBM

LA STRATEGIA IBM

IBM è da sempre attenta alla sicurezza e offre numerose soluzioni per tutti i settori di business e per tutti i più importanti aspetti in cui si articola l'universo "security". E in effetti, l'offerta di **IBM** (www.ibm.com/it/sicurezza) in questo ambito, vasta e strutturata, è in grado di proporre un reale approccio "one stop shopping", sia tramite le proprie soluzioni, tra le quali vi sono quelle "storiche" della gamma Tivoli, sia tramite l'integrazione di offerte di partner come Cisco. Senza dimenticare le acquisizioni, tra le quali si possono citare quelle di **Access360**, **Micromuse** e **Consul**, i cui prodotti sono stati inglobati nell'offerta di software Tivoli e la più recente: l'acquisizione di **Internet Security Systems** (ISS, www.iss.net), annunciata ad agosto 2006 e ormai completata, all'interno della struttura di Global Technology Services. I prodotti e le soluzioni di ISS vanno a complementare al meglio l'offerta di IBM nell'ambito della "Threat Mitigation", cioè quella relativa alla sicurezza perimetrale, volta a difendere l'infrastruttura dalle intrusioni non desiderate quali virus e hacker.

La combinazione con l'offerta di ISS permette a Big Blue di dare vita all'innovativa strategia di **Security On Demand**, che significa soprattutto servizi avanzati, completa scalabilità di costi e massima sicurezza anche nelle ore notturne, garantita dai Security Operation Center che coprono tutto il mondo 24 ore su 24 per 365 giorni all'anno. Infatti, al Centro operativo di sicurezza IBM di Boulder in Colorado si sono aggiunti i grandi centri ISS di Atlanta, Tokyo e Bruxelles, che, insieme ai centri regionali, portano a dieci il totale delle strutture operative a disposizione dei clienti. A livello mondiale, IBM conta più di 4.500 persone impegnate nell'ambito della sicurezza, presso i laboratori di sviluppo prodotti, tra i quali vi è il Tivoli Lab di Roma, e in attività di progettazione, implementazione, auditing e consulenza con i clienti. Sotto l'offerta di "IBM Security & Privacy", Big Blue comprende tutti i consulenti, gli architetti, i sistemisti e i capi progetto che collaborano con i clienti nella progettazione e nella realizzazione di soluzioni di sicurezza, oltre a fornire il supporto nelle fasi di esercizio.

LA METODOLOGIA DI SICUREZZA

L'obiettivo che guida le attività di IBM è quello di integrare la sicurezza all'interno dei processi aziendali, seguendo passi logici che coinvolgano tutti i livelli dell'organizzazione. Questo significa definire un programma di sicurezza efficace basato su un ciclo composto da varie fasi: Assess, Plan, Design, Implement e Run, con particolare enfasi sugli aspetti di analisi e gestione del rischio e sulle soluzioni. L'offerta IBM prende come riferimento l'Information Security Framework: una vera e propria roadmap che indica tutte le capacità messe a disposizione dei clienti da IBM per rispondere alle molteplici esigenze delle diverse aree di sicurezza. Nelle pagine seguenti, le più importanti saranno esaminate in dettaglio: si parte dalla "Governance e Compliance", che forma la base dei moderni sistemi di security in quanto si riferisce sia al monitoraggio dei rischi sia al rispetto delle normative di legge riguardanti la sicurezza. Vi è poi tutto il capitolo della "Threat mitigation", che comprende le misure atte a tenere lontane dal perimetro aziendale tutte le minacce provenienti dall'esterno, come le intrusioni da parte di hacker o l'ingresso di virus nella rete. L'aspetto "Identity e Access Management" verte invece sull'offerta di soluzioni, principalmente basate sui software IBM Tivoli, che permettono di gestire in maniera centralizzata ed efficace gli accessi ai sistemi aziendali da parte delle persone autorizzate. L'importante capitolo della "Transaction e Data Integrity" attiene invece ai numerosi sistemi per garantire la confidenzialità dei dati e delle transazioni, oltre alla loro integrità anche in presenza di eventi dannosi, nella remota ipotesi che le misure preventive non siano risultate efficaci. Infine, l'Information Security Framework di IBM affronta anche il tema della sicurezza fisica, che ha assunto crescente importanza nel quadro delle nuove minacce non solo di carattere per così dire "software", e il tema anch'esso fondamentale della "Personnel Security", cioè dei servizi di formazione per sensibilizzare il personale sui temi della security.

I SERVIZI DI SICUREZZA GESTITI IN OUTSOURCING

Nell'offerta **IBM Security On Demand** hanno assunto sempre maggiore importanza i Managed Security Services, cioè i servizi di sicurezza gestiti in outsourcing. Attualmente, questi contano, secondo IDC*, per un 10% circa del mercato, ma la tendenza è verso una rapida crescita di questo valore. Il perché è presto detto: da una parte le minacce si fanno sempre più sofisticate e, dall'altra, la loro individuazione e neutralizzazione richiedono continuamente maggiori risorse, che non tutte le aziende sono disposte a distogliere dal loro core business. Avere quindi a disposizione le competenze e le capacità sempre aggiornate di un player globale come IBM si rivela quindi cruciale per avere la massima protezione a costi ragionevoli. Con i Managed Security Services, IBM si propone infatti in veste di fornitore in outsourcing con una piattaforma ampia e completa di prodotti e servizi in grado di coprire tutte le esigenze di security, dal punto di vista hardware e software.

* Fonte: IDC - "Il mercato italiano della Sicurezza Informatica e della Business Continuity, 2004 - 2010". Marzo 2006.

CONTRIBUTORS

MARIANGELA FAGNANI
IBM Security & Privacy Service Leader, è laureata in Matematica e lavora in IBM dal 1981. Da diversi anni si occupa di sicurezza informatica. E' membro del Consiglio Direttivo del Clusit e socio onorario dell'associazione Itasforum. Possiede la certificazione CISA. Ha partecipato come relatrice sul tema della Sicurezza Informatica in molteplici convegni e seminari.

TIZIANO AIROLDI
Certified Executive It Architect, IBM Global Business Services, Security & Privacy Services, è in IBM dal 1979, dove ha maturato competenze consulenziali nel campo sicurezza. E' specializzato in progetti di Compliance & Regulation.

PIERFRANCESCO POCE
Global Technology Services Managing Consultant, è in IBM dal 1981, guida una task force di competenza formata da consulenti e di architetti It specializzati nell'analisi, nel disegno e nella realizzazione di soluzioni di sicurezza.

PAOLO TRIPODI
IBM Global Technology Services Security & Privacy Leader, è in IBM dal 1990, dove ha la responsabilità delle soluzioni di sicurezza per l'Europa Sud Occidentale. Paolo Tripodi ha lavorato per diversi anni nel Rome Tivoli Laboratory.

LUIGI DEL GROSSO
IBM Software Group Italia, è responsabile vendite delle soluzioni Tivoli di Security. E' laureato in Ingegneria e lavora in IBM dal 2000 dove si è sempre occupato del tema sicurezza toccando anche gli aspetti di Intrusion Detection.

GOVERNANCE E COMPLIANCE

POLITICA E STRATEGIA

Valutare attentamente i rischi, le misure e le policy, conformarsi alle normative di legge anche sulla privacy: la sicurezza parte da qui

Sono due gli aspetti principali dai quali partire per realizzare compiutamente la sicurezza: governance e compliance. La prima si riferisce al monitoraggio dei rischi e alle policy, mentre la seconda è basata sul rispetto delle policy di sicurezza stabilite dall'azienda e delle normative sempre più stringenti che vengono emesse nei vari Paesi. Infatti, l'offerta IBM in quest'area ha il principale obiettivo di fornire il supporto consulenziale e metodologico per la valutazione dei rischi di sicurezza e assicurare la conformità ai principali standard e alle leggi di settore, oltre al supporto in termini di politiche, quadro normativo, organizzativo e operativo. Oggi che i processi di business vanno ben oltre i confini della singola azienda e che molti si sono adeguati ai nuovi standard, implementando numerosi strumenti come sicurezza perimetrale, antivirus, firewall, filtri antispam o anti phishing, le funzioni di Governance e Compliance assumono importanza sempre crescente.

IBM TIVOLI PER TUTTE LE ESIGENZE

L'offerta IBM in questo ambito è tale da soddisfare tutte le esigenze, grazie alle soluzioni Tivoli, alcune delle quali sviluppate e supportate proprio nel laboratorio di Roma, che offrono una gamma completa di strumenti anche per le piccole e medie imprese, con l'offerta Tivoli Express. Si parla di soluzioni di Identity Management che consentono la gestione centralizzata e automatizzata delle identità informatiche presenti in azienda, oppure delle soluzioni di Access Management e Single SignOn, che permettono di centralizzare la gestione degli accessi. Inoltre, in seguito alla recente acquisizione della società specializzata Consul, i cui prodotti sono stati integrati all'interno delle soluzioni Tivoli, sono anche disponibili soluzioni ancora più specifiche per le tematiche di audit e compliance. In particolare la suite Consul InSight nell'area della gestione dei "log" all'interno dell'azienda, per vedere chi ha accesso a un determinato dato e in quale momento: si tratta di informazioni che assumono crescente importanza alla luce delle più recenti normative, per esempio quelle in materia di trasparenza finanziaria.

LA GESTIONE DEGLI EVENTI

IBM propone un modello basato su un approccio integrato che prevede la definizione di un unico schema aziendale di classificazione dei rischi. Lo scopo fondamentale è anche quello di correlare tutte le informazioni relative alla sicurezza, per poterla gestire in maniera integrata: non vedendola come un insieme di silos separati che lavorano ognuno per conto proprio, ma come un insieme unico che dia una visibilità di livello superiore su tutti gli eventi che riguardano la security, sia essa logica o fisica. La soluzione Tivoli Security Operation Manager, che ingloba anche i prodotti ereditati dall'acquisizione della società specializzata Micromuse, consente infatti di correlare gli eventi sia dal punto di vista della minaccia sia da quello del rischio, determinando da dove può giungere la minaccia più insidiosa e permettendo di adeguare le policy.

THREAT MITIGATION

LA PREVENZIONE INNANZITUTTO

La prevenzione è fondamentale: anticipare le minacce significa evitare danni incalcolabili

La sicurezza preventiva è l'unica soluzione che può mettere in condizione di anticipare le minacce. In questa area, che riguarda la neutralizzazione delle minacce esterne, per garantire la sicurezza perimetrale e delle infrastrutture tecnologiche, rientrano diverse soluzioni che IBM propone facendo leva sulle proprie competenze e sui propri prodotti, oltre che sull'importante apporto specifico dato dall'acquisizione di Internet Security Systems (ISS). Si tratta di soluzioni e servizi per migliorare la protezione dell'azienda e rendere efficace la gestione degli incidenti, riducendo le minacce derivanti dalla rete, monitorando le vulnerabilità, gli accessi ai contenuti Web oppure e-mail e i firewall. Perché prevenire gli attacchi sempre più sofisticati provenienti dall'esterno dell'azienda, cioè fuori dal suo perimetro, richiede uno studio approfondito e costante delle tecniche utilizzate e una piattaforma di prodotti avanzati.

LA RICERCA DI X-FORCE

L'offerta ISS si distingue tra l'altro per le attività di sicurezza condotte su scala mondiale e una serie di prodotti di sicurezza integrati. Alla base delle soluzioni ISS c'è la ricerca e sviluppo di X-Force, un servizio di intelligence per la sicurezza destinato alle applicazioni aziendali, ai sistemi operativi e a tutte le infrastrutture di rete attualmente presenti sul mercato.

Riconosciuto da tempo come il maggiore ed efficiente centro di ricerca e sviluppo al mondo per l'individuazione delle vulnerabilità, X-Force sviluppa le proprie conoscenze integrandole con quelle di altre fonti per compilare il database più completo delle principali vulnerabilità software, e costituire così la base di partenza delle soluzioni di sicurezza preventiva di ISS.

GESTIONE E PROTEZIONE PREVENTIVA

ISS gestisce le infrastrutture di sicurezza, 24 ore su 24, 7 giorni su 7 per 365 giorni all'anno, delle principali società e amministrazioni del mondo. Grazie al suo controllo su centinaia di reti sparse in tutto il globo, ISS si tiene costantemente aggiornata sulle vulnerabilità presenti in Internet, sfruttando i suoi punti di forza per anticipare i malintenzionati. Gli esperti in sicurezza di ISS analizzano il traffico sospetto, studiando le tecniche utilizzate negli attacchi e imparando a prevenirle e bloccarle. Infine, con la gamma di prodotti Proventia, ISS mette le sue soluzioni di protezione preventiva alla portata delle imprese. Proventia offre infatti soluzioni di sicurezza disponibili come prodotti indipendenti o come sistema modulare integrato. Quest'ultimo non solo integra una prevenzione avanzata delle intrusioni, firewall, antivirus, reti private virtuali (Vpn), oltre alla valutazione delle vulnerabilità, ma offre anche prestazioni di rilievo per la sicurezza della posta elettronica e il Web filtering.

In sostanza, quindi, le soluzioni di Internet Security Systems garantiscono la massima sicurezza perimetrale, mentre la gestione degli accessi basata sul controllo delle identità, con le soluzioni IBM Tivoli Identity & Access Management, permette di mettere in pratica il semplice ma efficace principio "Keep the bad guys out and let the good guys in", cioè teniamo i cattivi fuori e facciamo entrare solo i buoni.

IDENTITY & ACCESS MANAGEMENT

IL CUORE DELLE SOLUZIONI

Non c'è sicurezza senza controllo delle identità e degli accessi ai sistemi: la riduzione dei rischi e dei costi passa soprattutto da qui

L'Identity & Access Management è un punto centrale nella gestione della sicurezza, in quanto attiene al controllo delle "identità" alla base delle interrelazioni che intervengono tra oggetti e soggetti attraverso la rete. Si parla spesso di "identità digitali" in quanto ci si riferisce non solo ai soggetti fisici, come l'utente di un sistema o di una soluzione, ma anche agli "oggetti", come può essere il caso di un'applicazione o un servizio disponibile in azienda, che viene rappresentata e identificata attraverso le caratteristiche di un'identità digitale.

L'area dell'amministrazione e della gestione degli oggetti di sicurezza è una delle più delicate e critiche per le aziende, sia per i risvolti che questo ha sulla protezione degli asset sia per quanto attiene il costo che tale attività comporta. IBM si è focalizzata in modo particolare attraverso lo sviluppo dei prodotti software presenti nel portafoglio Tivoli e di competenze per indirizzare lo sviluppo di soluzioni a livello architetturale e specialistiche necessarie per la realizzazione dei progetti. L'esperienza di IBM consente alle aziende di realizzare soluzioni volte a migliorare la gestione delle identità digitali, governare i processi di provisioning, oppure ancora assegnare diritti di accesso in funzione di regole, modelli o ruoli definiti in base alle diverse policy aziendali di sicurezza, stabilite in fase di Governance.

SOLUZIONI LEADER DI MERCATO

Le soluzioni di Identity Management basate sui prodotti Tivoli Identity Manager e Tivoli Directory Integrator consentono la gestione centralizzata e automatizzata delle identità informatiche presenti in una struttura, costituite da tutte quelle informazioni necessarie a garantire l'accesso ai servizi It coerentemente con le politiche di sicurezza aziendali. Le soluzioni di Access Management e Single SignOn, basate soprattutto sui prodotti Tivoli Access Manager permettono di centralizzare la gestione degli accessi ai sistemi e al mondo applicativo.

Le soluzioni IBM in questo ambito consentono di: proteggere l'azienda da accessi e utilizzo non autorizzato a risorse informatiche o informative; gestire il ciclo di vita delle identità digitali, e soprattutto centralizzare il governo delle identità digitali a livello di intera azienda, evitando sovrapposizioni che si possono facilmente tradurre in minacce per la sicurezza; correlare le utenze alle persone fisiche che operano in azienda, siano queste dipendenti, consulenti, fornitori, partner; fornire soluzioni per rispondere a esigenze di password synchronization in ambienti eterogenei.

I VANTAGGI

Una gestione sofisticata del controllo accessi, ma nello stesso tempo trasparente per l'utente e coerente con il suo ruolo in azienda, quale quella proposta da IBM con le soluzioni Tivoli, oltre a consentire di ridurre in maniera drastica i rischi di frodi o furti di identità, permette anche di ridurre i costi associati alla gestione delle operazioni di autenticazione. Allargando il campo di visuale, la possibilità di dotarsi di strumenti di sicurezza sofisticati permette anche di progettare e offrire servizi nuovi e più "user friendly" agli utenti. Si pensi al caso di una banca che decida di offrire i propri servizi anche online, attraverso il Web: questa possibilità trova il primo fattore abilitante proprio nei sistemi di security adeguati, ma non complicati per l'utente.

SICUREZZA FISICA

LA NUOVA FRONTIERA

Non solo dati ma anche immagini che viaggiano in rete e vengono elaborate come vere e proprie informazioni: il futuro è ormai presente

La rivoluzione si è compiuta da poco tempo, ma è un dato di fatto acquisito. Tanto da far quasi completamente cadere il confine sottile tra sicurezza "logica", cioè quella attinente alle reti, ai sistemi aziendali, alle infrastrutture e ai dati, e sicurezza "fisica", riguardante il personale, i beni fisici dell'azienda o il territorio. Sono le nuove tecnologie ad aver guidato il cambiamento verso una maggiore importanza strategica della sicurezza, tramite l'utilizzo delle reti di trasmissione su protocollo Internet (Ip) da parte degli apparati anti-intrusione, quali telecamere o altri sistemi. Anche la sicurezza fisica è quindi sempre più collegata alla rete aziendale e connessa ai dati della sicurezza logica. E IBM è oggi ai vertici del mercato per la progettazione di tecnologia, sicurezza e soluzioni infrastrutturali basate su reti Ip e tecnologie digitali avanzate come l'elaborazione digitale delle riprese video e l'identificazione o l'autenticazione biometrica. La soluzione integra gli apparati di sicurezza attiva e passiva con le risorse informatiche, come i componenti di controllo accessi e i transiti veicolari e pedonali, l'anti-intrusione, la videosorveglianza, con un cruscotto centralizzato o un centro comando unificato di sedi singole o complesse.

IBM ANALYTIC SURVEILLANCE SOLUTION

Le nuove tecnologie permettono di ridurre di molte grandezze il tempo necessario a esaminare una video ripresa: se prima una persona, pur se esperta, era in grado di esaminare 24 ore di filmato in 8 ore, cioè in un terzo del tempo fisico di registrazione, e un sistema di videoanalisi ci metteva poco più di due ore, cioè un decimo del tempo fisico, i nuovi sistemi interamente digitalizzati impiegano pochi minuti. Nei quali sono in grado di estrarre dalle registrazioni ogni tipo di informazione, basandosi sulla più avanzata tecnologia di sorveglianza digitale del mercato: IBM Analytic Surveillance Solution.

Più in dettaglio, la nuova soluzione di IBM è l'unica tecnologia in grado di fornire le funzionalità per effettuare efficaci analisi dati su sequenze video, sia in tempo reale sia registrate. Basata su middleware open standard, la piattaforma Analytic Surveillance Solution permette di monitorare e analizzare eventi reali mediante sensori multipli, tra cui videocamere, radar, sensori elettrici o ingressi audio, ed è predisposta per integrare le tecnologie di molteplici vendor. Inoltre, Analytic Surveillance Solution incorpora nativamente diverse modalità ormai indispensabili per proteggere la privacy delle persone che si trovano all'interno delle aree monitorate dal sistema, come per esempio una schermatura automatica del volto.

L'INTEGRAZIONE CON LE TECNOLOGIE

IBM Analytic Surveillance Solution fornisce una soluzione integrata di sicurezza e video sorveglianza che può includere elementi quali macchine fotografiche, registratori video digitali, server, sistemi storage, software e dispositivi di rete. Per esempio, IBM Analytic Surveillance Solution sfrutta piattaforme standard di mercato quali i BladeCenter, i server System x, i sistemi di storage e le reti aziendali per consentire maggiore accesso a video, analisi video in tempo reale e aiutare nell'implementazione di un sistema video di livello avanzato.

DISASTER RECOVERY

PREVENZIONE È PROTEZIONE

Identificare le minacce, valutare i rischi e neutralizzarli. Ma per essere sicuri fino in fondo è necessario attrezzarsi per i disastri informatici

Nel caso dei disastri informatici, per proteggere adeguatamente i processi operativi è importante che un'organizzazione assicuri un adeguato bilanciamento fra le iniziative di carattere preventivo e quelle di carattere reattivo. Con il termine protezione vengono intesi gli aspetti relativi alla prevenzione, in quanto il costo delle misure di prevenzione è generalmente di molto inferiore ai costi conseguenti alla perdita dei beni e a quelli da affrontare per il reintegro degli stessi, e alla reazione alla perdita dei beni, in quanto nessuna misura di sicurezza può offrire una garanzia assoluta e perché un rapido ripristino dei beni danneggiati può limitare le associate perdite finanziarie. Poiché, a dispetto di tutte le possibili misure di sicurezza, l'eventualità che un evento indesiderato si verifichi non può mai essere esclusa. Perciò una organizzazione, al fine di garantire la possibilità di perseguire la propria missione, deve prevedere una opportuna strategia di ripristino. L'individuazione di tale strategia richiede la comprensione delle caratteristiche peculiari del business dell'organizzazione stessa. Infatti i beni di una azienda (infrastrutture, dati, rete, persone, tecnologia) sono risorse di cui un'azienda si dota per svolgere la propria missione. L'indisponibilità di tali risorse implica l'incapacità di perseguire il proprio business e questo può portare a impatti o anche perdite finanziarie estremamente gravi. Per questo si parla di strategia di disaster recovery, intendendo la definizione di un percorso composto da più soluzioni tra loro correlate che conduce alla realizzazione di una soluzione di ripristino, rispondente ai livelli di servizio richiesti dal business e coerente con le caratteristiche tecniche dei sistemi It presenti in azienda.

LA SOLUZIONE: IBM BUSINESS CONTINUITY AND RESILIENCY SERVICES

IBM Global Technology Services opera a livello mondiale nell'ambito dei servizi di disaster recovery, business continuity e business resilience, con la struttura specifica IBM Business Continuity and Resiliency Services (Bcrs), presente in 76 Paesi, tra i quali l'Italia, con 114 Centri di disaster recovery e oltre 15mila clienti. I Centri di disaster recovery sono sempre a disposizione degli utenti (in modalità 24x7x365) per attività di simulazione e per la gestione di reali condizioni di emergenza. IBM opera quindi come fornitore specializzato, in grado di realizzare progetti complessi, assicurare performance altamente professionali, fornire un supporto tecnologico elevato e garantire alti livelli di efficienza. Nel nostro Paese IBM Bcrs opera da più di quindici anni e, da poco meno di tre, da luglio 2004, dispone del nuovo Centro di disaster recovery e business continuity a Settimo Milanese. Questo Centro, primo in Italia per dimensioni, capacità ed eterogeneità di apparati, livelli di continuità garantiti e servizi forniti, si pone all'avanguardia anche in ambito europeo. Infatti, le caratteristiche infrastrutturali del Centro, la ridondanza degli impianti tecnologici, la potenza di calcolo disponibile e l'ampia scelta di connettività locale e geografica ne fanno uno dei più avanzati a livello internazionale. IBM Business Continuity and Resiliency Services Italia è certificata secondo lo standard ISO/IEC 27001 (Specification for Information Security Management) nella progettazione, realizzazione e gestione dei servizi e delle soluzioni di disaster recovery, high availability e business continuity.

LA SECURITY E LA SOA

UN INCONTRO NECESSARIO

La sicurezza è un tema che riguarda i "soggetti" ma anche gli "oggetti", come può essere il caso delle applicazioni o dei Web Services, sui quali si basa la SOA

Obiettivo delle aziende è quello di operare sul mercato attraverso nuovi modelli di business che portano le aziende ad estendere il loro territorio di business, ma che, allo stesso tempo, portano ad aprire il proprio sistema informativo con l'adozione di nuovi modelli architetturali basati sui nuovi paradigmi della SOA; l'architettura informatica orientata ai servizi, che permette di riutilizzare al massimo le tecnologie disponibili, gestire al meglio le esigenze del business e ridurre costi e complessità.

Tutto questo deve essere affrontato considerando con molta attenzione il tema della sicurezza in quanto le tecnologie abilitanti alla base del modello SOA sono quelle tradizionali utilizzate nel contesto Internet. I Web Services rappresentano lo strumento con cui è possibile realizzare il modello SOA, questi sono caratterizzati da identità digitali e, così come per i soggetti, anche in questo caso deve essere indirizzato il tema della loro identificazione e del controllo accessi. Il disegno di una soluzione SOA privo di soluzioni per indirizzare requisiti di sicurezza, rischia di esporre l'azienda a minacce e vulnerabilità tipiche di un contesto Web, ma soprattutto espone il sistema informativo dell'azienda.

PENSARE ALLA SOA ANCHE IN OTTICA SICUREZZA

Sono due le mosse necessarie. La prima è fare sempre in modo che i servizi che si vanno a esporre nell'ambito di un progetto SOA siano sempre accompagnati da adeguati servizi di sicurezza. La seconda è quella di predisporre una architettura di sicurezza a supporto di iniziative SOA attraverso la preparazione di componenti di sicurezza in grado di erogare la sicurezza come servizio. Stiamo parlando dei consueti servizi già presenti in azienda per la gestione delle identità, del controllo accessi, delle directory e altri. E' fondamentale pensare alle politiche e ai requisiti di sicurezza nello stesso momento in cui si sta procedendo alla modellazione del nuovo servizio. Le politiche di sicurezza e i modelli di "trust" definiti devono essere quindi trasformati in regole di controllo da applicare nei diversi punti dell'infrastruttura di sicurezza e quindi utilizzate per governare la sicurezza della SOA.

IBM dispone di un modello di riferimento utilizzato per il disegno di un'architettura di sicurezza in grado di supportare in modo effettivo una soluzione SOA sviluppato su tre livelli: Business Security Services, Security Policy Infrastructure e It Security Services.

L'approccio consigliato da IBM è affine al modello del ciclo di vita della SOA, e prevede di pensare e definire gli aspetti e i requisiti di sicurezza a partire dalla fase di Modellazione, o modellizzazione, poi l'Assemblaggio, il Rilascio (Deployment) e la Gestione (Monitor). In quest'ultima fase sono gestite le risorse legate ai servizi sottostanti e consente di monitorare gli indicatori chiave delle prestazioni per prevenire eventuali problemi. In tutte queste fasi entrerà in gioco un insieme di servizi per supportare le aziende nel valutare, progettare e implementare soluzioni e architetture di sicurezza integrate.

A questo scopo, IBM è in grado di affiancare i clienti nelle diverse fasi di un progetto SOA: security assessment, analisi dei requisiti, disegno e implementazione di architetture di sicurezza in linea con i requisiti di business.

HONDA, LA SICUREZZA È SEMPRE IN MOTO

Una soluzione realizzata da IBM per Honda Italia Industriale, il "braccio" nel nostro Paese della divisione motociclistica del colosso giapponese, per gestire in maniera efficace e immediata le esigenze di security dei singoli utenti aziendali

Honda Italia Industriale (www.hondaitalia.it) è la filiale italiana della divisione motociclistica della giapponese Honda, nome glorioso anche nel campo delle due ruote che non ha certo bisogno di presentazioni. Non solo perché si tratta del maggior produttore mondiale di moto, ma forse perché anche i non appassionati hanno ben presente vere e proprie pietre miliari che hanno fatto la storia delle moto, come la Honda CB 750 Four che all'alba degli anni Settanta reinventò il settore motociclistico, oppure la gloriosissima Gold Wing, tuttora presente nei listini della Casa, a più di trenta anni dalla sua prima comparsa sul mercato.

Con un fatturato 2006 superiore a 785 milioni di euro e oltre 800 addetti impiegati nelle sedi di Roma e di Bologna, e nello stabilimento di Atessa in provincia di Chieti che produce più di 170mila veicoli all'anno, Honda Italia Industriale è leader anche nel nostro Paese, con oltre il 21% del mercato complessivo delle "due ruote", grazie a cavalli di battaglia come lo scooter SH125i/150i (43mila unità consegnate nel 2006 alla clientela nelle due differenti cilindrate) o la moto Hornet 600 (oltre 7.500 esemplari venduti a oggi). Nell'impianto abruzzese, Honda Italia Industriale ha iniziato a produrre motocicli nel 1976 con il modello CB 125. Nel 1985 inizia l'esportazione, dapprima nei mercati europei e successivamente, con il modello NS 125, anche in Giappone. Oggi, oltre alla produzione di veicoli, lo stabilimento che sorge nell'area industriale della Val di Sangro sforna ogni anno oltre 750mila motori che vengono montati su apparecchi come i tagliaerba.

LE ESIGENZE DI SICUREZZA

Circa tre anni fa, nel 2004, la società decide di rivedere i propri sistemi informativi, cominciando a mettere mano alla server farm, per poi passare alla Lan e successivamente al software. L'aggiornamento riguarda anche i sistemi di security, pur se non vi erano mai stati problemi di sorta. Ma si sa che una delle prime regole delle policy di sicurezza è proprio quella che la prevenzione è molto più sensata di un intervento successivo, a danno verificato. Dal punto di vista delle vulnerabilità interne, «c'erano problemi con gli utenti che creavano password non sufficientemente lunghe oppure complesse, come richiesto dalle normative – spiega **Nicola Marrone dell'Information System di Honda Italia Industriale** –. Avevamo anche la necessità di assicurarci che tutti i computer fossero sempre aggiornati alle ultime patch di sicurezza. Inoltre, una direttiva internazionale della casa madre ci imponeva di uniformare il livello di sicurezza del nostro intero ambiente It, e ridurre anche i costi generali». L'esigenza di Honda Italia Industriale era infatti quella di gestire tutte le connessioni in rete dei computer che accedono al sistema dell'impresa, rispettando le policy aziendali e le normative sulla privacy. Quindi un'esigenza classica, si potrebbe dire, di "governance e compliance", visto che erano coinvolti sia i problemi di rispetto delle politiche aziendali in ordine alle password, agli antivirus, alla gestione delle patch e alle verifiche della presenza di firewall sui client, sia rispetto alla protezione della privacy dei singoli utenti. Inoltre, le esigenze non erano di poco conto, visto che si parla di circa 300 sistemi client, tra i quali una cinquantina di notebook: questi ultimi «godono di un'attenzione particolare, visto che per definizione sono spesso in giro e potenzialmente possono creare maggiori problemi di sicurezza», sottolinea Marrone.

UNA SOLUZIONE STANDARD

Sono stati valutati alcuni fornitori, ma la proposta migliore è stata giudicata quella proveniente da IBM Global Services, fornitore per così dire "storico" di Honda Italia Industriale, che ha proposto e realizzato una soluzione, tutta in tecnologie standard, che prevede l'uso di un sistema di ammissione alla rete basato sul software IBM Tivoli installato su server IBM System x con firewall di Cisco. Infatti, attraverso l'integrazione del software IBM Tivoli per la conformità delle policy di sicurezza e le tecnologie Cisco Systems facenti parte del programma Network Admission Control, l'obiettivo di automatizzare la verifica della conformità rispetto alle politiche di sicurezza, l'isolamento o l'adeguamento di dispositivi a rischio quali desktop, notebook e dispositivi wireless è pienamente raggiunto senza che l'utente debba, in qualche modo, modificare i propri comportamenti abituali. Tale collaborazione offre soluzioni preventive di "autodifesa" che consentono agli utenti di controllare automaticamente chi e che cosa possa avere accesso alla rete in base alle policy aziendali, aiutando in questo modo le aziende a ridurre il tempo normalmente speso per il ripristino di computer desktop e notebook a seguito di attacchi e incidenti.

LA SOLUZIONE IN DETTAGLIO

Più in dettaglio, la soluzione prevede due server IBM System x3850 con i sistemi operativi VMware ESX V3.0 server, VMware Virtual Infrastructure Node V3 e Windows 2000 Server, sui quali sono implementati i software IBM Tivoli Security Compliance Manager V5.1 e IBM DB2 V8 Data Archive Expert per multipiattaforma. L'applicazione IBM Tivoli Security Compliance Manager controlla che i computer presenti nella rete aziendale di Honda Italia Industriale abbiano una configurazione coerente con le politiche di sicurezza dell'azienda. Il software Tivoli si incarica infatti di controllare che sia il sistema sia le applicazioni software presenti nel computer non presentino vulnerabilità, come per esempio la presenza di virus, l'uso di password di lunghezza non adeguata, il mancato aggiornamento delle patch del sistema operativo, oppure vi siano definizioni di virus obsolete. In questo modo, vengono infatti verificate le eventuali violazioni alle policy aziendali di sicurezza. Se la macchina risponde ai requisiti, viene immediatamente collegata alla rete aziendale, ma se viene identificato un dispositivo che non risponde ai requisiti di sicurezza, si procede a metterlo in quarantena tramite il firewall Cisco. Grazie al software IBM Tivoli Provisioning Manager, le vulnerabilità riscontrate possono essere immediatamente corrette, per poi provvedere a riconnettere a pieno titolo il computer alla rete aziendale.

I VANTAGGI

«L'implementazione della soluzione ha richiesto poco meno di sei mesi, compresa la personalizzazione dell'ambiente – spiega Marrone –. E anche se per l'utente finale la soluzione si mostra in tutto e per tutto trasparente, visto che non presenta differenze rispetto al passato, va detto che abbiamo cercato di mantenere un approccio il più possibile "soft", evitando di bloccare subito l'utente se decide di utilizzare una password che non è in standard Iso: in questo caso, cerchiamo di fargli capire che sarebbe necessaria una password differente per evitare potenziali problemi».

Per quanto infine riguarda i benefici in termini economici, dalla funzione sistemi informativi di Honda Italia Industriale fanno sapere che cifre precise sono «difficili da calcolare, in quanto non abbiamo mai avuto alcun tipo di guaio. Ma se si pensa a quelli che potrebbero essere i danni qualora si verificassero intrusioni oppure perdite di dati, i risparmi sono sicuramente notevoli». Ma anche se i vantaggi non sono immediatamente quantificabili, forse questa è la migliore riprova che, di tutti gli investimenti in informatica, la sicurezza rimane un aspetto essenziale. E soprattutto irrinunciabile. **DM**

_GIORNALE DI BORDO DELL'INFRASTRUTTURA

_GIORNO 27: Tutte queste norme per la compliance ci stanno uccidendo! Audit. Incoerenze. Processi. Tempo. Denaro. Mi sento perseguitato dagli ispettori.

_Ma è vero, gli ispettori mi stanno dando la caccia! Corri!

_GIORNO 28: Ho trovato: il middleware IBM Tivoli. È la soluzione per automatizzare l'amministrazione del sistema e per standardizzare le nostre norme di compliance. Centralizza i processi e minimizza i grattacapi che ci derivano da normative nuove e in continuo cambiamento. E ci aiuta ad anticipare i problemi di sicurezza prima che si verifichino, oltre a salvaguardare il nostro business.

_Gigi è scocciato perché abbiamo sospeso la dieta ipercalorica.

IBM

Ogilvy & Mather

Tivoli

Una migliore gestione del tuo IT ti aspetta su:
IBM.COM/**TAKEBACKCONTROL**/COMPLIANCE/IT