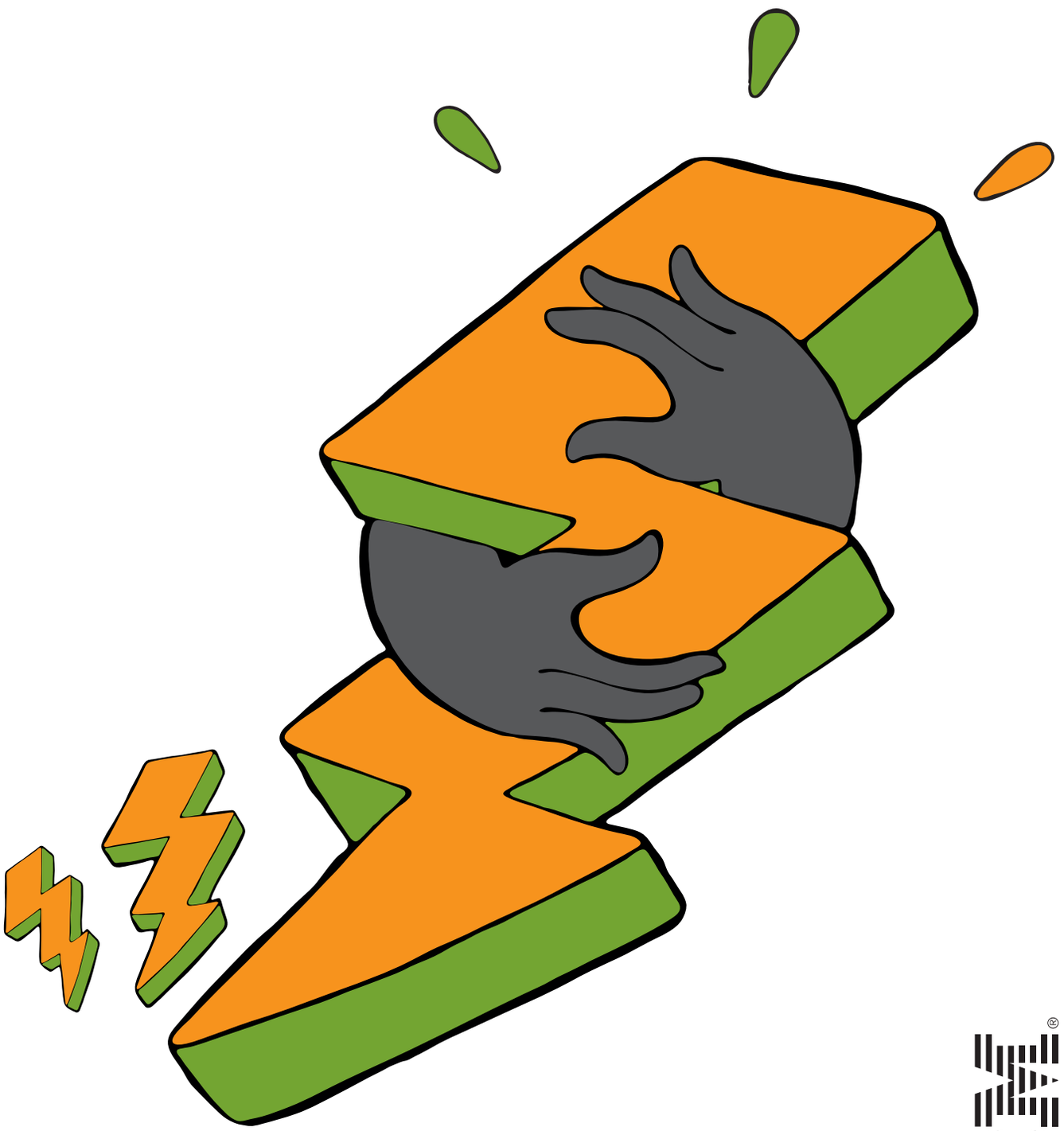
LA SICUREZZA NEL TERZO MILLENNIO

Un approccio integrato per la protezione del patrimonio aziendale in un mondo sempre più connesso e complesso.



THINK

La sicurezza nel Terzo Millennio

Un approccio integrato per la protezione del patrimonio aziendale in un mondo sempre più connesso e complesso

Realizzato da Reportec srl
www.reportec.it

Indice

La sicurezza nel Terzo Millennio

Introduzione

La sicurezza è al primo posto tra gli obiettivi dei CIO già da qualche anno e ancora risulta esserlo anche attualmente, come testimoniato dagli studi di diversi analisti. Contestualmente, la compliance alle normative nazionali e internazionali è tra le prime priorità dei CEO. È evidente, dunque, l'importanza di questo tema e la necessità di impostare una strategia per l'Information Security e la Compliance che sia pienamente integrata con la missione aziendale. Non è dunque un caso se IBM promuove una visione della sicurezza quale elemento abilitante per il business.
Le imprese, specialmente in alcuni contesti come quello bancario, sono consapevoli di questa valenza, perché hanno bisogno di risposte a temi come la dematerializzazione del patrimonio e degli asset informativi, l'adempimento alle leggi e agli standard di settore, l'esigenza di un più veloce time to market, la salvaguardia di un'immagine o comunque l'importanza di ottenere la fiducia della propria clientela e una serie di altri obiettivi che si possono sintetizzare nel bisogno di business agility.

Un approccio convergente

Appare sempre più richiesto un approccio basato sulla convergenza tra sicurezza logica e fisica e la parte applicativa. La sua adozione, sempre più importante, è effettivamente una risposta a un'esigenza molto sentita in molti ambiti, a partire, ancora una volta, da quello bancario, ma in estensione ad altri settori commerciali, dove si coglie il valore di tale convergenza in termini di maggiore efficacia nella prevenzione. In effetti, si tratta dell'unico elemento vincente per prendere misure efficaci in questo senso: si pensi, nel caso delle banche, alla possibilità di integrare le informazioni che arrivano dalle applicazioni con quella sulla sicurezza, per ridurre i rischi di frodi e attacchi informatici. Ma anche, alle possibilità offerte dalle nuove tecnologie per la videosorveglianza integrata in tutti quei contesti di contatto con un pubblico, come nelle attività commerciali di largo consumo.

Comprendere e scegliere la soluzione più adeguata alla propria realtà aziendale presuppone conoscere il valore dell'informazione e, in generale, del patrimonio aziendale per misurare il livello di rischio accettabile. Solo in questo modo si ottiene un riferimento, rispetto al quale valutare quali investimenti in tecnologia sostenere.

La gestione del rischio

Analizzando tutti i processi aziendali e tutti i pericoli cui sono soggette le componenti degli stessi, siano esse relative all'ICT, al personale aziendale o ad altri asset tecnologici o fisici, si può misurare il rischio connesso con gli eventi di security. Gestirlo, come già in ambito finanziario, è un primario obiettivo di business. Mitigarlo è, dunque, un risultato di business, che si può misurare per il valore che aggiunge all'impresa.
IBM è in grado di fornire un pieno supporto strategico e tecnologico per l'analisi del rischio e delle vulnerabilità cui è soggetta l'infrastruttura ICT aziendale. Soprattutto mette a disposizione framework e metodologie per valutare il legame tra il business e i suoi processi e le tecnologie e soluzioni di Information Security.
Proprio la gestione del rischio è l'obiettivo implicito nella maggioranza delle leggi e dei regolamenti che, più o meno direttamente, riguardano la sicurezza e l'Information Security in particolare. Impostare un sistema di sicurezza con l'obiettivo di gestire e mitigare il rischio, dunque, porta automaticamente alla compliance. Peraltro, anche la compliance va misurata, controllata e gestita, perché, come conseguenza della dinamicità della sicurezza stessa, la posizione dell'azienda è destinata a cambiare nel tempo.

La governance della sicurezza

La convergenza di tutti gli aspetti connessi alla sicurezza dell'intero patrimonio aziendale e l'adozione di un approccio orientato al risk management diventano un elemento strategico per la governance della sicurezza, a sua volta parte della governance aziendale. Il continuo controllo del rischio e, quindi, dei processi di business che sono l'oggetto di tale rischio, infatti, porta a una più efficace strategia per la governance aziendale.
IBM, propone un approccio integrato che abbraccia la sicurezza a tutti i livelli aziendali e da ogni punto di vista tecnico, in un'ottica di prevenzione delle minacce, gestione degli eventi di sicurezza, continuità del business e compliance. Un approccio integrato orientato alla governance della sicurezza per valorizzare al massimo i ritorni della sicurezza stessa.

Sono molte le aziende che hanno colto l'importanza strategica di un approccio del genere: banche e industrie, per esempio, ma anche, per certi versi, la Pubblica Amministrazione, stanno focalizzando la loro attenzione sulla governance, mentre in passato i loro sforzi erano soprattutto concentrati sulla protezione della rete e degli accessi. La complessità stessa della sicurezza, di fatto, suggerisce le necessità di governarla coerentemente con il resto dell'azienda.

L'apporto di IBM alle imprese parte dalla consulenza, con servizi che aiutano le aziende a impostare la strategia di governance. Soprattutto IBM è in grado di coniugare consolidate esperienze di Information Technology con competenze specifiche sugli aspetti di architettura e di processo. Questo significa in primo luogo definire le politiche per la sicurezza e, dall'altro, anche verificare i livelli di compliance.

Le scelte relative alla sicurezza sono complesse, data la vastità della materia e le implicazioni strategiche e tecnologiche che è necessario considerare e che sono trattate in questo volume. IBM è il partner fidato, dotato di competenze, soluzioni, servizi e capacità esecutiva per coprire tutti gli aspetti su elencati con un approccio integrato destinato a garantire la sostenibilità nel tempo della sicurezza e della compliance.

La sicurezza nel Terzo Millennio

1
Un approccio di business alla sicurezza

La sicurezza è strategica e, come per tutte le decisioni strategiche, spetta al business preoccuparsene. Gli aspetti tecnologici sono tutt'altro che trascurabili, ma comunque devono essere posti in secondo piano rispetto al bisogno di soddisfare le esigenze di business, che partono dalla gestione del rischio in maniera efficace ed efficiente, al fine di aumentare il valore dell'impresa. Adottando un processo di governance e risk management, oltre a mantenere nel tempo la conformità a leggi e regolamenti, si ottiene un rapido ritorno degli investimenti e un supporto per l'innovazione.

IBM è da sempre molto attenta alle tematiche della sicurezza e la robustezza, affidabilità, riservatezza delle architetture mainframe, che hanno fatto la storia dell'azienda e che tuttora caratterizzano i System z, lo testimoniano indirettamente. Negli anni, inoltre, IBM ha effettuato importanti acquisizioni, inglobando tecnologie, soluzioni e conoscenze su più fronti della sicurezza. Parallelamente, in seno ai Technology Global Services, i consulenti della società hanno maturato significative e vaste esperienze, sviluppando metodologie e strumenti per supportare le aziende in tutti gli aspetti che riguardano la sicurezza.
L'esperienza e la competenza accumulate hanno portato IBM a formulare un approccio integrato e olistico alla sicurezza, orientato alla governance della sicurezza stessa e legato al governo dell'impresa e alla gestione del rischio. In altre parole, un approccio strategico strettamente connesso al business, che abbraccia la sicurezza logica e fisica di tutta l'impresa.

1.1 Un approccio integrato per la sicurezza

I responsabili d'impresa devono affrontare diverse sfide, quali l'esigenza di innovare in un'atmosfera estremamente competitiva, il rispetto delle molte normative, la ricerca di ritorni rapidi dagli investimenti e la necessità di mettere al sicuro l'azienda da una vasta gamma di sofisticate minacce in continua evoluzione. Proprio quest'ultimo aspetto è probabilmente l'origine di una malaugurata abitudine. Normalmente, infatti, per ogni decisione e piano strategico riguardante l'impresa, il manager adotta un approccio legato al business. Ma, se si tratta di un problema sicurezza e tutte le sfide sopra riportate ne fanno parte, viene tipicamente impostato un approccio tecnologico.
Se è innegabile che la tecnologia ha un ruolo fondamentale nell'ambito dell'Information Security, è altrettanto chiaro che senza un approccio guidato dal business è difficile assicurarsi che gli obiettivi del business stesso siano rispettati. Mentre i fornitori di soluzioni specializzate per la sicurezza hanno una visione limitata e spingono spesso per un approccio tecnologico dal basso, IBM possiede le competenze e la capacità esecutiva per aiutare le imprese ad adottare un punto di vista che parte dal business per definire i propri requisiti in termini di sicurezza e compliance. Un punto di partenza che è facilmente individuabile perseguendo la gestione del rischio, una pratica ben nota al business manager. In quest'ambito significa dover assegnare a ciascun processo o asset aziendale un valore di priorità rispetto al quale valutare quanto critica sia la sicurezza.

La validità di un approccio orientato al business è determinata anche dalla crescente importanza che la sicurezza stessa ha assunto negli ultimi anni per l'intera impresa. L'utilizzo di Internet e le nuove tecnologie, in primis quelle per la mobility e la business collaboration, e anche l'apertura verso nuovi mercati con la globalizzazione hanno indotto significativi cambiamenti al concetto di sicurezza, in particolare per la centralità del ruolo assunto dalle informazioni e dalle tecnologie che sono diventate, insieme alle persone, alle infrastrutture e ai servizi primari, elementi fondamentali per la realizzazione della missione aziendale. È dunque evidente che occorre un approccio verso la sicurezza che tenga in giusto conto tutti questi elementi: un approccio integrato che consideri la protezione logica e fisica di informazioni, infrastrutture e persone.

In quest'ottica diventa primario comprendere il contesto di business nel quale opera l'azienda, per evitare non solo che s'interrompano i servizi di business, ma anche che il verificarsi di problemi possano arrecare danni alla reputazione dell'azienda. A questo scopo è fondamentale innanzitutto impostare una strategia per la sicurezza ben definita e articolata, in modo da evitare che eventi dannosi possano essere determinati o favoriti dall'inadeguatezza delle politiche aziendali sulla sicurezza e dai relativi comportamenti. Nel contempo, però, è altresì necessario impostare un sistema dotato di parametri convincenti e rilevanti per valutarne l'efficacia in relazione agli obiettivi di business. Senza queste caratteristiche, la sicurezza finirebbe con essere percepita come un puro costo per certi versi equiparabile a quello di un'assicurazione.

Una delle difficoltà maggiori che incontrano le organizzazioni nell'adottare un approccio di business consiste proprio nel trovare il collegamento tra le esigenze di business e le tecnologie atte a garantire il livello di sicurezza di cui tali esigenze hanno bisogno. Di primo acchito, appare assurdo pensare ad antivirus, firewall, intrusion prevention system e ad altre tecnologie per l'Information Security come a fattori di successo per le attività aziendali e, in effetti, lo è, perché si tratta di elementi facenti parte di quello che deve essere considerato come un unico sistema integrato. In passato tali tecnologie sono state implementate in silos separati, ciascuno dedicato a una specifica singola funzione. Anche da un punto di vista tecnologico, tale architettura risulta oggi inefficace, a causa delle strategie d'attacco che utilizzano tecniche miste. Dal punto di vista del business, inoltre, si tratta di un approccio estremamente inefficiente poiché implica costi di gestione e

manutenzione molto alti, nonché rallenta fino a intralciarli i processi di business. È proprio questo approccio che ha reso la sicurezza un peso e un fastidio per molte imprese.

1.1.1 La sicurezza per ogni processo di business

Il primo passo in un approccio integrato, come accennato, consiste nella valutazione del rischio collegato a ciascun processo di business e, conseguentemente, agli asset informativi e fisici che a tali processi fanno riferimento. La prima fase sarà dunque di analisi e assessment e dovrà evidentemente coinvolgere l'impresa a tutti i livelli.
L'esigenza di impiegare misurazioni e fattori di correlazione tra minacce e impatti sul business è fondamentale per realizzare l'Information Security Governance, ovvero per indirizzare un processo continuo teso al miglioramento del sistema per la gestione della sicurezza delle informazioni, allineato agli obiettivi di business dell'azienda.
Esiste una correlazione diretta tra la frequenza con cui si manifestano le minacce e gli impatti sul business, come illustrato nella figura seguente.

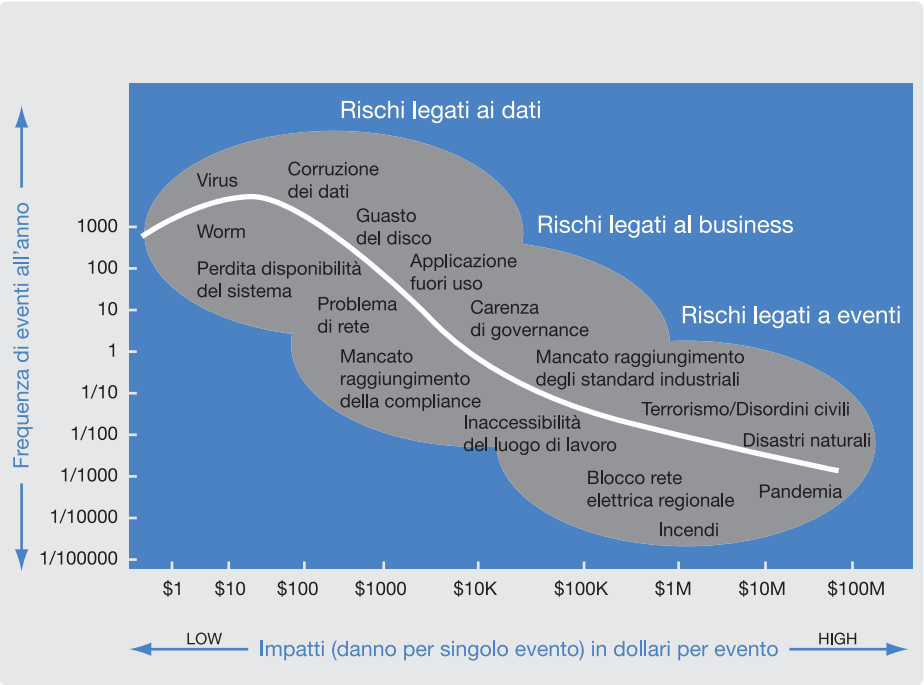


Figura 1.1
Frequenze e impatti di business

Le minacce generano impatti con rischi di tipologia diversa: rischi legati ai dati (data driven), rischi legati alla carenza di governance (business driven) e rischi legati agli eventi (event driven). È anche importante, però, saper valutare la portata dei possibili impatti: alcuni eventi, quali i virus, pur aven-

do una frequenza molto elevata hanno un basso impatto, mentre altri eventi meno frequenti, quali i disastri naturali, possono averne di devastanti. Pertanto emerge chiaramente la necessità per le aziende di contrastare l'intero spettro dei rischi che hanno impatti potenziali sul proprio business: non si può più accettare di avere piani di sicurezza, piani di governance e piani di disaster recovery separati. Quello che serve veramente è un piano strategico integrato che aiuti l'azienda a mitigare i rischi di natura data, business ed event driven.
In generale, si possono identificare cinque macro aree chiave che vanno esaminate perché identificano domini di rischio e impattano sui processi di business.

Individui e identità

L'accesso a risorse e informazioni aziendali deve essere garantito a tutte le persone che le devono utilizzare per portare avanti i processi di business. Sono inclusi ovviamente i dipendenti e, secondo i casi, una serie di altri individui che appartengono alla catena del valore: partner, consulenti, fornitori e clienti. Analogamente e con la stessa efficacia ed efficienza, il suddetto accesso deve essere negato a tutti coloro che sono estranei al business aziendale.
È dunque fondamentale riconoscere e gestire l'identità di tali individui, ma questo è solo l'aspetto tecnologico. Da un punto di vista di business, infatti, la sfida consiste nel riuscire a gestire la variazione dinamica delle forze di lavoro e, su un altro fronte, nel poter influenzare, se non imporre, elevati livelli di sicurezza a chi è autorizzato all'accesso, siano essi i dipendenti o gli esterni autorizzati. È chiaro che per i primi è più facile, ma anche per loro ci sono da considerare non pochi aspetti collegati alle normative sul trattamento dei dati personali nonché ai regolamenti interni e ai contratti sindacali.
Un sistema di sicurezza appropriato dovrebbe prevedere un insieme di controlli per gestire efficacemente i privilegi d'accesso di ciascun individuo per tutte le soluzioni tecnologiche in essere in azienda, compreso l'accesso all'edificio o ad aree riservate, per esempio laboratori di ricerca, magazzini, data center.

Dati e informazioni

La business collaboration è il nuovo paradigma dello sviluppo aziendale. Il valore apportato dalla capacità di combinare esperienze e team di lavoro con i partner è ben noto da tempo, ma la crescita dell'interazione resa possibile da Internet e dagli strumento del cosiddetto Web 2.0 apre ben altre possibilità, come hanno dimostrato attività innovative di marketing realizzate da Nike o Fiat per il lancio di nuovi prodotti, quali scarpe personalizzate e la nuova 500. D'altro canto, nuove problematiche di sicurezza vanno confron-

tate con le opportunità di business. Le imprese devono facilitare il business collaborativo mettendo a disposizione la tecnologia necessaria, ma, al tempo stesso, devono proteggere la riservatezza di dati e informazioni critiche. È necessario comprendere quali sono gli elementi di criticità e impiegare metodologie adeguate per classificare, assegnare delle priorità e quindi proteggere i dati, sia quelli residenti su appositi sistemi sia quelli in transito sulla Rete e scambiati tra gli attori della collaboration.
Da non dimenticare, poi, gli aspetti connessi con la compliance: non basta realizzare un sistema di protezione, ma occorre essere in grado di dimostrare, anche con la dovuta documentazione, che i controlli di sicurezza implementati sono efficaci. Molto spesso, la carenza di personale e di personale qualificato è il principale problema per l'impresa che si trova a fronteggiare la doppia complessità di un sistema per l'Information Security, che deve contemporaneamente garantire la potenza tecnologica dei controlli e della loro gestione e l'abilità nella produzione della reportistica per verificare la rispondenza alle normative.

Applicazioni

Le applicazioni sono la ragione stessa dell'infrastruttura informatica. Sono loro a rappresentare lo strumento di lavoro per i cosiddetti "information worker" in azienda e sono sempre le applicazioni a guidare i vari passi dei processi di business. La loro protezione da minacce esterne e interne è dunque critica e deve essere attuata in maniera preventiva e proattiva per il loro intero ciclo di vita (dalla progettazione, allo sviluppo, all'implementazione, alla produzione), per impedire che l'interruzione di servizio per un'applicazione possa creare un blocco del business.
Da un lato questo implica il dotarsi delle molte soluzioni di sicurezza che occorrono per tale protezione, ma, soprattutto, è, da un altro lato, fondamentale definire le politiche di sicurezza e i processi che rendono questa applicazione un elemento utile e abilitante per il business, piuttosto che un più o meno inutile elemento di rischio aggiuntivo.

Rete ed endpoint

Tutti gli elementi che costituiscono l'infrastruttura ICT devono essere protetti, a partire dalla rete per toccare tutti i sistemi che a questa sono collegati (server, sistemi storage, client, notebook, palmari e altri che magari devono ancora essere inventati). Più precisamente, ne deve essere garantita la sicurezza d'accesso e la disponibiltà e impedito ogni possibile abuso. Negli ultimi anni gli attacchi sono diventati mirati e sono sempre più

sofisticati, il che impone un continuo aggiornamento delle tecniche di protezione. Analogamente, obiettivi di business come la crescita dell'agilità aziendale o la capacità di rilasciare nuovi servizi alla clientela più rapidamente, pongono altre questioni circa l'utilizzo di strumenti per la virtualizzazione. Un sistema di sicurezza adeguato a tali esigenze di business deve dunque essere in grado di trattare sistemi fisici e virtuali allo stesso modo e garantire una sicurezza end to end per la continuità operativa.

Infrastruttura fisica

L'integrazione del sistema di sicurezza non può riguardare solo le tecnologie di protezione da attacchi informatici, bensì deve riguardare la convergenza tra sicurezza fisica e logica. Per il business, infatti, come e per la stessa confidenzialità delle informazioni è altrettanto importante la salvaguardia degli asset fisici e la tutela di impiegati e clienti. Per esempio, sorvegliare l'accesso a un data center con telecamere e altri dispositivi di monitoraggio ambientale è comunque un elemento a garanzia della continuità del business, che potrebbe essere messa a repentaglio da sabotaggi o da malfunzionamenti nell'impianto di condizionamento.
Aziende a contatto con il pubblico, come le banche o i supermercati, entrambe sensibili al pericolo di furti e rapine, già da tempo utilizzano sistemi di sorveglianza, ma l'integrazione tra sistemi di sicurezza logica e fisica forniscono vantaggi per tutte le tipologie d'impresa, accrescendone anche l'immagine e con essa il valore di capitale dell'azienda stessa.

1.1.2 Gli standard di riferimento per la Sicurezza delle Informazioni

L'International Standard Organization ha da tempo individuato nella famiglia ISO/IEC 27000 gli standard di riferimento in materia di Sicurezza delle Informazioni.
Gli standard di questa famiglia sono in fase di completamento ma a oggi possiamo contare senz'altro sui primi due:
ISO/IEC 27001 - Information Security Management Systems, che definisce i requisiti del Sistema di Gestione della Sicurezza delle Informazioni e ne individua le principali fasi e attività;
ISO/IEC 27002 - Code of Practice for Information Security Management, che individua gli 11 principali domini in cui si articola la Sicurezza delle Informazioni e fornisce indicazioni sulle Best Practices da adottare in ciascuno di essi.
Lo Standard ISO/IEC 27001 definisce i requisiti del Sistema di Gestione della Sicurezza delle Informazioni (Information Security Management

System - ISMS), è lo standard per “stabilire, attuare, condurre, monitorare, riesaminare, mantenere attivo e aggiornato, e migliorare un sistema di gestione per la sicurezza delle informazioni”.
È una norma indirizzata alla linea manageriale delle organizzazioni e rappresenta il punto di partenza delle iniziative che dovranno essere avviate in materia di sicurezza delle informazioni prevedendo la definizione di un processo continuo di miglioramento istanziato tramite le fasi di Plan-Do-Check-Act.
L’adozione del sistema di gestione deve essere parte della strategia di ogni organizzazione. La sua progettazione e la messa a punto saranno correlate alle esigenze e agli obiettivi dell’organizzazione, ai suoi requisiti di sicurezza, ai processi e ai beni da proteggere, alla sua dimensione e struttura.
Lo standard puntualizza l’architettura del controllo per la sicurezza delle informazioni: ne definisce i requisiti minimi, individua le aree di criticità, i relativi obiettivi di controllo e i controlli a essi correlati. La scelta degli obiettivi di controllo e dei controlli da introdurre, tra quelli proposti dalla norma, è conseguente alla identificazione e alle azioni di contrasto ai rischi potenziali cui sono esposte le informazioni, alle prescrizioni legali o regolamentari, agli obblighi contrattuali e ai requisiti per la sicurezza delle informazioni delle attività istituzionali/business dell’organizzazione.
Tra i principali requisiti alla base dello sviluppo del Sistema di Gestione della Sicurezza delle informazioni la norma indirizza:

- la definizione dell’ambito d’azione della sicurezza delle informazioni,
- la formulazione di una politica di gestione della sicurezza che tenga conto delle attività istituzionali dell’organizzazione, delle sue dimensioni, delle relative strutture tecnologiche, dei beni da proteggere;
- la conduzione di un risk assessment che individua e classifica i rischi, e promuove la formulazione di decisioni sulle azioni di mitigazione, raccordandole allo sforzo finanziario da sostenere per la loro realizzazione;
- la scelta degli obiettivi di controllo finalizzati alla mitigazione dei rischi nei diversi componenti del sistema;
- la scelta dei controlli utili a soddisfare gli obiettivi di controllo prescelti;
- il concorso decisionale della direzione per l’accettazione dei rischi residui;
- un processo che assicuri il continuo riscontro di tutti gli elementi del sistema di gestione della sicurezza attraverso interventi audit, monitoraggio delle azioni correttive, e verifiche manageriali;
- un processo che promuova il continuo miglioramento degli elementi del sistema;

- la predisposizione da parte della struttura responsabile di una "Dichiarazione di applicabilità" che puntualizzi le decisioni circa il trattamento dei rischi e il livello di rischio residuo accettato, descriva gli obiettivi di controllo e i controlli che sono stati attivati parzialmente, o non lo sono stati affatto, e formalizzi le opportune motivazioni.

La norma precisa anche le responsabilità della direzione per il mantenimento dell'impegno manageriale nella gestione dell'intero sistema, per la gestione delle risorse umane e tecniche dedicate, e per la divulgazione della cultura della sicurezza.
Lo Standard ISO/IEC 27002 individua 11 diversi domini di controllo, ognuno dedicato a una specifica area di soluzioni di sicurezza. Le singole aree affrontano e individuano le best practices di riferimento relativamente alle seguenti tematiche:

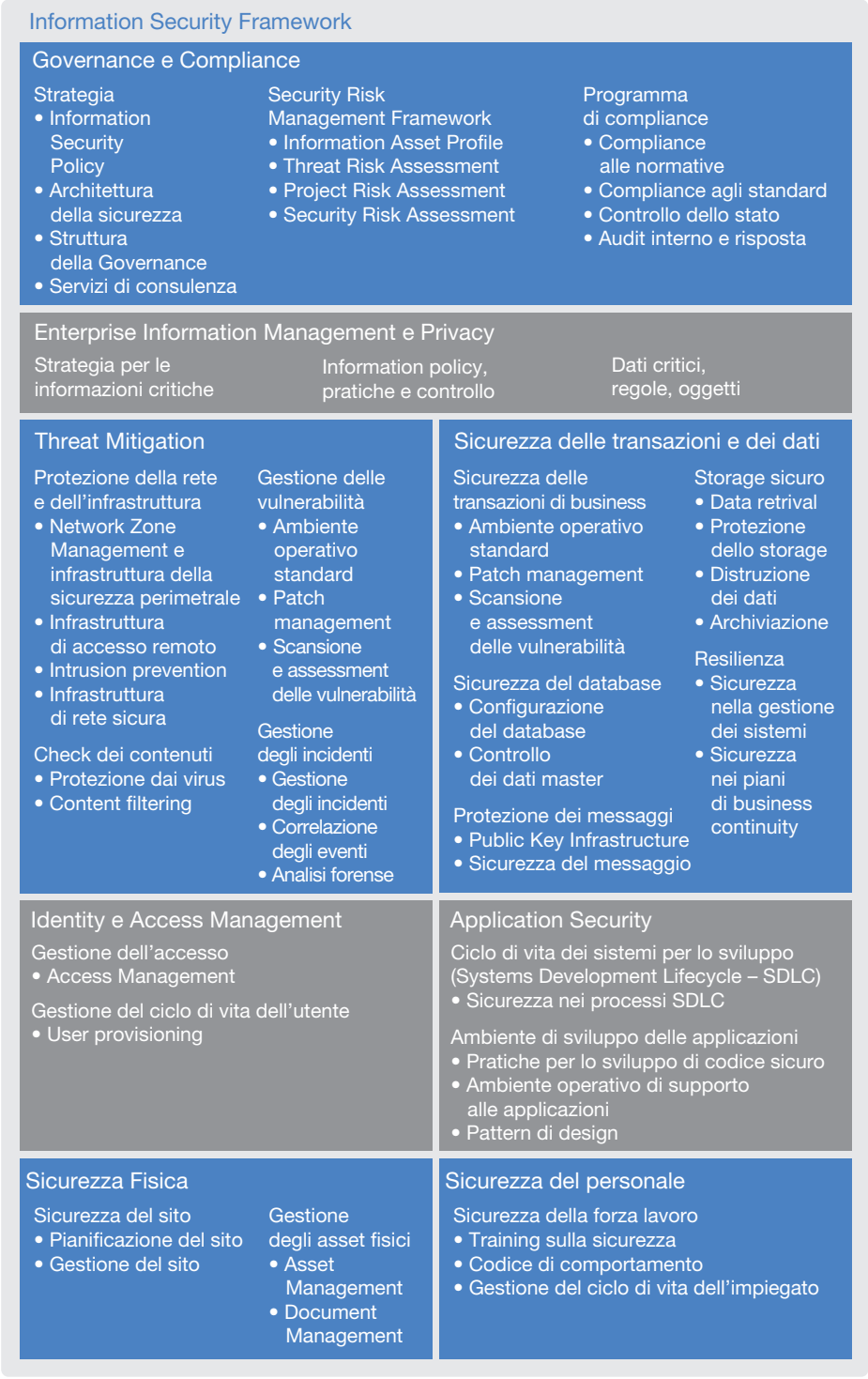
- **Politica di sicurezza**: documento riportante le policy e le regole di sicurezza emanate dall'azienda, la loro diffusione presso il personale e la periodicità dell'aggiornamento;
- **Organizzazione di Sicurezza**: struttura competente per quanto concerne le regole aziendali, le procedure, le modalità operative e gestionali dell'area sistemi informativi, i ruoli e le responsabilità di sicurezza e controllo, incluse le responsabilità delle terze parti coinvolte nella gestione dei servizi;
- **Controllo e classificazione degli Asset**: inventario e valutazione degli asset informatici (dati, applicazioni, software, sistemi hardware) considerati riservati/sensibili, critici o vitali in relazione agli obiettivi e alle strategie dell'azienda;
- **Sicurezza del personale**: piani di formazione delle risorse e del livello di sensibilizzazione del personale in tema di sicurezza, compresa la conoscenza delle procedure per la reazione a fronte di incidenti o malfunzionamenti;
- **Sicurezza Fisica e ambientale**: protezione fisica delle risorse informatiche (server, apparati TLC) e modalità di controllo accessi ai locali ove sono installate (CED);
- **Gestione operativa e comunicazioni**: riguarda la sicurezza di PC/Workstation, Backup e ripristino, Server di rete e applicativi (posta elettronica, navigazione Internet, etc);
- **Controllo degli Accessi**: meccanismi di protezione attivati sui sistemi informatici e sulla rete, la loro integrazione e le modalità operative sui vari ambienti e piattaforme;

- **Acquisizione, sviluppo e manutenzione dei sistemi**: separazione ambienti di sviluppo e produzione; modalità di definizione della sicurezza applicativa, modalità di collaudo e di passaggio in produzione, verifica delle procedure esistenti in relazione alla manutenzione delle applicazioni, gestione software applicativo acquisito dall'esterno;
- **Gestione degli incidenti**: capacità dell'azienda di gestire gli incidenti informatici attraverso la verifica della corretta definizione di ruoli e responsabilità e della presenza di procedure specifiche che, abilitando una immediata reazione correttiva, permettano di proteggere adeguatamente gli asset aziendali;
- **Business Continuity**: capacità di garantire la continuità delle attività di business dell'azienda tramite un piano di Business Continuity che preveda le soluzioni tecnologiche e le responsabilità organizzative per la ripartenza in casi di anomalie o di incidenti;
- **Compliance**: Adeguamento rispetto a standard di settore, indicazioni di legge (D.lgs.n.196/03, copyright, etc) e vincoli contrattuali verso terze parti.

1.2 L'IBM Information Security Framework

IBM è uno dei principali fornitori di sicurezza e uno dei pochi a poter garantire un paniere di soluzioni e servizi, al tempo stesso completo e all'avanguardia, per aiutare le imprese a implementare un approccio integrato e olistico alla sicurezza, allineato con una strategia di IT governance. Per gestire il rischio e accrescere il valore del business, IBM aiuta le imprese a semplificare e automatizzare i controlli di business, ottimizzando i costi e consentendo una più accorta allocazione di fondi e risorse. IBM può abilitare le aziende a monitorare dinamicamente e quantificare i rischi connessi alla sicurezza, a meglio comprendere l'impatto sul business di minacce e vulnerabilità, a rispondere con efficacia e tempestività agli eventi di security, attraverso controlli che ottimizzano i risultati di business, e a dimensionare con efficienza e secondo priorità adeguate i propri investimenti in sicurezza.
La completezza del supporto fornito da IBM alle imprese è ben rappresentato dall'Information Security Framework, che è frutto del lavoro e dell'esperienza maturata dai consulenti di IBM in questo campo. Si tratta di uno schema di riferimento progettato per aiutare le organizzazioni nella creazione di un programma di sicurezza efficiente, che possa rispondere

Figura 1.2
Information Security Framework



alle minacce, ai rischi e alle necessità di business, fornendo, allo stesso tempo, un percorso chiaro per migliorare i livelli di sicurezza all'evolvere delle condizioni e delle situazioni. Tale framework rappresenta un approc-

cio alla sicurezza integrato e completo, strutturato grazie alle best-practice, ai risultati della ricerca di IBM e agli standard per la gestione della sicurezza (come, per esempio, l'ISO27001).
Le aree chiave della sicurezza che vengono indirizzate dalle best practice in questo modello sono: governance, privacy, mitigazione delle minacce, integrità delle transazioni e dei dati, Identity e Access Management, sicurezza delle applicazioni, sicurezza fisica, sicurezza personale.
Le diverse aree identificate dall'IBM Security Framework sono ampiamente trattate nel presente volume, a partire dalla Governance, attorno cui ruota la strategia per la sicurezza di IBM e che sarà oggetto del prossimo paragrafo.
Alle spalle del framework, si trovano tutte le soluzioni, i prodotti e i servizi di IBM, che forniscono una copertura totale delle problematiche di sicurezza secondo l'approccio integrato proposto da IBM stessa.
In particolare, il framework comprende: un "reference model" per l'Information Security, un modello di maturità e un tool di self assessment. Il modello di riferimento è appunto raggruppato nelle suddette aree identificate dallo schema e "riempite" dalle best practice. La costruzione di un reference model aziendale per la security è il primo passo nella creazione di un programma di sicurezza omnicomprensivo per le necessità e gli obiettivi di business. Il secondo passo di questo processo prevede l'utilizzo di un tool di assessment. In tal modo si determina la situazione corrente della sicurezza aziendale.
Attraverso questi strumenti si effettua una misurazione che stabilisce il livello di maturità posseduto da ogni area chiave della sicurezza, per i seguenti componenti "dell'Enterprise IT Security Model": principi, politiche, standard, procedure, architetture e prodotti. La scala di misurazione prevede, per ogni area chiave, i seguenti gradi: iniziale, base, capace, efficiente e ottimizzato. Questo processo di discovery considera l'intero ambiente di sicurezza aziendale, quindi non solo i componenti individuali, aiutando nel contempo a definire un'accurata baseline della situazione presa in esame.
È importante sottolineare come il tool di assessment contribuisca a determinare i rischi potenziali associati a ognuna delle aree chiave. Inoltre, il tool individua quali siano i passi necessari per poter elevare il livello di sicurezza dell'organizzazione al gradino superiore, nel caso gli attuali rischi non siano accettabili dal business corrente. In tal modo vengono inoltre evidenziate le iniziative progettuali necessarie. L'offerta IBM permette altresì di definire il corretto "macro design" di tali progetti, dando una precisa misurazione delle attività richieste, sia in termini di tempi, sia di professionalità coinvolte sia di tecnologie, in armonia con i limiti di budget imposti dall'organizzazione.

Privacy

Per quanto riguarda la privacy, è fondamentale considerare gli aspetti strategici legati alla gestione delle informazioni e dei dati. In particolare, i dati critici, normalmente, sono quelli anagrafici, dati sulla situazione di vita (quali elementi finanziari, credo religioso o appartenenza ad associazioni varie, stato di salute), quelli biologici (gruppo sanguigno, DNA e dati biometrici), dati derivati (come informazioni su polizze stipulate, livello di credito), dati soggettivi (valutazione sulla produttività e altre osservazioni raccolte dall'ufficio del personale) e altre informazioni ricavate da osservazioni varie (come le abitudini di acquisto, la dieta alimentare, gusti musicali). Nelle aziende, specie quelle grandi, spesso sono conservate molte più informazioni di quanto si immagini: basta considerare quanto tempo passa in ufficio e come, senza contare tutto quello che normalmente concerne contabilità e fiscalità, viene comunicato in azienda, magari per usufruire dell'organizzazione di attività di gruppo, la mensa o l'asilo aziendale, per avere l'accesso a sconti o facilitazioni presso negozi, spacci e affini o a possibilità di supporto, come appoggiarsi all'azienda per chiedere un mutuo, una polizza. Una gestione accurata di questi dati. per esempio, aiuta a ridurre i rischi associati con la loro presenza in azienda, eliminando le ridondanze e implementando un'adeguata politica di controllo degli accessi e autorizzazioni.

Mitigazione delle minacce e protezione di transazioni e dati

In questa area le problematiche sono soprattutto di natura tecnologica e sono relative alla protezione dell'infrastruttura. Si tratta della "prima linea" nella cosiddetta Cyber War: da un parte i "cattivi" che sviluppano sempre più sofisticate minacce per sferrare attacchi fortemente mirati e, dall'altra, i "buoni" che attuano logiche preventive per anticipare le mosse dell'avversario.
L'aspetto di business più importante da considerare in quest'area riguarda le priorità da assegnare ai vari elementi da proteggere, ma queste sono normalmente critiche: basti pensare alle transazioni che sono parte integrante, ormai, di tutti i processi di business, sempre più dipendenti dalla tecnologia informatica.

Identity e Access Management

Per quanto concerne il business, è importante capire che l'assegnazione di privilegi per l'accesso alle risorse non è una decisione strategica dell'IT, ma di chi assegna a ciascun individuo le mansioni che egli dovrà esercitare. Sempre più si tende a coinvolgere il responsabile delle risorse umane

e altre figure di business nella definizione di ruoli standard per rendere il più automatica possibile la definizione dei profili utente. È fondamentale, comunque, documentare adeguatamente, anche ai fini della compliance, chi può fare cosa e comunicarlo con accuratezza ai diretti interessati.

Application Security

La sicurezza deve essere applicato a tutto il ciclo di vita delle applicazioni, dal loro sviluppo finché deve esserne garantita la disponibilità IBM fornisce strumenti per la programmazione di software sicuro, per esempio, IBM Rational AppScan Standard Edition è un motore di collaudo di sicurezza delle applicazioni Web che consente di verificare in modo continuo e automatico le applicazioni Web, di risolvere i problemi di sicurezza e di creare report con suggerimenti per semplificare il processo di correzione dei problemi. La scelta strategica proposta da IBM, peraltro, è quella in linea con le tendenze di mercato, che vedono nella SOA (Service Oriented Architecture) l'architettura in grado di garantire ottimizzazione dei costi e agilità. Le soluzioni IBM consentono di coprire anche la sicurezza della SOA.

La sicurezza fisica e del personale

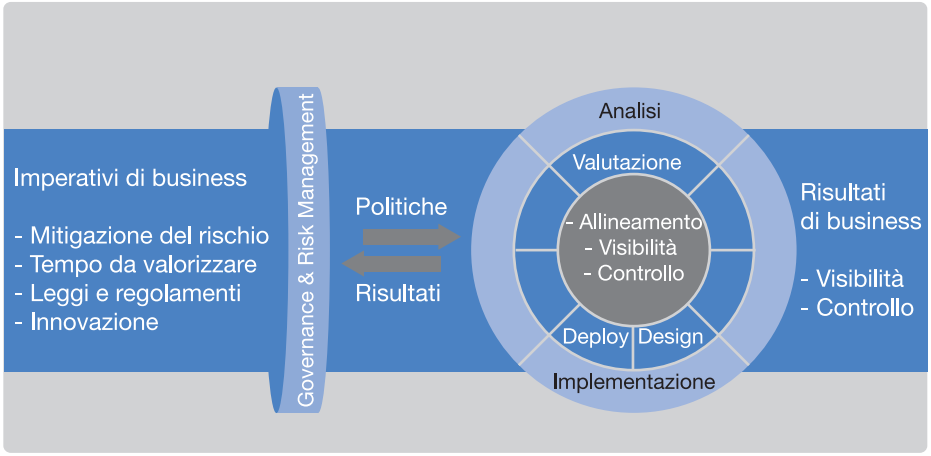
Come è già stato accennato, è fondamentale considerare un approccio integrato per garantire l'adeguata protezione agli asset fisici e a tutti gli individui che hanno rapporti con l'azienda.

1.3 L'Information Security Governance

La necessità di legare sicurezza e business si esplica attraverso un approccio orientato alla governance della sicurezza, in quanto parte dell'IT Governance a sua volta elemento della Governance d'impresa. Il governo della sicurezza parte da un concetto molto semplice: non esiste la sicurezza al 100%, né la sicurezza eterna. Se è dunque necessario accettare un livello di rischio, è evidentemente opportuno imparare a gestire questo rischio e questa è una pratica di business.
L'Information Security Governance rappresenta il framework di riferimento necessario per indirizzare e controllare l'implementazione di un programma di sicurezza in un'organizzazione. Descrive le strategie, le politiche, i ruoli, le responsabilità e i servizi attraverso i quali predisporre in modo strutturato iniziative di sicurezza in linea con gli obiettivi di business definiti dai vertici dell'azienda.

La realizzazione di un sistema di governance dell'IT e della sicurezza aziendale richiede l'adozione di un approccio metodologico che sia in grado di tradurre le politiche e le strategie aziendali in pratica quotidiana, di gestire l'evoluzione della domanda del mercato, minimizzare i rischi e gli impatti per l'operatività dell'azienda, attraverso un processo continuo e integrato che armonizzi le richieste del business e quelle dell'IT.
La figura 1.3 illustra come sia possibile mettere in relazione il ciclo di vita dell'Information Security Governance e della gestione del rischio tramite la messa in opera di politiche di governance corrette, ovvero allineate ai requisiti di business, e la gestione corretta del rischio, ovvero implementata tramite un processo continuo di miglioramento della sicurezza.

Figura 1.3
Governance e Risk Management Lifecycle



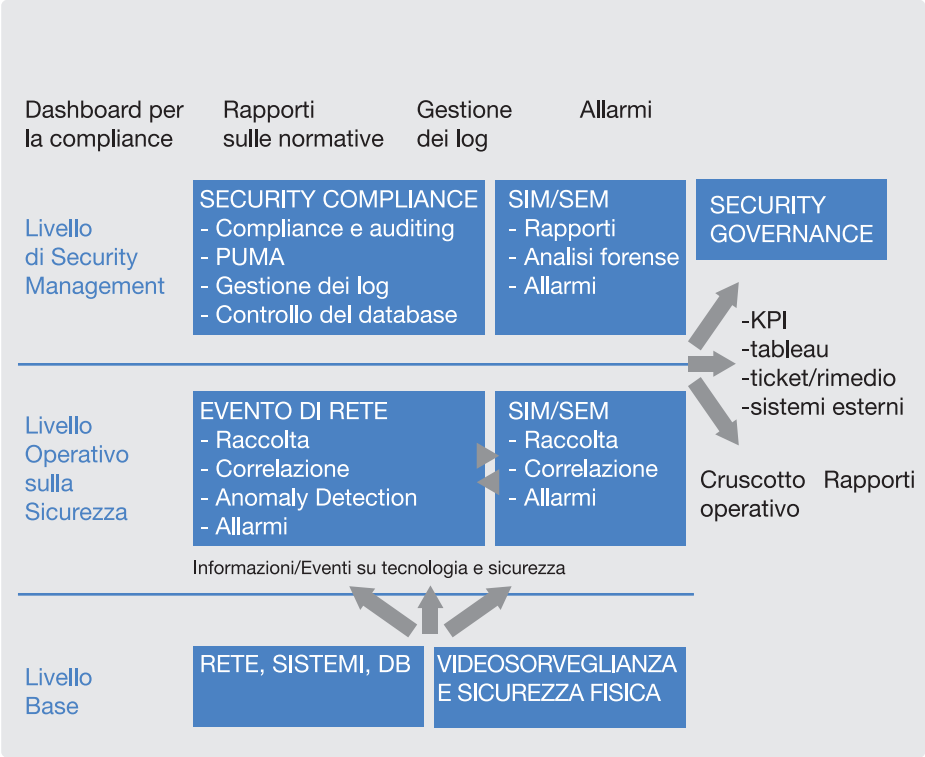
Le policy hanno l'obiettivo di dimostrare che l'azienda fornisce risposte in merito alle crescenti richieste di integrità, trasparenza, responsabilità e consapevolezza del ruolo etico e sociale svolto. Le imprese sono tenute a tutelare i dati dei clienti e a utilizzare le informazioni, i sistemi e le reti in modo da soddisfare aspettative ampiamente riconosciute dal mercato. Queste aspettative sono stabilite da regole sociali, obblighi, norme per l'uso responsabile di Internet, codici etici aziendali e professionali e un insieme crescente di leggi nazionali e internazionali che richiedono la compliance da parte dell'azienda.
Le politiche devono indirizzare l'utilizzo etico delle informazioni, riportando la titolarità, i requisiti di privacy e individuando i potenziali rischi di business per l'azienda e i legittimi proprietari. Questi ultimi stanno dimostrando nel tempo una crescente attenzione verso gli aspetti dell'etica e richiedono che i propri interessi vengano rispettati.

Il processo di gestione del rischio dovrà essere sviluppato attraverso le fasi di:

- **Assessment**, ovvero di valutazione e analisi delle minacce e degli impatti sugli asset aziendali (infrastrutture, informazioni, applicazioni, organizzazione e processi).
- **Plan**, ossia l'individuazione degli obiettivi di sicurezza, delle modalità tecniche e organizzative di protezione e la definizione del sistema di misurazione del livello di sicurezza.
- **Implement**, che consiste nella realizzazione delle soluzioni tecnologiche e delle procedure di prevenzione e di controllo.
- **Manage**, ovvero il monitoraggio e il controllo continuo delle infrastrutture di sicurezza, il rispetto della conformità alle normative, il miglioramento della capacità di reazione agli incidenti, nonché l'incremento dei livelli di servizio forniti all'organizzazione e agli utenti.

Strettamente connessa a queste attività nasce poi l'esigenza di monitorare e misurare il rispetto delle politiche e dei processi stabiliti dall'azienda: questi controlli costituiscono infatti la base indispensabile per dimostrare il raggiungimento dei risultati attesi e migliorarne i valori nel tempo.
In particolare, per quanto riguarda la suddetta fase di "manage", ovvero di monitoraggio e controllo nel processo di Governance e Risk Management, è possibile definire e applicare un preciso modello di governo. Gli obiettivi della governance, infatti, si possono ottenere con la predisposizione di modelli operativi e di strumenti attraverso cui rilevare, misurare e valutare lo stato della sicurezza in funzione di obiettivi pianificati, aspetto fondamentale per comprendere e attuare un processo di continuo miglioramento della sicurezza.
Il modello operativo di governo, riportato nella figura 1.4, riprende il tema del Security Information & Event Management (che sarà ulteriormente approfondito nel capitolo 2), processo fondamentale per consentire di operare valutazioni e azioni in funzione del livello di responsabilità in una organizzazione, attraverso un il monitoraggio e controllo della sicurezza.
A partire dai controlli implementati a livello tecnologico sul campo, attraverso opportune aggregazioni, correlazioni e analisi è possibile controllare gli indicatori di qualità della sicurezza in essere e intervenire con azioni di miglioramento.

Figura 1.4
Il modello operativo di governo



Sono riportati a titolo di esempio due livelli di attenzione in funzione del livello e dei ruoli di responsabilità all'interno dell'organizzazione: Security Operation Level e Security Management Level. Per ciascun livello di management sono disponibili informazioni nella forma di cruscotti, rapporti, log e sistemi di allarme, compatibili con i ruoli organizzativi interessati; le informazioni prodotte consentono di avere una visione completa ed esaustiva del modello di governo della sicurezza anche in ottica conformità e supporto ai processi di audit (interni/esterni).

1.3.1 Il Data Centric Security Model

Generalmente i decision-maker delle aziende non sono direttamente coinvolti con gli aspetti di gestione delle infrastrutture di sicurezza presenti nelle loro imprese. Tradizionalmente infatti la gestione delle risorse in materia di sicurezza è affidata a un piccolo gruppo di professionisti specializzati e competenti, che poi provvedono a mantenere informata la dirigenza dell'azienda.
Il fenomeno della diffusione di minacce informatiche sempre più sofisticate e articolate e il fatto che la protezione delle risorse critiche aziendali richiede soluzioni di sicurezza sempre più complesse, non sempre trova un riscontro efficace a causa del difetto comunicativo che a volte esiste tra i decision-

maker e i responsabili della sicurezza IT. Per gli stessi motivi sta aumentando anche il rischio di interpretare in maniera errata le strategie e le politiche dell'azienda proprio quando, nelle fasi di rapida trasformazione della stessa, le strategie e le politiche devono tradursi in controlli tecnicamente sicuri.
Un modello per la gestione della sicurezza aziendale che permette di superare questo ostacolo è il Data Centric Security Model (DCSM), la cui caratteristica principale è proprio quella di affidare la gestione delle politiche di sicurezza agli stessi decision maker. In questo modo le decisioni aziendali possano essere attuate in maniera diretta senza l'effetto dispersivo di un'interpretazione a più livelli dell'organizzazione e con il beneficio di riuscire a cogliere la correlazione diretta tra le strategie dell'azienda e i meccanismi di sicurezza a supporto. L'approccio DCSM vuole essere un punto di partenza per un dibattito costruttivo e fornisce altresì una ricca piattaforma di ricerca in materia di gestione della sicurezza "business-driven".
Come è stato evidenziato, è difficile ma fondamentale definire le priorità di intervento in base alle esigenze di business e determinare e implementare il livello adeguato di sicurezza IT necessario per la loro protezione, cosa che si propone di fare il Data Centric Security Model.
Il punto di partenza è la strategia aziendale che il business manager deve aver sviluppato per realizzare la visione dell'azienda. Una strategia aziendale consiste in un piano d'azione con cui un'impresa si propone di ottenere e sostenere un vantaggio competitivo. I suoi obiettivi, che fungono da indicatori per la misurazione e valutazione del suo successo, sono generalmente incentrati sui seguenti aspetti:

- Massimizzazione del valore per gli azionisti.
- Mantenimento e acquisizione di clienti.
- Riduzione dei costi di gestione del business.
- Mantenimento e miglioramento della competitività di mercato.
- Mantenimento della continuità aziendale e della capacità di ripresa.
- Ottenimento e mantenimento della conformità alle norme esistenti.
- Gestione e potenziamento dell'immagine aziendale sul mercato.
- Attuazione di nuovi investimenti.
- Identificazione e sfruttamento di nuove opportunità commerciali.

Le informazioni assumono un'importanza chiave nella realizzazione di tali obiettivi strategici. Le tecnologie IT di sicurezza, quali sistemi di intrusion detection e prevention, soluzioni di data leak protection, antivirus, firewall, strumenti per l'applicazione delle politiche di protezione dei dati e

le soluzioni VPN svolgono un ruolo fondamentale nell'ottenere una protezione efficace dei sistemi necessari alla realizzazione dei suddetti obiettivi di business. Questi non sono obiettivi strategici in quanto tali, tuttavia, guardando oltre i dettagli specifici delle varie tecnologie e sistemi, si osserva che la sicurezza IT contribuisce a stabilire un senso di fiducia e a mitigare i fattori di rischio. In questo senso, ha quindi un impatto considerevole sulla maggior parte dei suddetti obiettivi.

La priorità principale sul piano della sicurezza deve essere quella di proteggere i dati critici, i processi core nonché la fiducia riposta nell'azienda da altre imprese, dai clienti e dagli azionisti. I clienti e le aziende sono più propensi a stabilire rapporti di collaborazione con organizzazioni di cui si fidano. Un'azienda, specie se si propone come brand, sarà molto preoccupata di riuscire a mantenere la propria reputazione di partner di business fidato. Con riferimento alla sfera IT, la fiducia si manifesta principalmente nei metodi con cui vengono creati, raccolti, immagazzinati, elaborati e infine distribuiti i dati.

Le interdipendenze tra gli obiettivi di business e quelli della sicurezza si manifestano nell'implementazione e nel supporto dei processi di business. Ne consegue che il primo intervento da effettuare, al fine di ridurre il divario tra sicurezza e obiettivi di business, è quello di identificare le risorse aziendali chiave ed esaminare i rischi a esse associati. Fondamentalmente le aziende dipendono in larga parte dalle risorse informative di cui dispongono. Queste rappresentano infatti il "manufatto" commerciale più rilevante e prezioso che una società possa possedere, in quanto: le informazioni costituiscono il know-how di un'azienda, i processi di business essenziali per l'azienda operano in funzione delle informazioni e I rapporti di fiducia tra le società sono mantenuti attraverso lo scambio di informazioni (spesso sensibili).

Il Data Centric Security Model parte dal dato di fatto che non tutte le informazioni hanno la stessa importanza e il livello di sicurezza da adottare deve essere determinato in funzione del loro valore di business. Al fine di identificare quest'ultimo, un'impresa può analizzare tre aspetti significativi: il valore di business delle informazioni, i processi di business che le utilizzano e le relazioni di business che esse supportano. Questo è un compito complesso che deve essere adattato alle esigenze specifiche di ciascuna azienda: per esempio, le società finanziarie tendono a essere più interessate alle informazioni relative agli investimenti dei loro clienti piuttosto che alle informazioni relative ai loro dipendenti.

Una volta determinato il valore dei dati si può procedere alla definizione e conseguente giustificazione dei relativi controlli di sicurezza da realizzare, sulla base delle esposizioni ai rischi.
Il DCSM consente alle organizzazioni di far fronte alla mancanza di correlazione tra la tecnologia di sicurezza IT e gli obiettivi della strategia di business. Il modello propone infatti di collegare i servizi di sicurezza direttamente ai processi di business, instaurando una correlazione diretta tra i servizi di sicurezza e i dati stessi che si vogliono proteggere. Tale rapporto viene molto spesso oscurato dalla percezione della sicurezza come entità fine a se stessa.
Nel DCSM il focus del modello si concentra sulla classificazione dei dati in base al livello di sicurezza da garantire loro. Questa determina poi le proprietà e le politiche di controllo dell'accesso che disciplinano l'utilizzo dei dati da parte delle applicazioni, le quali gestiscono i processi di business. Dai servizi di sicurezza e i meccanismi su cui essi si fondano, possono essere ricavate le interfacce per il supporto diretto delle politiche e per la gestione dei dati. Il DCSM non richiede importanti modifiche dell'assetto dei servizi di sicurezza, anzi esso ne sfrutta le funzionalità esistenti integrandole e adattandole in modo da essere interpretate e capite direttamente dai soggetti responsabili della definizione e gestione dei processi di business. In questo modo, la sicurezza può essere intesa come elemento di supporto diretto sia ai processi sia agli obiettivi di business.
L'approccio DCSM non crea questo legame attraverso i dati, ma porta alla luce quei componenti dei dati relativi alla metodologia di sicurezza, che spesse volte sono oscurati dalle formalità e dalla terminologia tipica della sicurezza. Il fine di tutte le tecnologie della sicurezza è quello di proteggere i dati, e tutti i protocolli e le funzioni di sicurezza sono rivolte a un uso appropriato dei dati.
Il principio espresso dal DCSM è in sostanza un riposizionamento delle funzionalità di controllo dei dati con il supporto dei servizi di sicurezza IT nell'ambito dei modelli di sicurezza esistenti. Si sposta l'attenzione sulle Informazioni ("I") e il loro valore rispetto alla Tecnologia ("T") in un contesto di IT Security.
Generalmente, queste funzionalità di controllo dei dati non vengono enfatizzate a sufficienza, ma è proprio questo aspetto dei servizi di sicurezza che creerà il legame con i processi di business. Inoltre, il DCSM non dipende esplicitamente da tecnologie o prodotti di sicurezza specifici ed è altresì indipendente dall'infrastruttura di base. Il DCSM

non implica nessun tipo di modifica ai metodi di applicazione delle politiche al sistema IT di base, esso fornisce semplicemente uno strumento per individuare e monitorare i requisiti di business sulla base di controlli di sicurezza tangibili.
La prima funzione del modello DCSM è quella di definire una serie di direttive per la gestione integrata dei dati, in funzione delle politiche di business. La seconda funzione del DCSM è quella di determinare quali siano i servizi di sicurezza adeguati a sostegno di tali direttive. Le direttive sono divise in due parti, di cui la prima si occupa della classificazione dei dati di business. Una classe può essere determinata in funzione della proprietà dei dati e di specifici requisiti di sicurezza, per esempio:

- Da dove provengono i dati?
- Chi è il proprietario dei dati?
- Chi controlla i dati?
- Chi o cosa conserva i dati?
- Di che tipo di dati si tratta?

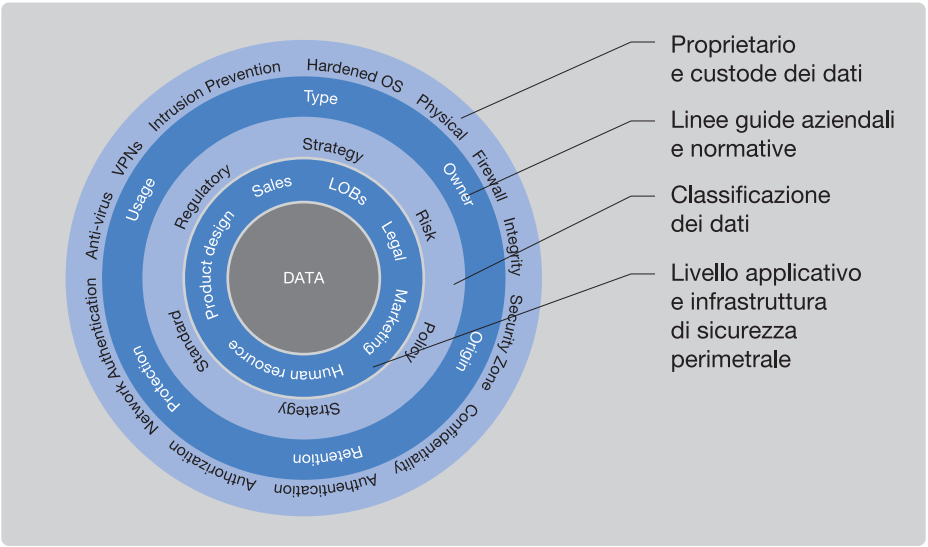
Per ciascuna classe di dati, vengono definiti specifici requisiti di sicurezza business-oriented che disciplinano come devono essere trattati e protetti i dati in funzione della classe di appartenenza. Per esempio le decisioni di politiche che definiscono le modalità di gestione dei dati possono includere:

- Chi o cosa può utilizzare i dati?
- A quale scopo?
  - Possono essere condivisi?
  - A quali condizioni?
- Dove verranno conservati i dati?
- Per quanto tempo verranno conservati?
- È necessario proteggerli?
  - A riposo?
  - Quando viene fatto il back-up?
  - Durante l'utilizzo?
- Quali sono le modalità di diffusione dei dati?
  - Quale sottoclasse di dati può essere diffusa?
  - Che tipologia di protezione deve essere attuata?
  - Occorre distorcere i dati o proteggerli con la tecnica del watermark?

Ciascuna di queste problematiche relative alla gestione dei dati ha un impatto diretto sul business: più precisamente, sulla protezione della conoscenza intellettuale e di business, il mantenimento dell'integrità dei processi di business e infine il rispetto delle normative vigenti.
L'interdipendenza tra le suddette direttive e i servizi di sicurezza è altrettanto evidente: infatti, la conferma dell'origine e proprietà dei dati dipenderà dai servizi di autenticazione e provenienza, la modifica dei dati dai servizi di autorizzazione, gestione, revisione e controllo di accesso; la tutela dei dati dai servizi sulla riservatezza, privacy e controllo della divulgazione;infine l'archiviazione dei dati dai servizi di integrità e affidabilità. I meccanismi alla base di questi servizi di sicurezza possono essere complessi e fanno parte dei servizi relativi all'infrastruttura IT. Tali dettagli sono però nascosti nel modello DCSM.
Nell'ambito della gestione della sicurezza, l'enfasi si sta spostando dalle difese di tipo network-based a quelle di tipo host-based. Estendendo questo approccio di difesa a strati oltre il modello di sicurezza host-based ai dati che vengono protetti su quegli stessi host, si arriva proprio alla soluzione DCSM. Al fine di riuscire a gestire questi strati difensivi multipli, il DCSM definisce un approccio integrato che unisce insieme requisiti e politiche. Nella figura 1.5 si può osservare questo principio nell'ambito del modello DCSM, dove i dati sono posti al centro di tutte le attività e le operazioni.
Dal punto di vista del business, l'obiettivo primario nel creare un DCSM è quello di identificare il proprietario dei dati, sia esso un individuo, un cliente o un settore di attività. I requisiti necessari vengono raccolti sia nell'ambito legislativo sia di business, in particolare da norme e direttive che disciplinano l'utilizzo e la gestione di tipologie specifiche di dati. I dati vengono classificati utilizzando una terminologia commerciale mentre le politiche di controllo dell'accesso vengono definite tramite l'utilizzo di ruoli organizzativi.
I due componenti principali alla base del Data Centric Security Model sono i servizi per la gestione delle politiche di sicurezza (Policy Pillar) e quelli relativi la gestione dell'accesso alle informazioni (Data Pillar), come mostrato nella figura 1.6. Naturalmente il modello è integrato da servizi di Identity Management necessari per la gestione delle identità, delle utenze e dei relativi profili autorizzativi.
Le politiche e le normative societarie così come le norme legislative esprimono politiche di gestione dei dati in termini di requisiti, sia interni sia esterni all'impresa. Il modello prevede l'utilizzo di tali requisiti al fine di determinare una classificazione dei dati di business di carattere generale,

Figura 1.5

Il Data Centric Security Model pone i dati al centro della strategia per la sicurezza



rappresentativa dell'insieme delle categorie e attributi utilizzati. Il fine è quello di identificare le politiche generali di governance dei dati. La classificazione dei dati e le regole per il loro trattamento vengono quindi codificate all'interno di norme di controllo Data Control Rules (DCR) che rappresentano le politiche di gestione e controllo dei dati.

Il data pillar del DCSM poggia su un'infrastruttura di sicurezza che fornisce funzioni di sicurezza base, quali difesa perimetrale, protezione dei dati e incapsulamento dei dati durante le fasi di trasmissione.

L'accesso ai dati e le azioni permesse in riferimento a essi vengono controllate dal Data Control Layer (DCL). Questo servizio è studiato per implementare le politiche (astratte) espresse in termini di regole di controllo accesso (DCR) e fa affidamento sui servizi di sicurezza e protezione dati presenti all'interno dell'infrastruttura IT. Il servizio ottiene il contesto di accesso (es. utenti autenticati) e poi lo utilizza per determinare se può essere consentito l'accesso ai dati. L'infrastruttura IT è configurata per supportare le politiche di sicurezza che sono state ricavate dai DCR. Le applicazioni di business hanno accesso ai dati attraverso il DCL, il quale utilizza le politiche di governance dei dati così come previste a livello DCR.

Nella parte alta del data pillar si trova un componente di autenticazione role-based, che identifica gli utenti e assegna loro determinati ruoli in funzione delle politiche di autenticazione fornite dal policy pillar. Per garantire la protezione senza il bisogno di apportare significative modifiche alle applicazioni, si fa leva su un modello di astrazione dell'applicazione che consente di mappare la terminologia tra i vari contesti applicativi, in funzione delle normative societarie di governance dei dati. Questo consente

al DCL di comprendere il contesto dell'applicazione senza il bisogno di particolari adattamenti dello stesso alle politiche di sicurezza.
Il DCSM fornisce strati di protezione che sono coerenti con le politiche e le normative organizzative e societarie; gli standard societari sono invece utilizzati per vietare (o consentire) l'accesso ai dati da parte degli utenti. Il grado di sensibilità dei dati determinerà poi le giuste misure di protezione da adottare in ogni fase del processo di richiesta dei dati.

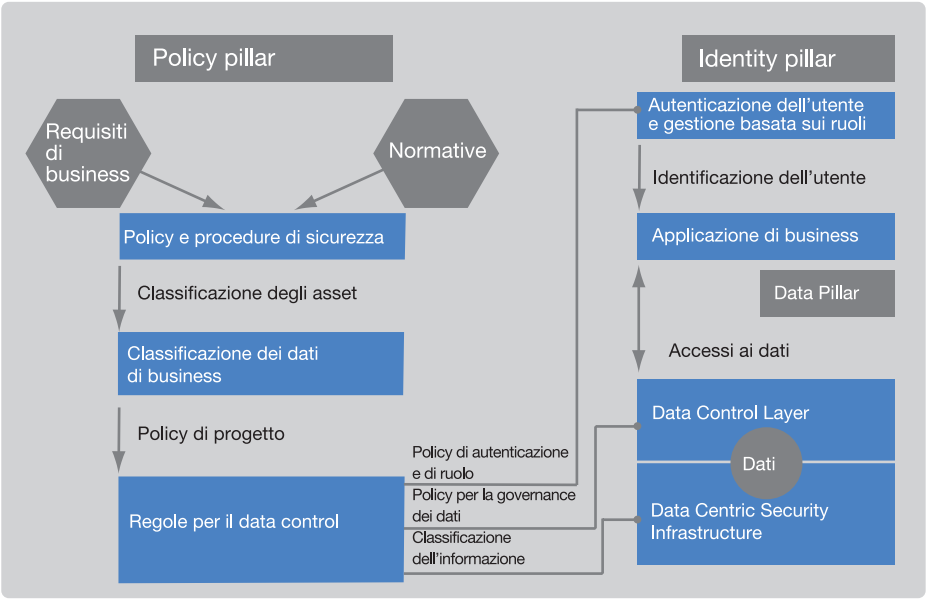


Figura 1.6
I componenti principali del Data Centric Security Model

I servizi all'interno dell'infrastruttura vengono impiegati per proteggere i dati critici, mentre dal piano societario di accettazione del rischio dipenderà l'utilizzo appropriato delle tutele tecniche a livello infrastrutturale e di applicazione.
La figura 1.7 mostra un esempio di deployment logico del DCSM. L'infrastruttura di sicurezza fornisce al DCL servizi che sono definiti in termini di politiche di controllo dei dati. In questo contesto, un'istruzione contenuta in una policy, come per esempio "dati di tipo X da trasportare in maniera sicura", si tradurrebbe in una richiesta da parte del DCL al servizio di trasporto protetto dell'infrastruttura di sicurezza. Tale servizio, a sua volta, potrebbe fare affidamento su un protocollo quale l'SSL, che a sua volta potrebbe utilizzare autenticazioni basate su certificati in svariati modi. In ogni caso queste informazioni rimarrebbero nascoste al DCL. Se il richiedente dei dati è un dipendente mobile, il requisito di trasporto protetto potrebbe essere soddisfatto semplicemente utilizzando una connessione VPN protetta, dettaglio ancora una volta tenuto nascosto al DCL.

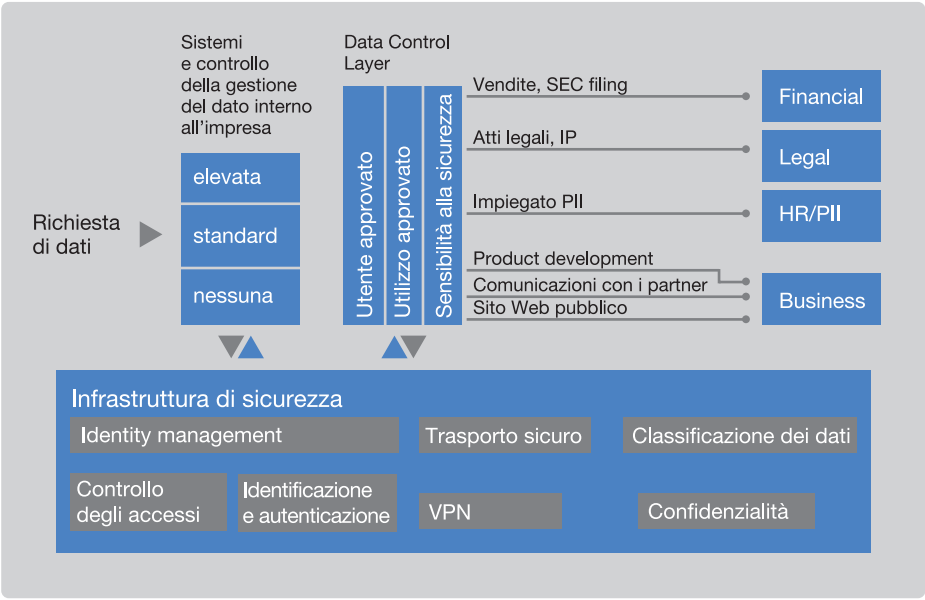
1.3.2 La strategia e l'offerta di IBM per la Security Governance

Nel corso degli ultimi anni IBM ha effettuato significativi investimenti nell'area della sicurezza per la creazione di asset e metodologie a supporto della governance e del risk management, nonché per l'acquisizione di aziende leader nel mercato delle soluzioni e dei servizi di sicurezza: basti ricordare, a tal proposito, Internet Security Systems, Watchfire, Consul e Micromuse.
Grazie alle recenti acquisizioni IBM ha sviluppato un'offerta di prodotti e servizi che aiuta le aziende nel disegno e nella realizzazione di un sistema di governance per:

- monitorare, in tempo reale, gli impatti sul business indotti dai rischi correlati alla Sicurezza delle Informazioni;
- controllare la Sicurezza delle Informazioni e nel contempo fornire al management le metriche di governo;
- automatizzare le operazioni di controllo, migliorando l'efficienza e l'efficacia dell'organizzazione, riducendo i costi e liberando risorse per sostenere l'innovazione dei processi aziendali.

Il sistema di governance, come rappresentato nell'Information Security Framework, è trasversale a tutte le aree della sicurezza e a tutti i "layer" dell'infrastruttura IT: rete, server, applicazioni, dati. Inoltre, deve sostituire il tradizionale approccio di tipo reattivo con tecnologie che ne adotta-

Figura 1.7
Il deployment logico del Data Centric Security Model



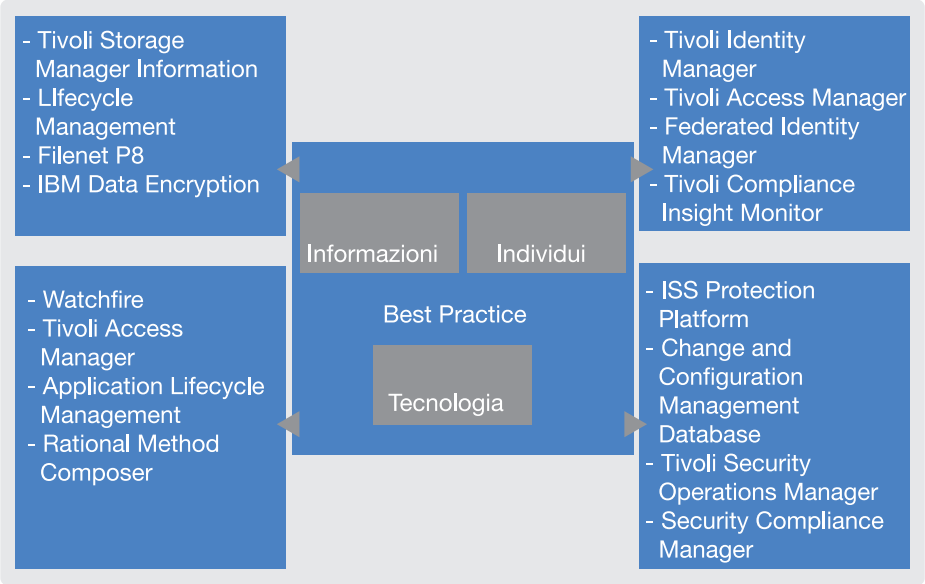
no uno di tipo preventivo, che hanno, cioè, il compito di evitare l'insorgere di problemi di sicurezza, individuando e rimuovendo le potenziali esposizioni ai rischi.
L'offerta di IBM, ispirandosi alle best practice, garantisce:

- la confidenzialità e l'integrità delle informazioni attraverso le soluzioni Tivoli Storage Management, Filenet, Data Encryption;
- il controllo degli accessi e la gestione delle identità digitali, anche in ambienti federati, attraverso le soluzioni Tivoli Identity Manager, Tivoli Access Manager, Tivoli Federated Identity Manager;
- il controllo dell'infrastruttura, grazie ai prodotti e servizi gestiti di Internet Security Systems, al Tivoli Security Operation Manager, Tivoli Compliance Insight Manager;
- il controllo delle applicazioni, attraverso l'analisi delle vulnerabilità effettuata da Rational APPScan.

1.4 La compliance alle leggi sulla sicurezza

Il panorama legislativo nazionale e internazionale in materia di sicurezza delle informazioni ha visto negli ultimi anni un notevole impulso. Tuttora è un processo in corso per certi versi inarrestabile, tanto è pervasivo il problema della sicurezza in tutte le attività sia nel settore privato sia in quello pubblico. Alle leggi emanate dai governi, inoltre, si aggiungono i regolamenti imposti da associazioni e consorzi. Il problema principale è che questa moltitudine di norme, alcune direttamente altre indirettamente o parzialmente riguardanti la sicurezza, esprimono requisiti non sempre chiaramente individuabili e a volte in contrasto tra loro.
L'atteggiamento che più di frequente si riscontra nelle imprese italiane è quello di affrontare l'esigenza di conformità con un approccio di tipo reattivo, orientato di volta in volta a indirizzare i requisiti di conformità di ciascuna specifica normativa in modalità "verticale", realizzando controlli di sicurezza strutturati a "silos" e vivendo l'incombenza come un obbligo, un fastidio che "ingessa" le attività di business. Questa visione poco lungimirante porta ad assegnare alla security compliance e alla sicurezza in generale il minimo delle risorse possibili.
Un atteggiamento ben testimoniato dalle esperienze, consolidate ormai da un decennio, per la conformità alla legge sulla "Privacy": a malapena le aziende indirizzano le cosiddette "misure minime" e il concetto di "Sicurezza delle Informazioni", basato sulla gestione del rischio e quindi

Figura 1.8
L'offerta di IBM legata alle best practice Security Capabilities



sulle misure "idonee", è ampiamente disatteso. Lo stesso Garante della Privacy ha più volte riscontrato una certa superficialità da parte delle aziende italiane nel trattare la sicurezza dei dati personali: il più delle volte si "aggiustano" gli adempimenti di natura formale ma vengono tralasciati quelli di natura sostanziale.

Questo "tamponare" la situazione impedisce alle imprese di attivare le possibili sinergie tra i controlli di sicurezza, in modo da indirizzare in maniera integrata i requisiti delle diverse normative. Un esempio è la recente normativa della PCI (Payment Card Industry), che impone diversi requisiti per consentire l'utilizzo delle carte di pagamento. Molte imprese sono preoccupate di dover ottemperare a una nuova legge e spendono tempo a cercare scappatoie, mentre, se avessero un sistema efficace di controllo della security compliance, probabilmente si accorgerebbero di essere già conformi allo standard PCI per la sicurezza, che riprende, infatti, molti aspetti già coperti da altre leggi o regolamenti.

Il monitorare nel tempo il mantenimento della compliance, inoltre, non è semplicemente un'azione opportuna, ma un'esigenza dovuta alla dinamicità delle minacce e del concetto stesso di sicurezza. Il problema di natura culturale e organizzativo verso l'Information Security rimane il principale fattore di ostacolo alla possibilità di concepire la conformità normativa, e i relativi requisiti di sicurezza, come una vera opportunità per la pianificazione, lo sviluppo, la gestione e il monitoraggio di un sistema di gestione dell'Information Security integrato e basato sulla gestione del rischio.

1.4.1 Un corretto approccio alla security compliance

Quando si parla di sicurezza ICT, in molte imprese si pensa subito che si tratta di un argomento che riguarda esclusivamente il dipartimento dei sistemi informativi. Anche nel caso delle medie imprese, spesso, si tende ad affidare tutto il processo della compliance connesso alla sicurezza al consulente esterno, rifugiandosi dietro una sostanziale ignoranza. Per quanto la sensibilità al tema sicurezza si stia diffondendo, solo in poche realtà illuminate è chiaro che l'Information Security Compliance riguarda l'organizzazione nel suo complesso, in quanto tale tematica dovrebbe essere considerata come una componente del più ampio "Processo di Compliance" aziendale.

In tale contesto la specificità dell'Information Security Compliance riguarda in particolare i requisiti di integrità, confidenzialità e disponibilità delle informazioni, rispetto ai quali è necessario dimostrare di aver implementato il sistema più adeguato alle proprie esigenze di sicurezza. Tali requisiti dovrebbero essere soddisfatti impostando una strategia che consenta di gestire nel tempo e in modalità "cost effective" gli aggiornamenti e la complessità legata al crescente numero di nuove disposizioni con valenza giurisdizionale multipla. La strategia dovrebbe inoltre indirizzare l'armonizzazione con le politiche interne assicurando il minimo impatto possibile sui processi operativi aziendali.

È evidente, dunque, che la strategia per la sicurezza deve essere definita da parte del top management aziendale, coinvolgendo tutti gli attori responsabili dei diversi aspetti legati alla conformità: Ufficio Legale, Risorse Umane, Compliance Manager, Risk Manager, Security Manager, IT Department, Operation e così via.

L'approccio corretto all'Information Security Compliance nelle aziende dovrebbe essere pertanto quello di indirizzare i requisiti di conformità in modalità proattiva e sistematica, tramite lo sviluppo di uno specifico processo cross-aziendale per la gestione della compliance che consenta di:

- individuare, e monitorare nel tempo, le diverse normative che implicano obblighi di Sicurezza delle Informazioni;
- interpretare e armonizzare gli obblighi di Sicurezza delle Informazioni provenienti dalle diverse normative (per esempio "Sicurezza vs Privacy");
- identificare i requisiti di Sicurezza delle Informazioni che consentono di soddisfare gli obblighi precedentemente interpretati per ciascuna normativa;

- selezionare e implementare le misure di sicurezza di natura organizzativa, procedurale e tecnologica, atte a indirizzare i requisiti individuati;
- individuare e implementare un sistema di indicatori atti a fornire le evidenze dei controlli implementati;
- monitorare nel tempo il mantenimento della conformità.

1.4.2 Il supporto di IBM per la compliance alle normative sulla sicurezza

Come già evidenziato, IBM, anche attraverso acquisizioni, ha messo a punto un'offerta articolata di servizi e soluzioni per la sicurezza integrata, che coprono adeguatamente tutte le esigenze delle aziende e le supportano nello sviluppo e nell'attuazione del processo di Information Security Compliance Management. Tramite i servizi di natura consulenziale e grazie alle esperienze sviluppate da molti anni a livello nazionale e internazionale, inoltre, IBM ha sviluppato approcci metodologici e specifiche competenze professionali per supportare le aziende nelle attività di sviluppo e gestione dell'Information Security Compliance Management Process tramite:

- individuazione e analisi degli obblighi e dei requisiti di Information Security derivanti dalle normative;
- analisi dei rischi, selezione delle misure di sicurezza di natura organizzativa, procedurale e tecnologica, atte a indirizzare i requisiti individuati;
- sviluppo del Piano di Information Security in linea con le best practice e gli standard di riferimento;
- sviluppo di politiche e procedure di Information Security specificamente orientate alla conformità normativa;
- disegno e implementazione degli aspetti di processo legati all'Information Security Compliance e alla gestione dei relativi indicatori di conformità;
- disegno e implementazione di soluzioni tecnologiche e architetture di Enterprise Security Management orientate alla conformità normativa e alle esigenze di monitoraggio;
- sviluppo ed erogazione di piani di formazione e sensibilizzazione in materia di Information Security.

Le soluzioni che sono state già elencate relativamente all'IBM Security Framework vanno evidentemente a coprire anche le esigenze tecnologiche d'Information Security Compliance, per le quali è disponibile un'offerta integrata di tecnologie hardware e software e di servizi di gestione da

remoto. Inoltre, specificatamente per queste problematiche IBM, ha sviluppato un approccio metodologico orientato allo sviluppo del Modello di Monitoraggio dell'Information Security nel suo complesso, che si avvale di soluzioni tecnologiche per la gestione degli eventi di sicurezza e dei molti dati da registrare, documentare e archiviare per la compliance.

Modello di Monitoraggio della Sicurezza

Un modello di monitoraggio "operativo", in grado cioè di guidare la realizzazione concreta di una architettura e supportare la governance, si deve basare su due componenti fondamentali: un modello di riferimento (o framework) e una o più metodologie. Entrambi, nel caso specifico della sicurezza, non potranno essere "generici" ma sviluppati e sperimentati nel campo in questione.
Il modello IBM di riferimento è denominato Unified Governance Framework for Security (brevemente UGF). È stato sviluppato dal laboratorio IBM di Zurigo in collaborazione con i servizi professionali di consulenza IBM. L'aspetto più innovativo dell'UGF consiste nel fatto che estende un modello, il Component Business Model (CBM), creato da IBM per disegnare architetture di tipo SOA, adattandolo allo standard ISO/IEC 27001 e al relativo Information Security Management System (ISMS).
C'è una logica forte dietro questa scelta. Una moderna architettura di sicurezza non può oggi prescindere da concetti quali: componenti/servizi riusabili e "policy driven". Un'architettura SOA non limita i suoi benefici al mondo applicativo classico, ma li estende pienamente in tutti i campi dell'IT e in particolare a quello della sicurezza.
Lo sviluppo del Modello di Monitoraggio si avvale inoltre delle metodologie proprietarie IBM "Methodology for Architecting Secure Solutions" (MASS) ed "Event Management & Correlation Design Methodology" (EMCD). La prima viene utilizzata come guida alla base delle attività previste nelle fasi di analisi e disegno del modello e dell'architettura di monitoraggio. La seconda è usata per le attività relative all'identificazione degli eventi/informazioni da trattare e, quindi, per la definizione di regole e politiche di correlazione.

Unified Governance Framework for Security

Il Framework di Governo per la Sicurezza (Unified Governance Framework, nel seguito UGF) sviluppato da IBM è tale da supportare il tema della governance a livello enterprise a partire da servizi, controlli e processi IT disponibili in ambito sicurezza; con l'obiettivo di indirizzare e monitorare la realizzazione di un programma di sicurezza consistente e coerente con le politiche dell'azienda e con gli obiettivi strategici e di business.

La struttura del framework UGF si basa su un modello a componenti (component model) e un approccio per la gestione del ciclo di vita del framework stesso (Plan-Do-Check-Act), secondo quanto previsto dallo standard ISO/IEC 27001 e relativo Information Security Management System (ISMS).
Il framework è costituito da tre livelli su cui sono posizionati i componenti di servizio di base per la sicurezza correlati e consistenti con il Component Business Model (CBM) di IBM. Per ciascuno dei componenti afferenti al business sono riportati i componenti di sicurezza abilitanti e a supporto. Dalla semantica del CBM i livelli su cui si collocano i componenti sono identificati come segue:

- Strategy (Directing): Strategie di sicurezza a supporto delle strategie di business.
- Tactics (Controlling): Modelli operativi e di servizio per la gestione della sicurezza.
- Operations (Executing): Componenti IT per implementare i controlli di sicurezza.

In particolare il disegno del modello di Monitoraggio della Sicurezza trova la sua collocazione all'interno del livello denominato Tactics (Controlling) del framework. Si stabiliscono nello specifico e con un adeguato livello di dettaglio i controlli che necessitano di essere eseguiti con l'obiettivo di supportare gli obiettivi di business attingendo da requisiti espressi in termini di Strategie Prestazionali, Strategie di Conformità e Strategie di Gestione del Rischio, previsti nel livello di Business Strategy (Strategy – Directing).
Così come per tutti i componenti a questo livello, sono previste regole e politiche di valutazione e misurazione dell'efficacia ed efficienza del controllo operativo sottostante.
Il componente di monitoraggio presente a livello Operation (Executing) si sviluppa quindi a partire dal modello di monitoraggio della sicurezza sviluppato e realizzato secondo un percorso Model-Develop-Deploy caratteristico di un processo di sviluppo.
Il modello di monitoraggio si sviluppa e trova la sua rappresentazione nel framewok di governo in termini di componente e come tale sono identificabili un insieme di interfacce, relazioni e servizi espressi in forma sintetica.
Il modello di monitoraggio della sicurezza, realizzabile tramite l'approccio metodologico sopra illustrato, consentirà di guidare la realizzazione di una soluzione di Security Information ed Event Management (SIEM) con obiettivi quali la raccolta, l'analisi e la correlazione, l'utilizzo e la storicizzazione

degli eventi e delle informazioni di sicurezza generate da piattaforme tecnologiche presenti nel sistema informativo. Tali soluzioni offrono servizi per supportare un'organizzazione nella raccolta di eventi di sicurezza a partire da sorgenti informative e da componenti di sicurezza diversi con obiettivi di servizio in ambito sicurezza tra loro eterogenei.
A partire dai dati raccolti e sulla base di politiche e regole di correlazione è possibile evidenziare situazioni di potenziale allarme e comunque tali da richiedere l'attenzione dei processi di sicurezza in essere. La base dati gestita dalla soluzione SIEM rappresenta inoltre una fonte preziosa di informazioni a supporto di eventuali processi di analisi forense.
I fattori chiave che giustificano investimenti in tale direzione si possono ricondurre a tre esigenze a cui spesso un'organizzazione non è in grado, se non parzialmente di dare una risposta:

- dimostrare la conformità a requisiti normativi o a standard di settore;
- assicurare una appropriata protezione alle informazioni critiche aziendali attraverso un controllo della sicurezza;
- gestire i processi di sicurezza con il supporto di strumenti di governance efficienti e efficaci.

Il modello di monitoraggio e la soluzione SIEM proposta da IBM si sviluppa a partire da due componenti distinti ma tra loro perfettamente integrati:

- Security Information Management (SIM);
- Security Event Management (SEM).

Il componente SIM fornisce servizi di analisi e reporting a partire da informazioni raccolte da sistemi e applicazioni, così come da dispositivi di sicurezza con l'obiettivo di fornire analisi correlate e report utili a indirizzare e supportare temi quali la verifica di conformità e il rispetto delle politiche di sicurezza, così come una gestione efficace dei processi per il threat management. Le informazioni su cui si basa principalmente il componente SIM sono rappresentate dai vari file di registrazione eventi e di accesso (come quelli di log), generati da dispositivi o applicazioni di sicurezza e disponibili a livello di sistema operativo sui sistemi.
Il componente SEM dispone di caratteristiche e servizi tali da integrare e processare eventi di sicurezza (per esempio trap SNMP), collezionati in tempo reale dai dispositivi di rete e di sicurezza; l'obiettivo è quello di supportare i processi di gestione della sicurezza per un controllo continuo dell'infrastruttu-

ra alla ricerca di ogni possibile attacco/intrusione (interno/esterno) o irregolarità di accesso. Rappresenta inoltre un valido supporto per migliorare le qualità e le capacità di un processo per la risposta agli incidenti di sicurezza.
L'insieme dei due componenti costituisce la soluzione SIEM di riferimento i cui servizi saranno a supporto del modello di monitoraggio della sicurezza.
Il modello è suddiviso in tre macro sezioni ciascuna afferente a servizi di base a supporto della soluzione SIEM; in particolare nella parte bassa del modello è indicato il servizio di raccolta e memorizzazione delle Informazioni e Eventi di Sicurezza generati dalle diverse sorgenti quali dispositivi e applicazioni integrate nel sistema.
Nella parte centrale del modello sono presenti i servizi per la definizione delle politiche e delle regole utili alla correlazione degli eventi/informazioni e da questi le logiche per la predisposizione di report, allarmi e supporto all'analisi forense.
La parte alta del modello rappresenta i servizi di console e di cruscotto attraverso i quali dare evidenza, per ciascuna tipologia di utente, di informazioni e indicatori di sintesi di quanto elaborato dalle logiche di correlazione e dalle politiche implementate dal modello.

IBM Tivoli Security Information and Event Manager (TSIEM)

La proposta IBM per la realizzazione del Sistema di Monitoraggio della Sicurezza prevede l'utilizzo di soluzioni IBM Tivoli Security Information and Event Manager (TSIEM) che permettono di rilevare e gestire tutte le informazioni di sicurezza provenienti dalle infrastrutture delegate alla sicurezza, nonché da sistemi, dispositivi di rete o applicazioni in grado di inviare dati relativi alla propria "security posture".
Il valore della soluzione TSIEM si traduce nei seguenti elementi distintivi:

- riduzione del tempo speso per attività di monitoraggio, compliance e audit, grazie al motore di log management (centralizzazione e storicizzazione), alla semplice e funzionale dashboard e alla forte capacità di reporting;
- supporto nella salvaguardia della proprietà intellettuale e della privacy attraverso l'audit delle attività svolte dagli utenti;
- incremento dell'efficacia ed efficienza delle attività di sicurezza, con messa in evidenza dei security alert, tramite motori di correlazione eventi, assegnazione di priorità agli stessi, investigazione e azioni correttive;
- integrabilità con gli standard di mercato per sistemi operativi, mainframe, database e applicazioni;
- capacità di definizione di differenti profili di utenza mediante un apposito user directory.

La soluzione TSIEM proposta da IBM è realizzata tramite l'utilizzo e la completa integrazione dei seguenti moduli:

- Tivoli Security Operation Manager (TSOM);
- Tivoli Compliance Insight Manager - (TCIM).

IBM Tivoli Security Operation Manager (TSOM)

IBM Tivoli Security Operations Manager (TSOM) è la piattaforma centralizzata per la raccolta e la correlazione di eventi di sicurezza in real-time, che fornisce le seguenti funzionalità di base:

- automatizzare l'aggregazione, la correlazione e l'analisi dei log;
- riconoscere, indagare e rispondere agli incidenti sulla sicurezza automaticamente;
- snellire il reperimento, la gestione e la risoluzione degli incidenti attraverso uno strumento interno per il tracking della gestione degli incidenti di sicurezza;
- consentire la descrizione di regole di correlazione per l'attivazione automatica di azioni su pattern noti;
- rendere disponibile un'efficiente dashboard operativa con viste personalizzate per consentire un'analisi efficiente degli incidenti di sicurezza;
- integrare tool d'investigazione per consentire indagini su incidenti di sicurezza o su attività anomale;
- preparare i report atti a documentare le attività relative alla conformità.

La tecnologia TSOM supporta nella rilevazione di attacchi, abusi e attività anomale, attraverso quattro tecniche complementari di correlazione:

- Rule-based correlation - rileva gli attacchi tramite regole di correlazione eventi.
- Vulnerability correlation - traccia attacchi noti conoscendo le vulnerabilità del sistema.
- Statistical correlation - identifica anomalie eseguendo un'analisi avanzata degli eventi dal punto di vista statistico.
- Susceptibility correlation - determina la probabilità di esposizione per tutto il sistema.

In aggiunta, il TSOM può usare le "business priority", per pesare l'importanza degli asset durante il processo di correlazione, e un processo di aggregazione per la definizione di report statistici su archi temporali più o meno lunghi.

Per quanto riguarda la correlazione, si osservi che i relativi motori consentono di determinare il livello di minaccia per ogni evento. La logica di correlazione nativa, denominata correlazione statistica, permette di eseguire in maniera automatica una serie di attività quotidiane quali il "sorting" degli eventi e la determinazione delle relazioni esistenti tra gli eventi stessi grazie all'assegnazione di un peso a ogni classe di evento, alla sorgente e alla destinazione dell'evento stesso.
La configurazione delle regole fornisce un ulteriore approccio per la determinazione del peso di una minaccia di sicurezza. Applicando regole stateless e stateful sono valutati i flussi di eventi nei confronti di regole definibili a livello enterprise. In sostanza non ci si limita a filtrare il singolo evento in base alla sua provenienza, alla sua destinazione e al contenuto, ma lo si pone in contesto con le attività che sono accadute sulla rete per identificare eventuali schemi di attacco che altrimenti non sarebbero riconoscibili. Sulla base di tali "trigger" è possibile attivare azioni automatiche quali la creazione di un meta evento, l'invio di un allarme, l'invio di una trap SMNP o lanciare l'esecuzione di un qualunque eseguibile

IBM Tivoli Compliance Insight Manager

Il TCIM è una suite software per il monitoraggio dei sistemi, il log management e la generazione di resoconti mirati a velocizzare il processo di verifica della conformità a standard e normative. Il prodotto è formato da diversi componenti ed è dotato di un'interfaccia Web accessibile da browser di supporto nel rispondere a requisiti di audit, di logging e d'investigazione.
I servizi disponibili con il prodotto TCIM consentono d'implementare una soluzione centralizzata per:

- raccogliere dati di log a partire da sorgenti eterogenee disponibili sulla rete;
- normalizzare ed elaborare le informazioni raccolte in relazione a politiche di sicurezza;
- attivare in modo automatico azioni e allarmi puntuali in relazione ad attività sospette o non in linea con le politiche definite;
- archiviare i log originali raccolti e normalizzati, per supportare attività d'analisi forense;
- fornire una vista consolidata e report attraverso un'unica interfaccia di gestione.

Il prodotto, inoltre, può dare un supporto nell'ambito delle analisi forensi che, a partire da una vista di alto livello sulla conformità dei sistemi aziendali alle

normative di sicurezza, permettono di arrivare in “drill-down” fino al recupero dei log originari in cui sono registrati i singoli eventi oggetto di auditing.
TCIM usa una metodologia proprietaria particolarmente avanzata per consolidare, normalizzare e analizzare grandi volumi di dati relativi alle attività degli utenti e dei sistemi. Attraverso tale metodologia, chiamata “W7”, e a seguito della centralizzazione di tutti i file di log, le informazioni in essi contenuti vengono tradotte o interpretate secondo 7 (sette) criteri fondamentali (Who, What, When, Where, Where from, Where to, on What), attraverso i quali qualsiasi tipo di evento può essere rappresentato. L’insieme di queste 7 istanze, permette di descrivere con criteri di uniformità tutti gli eventi registrati all’interno del sistema, a prescindere dal formato originario con cui questi sono stati creati.

1.5 La Security PCI Compliance

In ogni settore industriale esistono molte tematiche specifiche relative e che coinvolgono direttamente l’Information Security. Un settore estremamente attento alla sicurezza è quello finanziario, per esempio, e uno di tali temi “scottanti” è quello della conformità allo standard per la sicurezza nella PCI (Payment Card Industry).
Si utilizzano ancora troppo denaro contante e assegni come sistema di pagamento usuale, con costi elevati per le banche che si ripercuotono sulla società.
Per far crescere diffusione e adozione delle carte magnetiche o intelligenti, come sistema alternativo, le soluzioni che ne utilizzano e conservano i dati sensibili da esse contenuti devono essere assolutamente sicure e protette contro tentativi di effrazione o lettura di tali dati. L’utilizzo fraudolento apporta danni economici diretti consistenti sia al proprietario sia all’ente emittente e ancora più consistenti risultano essere i danni per l’immagine aziendale dell’istituto finanziario coinvolto. Il rischio primario, infatti, è la perdita di fiducia e confidenza con il cliente, che può essere portarlo a rivolgersi ad altri enti finanziari. Con il rischio di emulazione da parte anche di altri proprietari del medesimo tipo di card.
Gli attacchi alla sicurezza nell’utilizzo delle carte credito si stanno poi moltiplicando ed espandendo, per esempio anche a seguito della progressiva diffusione di negozi online e della familiarità con cui si utilizza Internet.
Il settore finanziario ha così finito, nel corso degli anni, con l’emettere continuamente normative regolamentari sempre più severe per quanto concerne

le modalità di realizzazione e di protezione dei sistemi di pagamento e delle card che vengono utilizzate nell'ambito dei diversi circuiti di pagamento. Tra questi, lo standard Payment Card Industry (PCI) Data Security Standard (DSS) ha un ruolo molto importante e ha visto l'adesione di tutte le principali società di carte di credito. La mancata aderenza allo standard di sicurezza PCI può implicare severe multe per le aziende bancarie.
Contrariamente ad altri casi infatti, la richiesta di conformità alle norme stabilite dallo standard è particolarmente severa ed è del tipo tutto o niente. Non è prevista un'adesione parziale o il rispetto esclusivamente di alcune sue parti.
Inoltre, osservare i requisiti di tale standard e quindi gestire in modo adeguato la sicurezza di un sistema di pagamento elettronico presenta indubbi costi. Per esempio, sono necessarie risorse ed esperienze che non tutti i retailer hanno e che devono essere garantite dall'ente emittente o da società cui viene demandato il compito. Eppure, per le società di credito è fondamentale ridurre i costi di adesione alle varie normative che sono sempre più complesse, per non dover trasferire sugli utilizzatori e sulle transazioni il costo del sistema. Il rischio è di disincentivarne l'uso invece che di favorirne la progressiva adozione.
D'altro canto, società di ricerca specializzate e indipendenti hanno dimostrato che l'adesione stretta allo standard PCI DSS apporta benefici che superano ampiamente il peso economico e organizzativo della compliance.

Il ruolo del Security Council per la sicurezza

Il compito di governare la definizione e l'adozione di standard per la sicurezza validi per l'intera industria delle carte di pagamento è stato assunto dal PCI Security Standards Council (PCI SSC), un ente a cui partecipano Visa, Master Card, American Express, Discover, JCB e Diner's Club.
L'ultima versione dello standard, denominata PCI SSC v1.1, fornisce un chiarimento sui requisiti o "requirements", concede maggior flessibilità per quanto concerne i controlli in ambienti complessi, quali l'encryption dei dati, e prende in considerazione i pericoli emergenti per le applicazioni inerenti la sicurezza.
Le entità e le persone interessate a soluzioni compliant con lo standard PCI DSS sono raggruppabili in due diversi insiemi:

- Industrie: società che svolgono attività commerciale, mercantile o service provider che immagazzinano, elaborano o trasmettono in qualsiasi modo i dati delle persone che possiedono una regolare carta di pagamento e utilizzano un software che supporta il commercio elettronico. È

un gruppo molto ampio che comprende, solo per citare alcuni esempi, società del retail, dell'hospitality (ristoranti, hotel e così via), dei trasporti (linee aeree, car rental, ferrovie), dei servizi finanziari (banche, gestori carte di credito, broker, assicurazioni), Ospedali, utility pubbliche.

- Responsabili: spaziano dai CIO agli IT manager sino ai manager responsabili della compliance.

A entrambe le categorie lo standard PCI mette a disposizione un insieme di regole che aiutano adeguatamente nell'implementare una politica per la sicurezza dei dati inerenti i proprietari di carte di pagamento. Lo standard, dunque, risponde alla richiesta crescente da parte degli utilizzatori che siano adottate pratiche approfondite e accurate per la sicurezza delle carte per il pagamento elettronico. Questo, almeno dal punto di vista del consumatore, ma la visione è un po' meno positiva dal lato delle aziende della filiera, che lo vedono aggiungersi agli altri standard imposti dagli enti regolatori del settore o da singoli governi. Come tale, infatti, richiede a sua volta investimenti e risorse per essere opportunamente affrontato e tenuto in considerazione all'interno dei propri processi aziendali.
Nella maggioranza dei casi, però, si tratta di timori infondati, visto che in genere le aziende interessate dallo standard, per la natura del loro business, hanno già adottato criteri di sicurezza particolarmente robusti, come quelli derivanti da altri standard, quale l'ISO 17799, e quindi hanno già in essere security policy di buon livello. Anche se di non facile e immediata attuazione lo standard PCI DSS rientra quindi tra gli argomenti e le tematiche già conosciuti a livello aziendale.

1.5.1 Lo standard PCI DSS

Il perché di uno standard aggiuntivo a quanto stabilito dall'ISO deriva dalle sopra evidenziate esigenze specifiche del settore del finance e del pagamento tramite carte di credito/debito, che mette in gioco enormi aspetti economici e rischi altrettanto elevati per il sistema economico stesso e per le entità coinvolte. Inoltre, per un ente pubblico e privato poteva verificarsi il caso di essere aderenti a quanto stabilito dall'ISO ma non esserlo poi ai fini della trafugabilità di dati sensibili relativi ai sistemi di pagamento elettronico ed essere quindi soggetti a risvolti penali e civili anche molto onerosi.
Un esempio lo si ha se si considera un comune apparato POS, che, in quanto tale, è soggetto a guasti. In questi casi, la procedura normale prevede l'intervento di un tecnico, che accede all'apparato, esegue il tracking delle operazioni, verifica il software, può entrare nella sua memoria e nei suoi registri, accedere a informazioni riservate e da qui in poi il rischio è evidente.

Il problema della riservatezza interviene già a questo livello, non solo o non tanto per sfiducia nei confronti del tecnico, ma perché alla fine delle operazioni alcuni dati sensibili possono essere rimasti memorizzati nella sua strumentazione o nel suo portatile. Se poi la sua azienda ha una politica adeguata di backup, questi dati dopo un tempo prefissato vengono automaticamente salvati in un sistema di backup e quindi replicati ulteriormente. Senza contare che il portatile è potenzialmente accessibile a un hacker o può essere rubato o smarrito. In sostanza, quelli che sono dati riservati di uno o più utilizzatori di carte di pagamento si ritrovano in breve a essere replicati su più sistemi e aperti all'accesso di utilizzatori non autorizzati.
A questo e ad altri aspetti si propone proprio di porre rimedio lo standard PCI DSS, stabilendo requisiti che in parte incorporano e in parte estendono quanto previsto dall'ISO in modo che meglio risponda alle esigenze specifiche di chi gestisce, tratta, archivia o trasmette in qualsiasi maniera i dati relativi ai proprietari di carte di pagamento, sia di debito che di credito.

I dodici punti del PCI DSS

Come già visto per lo standard ISO anche il PCI indirizza una serie di requirement, dodici in questo caso, che sono suddivisi in sei diversi temi di intervento e che nel complesso stabiliscono i criteri e le attività di sicurezza da espletare nell'ambito di un sistema/processo che tratti i dati di un proprietario di una card, di debito o di credito, utilizzata come sistema di pagamento. Dal punto di vista complessivo, peraltro, il PCI DSS (Payment Card Industry Security Standard) è una combinazione tra "software utilizzato per il processo transazionale" e "ambiente di supporto costituito dalla rete e dai commercianti". La somma dei fattori porta alla PCI DSS compliance.
I sei temi sono:

Realizzazione e mantenimento di una rete sicura

- Requirement 1: installazione e manutenzione di firewall per proteggere i dati inerenti il possessore di una card.
- Requirement 2: non utilizzare i dati di default forniti dal venditore come password di sistema o per altri parametri inerenti la sicurezza.

Protezione dei dati del possessore di una card

- Requirement 3: proteggere i dati di un proprietario di card che siano stati memorizzati in un sistema di storage aziendale.

- Requirement 4: criptare i dati del possessore di card quando gli stessi vengono trasmessi su qualsiasi tipo di rete, fissa o mobile, privata o pubblica.

Mantenimento di un programma di gestione delle vulnerabilità

- Requirement 5: utilizzare e aggiornare con regolarità il software delle applicazioni antivirus.
- Requirement 6: sviluppare e mantenere adeguatamente il sistema di sicurezza e le applicazioni.

Implementazione di misure forti di controllo dell'accesso

- Requirement 7: limitare l'accesso in aderenza al concetto di need-to-know, ovverossia concederlo esclusivamente a coloro che hanno degli ottimi motivi per farlo.
- Requirement 8: assegnare un unico identificatore ID a ogni persona che abbia accesso ai computer interessati alla gestione o alla trasmissione dei dati di un proprietario di card.
- Requirement 9: limitare l'accesso ai dati di un proprietario di card anche dal punto di vita fisico.

Test e monitoraggio periodico della rete

- Requirement 10: effettuare il tracciamento e il monitoraggio di tutti gli accessi alle risorse di rete e ai dati dei proprietari delle card.
- Requirement 11: effettuare regolarmente il test sia del sistema di sicurezza sia dei singoli processi.

Mantenere una adeguata policy per la sicurezza delle informazioni

- Requirement 12: mantenere e aggiornare costantemente una policy che indirizzi il tema della sicurezza delle informazioni.

Come accennato, molti dei punti elencati trovano risposta e formulazione nello standard ISO 17799, a cui si rimanda per ulteriori approfondimenti. Nel complesso si tratta di interventi che richiedono uno skill elevato e che trovano in società come IBM ISS sia la piattaforma tecnologica che la capacità di assessment e di analisi della realtà esistente in modo da realizzare e mantenere attiva una soluzione di sicurezza aderente allo standard PCI DSS ma che risulti il meno possibile invasiva rispetto a quanto eventualmente già esistente.
Gli interventi che IBM ISS è in grado di realizzare permettono di rispondere in modo adeguato ai requirement dello standard e a eliminare le conseguen-

ze che possono derivare per un'azienda dalla mancanza di conformità. Tra i fenomeni che possono gravare sul bilancio aziendale vi sono:

- La svalutazione del valore azionario a seguito dell'impatto negativo sul pubblico
- Le multe da parte dell'emettitore delle carte di pagamento o dalle banche
- Le penali da corrispondere a seguito della perdita dei dati del proprietario della carta e delle attività legali che ne conseguono, per esempio esami forensi o i costi per risolvere le dispute che ne possono derivare.

1.5.2 Il supporto di IBM ISS per la compliance PCI

Il percorso che porta verso una corretta applicazione dei principi stabiliti nei dodici punti PCI è complesso e non tutte le organizzazioni aziendali dispongono delle competenze e delle risorse necessarie, anche semplicemente per poterlo completare nei tempi imposti dagli enti di categoria o sovranazionali.
Per venire incontro alle necessità dei propri clienti, IBM ISS ha sviluppato sia le tecnologie sia le capacità di analisi e supporto che possono affiancare un'azienda nel percorso verso la completa aderenza allo standard PCI.
Il punto di partenza è costituito da un affiancamento del personale aziendale

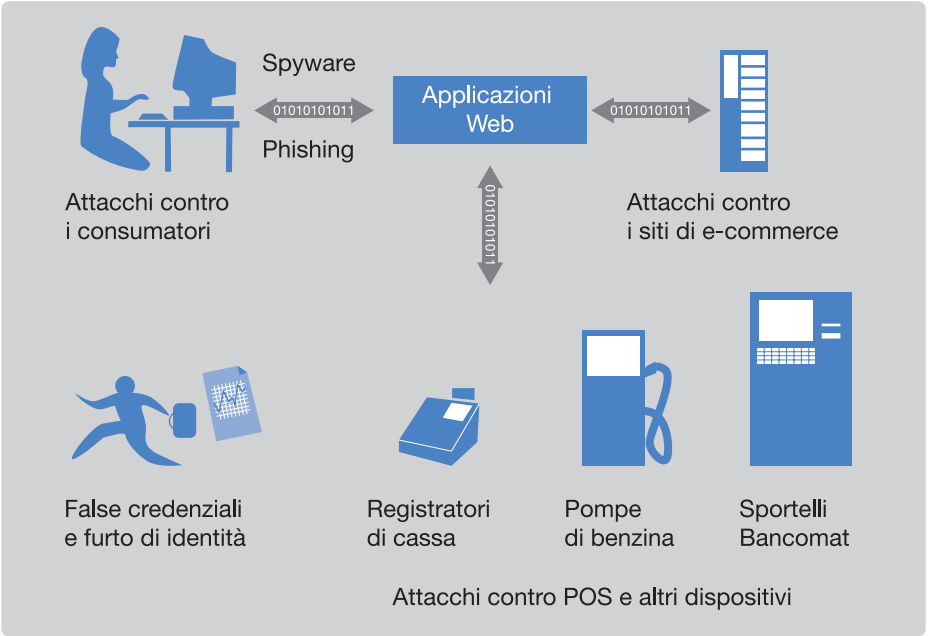


Figura 1.9
Sono almeno quattro i punti di attacco per rubare i dati sulle carte di credito; in maggior parte i furti avvengono alle pompe di benzina

coinvolto con esperti IBM ISS, in modo da capire la situazione reale, comprendere ed esplorare i punti di maggior criticità che si presentano nel percorso di aderenza allo standard e di adeguamento delle infrastrutture esistenti e, infine, nel disegnare la soluzione che affronta e risolve tali criticità.
L'approccio identificato da IBM come meglio rispondente alle esigenze di compliance di un'azienda di qualsiasi dimensione prevede tre diversi interventi:

- Assessment: è realizzato da esperti di IBM ISS o di IBM GBS (Global Business Services).
- Remediation: è realizzato da esperti di IBM ISS, IBM GBS, IBM GTS (Global Technology Services) o IBM SWG (SoftWare Group).
- Certification: è realizzato da esperti di IBM ISS, che sono "Globally Certified" per realizzare i servizi PCI, possedendo certificazioni Qualified Security Assessor (QSA), Approved Scanning Vendor (ASV), Qualified Payment Application Security Company (QPASC), Qualified Incident Response Company (QIRC).

Le tre fasi fanno riferimento a una realtà di tipo "green field". In situazioni diverse, per esempio in cui la fase di assessment sia già stata realizzata in house o con il supporto di altre entità consulenziali, IBM ISS può intervenire direttamente nella fase di Remediation fornendo esclusivamente le soluzioni software e i servizi identificati come necessari e fornendo la successiva fase di certificazione.
Un elemento essenziale nel processo verso la compliance è rappresentato dalla Gap Analysis. Si tratta di un intervento di alto livello che permette di stabilire la situazione esistente e identificare il punto di arrivo del percorso, in modo da capire quanto ci si discosti da quest'ultimo in base all'organizzazione, ai processi, gli strumenti, le competenze e il personale di supporto già presente in azienda.
La fase di Gap analysis ha l'obiettivo di descrivere la realtà attuale mediante domande svolte ai diversi livelli aziendali coinvolti nella gestione dei dati sensibili delle transazioni di carte di pagamento e, nel complesso, permette di individuare la posizione delle diverse componenti aziendali nei confronti della sicurezza. I punti che vengono affrontati permettono, per esempio, di chiarire se:

- Viene condotto e da parte di chi un audit annuale della situazione per quanto concerne la sicurezza e se esiste un assessment trimestrale delle risorse.

- Ci sono dei vincoli particolari per quanto concerne le risorse disponibili in relazione alle esigenze di sicurezza.
- Viene condotto un penetration test periodico, per esempio su base annuale, volto a evidenziare il grado di esposizione dei sistemi ai rischi provenienti da Internet.
- È noto chi ha libero accesso ai dati inerenti i dati di transazioni finanziarie sensibili.
- Si dispone di una dashboard per il reporting immediato e correlato del grado di compliance alle policy di sicurezza.
- Si è in grado di rimuovere rapidamente i diritti di accesso ai dati sensibili quando un dipendente cambia lavoro o lascia l'organizzazione.
- Si dispone di un piano da porre in azione in caso di incidente che metta in forse la sicurezza.

Di notevole importanza è anche la fase successiva, che permette di definire la roadmap da seguire e che prevede interventi di esperti su quattro diversi aspetti:

- Focalizzazione sui punti di maggior criticità per l'azienda.
- L'identificazione del corretto mix di hardware, software e servizi.
- Interazione spinta tra gli esperti delle diverse componenti di una soluzione PCI.
- Identificazione del percorso più breve per mettere in atto la Remediation e giungere alla certificazione della soluzione PCI adottata.

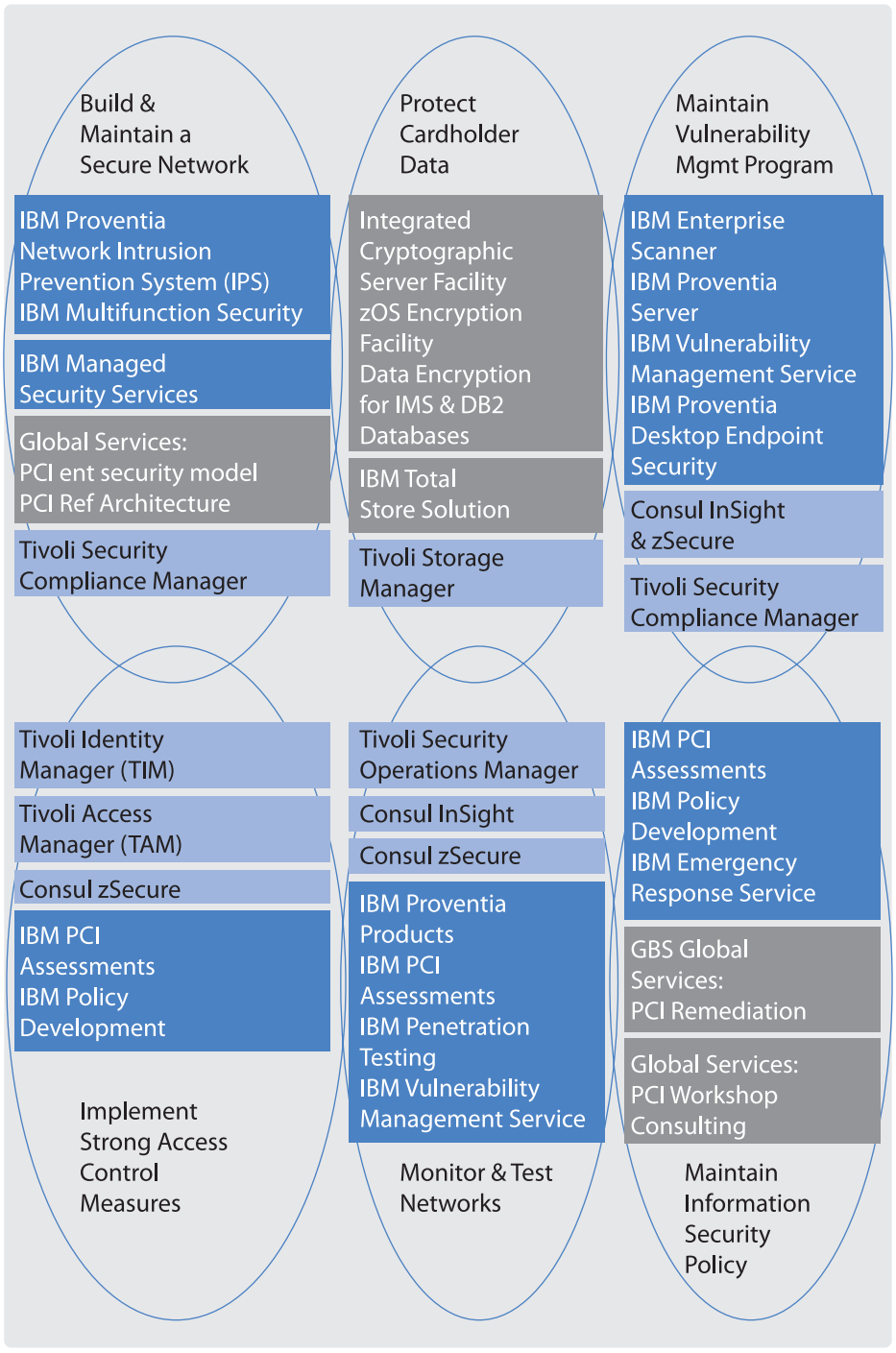
Le soluzioni a supporto della compliance PCI

Le soluzioni IBM indirizzano l'intero insieme dei requirement stabiliti dallo standard PCI.
Le soluzioni sviluppate, peraltro, rispondono alle esigenze di sicurezza basandosi su solide considerazioni sia economiche sia tecnologiche.
Analisi da parte di primarie società di ricerca evidenziano infatti che il costo della perdita di dati è pari a circa 300 dollari per utente mentre il costo della protezione scende a soli 16 dollari per utente, quindi con un rapporto di circa 20:1.
Inoltre, se la cifratura dei dati è un elemento molto importante, non è però di per sé sufficiente a garantire la sicurezza delle informazioni. Oltre a essa servono soluzioni che permettano anche di disporre sistemi di controllo dell'accesso e dell'identità, in grado di realizzare una segmentazione molto dettagliata dei dati di una card, di monitorare in modo approfondito le attività che

coinvolgono il database in cui i dati sono memorizzati nonchè di disporre di adeguati servizi di gestione della sicurezza in caso di outsourcing.
Le soluzioni IBM indirizzano nel complesso tutti e sei i diversi temi che raggruppano i requirement previsti dallo standard PCI. Più precisamente, per quanto riguarda la gestione e manutenzione di una rete sicura, IBM fornisce i servizi di consulenza sulla PCI dei Global Services, cui abbina le soluzioni di sicurezza IBM ISS Proventia IPS (Intrusion Prevention System) e IBM ISS Proventia Multifunction Security, nonché quella di gestione IBM Tivoli Security Compliance Manager.
Per la protezione dei dati relativi al possessore di una card, IBM mette a disposizione le soluzioni Integrated Cryptographic Server Facility, IBM Total Store Solutions e IBM Tivoli Storage Manager. Il mantenimento di un programma per il monitoraggio e controllo delle vulnerabilità è invece coperto dalle soluzioni e servizi IBM ISS Enterprise Scanner, IBM ISS Proventia Server, IBM ISS Vulnerability Management Service, IBM ISS Proventia Desktop Endpoint Security, nonché dalle soluzioni IBM Tivoli Consul InSight e Consul zSecure e IBM Tivoli Security Compliance Manager. Sempre le soluzioni Tivoli sono protagoniste nell'implementazione di un sistema forte di controllo degli accessi. In particolare, grazie a sistemi come IBM Tivoli Identity Manager, Tivoli Access Manager e Tivoli Consul zSecure, cui si affiancano i servizi di consulenza IBM ISS PCI Assessment e IBM ISS Policy Development.
L'accoppiata IBM Tivoli e ISS è ancora di spicco nel test e monitoraggio delle reti, grazie alle soluzioni IBM Tivoli Security Operations Manager, IBM Tivoli Consul InSight e Consul zSecure, da un lato, e, dall'altro, ai prodotti hardware e software IBM ISS Proventia e ai servizi IBM ISS PCI Assessment, IBM ISS Penetration Testing, IBM ISS Vulnerability Management Service.
Infine, sempre i servizi IBM ISS, più precisamente IBM ISS PCI Assessment, IBM ISS Policy Development e IBM ISS Emergency Response Service sono alla base, insieme, a quelli di IBM Global Service PCI Remediation e PCIWorkshop Consulting della copertura inerente il mantenere policy adeguate per l'Information Security.

Figura 1.10

Le soluzioni IBM per i sei temi dello standard PCI



2
La mitigazione delle minacce all'infrastruttura

Il crimine informatico si è evoluto, perché è diventato "silenzioso", mirato e molto pericoloso, scatenando una Cyber War che tocca tutti. La complessità da gestire impone automatismi e spinge verso l'adozione di servizi, che si orientano verso la protection on demand. Un approccio olistico orientato al business e un partner fidato sono fattori determinanti in un sistema per la sicurezza di dati e informazioni da attacchi esterni e interni.

2.1 Internet e la nuova era della sicurezza informatica

Con la crescita e la diffusione degli strumenti connessi a Internet, posta elettronica in primo luogo sono cominciati a sorgere i primi grandi problemi di sicurezza. Non che prima non ce ne fossero, ma prima di Internet avevano caratteristiche completamente differenti. Per anni, infatti, l'Information Technology era stata una disciplina per pochissimi eletti, "segregata" in stanzoni enormi accessibili solo agli addetti e occupati per la quasi totalità della superficie da giganteschi calcolatori, la cui potenza elaborativa era infinitamente inferiore a quella oggi fornita da un chip poco più grande di un polpastrello. Le reti erano connesse a questi sistemi e il loro accesso era non solo protetto, ma anche fisicamente poco raggiungibile. Ancora oggi IBM fornisce funzioni di sicurezza avanzate sui propri sistemi, ma con l'avvento del personal computer, prima, e dei modem, dopo, diverse cose sono cambiate, venendosi a creare il concetto di "online". Nel corso degli anni, le minacce hanno seguito l'evoluzione delle abitudini diffuse tra gli utilizzatori di computer e sfruttato quella della tecnologia di Information e Communication Technology.
È, per certi versi assurdo, che Internet, nata da una rete creata per la sicurezza nazionale, sia diventata oggi il terreno di battaglia della nuova guerra di frontiera: la Cyber War. È attraverso Internet, infatti, che si diffondono le minacce ai gangli vitali della società moderna: quei sistemi informatici su cui si basa ormai tutta l'organizzazione sociale ed economica di una nazione.

A metà degli anni Novanta il fenomeno degli hacker ha cominciato la salita su una curva di crescita esponenziale. Tecniche più sofisticate hanno iniziato a sfruttare i difetti di alcuni programmi, in particolare, per superare i controlli d'autenticazione ed entrare nei sistemi senza autorizzazione. In taluni casi, si cercava di assumere il controllo di grandi quantità di capacità di calcolo. Una delle sfide, infatti, consisteva nello scovare le chiavi di crittografia, i cui algoritmi venivano viepiù complicati. Le cose cambiano. Macchine sempre più potenti, tool sempre più sofisticati a disposizione e, soprattutto, nuove motivazioni hanno modificato dapprima le regole e poi il gioco stesso. Dal 2004 e, in misura ancora maggiore, dal 2005, il livello di pericolo si è elevato. Gli esperti di IBM Internet Security Systems, a partire dal team di ricerca e sviluppo X-Force, hanno rilevato una "violenza" inedita negli attacchi che non sono più animati da una semplice sfida

Tabella 2.1

Come sono cambiate le caratteristiche degli attacchi dalla prima alla seconda decade di Internet

Caratteristiche dell'attacco	I primi attacchi	Gli attacchi della nuova Era
Motivazioni	Gloria e fama	Profitto
Complessità	Monodimensionale	Multi-dimensionale
Scopo	Massima risonanza	Attacchi mirati che passano inosservati
Rischio primario	Downtime e sistemi da ripristinare	Furti di informazioni. Perdite dirette di denaro.
Target degli attacchi	Alto profilo o grandi volumi	Precisione laser per colpire industrie o individui specifici
Difese efficaci	Antivirus e approcci reattivi	Protezione multi livello. Approccio pre-emptive con analisi sui comportamenti
Ripristino dopo l'attacco	Scansione e rimozione	Non sempre possibile senza un backup dell'immagine di sistema
Tipi di attacco	Virus, Worm, Spyware	Designer Malware, Root kits, Ransomware, Spear Phishing
Approccio d'attacco	Network traffic: operazioni con la grancassa	Malicious code: operazioni in tuta mimetica

dimostrativa né tanto meno goliardica, bensì spinti dal desiderio di profitto o, peggio ancora, dall'odio o dalla vendetta. Vere e proprie associazioni criminali e gruppi terroristici hanno cominciato a utilizzare le tecniche di hacking, accrescendo i tempi di sviluppo e la raffinatezza dei codici malware, oltre che orchestrando attacchi articolati in più fasi e più tecniche.
È cominciata quella che viene da alcuni chiamata Cyber War, ma che non sembra avere nulla a che vedere con la rivoluzione culturale "post-fantascientifica" preconizzata sul finire degli anni Ottanta. Molto più prosaicamente, l'hacker si è dato al professionismo: il ragazzino smanettone è diventato maggiorenne e unisce l'utile al dilettevole, violando siti e sistemi su commissione, causando danni mirati. Spionaggio industriale ma anche attacchi tesi a mettere in difficoltà un qualche concorrente. Poi truffe e frodi informatiche, che nell'Era di Internet e dell'e-business stanno progressivamente sostituendo le rapine in banca.

L'evoluzione continua e sfrutta le caratteristiche del cosiddetto Web 2.0, in cui si è passati dalla tipica interazione uomo-macchina della prima decade di Internet (l'utente che si collega a un Web server per scaricare programmi e informazioni) a un'interazione sempre più diretta tra utenti. Utenti che ingenuamente pubblicano numerosi dettagli privati fornendo preziose informazioni per il social engineering e il phishing. Ma già si parla del Web 3.0, che secondo alcuni sarà caratterizzato dall'interazione tra macchina e macchina. Non è un futuro poi così lontano, già oggi è possibile, per esempio, collegare tramite Internet sistemi di controllo di impianti industriali con sensori che rilevano determinati parametri. Nuove frontiere che si aprono anche per la sicurezza.
Sempre più, si prospetta la necessità di un approccio integrato e a 360 gradi, come quello che da tempo persegue IBM. In particolare, per quan-

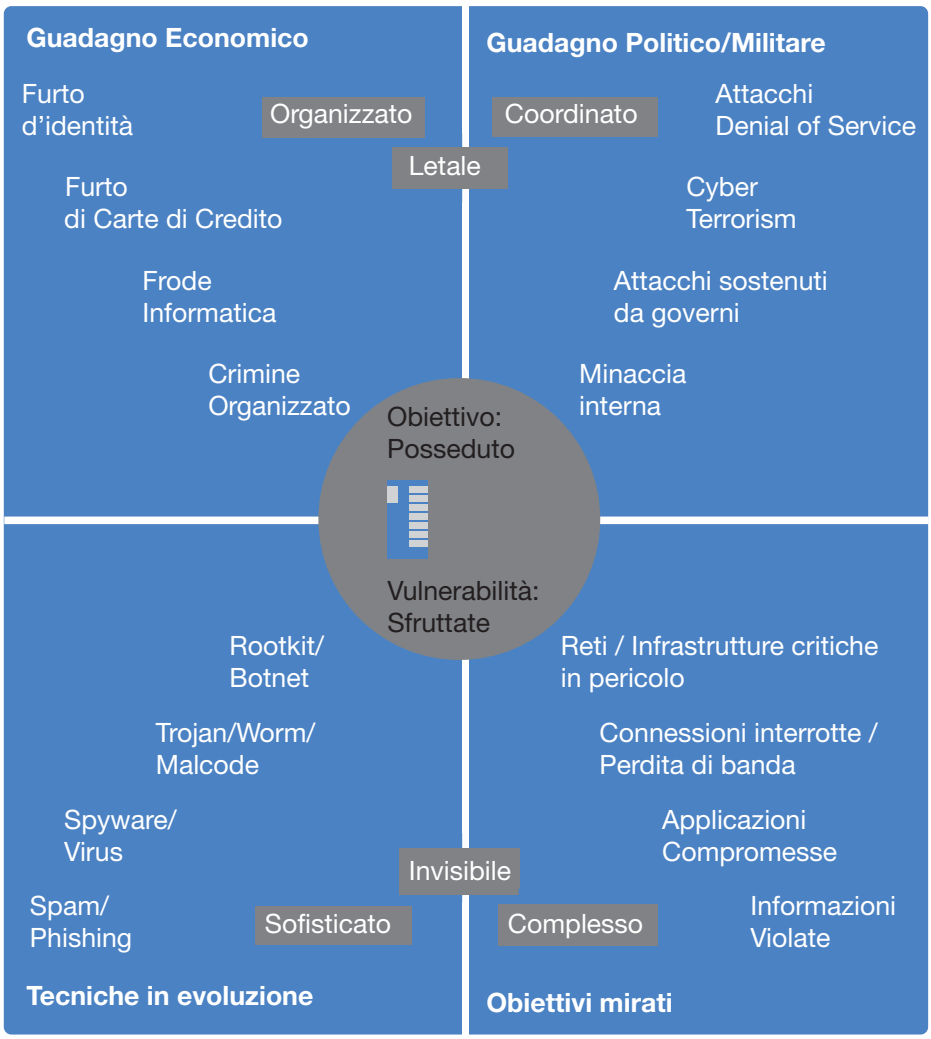


Figura 2.1
Le forze dinamiche nell'evoluzione delle minacce

to riguarda la protezione dalle minacce, IBM propone i servizi, le soluzioni e le tecnologie best of breed IBM Internet Security Systems.

IBM Internet Security Systems è stata la prima a sviluppare un sistema di vulnerability assessment e la prima a commercializzare un sistema di Network Intrusion Detection. Negli anni ha poi sviluppato un'architettura end to end, che estende il concetto di rilevamento delle intrusioni verso la protezione delle informazioni, andando oltre la sicurezza passiva fino al riconoscimento delle attività sospette e delle potenziali esposizioni al rischio. Propone dunque un approccio preventivo, che anticipa le minacce ed evita costosi danni agli asset aziendali, e proattivo, cioè abilitando la rete ad adattarsi automaticamente al mutare delle condizioni di minaccia. Un'adattabilità che non si può più basare su sistemi o suite che risolvono specifici problemi, ma deve fondarsi su una piattaforma, che integri la gestione delle minacce e utilizzi strumenti flessibili per realizzare una sicurezza multilivello. Tali strumenti contemplano anche servizi gestiti, tradizionali e innovativi, e servizi on demand. In quest'ottica, la filosofia per la protezione dalle minacce s'integra appieno con quella di approccio integrato e olistico di IBM.

2.1.1 La ricerca e sviluppo di X-Force a tutela della sicurezza

Nessuno può dirsi completamente estraneo alla Cyber War. Certamente non tutte le imprese o i computer di ciascun individuo sono target "economici" interessanti, ma i dati che contengono sono in ogni caso utili, perché le identità elettroniche stesse rappresentano una merce per il mondo del Web marketing e, soprattutto, perché possono essere impiegati per secondi fini. Così come le risorse d'elaborazione di un pc qualsiasi, purché connesso in rete, possono essere utilizzate come capacità di calcolo per sferrare attacchi mirati contro terzi. Sono possibilità, tra l'altro, previste dalla legge, che sancisce la responsabilità di chi, non avendo attuato misure di protezione, favorisce involontariamente la "presa di possesso" anche temporanea delle proprie infrastruttura informatiche.
Un altro aspetto fondamentale, in questo contesto, è lo sviluppo tecnologico delle minacce stesse. Oltre ad alimentarsi nelle comunità di hacking, come avveniva tradizionalmente, l'evoluzione sulle tecniche di attacco può contare su veri e propri centri di ricerca e sviluppo. La situazione è inoltre complicata dalla crescita continua delle vulnerabilità, da un lato, e della pericolosità espressa dalle nuove forme di attacco. Non solo, perché

accelera notevolmente anche il ritmo con cui si susseguono gli attacchi e con cui vengono sviluppate le varianti di un exploit, con continue ricorrenze e riutilizzo di codice.
Per affrontare queste problematiche è necessario un approccio altrettanto avanzato e approfondito in termini di ricerca. Per questo IBM X-Force rappresenta un punto di riferimento non solo per IBM, ma per i suoi clienti e le comunità internazionali di lotta al crimine informatico. IBM X-Force è il team di ricerca e sviluppo di IBM Internet Security Systems e anche uno dei security advisor più noti a livello mondiale, la cui missione è la ricerca e la valutazione delle vulnerabilità e delle problematiche di sicurezza, per sviluppare una tecnologia di assessment e delle contromisure per i prodotti di IBM ISS, nonché educare i media e le comunità di utilizzatori su tali problematiche emergenti. Non a caso il team di ricerca e sviluppo di IBM Internet Security Systems rappresenta una delle ragioni che hanno portato alla nomina di ISS come security provider dell'Information Technology Information Sharing and Analysis Center (IT-ISAC) nel 2000, all'atto della sua fondazione.

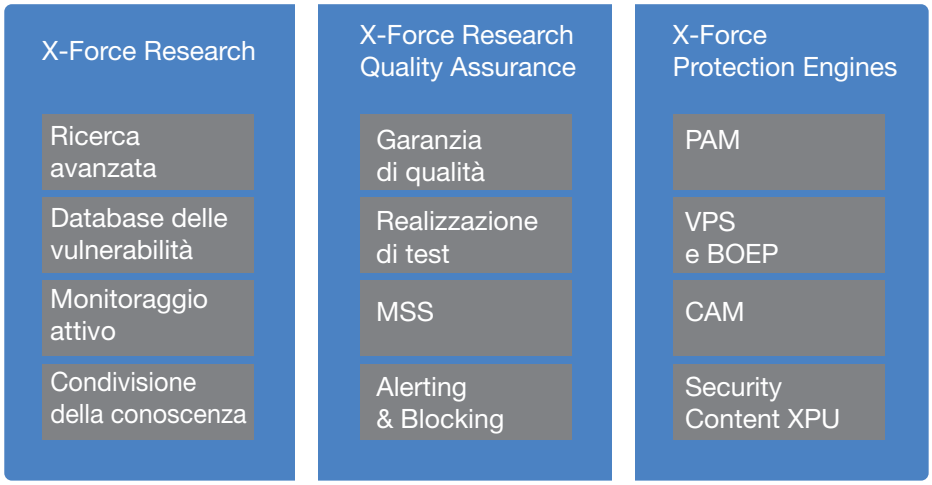


Figura 2.2
Le tre componenti del lavoro di X-Force

Tre sono gli ambiti in cui opera X-Force per tener fede a tale missione: la ricerca, la garanzia di qualità e lo sviluppo dei sistemi di protezione.
La ricerca avanzata comprende la costruzione di un database sulle vulnerabilità. Di fatto, viene svolta una ricerca "originale" alla scoperta delle vulnerabilità, analizzando le nuove e le prossime tecnologie, studiando le implementazioni dei protocolli e dei prodotti e concentrandosi sui sistemi più diffusi per portare alla luce i loro punti di debolezza. A questa si aggiunge l'analisi sui "proof of concept" e i codici per gli exploit che sono stati identificati e quelli che sono stati annunciati. In

molti casi, si adottano tecniche di reverse engineering, partendo da vulnerabilità, exploit o patch, per arrivare a comprendere come coprire tutte le varianti di una minaccia o nuovi modi di sfruttare le vulnerabilità o debolezze imparentate con queste.

Il Threat Insight Report e l'AlertCon

Lo studio delle vulnerabilità è il punto di forza di X-Force e il database che ne deriva lo dimostra: oltre 22mila vulnerabilità catalogate a partire dagli anni Novanta, con continui aggiornamenti.
Ogni mese X-Force rilascia il Threat Insight Report. Si tratta di un documento unico per quantità e qualità di informazioni prodotte e rese note. Ogni giorno gli esperti di X-Force trovano nuove vulnerabilità nei sistemi più diffusi in uso nei sistemi informativi in tutto il mondo. Sono centinaia e ciascuna sottointende un proliferare di nuove minacce. La tendenza, poi, è di una continua crescita e non è un caso se X-Force ha modificato la periodicità del rapporto da trimestrale a mensile (peraltro, un documento di sintesi trimestrale è tuttora prodotto, corredato di ulteriori analisi di medio-lungo periodo).
Il lavoro svolto da X-Force è inoltre fondamentale per capire come stanno evolvendo le strategie e le tattiche di attacco. In stretto contatto con i ricercatori di tutte le altre società impegnate nella security nonché attento osservatore del lavoro delle comunità "underground" di hacking, il team di X-Force ha il merito di scoprire il maggior numero di vulnerabilità rispetto a qualsiasi altra organizzazione. Addirittura, nel 2005 secondo la società di analisi indipendente Frost & Sullivan, ben il 51% delle vulnerabilità identificate in tutto il Globo furono portate alla luce da X-Force.
I Security Operation Center di IBM ISS, inoltre, raccolgono le informazioni sulla sicurezza registrate durante l'erogazione dei Managed Security Services e quelle provenienti dalle innumerevoli sonde (a partire da quelle di intrusion detection e prevention), presenti sulle reti aziendali e di service provider di tutto il mondo (sono oltre 13mila i clienti di IBM ISS a livello internazionale, più di 700 dei quali in Italia, comprese le più grandi aziende del Paese). In questo modo, X-Force è in grado di condurre un'attività di monitoraggio senza eguali, che permette di verificare in tempo reale l'evolversi delle minacce alla sicurezza online. Sfruttando tutte le informazioni che gli esperti di IBM ISS raccolgono in queste loro attività, X-Force oltre a lanciare allarmi e rilasciare bollettini continui sullo stato della sicurezza, pubblica uno

strumento di facile e immediata lettura. A disposizione di tutti sull'home page di IBM ISS (*www.iss.net*), AlertCon fornisce una misura diretta di tale stato, classificando la situazione da 1 a 4, dove con AlertCon pari a 1 s'intende un basso livello di minacce, affrontabile con la "normale" attività di monitoring, mentre un livello 4 presuppone rischi elevati che richiedono l'applicazione di soluzioni avanzate per la protezione.

Un aspetto importante del lavoro di X-Force è rappresentato dall'importanza che viene data alla qualità nella scrittura del codice e nella validazione del software prodotto. Si tratta, infatti, di un aspetto fondamentale, anche se spesso trascurato, che ha ripercussioni importanti sul reale livello di sicurezza raggiunto. Non è un caso, del resto, che le vulnerabilità nei sistemi di Microsoft sono diminuite sensibilmente da quando la casa di Redmond ha adottate le politiche di Trustworthy Computing Program che impongono lo sviluppo di codice sicuro. Nel caso di codici per l'analisi dei protocolli è ovviamente necessario conoscere a fondo quello che un protocollo dovrebbe essere e cosa si suppone debba fare. Questo esclude subito il filtro tradizionale dell'antivirus, basato sul pattern matching (come il confronto su uno script) e pone il problema di come scrivere un "protocol parser", cioè l'applicazione che è in grado di capire e decodificare un dato protocollo. Non è semplice e un aspetto fondamentale è controllare, una volta che sia stato scritto, che sia effettivamente capace di rilevare tutte le varianti di utilizzo del protocollo. Ma anche verificare se l'analisi mantenga le prestazioni nei limiti prestabiliti. Questo per ogni protocollo. Per questo non basta un programmatore abile, occorre che sia anche scrupoloso e attento a seguire i nostri processi di quality assurance.

Infine, un'altra attività molto delicata è quella relativa ai test sul campo degli algoritmi di decodifica. La prevenzione deve contemplare il blocking del traffico, perché non ci si può basare sulla reattività umana. Ma occorre almeno un mese di verifiche accurate prima che a un codice si permetta di bloccare il traffico, perché bisogna essere certi che non ci siano falsi positivi. Per questo gli esperti di X-Force non si limitano ai test di laboratorio, che, per quanto "cattivi", non rappresentano il mondo reale, e conducono attività importanti in collaborazione con partner fidati.

2.2 L'approccio olistico alla sicurezza e il vulnerability assessment

La sicurezza abilita nuovi processi e l'utilizzo di nuove tecnologie, dalla mobilità alla business collaboration, per fare due esempi, che portano vantaggi in termini di ottimizzazione e produttività. Sono aspetti, evidentemente, che coinvolgono principalmente i business manager e che hanno un impatto su tutta l'impresa. Per questo è necessario che la sicurezza sia affrontata ad alto livello, con un taglio strategico.

Il discorso vale in generale per tutto il sistema di security aziendale ma anche in particolare, per quel che concerne la mitigazione dalle minacce e la data security. Prima degli aspetti tecnologici, infatti, è necessario affrontare problematiche di tipo strategico e precisamente legate alla gestione del rischio con un approccio olistico.

Un tale approccio per la security risponde anche alle esigenze organizzative, perché impostato come un processo di business e soprattutto perché deve essere gestito in sinergia con tutti gli altri processi operativi. Si deve dunque partire da una fase di valutazione della situazione esistente, una di realizzazione e una di gestione per poi rimettere tutto il sistema in discussione ripartendo con una nuova valutazione. Nel caso della sicurezza si tratta di verificare ciclicamente il livello di protezione attraverso un assessment che deve necessariamente considerare il rischio. Un termine che dovrebbe essere ben chiaro ai business manager abituati a gestirlo nell'ambito della governance aziendale. Il rischio alla sicurezza non va confuso con le minacce che discendono dal diffondersi di sempre più numerosi e variegati attacchi ai sistemi informatici. Esso è infatti da calcolare in base alla probabilità che tali attacchi possano impattare sull'infrastruttura aziendale e ai danni che da una simile eventualità deriverebbero.

L'approccio sistemico alla sicurezza che parte dall'analisi del rischio permette chiaramente di capire come procedere, seguendo un ciclo ben preciso che inizia con un assessment iniziale dello stato della sicurezza aziendale. Per proteggere adeguatamente informazioni e processi di business, e decidere come e dove investire in sicurezza, nonché quale tipo di partner può eventualmente essere di supporto, è infatti necessario disporre di una iniziale valutazione del rischio che caratterizza l'ambiente IT.

Valutare il rischio complessivo permette di costruire opportunamente un processo volto a mitigare il rischio stesso e a effettuare le scelte più adatte in termini di infrastruttura di sicurezza e in correlati investimenti. Valutare

il rischio è però un processo complesso, che richiede esperienza e la conoscenza dei diversi possibili attacchi, delle normative esistenti, delle tecnologie necessarie per affrontare il problema, delle metodologie che meglio si applicano a uno specifico settore industriale.
Sono conoscenze che difficilmente sono disponibili all'interno di un'azienda e anche tra le aziende che operano sul mercato in tale settore non sempre è presente l'efficacia e l'esperienza necessaria. IBM presenta da questo aspetto molti vantaggi per l'azienda interessata ad adottare un approccio di business per la sicurezza e a tramutare gli interventi necessari non in un costo ma in una fonte di profitto per il business core dell'azienda e la sua immagine sul mercato. IBM Internet Security Systems, in particolare, è un advisor per la sicurezza, la cui esperienza è certificata sia per l'ambito governativo sia per quello privato, in grado di realizzare e definire con il cliente un approccio calcolato al risk management che permetta di massimizzare il valore della sicurezza del sistema informativo, in modo da tramutarlo in una leva che contribuisca a incrementare l'efficacia delle altre aree di business aziendale. Un po' più in dettaglio, IBM ISS dispone di metodologie, competenze e soluzioni per aiutare le organizzazioni ad affrontare alcuni degli aspetti più delicati nel processo di risk management, quali definire la policy aziendale per la sicurezza, determinare gli asset esistenti dei sistemi informativi e delle applicazioni, assegnare a ogni processo di business il valore relativo che il medesimo assume nel contesto produttivo e di mercato di un'azienda.
Nell'approfondimento di queste aree, le aziende devono affrontare specifici passaggi, per i quali ancora una volta IBM ISS mette a disposizione best practice e metodologie. In particolare, è necessario scoprire le vulnerabilità, determinare i pericoli, valutare la protezione esistente, calcolare il livello di rischio accettabile per l'ambiente informativo (posto che la sicurezza totale non esiste).
Una volta che il livello di rischio esistente è stato determinato diventa possibile ai responsabili della sicurezza stabilire quali azioni è opportuno intraprendere e, soprattutto, in che ordine. Stabilite le priorità è possibile adottare protezioni avanzate per alcuni degli asset aziendali che si sono evidenziati tra i più critici. Alcuni dei prodotti di IBM ISS sono volti proprio a far fronte a questa necessità e a farlo in modo preventivo, e cioè prima ancora che un pericolo insorga o lo strumento necessario all'attacco (per esempio un nuovo virus) venga rilasciato. IBM ISS si riferisce a questo modo di operare con il termine di "Preemptive Protection" o protezione preventiva. Una volta che si è stabilità la priorità degli interventi e si sono

messe in campo le misure di sicurezza addizionali ritenute necessarie, giunge il momento di verificare che le azioni intraprese abbiano una reale efficacia. Da questo punto di vista, ciò può essere ottenuto tramite servizi di management della vulnerabilità, soluzioni di assessment della vulnerabilità ed esperti nella sicurezza che possono produrre report sulla vulnerabilità attuale a cui è stato posto rimedio, e che permettono di valutare la diminuzione effettiva del rischio.

2.2.1 Il vulnerability assessment con le soluzioni IBM Internet Security Systems

Fondamentale per questo approccio analitico è la fase di vulnerability assessment, che vede IBM Internet Security Systems leader del settore, essendo proprio nata con la realizzazione del primo strumento di scansione per la ricerca di vulnerabilità.
Chiamato Internet Security Scanner, tale strumento nel 1992 fu messo a punto da Christopher Klaus, all'età di 19 anni, e da lui messo a disposizione come freeware su Internet. Klaus vi aveva cominciato a lavorare durante un internato presso il Department of Energy degli Stati Uniti quando ancora andava al liceo. Successivamente, frequentando il Georgia Institute of Technology, Klaus approfondì le proprie conoscenze e, dopo aver conseguito la prima vendita di Internet Security Scanner 1.0, fondò nel 1994 Internet Security Systems. Internet Scanner, oggi disponibile come software e come appliance e in grado di realizzare oltre 1300 controlli di vulnerabilità, è anch'esso parte della famiglia di soluzioni Proventia di IBM ISS e, insieme ad altre soluzioni, prime fra le quali Proventia Enterprise Scanner e Proventia Network Scanner, rappresenta tuttora la soluzione di riferimento per il vulnerability assessment.
Parte della soluzione sono anche una serie di soluzioni relative alle varie componenti del sistema informativo, dalle reti wireless a tutti i server e i dispositivi che sulla rete afferiscono. Solo attraverso questo approccio integrato, infatti, è possibile avere una visione completa dei punti di vulnerabilità, sfruttando i quali è possibile penetrare nella rete e accedere a tutte le risorse aziendali o sferrare un attacco.
L'appartenenza all'Enterprise Security Platform di ISS, consente a Proventia Network Scanner di fornire la protezione e la gestione "scan-and-block" della vulnerabilità attraverso l'integrazione totale della tecnologia di valutazione della vulnerabilità e di intrusion prevention all'interno di una singola piattaforma.

2.3 La ISS Protection Platform

Già da qualche anno, IBM Internet Security Systems ha spostato l'attenzione dalla lotta alla singola minaccia a un approccio integrato, arrivando a costituire una piattaforma di protezione che adotta appunto un sistema olistico per la sicurezza preventiva con un meccanismo di gestione e controllo centralizzato. Un approccio unificato, che include prodotti e servizi di sicurezza per la protezione dell'infrastruttura IT aziendale, compresi i desktop, i server, le reti e gli uffici remoti, bloccando le minacce prima che abbiano impatto sull'organizzazione.

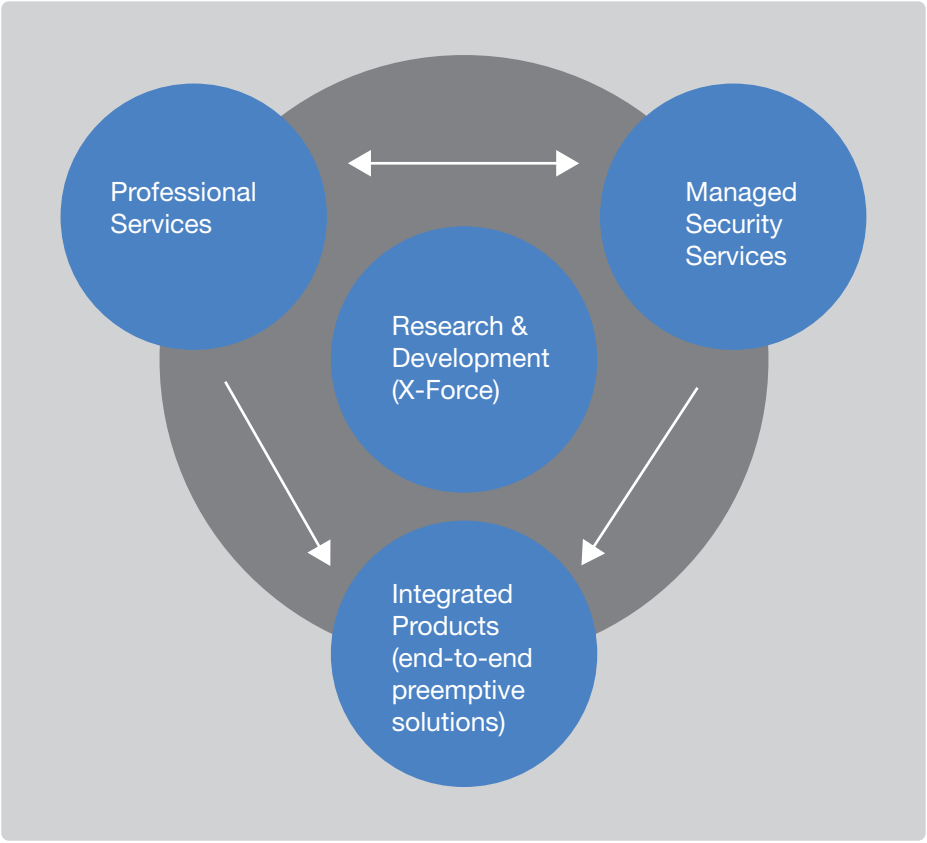


Figura 2.3
Gli elementi che costituiscono la IBM ISS Protection Platform

Alla base della piattaforma di protezione c'è un l'Enterprise Security Platform (ESP) che consente la costruzione di un sistema di sicurezza flessibile e affidabile, tanto da poter garantire la business continuity di cui l'impresa oggi necessita. Grazie a questi presupposti la IBM ISS Protection Platform permette di realizzare la "0 day protection", cioè di assicurare che, per tutte quelle vulnerabilità scoperte da X-Force (e non solo), è assicurata la protezione sin dal giorno in cui viene annunciata la vulnerabilità (se non da prima). È l'approccio pre-emptive promosso da IBM ISS: evi-

tare che un attacco possa arrivare a fare danni, prima ancora che l'attacco sia stato ideato.
Le sfide che vengono lanciate dai continui sviluppi delle tecnologie maligne, rafforzano IBM ISS nella propria strategia orientata alla prevenzione, allo studio delle vulnerabilità e all'integrazione multilivello e multi- analisi delle proprie soluzioni. Ma al centro di tutto deve esserci una logica di gestione della sicurezza, che deve essere affidata a personale sempre più esperto, da un lato, e che deve essere supportata da strumenti intelligenti dall'altro.
Per questo, le soluzioni appartenenti alla IBM ISS Protection Platform sono tutti gestibili dalla stessa console (Proventia SiteProtector integrata con il sistema di management IBM Tivoli) e, soprattutto, sono tutti dotati di intelligenza sufficiente a intervenire quando la situazione lo richiede.
Per aumentare ulteriormente il livello di sicurezza, IBM ISS offre tutto questo sotto forma di servizi, permettendo alle imprese di ogni dimensione di scegliere "on demand" il proprio sistema di sicurezza adattandolo dinamicamente alle esigenze del proprio business o alle mutevoli condizioni di sicurezza su Internet, grazie alla possibilità di aggiungere, togliere e modificare il paniere di servizi sottoscritti.
È questa logica dinamica e proattiva che fanno di IBM ISS un punto di riferimento per la sicurezza e la protezione dalle minacce di ieri, oggi e domani.
Come accennato, alla base di questa visione vi è la Proventia Enterprise Security Platform, che fornisce una sicurezza integrata con le attività IT, mantenendo l'equilibrio tra le prestazioni richieste al sistema informativo, la disponibilità e il rischio.
Contrariamente a un approccio tradizionale focalizzato sul tempo di reazione, la strategia ISS è votata a evitare tutti gli incidenti di sicurezza, rendendo la stessa parte integrante del sistema informativo e un fattore di business abilitante.
Basata sulla strategia di pre-emption, che fornisce sicurezza con costi allineati al rischio e alle esigenze aziendali, Proventia ESP è strutturata su:

- Vulnerability Mapping - il continuo controllo delle vulnerabilità, abbinato a tecniche di discovery e monitoraggio attivo e passivo della rete;
- Protection Prioritization - la definizione di criteri per stabilire cosa proteggere prioritariamente, in base all'importanza degli asset, alla configurazione della rete e all'esperienza di ISS;
- Virtual Patching e Remediation - la tecnologia e i metodi di protezione di ISS contro le vulnerabilità.

- Reporting e Benchmarking – la reportistica personalizzabile che mostra la progressiva riduzione del rischio e una visione dettagliata necessaria per la conformità agli standard di legge, nonché utile per la network forensic.

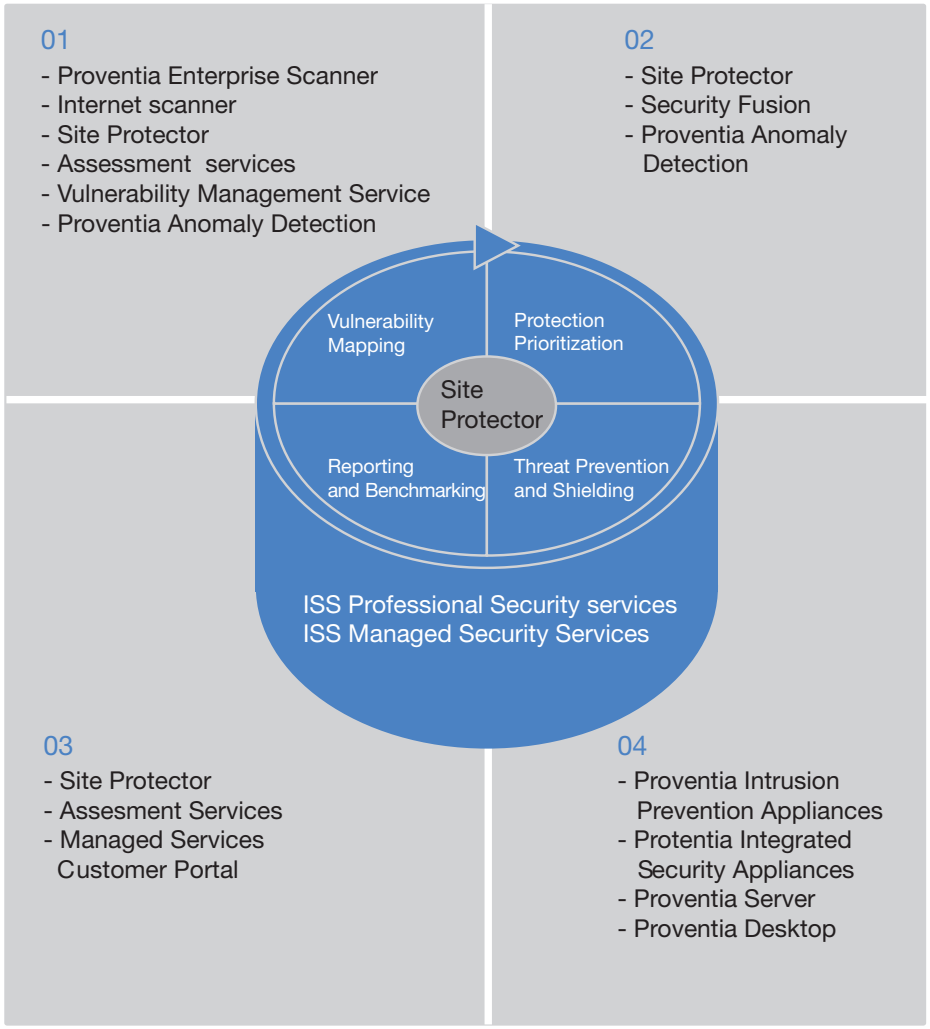


Figura 2.4
Una visione dei prodotti e servizi per la Proventia Enterprise Security Platform

Le componenti della piattaforma Proventia ESP sono i servizi, le soluzioni e le tecnologie che IBM Internet Security Systems ha progettato in modo che possano interagire con SiteProtector, la piattaforma di gestione centrale per l'Enterprise Security Platform, non solo fornendogli informazioni sullo stato della sicurezza. Per esempio, Proventia Network Enterprise Scanner scansiona automaticamente il sistema alla ricerca di vulnerabilità, interfacciandosi con SiteProtector, il sistema di gestione centralizzata della sicurezza. Quando viene trovata una vulnerabilità su un sistema, SiteProtector, in automatico, si collega alla base dati dell'as-

set management per controllare lo stato di tale sistema e in conseguenza di questo genera l'azione opportuna: eventualmente attivando il sistema di ticket processing, se fosse necessaria l'apertura di una richiesta sull'help desk, oppure inviando una mail al security manager o altro ancora. In ogni caso, vengono informati anche i dispositivi di intrusion prevention e/o detection.
Di fatto, le caratteristiche dell'ESP permettono di gestire le vulnerabilità in base a vari parametri, che non è detto dipendano direttamente dalla soluzione di sicurezza, ma possono essere considerate grazie all'interazione dell'interfaccia di gestione con gli altri sistemi attraverso l'infrastruttura aziendale.

2.3.1 L'intrusion pre-emption

Con la connettività globale permessa da Internet le minacce alla sicurezza hanno cambiato completamente approccio. Si pensi ai primi virus diffusi principalmente dai dischetti e alla rapidità di propagazione permessa dalle reti, ma soprattutto si consideri la combinazione di più tecniche per sferrare attacchi sempre più complessi. Di fatto, si è sempre più vicini allo "zero day threat", cioè alla minaccia pronta il giorno stesso in cui viene annunciata una vulnerabilità. Nella migliore delle ipotesi, l'annuncio viene effettuato contestualmente al rilascio della patch, ma, soprattutto a livello enterprise, è impossibile riuscire a installare una patch e portarla in produzione istantaneamente. Tra l'altro, anche se normalmente è così, non sempre quando viene annunciata una vulnerabilità è già disponibile la patch.
L'evoluzione delle minacce presenta però anche altri aspetti che è bene considerare attentamente quando si deve affrontare il problema della sicurezza aziendale. Innanzitutto, la diffusione delle reti le ha rese un bersaglio diretto dei tentativi di intrusione. In secondo luogo, lo sviluppo di diverse modalità di accesso ha contribuito a complicare lo scenario da controllare. Infine, il proliferare di sistemi (dal router, al firewall, al server, al client) ha determinato una crescita dei punti di debolezza attraverso i quali penetrare nel sistema informatico per carpire informazioni o causare danni. A questo si deve poi aggiungere il successo del wireless e delle tecnologie per la mobilità, che hanno definitivamente reso i confini del sistema informativo aziendale elastici e talvolta impalpabili. Infine, il successo del Web 2.0, con la sua interazione sempre più spinta tra gli utenti della rete, ha determinato una crescita del social networking. Una manna, in un certo

senso, per i malintenzionati in cerca di informazioni, che possono mettere in atto tecniche di social engineering sfruttando facilmente le sempre più informazioni disponibili online. Si consideri, per esempio, la scheda pubblicata da un utente su YouTube. Insieme ai suoi video rappresenta un'ottima base per cominciare a "disegnare" un'identità elettronica.
In questo scenario è fondamentale lo sviluppo di sistemi end to end, che abbracciano tutte le risorse ICT.

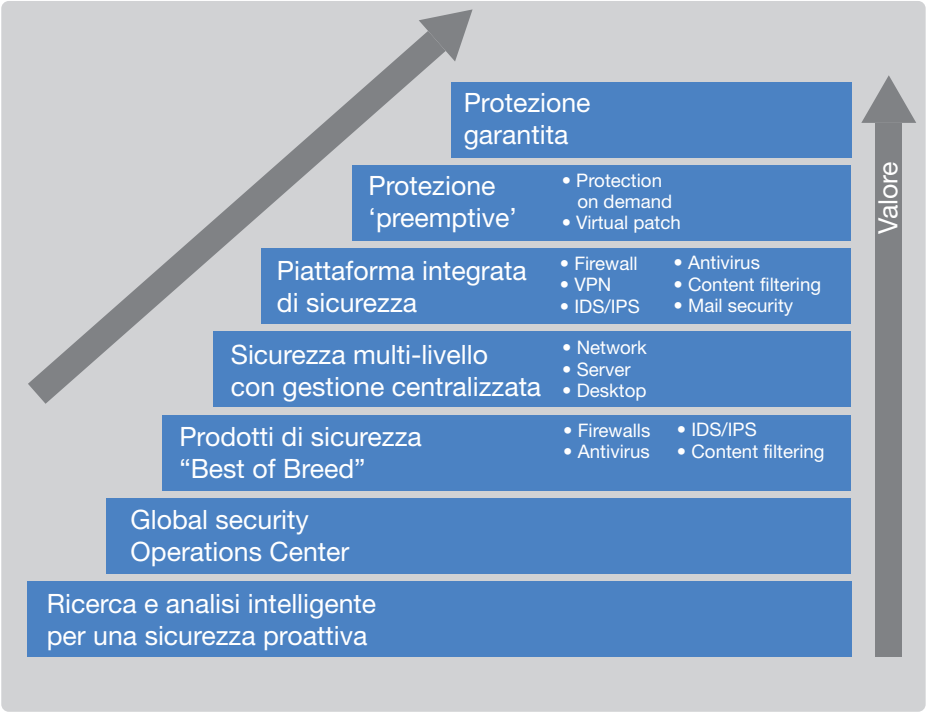


Figura 2.5
L'evoluzione degli approcci alla sicurezza ICT

Partendo dai propri punti di forza tradizionali, vulnerability assessment e intrusion detection, IBM Internet Security Systems ha messo a punto negli anni un sistema multi-livello sofisticato per indirizzare la sicurezza end to end.
Innanzituto, per quanto riguarda l'architettura dei sistemi per l'intrusion prevention, il punto è che la prevenzione deve essere più che affidabile, perché la velocità con cui agiscono gli attacchi non concede tempo per indugiare. In altre parole è necessario bloccare il traffico "maligno" prima che l'attacco abbia un effetto sulla rete, che è quanto permette di fare una protezione "pre-emptive". È altresì evidente che se si ferma un flusso di dati "buono", di fatto, si genera involontariamente un disservizio.

Un sistema di pre-emptive protection deve quindi evitare i falsi positivi (come sono chiamati errori del genere in gergo), altrimenti è esso stesso a determinare impatti negativi sulla rete. D'altro canto, è bene ricordare sempre che la sicurezza non è un concetto assoluto e che è preferibile stare alla larga dalle "sirene pubblicitarie" che parlano di protezione completa promettendo un livello di sicurezza del 100%. La realtà dinamica delle minacce rende impossibile realizzare questo obiettivo, a meno che non sia confinato in uno specifico segmento tecnologico e riferito pertanto a un limitato numero di minacce. Per allargare l'orizzonte protettivo è necessario riconoscere che non basta una singola tecnica di intrusion prevention per fronteggiare tutti i tipi di minaccia conosciuti e non.

L'architettura di intrusion prevention IBM ISS si basa su agenti di controllo e tecnologie di scansione che esplorano tutte le risorse del sistema informatico, con un'ottica integrata che assicura la completa compatibilità degli elementi di protezione e riduce il total cost of ownership, evitando di replicare funzionalità all'interno del sistema. L'accuratezza dell'architettura di IBM ISS è innanzitutto rappresentata dall'avanzata tecnologia di scansione e controllo della rete e degli host. La tecnologia di intrusion detection, sul lato rete, comprende un'analisi dei protocolli molto raffinata, estesa su tutti i 7 livelli della pila OSI. Inoltre, il sistema è in grado di rilevare le anomalie nell'utilizzo di qualsiasi protocollo di rete e di realizzare la deep stateful inspection dei pacchetti, la verifica in tempo reale degli attacchi (con risposta da parte dei server), il pattern-matching delle signature.

Più in dettaglio, le tecnologie di protezione attuate dai sistemi di detection e prevention di IBM ISS ricadono in due macro categorie: le tecniche di identificazione e quelle di analisi. Le prime sono quelle che permettono di identificare con accuratezza quali protocolli sono utilizzati dai pacchetti che stanno transitando sulla rete. Gli strumenti di analisi, invece, consentono di esaminare l'uso che viene fatto dei protocolli identificati per cogliere un eventuale abuso, indice di un possibile attacco. Inoltre, IBM ISS ha aggiunto una tecnica basata sull'analisi del comportamento, che, tra l'altro, risulta particolarmente utile nel rilevare attacchi dall'interno. In particolare l'anomaly detection rileva comportamenti sospetti di utenti, applicazioni e servizi. Per la loro capacità d'analisi approfondita, i sistemi di anomaly detection forniscono ai network manager una visione molto accurata di quello che accade sulla propria rete.

IBM ISS ha esteso nel tempo le tecniche utilizzate, garantendo nel contempo le prestazioni, in modo da aumentare il livello di accuratezza

nell'identificazione e da ridurre al minimo la percentuale di falsi positivi e negativi, portandola vicino allo 0%.
Ciascuna tecnologia ha i suoi punti di forza e punti di debolezza: è la loro combinazione, dunque, che consente di eliminare virtualmente i falsi positivi e i falsi negativi, permettendo di rilevare e proteggere anche nuovi tipi di attacchi in precedenza sconosciuti.
Per molte tipologie d'attacco, peraltro, la registrazione di un'anomalia in sé non necessariamente comporta una minaccia e potrebbe essere trascurata. Al massimo, comunque, genera un log che finisce nel "mucchio". Per questo, punto di forza dell'architettura per l'intrusion detection è la piattaforma di gestione rappresentata dalla suite SiteProtector di IBM ISS. Questa, oltre a fornire una visione combinata di tutte le informazioni raccolte dai vari sensori posti su rete e host, mette a disposizione un motore di correlazione che riduce drasticamente e automatizza le operazioni realizzate "manualmente" dell'utente. In questo modo, accresce anche la sicurezza complessiva, che non viene a dipendere totalmente dalla competenza dell'amministratore.
L'approccio alla correlazione di IBM ISS parte dal presupposto che i rischi cui l'azienda è esposta sono il risultato dell'interazione tra le vulnerabilità dei propri sistemi e gli attacchi che essi subiscono. IBM ISS da tempo ha messo in interazione il sistema di vulnerability assessment e l'IDS, potendo stabilire se gli attacchi sono andati a buon fine, se sono stati bloccati da una sonda Network o Server o se sono da ritenersi innocui per i server aziendali. Il sistema di IBM ISS, peraltro, non si limita a estrapolare dati: secondo la società statunitense, infatti, correlare eventi di sicurezza con eventi di rete, significa capire, implementare e tenere in continuo aggiornamento i criteri e la logica di analisi. È necessario studiare le tipologie di attacco e le vulnerabilità per avere sempre i criteri di correlazione aggiornati. Questo è uno dei compiti di X-Force, il team di ricerca e sviluppo che fornisce l'esperienza di ingegnerizzazione essa al servizio dei clienti.
Nelle reti convergenti di nuova generazione, inoltre, si presentano problematiche di sicurezza particolari. Le tecnologie di analisi IPS di IBM ISS permettono di bloccare anche gli attacchi che superano i firewall VOIP-aware e forniscono una protezione ulteriore anche a quelle parti di una rete VLAN o VPN (rispettivamente per l'ambito locale e geografico) su cui transita traffico voce. I prodotti rappresentano quanto di più tecnologicamente innovativo vi è per la protezione delle comunicazioni, a partire dalle dettagliate capacità di analisi dei protocolli adottati per la VOIP, compreso tra questi: SIP, MGCP, H.323 e SCCP.

Un beneficio aggiuntivo deriva dalla capacità della soluzione di riconoscere le anomalie nel comportamento dei flussi di traffico al loro primo insorgere. Si tratta quindi di un sistema che auto-apprende gli schemi di comportamento e che identifica immediatamente qualsiasi differenza dovesse incorrere a causa di attacchi esterni al sistema VOIP. In questi casi provvede ad allertare immediatamente i gestori del sistema, al fine di permettere interventi immediati oppure, se previsto dalle procedure e dalle best practice, bloccare immediatamente il relativo traffico. Si tratta quindi di una soluzione che è in grado di operare in modo preventivo e proattivo nell'assicurare la sicurezza della rete VOIP.

2.3.2 Il Virtual Patching e la Zero Day Protection di IBM ISS

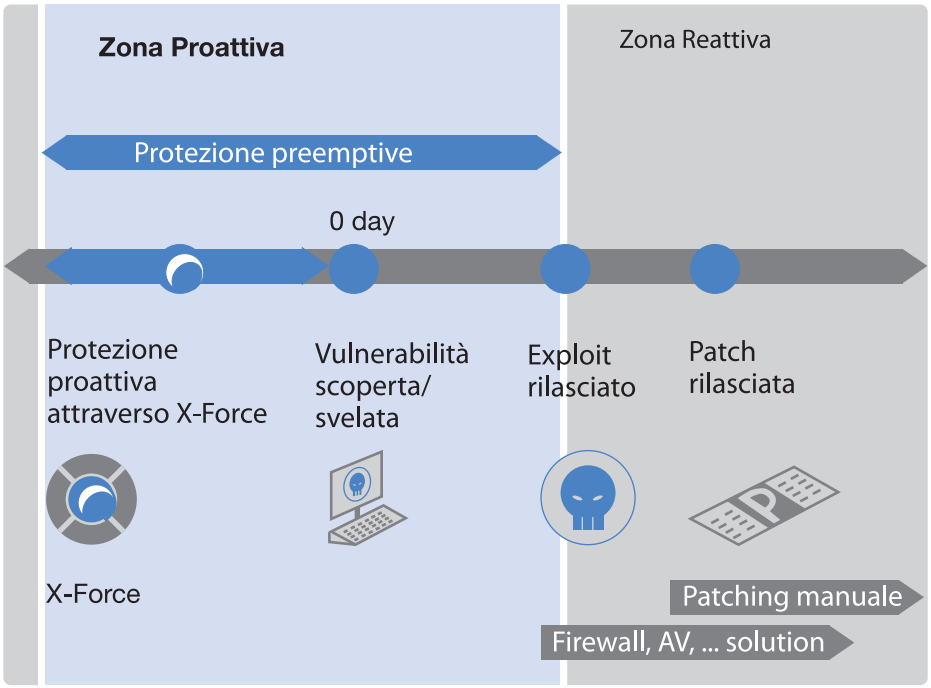
È praticamente da escludere che si possa scrivere un codice che risulti completamente privo di errori al 100%. In passato, inoltre, i fornitori di software non si ponevano neanche questo obiettivo: il loro scopo era ovviamente garantire il funzionamento nello svolgimento delle applicazioni per le quali il software è programmato. Pian piano, negli anni, i produttori di software hanno cominciato a considerare con maggior attenzione il problema della sicurezza. In molti casi solo per evitare gli echi mediatici e i malcontenti che, con l'aumentare delle minacce e degli attacchi, aumentavano presso i loro clienti. Molte società hanno quindi cominciato a implementare precise procedure per la ricerca delle vulnerabilità nei propri sistemi e la realizzazione delle cosiddette "patch". Queste ultime sono letteralmente delle "toppe", cioè un pezzo di codice che va a sostituire la parte "errata" o a porre rimedio a qualche impostazione che apre la strada agli hacker. Più recentemente, inoltre, alcuni software vendor hanno introdotto ulteriori procedure per progettare e scrivere le applicazioni in modo da risultare più sicure.
È buona regola installare le patch non appena queste sono disponibili, ma di fatto è impossibile: innanzitutto, infatti, è necessario controllare che il codice aggiunto non crei conflitti con le applicazioni esistenti, causando danni al sistema di produzione. In secondo luogo, i tempi tecnici per l'installazione della patch su tutti i sistemi lasciano comunque una finestra temporale a disposizione dei malintenzionati.
Per questo, IBM ISS ha sviluppato da tempo una strategia e una tecnologia: la prima consiste essenzialmente nel lavoro di X-Force a caccia di vulnerabilità, mentre la seconda è il Virtual Patching.
Quest'ultima garantisce una protezione attraverso una sorta di "aggiornamento" virtuale dei sistemi vulnerabili. Fulcro di questa protezione

virtuale è il servizio automatico di aggiornamento X-Press Update (X-PU), che non impatta su alcun sistema o applicazione, perché semplicemente aggiorna il database delle sonde per l'intrusion detection/prevention. In pratica, quando gli esperti di X-Force rilevano una vulnerabilità e identificano un modo in cui questa può essere sfruttata, studiano i possibili exploit. In altre parole, anticipano le mosse che potrebbero essere utilizzate da un malintenzionato per sfruttare una vulnerabilità e analizzano le modalità con cui è possibile accorgersi di questo (per esempio, dall'utilizzo di un protocollo di rete in un determinato modo). Di fatto i sistemi di intrusion prevention di IBM ISS sono allertati e possono bloccare il traffico maligno con il quale si sta tentando l'attacco. La soluzione IBM ISS, in pratica, protegge i server come se fossero stati "accomodati" con la patch, mentre a essere aggiornato è solo il database del sistema di rilevamento delle intrusioni. In questo modo gli IT manager possono valutare con calma quali patch converrà realmente installare (spesso comportano altri vantaggi, per esempio di tipo prestazionale) e, soprattutto, prendersi il tempo necessario.

L'azione del virtual patching è dunque preventiva, perché prima che sia stato sferrato l'attacco la protezione è già in essere. Poiché è nella maggior parte dei casi IBM ISS la società che scopre la vulnerabilità, è abbastanza normale che i suoi esperti abbiano il tempo di scoprirne a fondo tutte le caratteristiche e di preparare la "virtual Patch". L'annuncio di una vulnerabilità, infatti, viene ritardato, possibilmente fino a quando il fornitore del sistema debole non abbia pubblicato la relativa patch. In taluni casi, soprattutto quando la vulnerabilità è considerata di bassa gravità o quando è relativa a sistemi di minor diffusione e fa capo ad aziende più piccole, i tempi per lo sviluppo di un rimedio ufficiale si allungano. Può dunque essere che IBM ISS decida di annunciare la vulnerabilità in contrasto con il produttore del sistema, ma evidentemente questo accade comunque quando la patch, anche se virtual, è disponibile presso IBM ISS stessa. In realtà, grazie al servizio X-PU la protezione è già attiva, anzi pro-attiva, nelle soluzioni di sicurezza dei suoi clienti.

Tutto il tempo che precede il lancio di un attacco o il tentativo di un exploit, rappresenta il periodo di relativa tranquillità, detta "proactive zone", durante la quale si possono appunto intraprendere azioni preventive. Il giorno in cui viene annunciata una vulnerabilità è detto "0 day", perché è da qui che si comincia a calcolare quanto tempo ci mettono le comunità di hacker a ideare un exploit. Dopo che questo viene lanciato, parte un periodo di allarme, che sarà tanto più grande quanto più lungo e difficile risulterà lo sviluppo di

Figura 2.6
La protezione pre-emptive di ISS



una patch. Solo dopo il rilascio di quest'ultima la tensione comincerà a calare, parallelamente alla capacità di propagazione dell'attacco.
L'abilità di sviluppo degli hacker si va affinando grazie a supporti, anche economici, impensabili fino a pochi anni fa. Questo porta a un'estrema riduzione della finestra temporale tra il giorno "0" e il giorno dell'exploit: il cosiddetto "threat day". Tanto che già da un po' si pronostica la "0 day threat", cui IBM ISS ha contrapposto la "0 day protection". Come si è detto, peraltro, il rimedio ideato da IBM ISS può essere disponibile finanche prima del giorno "0", quindi con una capacità che risulta essere più che preventiva e che, per questo, IBM ISS chiama "pre-emptive".

2.3.3 La sicurezza per gli endpoint

Prima ancora delle tecniche sono evoluti gli obiettivi degli attacchi provenienti da Internet: inizialmente era la rete, poi hanno cominciato a essere gli host. Successivamente, più in generale sono gli endpoint, cioè server, pc, notebook, PDA e sistemi portatili di vario tipo connessi alla rete corporate. Questi, infatti, possono essere uno strumento per penetrare nel sistema informativo, ma anche, più semplicemente, una ricca fonte di informazioni e dati sensibili che spesso vi risiedono, talvolta dimenticati. Tra l'altro, possono anche essere un tramite per acquisire capacità di elaborazione oppure un "ponte" per sferrare ulteriori attacchi verso altri obiettivi, anche esterni all'azienda.

Tipicamente, questi apparati sono soggetti a una varietà di minacce che costringono i responsabili dei sistemi a installare una miriade di soluzioni per la sicurezza, a protezione dai virus, dallo spam, dagli spyware e dalle altre minacce. Il continuo acquisto di prodotti per la sicurezza tra loro incompatibili e di agenti endpoint sta però non solo rapidamente diventando per le imprese una questione impossibile da gestire ma anche un metodo di risposta inefficace, dato che le minacce moderne sono sempre più strutturate in diversi livelli ibridi.
Tutto ciò amplifica i benefici ottenibili attraverso l'adozione di piattaforme di protezione integrate e multilivello. Questo approccio consente di usufruire di uno strumento integrato, aggiornato automaticamente e facile da gestire, cui, soprattutto, un singolo produttore si impegna ad aggiungere continuamente i layer di protezione nonché garantire sinergia tra le diverse funzioni e consistenza nell'aggiornamento.
Parte integrante della "0 Day Protection" sono dunque anche una serie di soluzioni che attuano controlli capillari su tutti gli eventi di sicurezza a protezione della posta elettronica, dei contenuti e dei terminali. Si tratta di sistemi per il controllo dei virus, dello spam, dello spyware e di varie tipologie di attacco sofisticate.

Virus, antivirus e il Virus Prevention System

L'esperienza insegna che anche in presenza di antivirus e soluzioni firewall, gli attacchi dei virus sono in grado di penetrare le difese delle reti aziendali. Le operazioni necessarie ai produttori di antivirus per rilasciare un aggiornamento del proprio sistema di protezione e, all'azienda, per testarlo, implementarlo e distribuirlo anche sui notebook degli utenti remoti, spesso espone gli asset aziendali a possibili rischi per un tempo eccessivamente lungo. Basti pensare che un pc infetto è in grado di riprodurre 10 copie del virus ogni secondo, per comprendere immediatamente come alcuni codici dannosi abbiano potuto espandersi ai livelli a tutti noti.
Inoltre, l'incremento di sofisticazione delle minacce ibride provenienti da Internet si accompagna a metodi sempre più sofisticati nell'utilizzo delle tecniche per il social engineering. Per fronteggiare questi attacchi, l'utilizzo di un "semplice" antivirus si dimostra, pertanto, troppo spesso inefficace ed è per questo che IBM ISS ha sviluppato una tecnologia avanzata, chiamata Virus Prevention System (VPS). Il previene virus e, più in generale, codici maligni, sfruttando i punti di forza dei metodi tradizionali per il rilevamento dei virus e superando i loro limiti, fornendo così una protezione preventiva ed efficace da attacchi nuovi e sconosciuti.

Il VPS entra in funzione quando viene richiesta l'esecuzione di un file. Questo potrebbe quindi anche essere stato copiato (per esempio l'ActiveX scaricato da Internet), ma non sarebbe in grado di compiere danni, perché verrebbe bloccato prima di essere eseguito. Il punto di partenza della tecnologia VPS è un sistema di testing basato sul comportamento che analizza ciò che fa il codice quando viene eseguito sul sistema reale. Per farlo VPS esamina ed esegue il codice sotto esame all'interno di uno spazio di pre-esecuzione, utilizzando un ambiente virtuale in modo che l'esecuzione vera e propria del codice non possa arrecare danni, compromettere il sistema o determinare danni collaterali durante l'individuazione. La pre-elaborazione viene effettuata una volta sola per ciascun file, in modo da non penalizzare le prestazioni, l'impatto sulle quali, in questo modo, è paragonabile a quelle di altri sistemi di protezione desktop e, comunque, contenuto all'interno di un range di circa il 2-3%, non percepibile con le CPU di ultima generazione (a meno che non siano stressate al massimo).

VPS effettua un'analisi completa e granulare per esaminare il comportamento dei virus in dettaglio individuando particolarità e specificità. Prima di effettuare una diagnosi VPS raccoglie uno scenario completo dell'intera esecuzione del codice, in modo da fornire un elevato livello di rilevamento e ridurre al minimo le probabilità di generare un falso positivo.

Poiché tutti i nuovi virus contengono, di fatto, materiale riciclato o utilizzano metodi comuni, VPS è in grado di riconoscere queste tecniche ovvero la combinazione delle attività del computer utilizzate solitamente da un codice malevolo. Quando VPS ha compreso la tecnica, ogni nuovo virus sconosciuto che utilizza quella tecnica viene eliminato.

Un'altra caratteristica fondamentale di VPS è che non richiede aggiornamenti continui per individuare nuove varietà di virus, come i tipici antivirus ma, semplicemente, di un upgrade due o tre volte l'anno, quando vengono categorizzati nuovi comportamenti. In ogni caso, anche in assenza di un aggiornamento della signature, VPS blocca ben oltre il 90% dei nuovi virus.

Va infine ricordato che VPS non si propone come una tecnologia sostitutiva agli antivirus, ma complementare agli esistenti programmi secondo un'ottica strategica di protezione multilivello. Poiché oggigiorno le minacce miste provengono sia dal lato applicativo sia da quello della rete l'approccio multilivello è in grado di garantire una protezione adeguata sia per i vettori che sfruttano le applicazioni sia per quelli che utilizzano il network. Proprio in quest'ottica VPS può essere implementato sia a livello host sia di gateway.

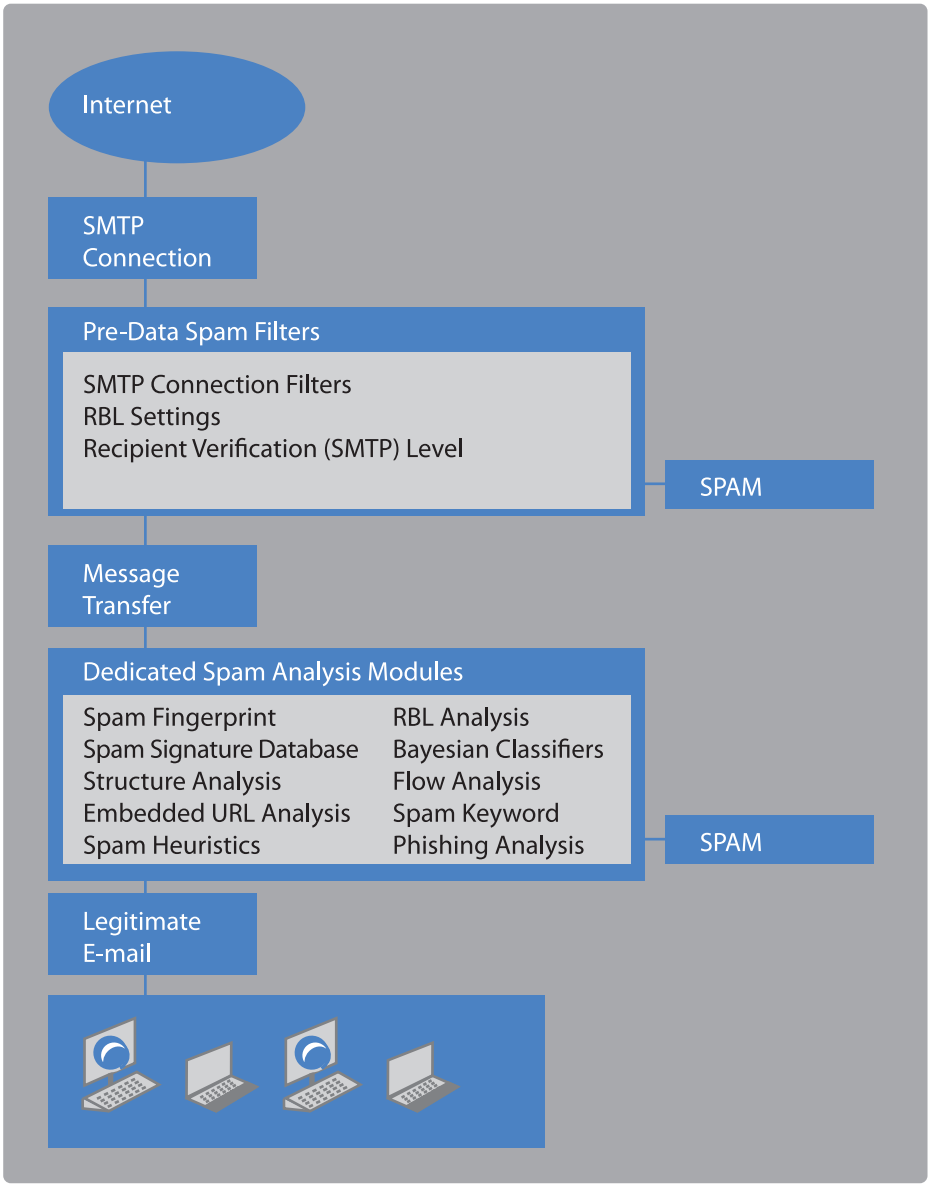
Spamming ed email security

La posta elettronica è ormai affermata in tutte le imprese ed è diventata uno degli strumenti primari per la comunicazione aziendale. Da quando la legge italiana ha definito le caratteristiche che un email deve possedere per essere riconosciuta come documento ufficiale e legate, la posta elettronica è inoltre entrata a far parte delle applicazioni mission critical per le imprese.
Due noti fenomeni, però, sono tristemente collegati a questo canale di comunicazione: la diffusione dei malware e lo spamming. Quest'ultimo nasce essenzialmente in seguito all'invio di una quantità spropositata di email "pubblicitarie", secondo una strategia basata sui grandi numeri: nel mucchio qualcuno si "pesca". Molti dei messaggi spam sono innocui e generati dai tanti utilizzatori che spediscono di tutto: dalle barzellette alle petizioni fino a quelle che diventano vere e proprie leggende di Internet. Il fenomeno è quindi essenzialmente fastidioso e sarebbe innocuo se il meccanismo non fosse anche utilizzato per scopi criminosi, in particolare per il phishing, cioè il furto di informazioni riservate relative perlopiù a identità elettroniche e a dati per l'accesso a servizi bancari, utilizzati successivamente per commettere frodi online.
Le tecniche per la diffusione dei messaggi, nonché per l'inserimento di malware o link a indirizzi Web falsi, sono molto evolute nel corso degli ultimi tre o quattro anni, da quando il fenomeno è prepotentemente esploso.
Gli strumenti preposti per quantomeno arginare il fenomeno sono normalmente indicati come anti-spamming e vengono abbinati ad altre soluzioni per il filtraggio dei virus e dello spyware, più in generale appartenendo alla categoria della Content Security.
IBM dispone di due moduli software per la content security, destinati alla piattaforma multifunzione Proventia M, ma disponibili anche separatamente con il nome di Proventia Web Filter e Proventia Mail Filter. A questo si aggiunge un'appliance dedicata, chiamata Proventia Network Mail Security, e una versione "virtuale" (attualmente in grado di supportare la piattaforma di virtualizzazione VMware ma in futuro è previsto il supporto per altri sistemi).
Il primo punto di forza della tecnologia di content filtering IBM ISS è la disponibilità di un database di contenuti gigantesco, superiore a quello utilizzato da Google per le sue ricerche sul Web, per numero di immagini catalogate.
L'altro aspetto fondamentale è legato il motore di filtraggio dei contenuti, che non si limita, si fa per dire, a controllare le email in ingresso per bloccare eventuale spamming. Più che un controllo, viene effettuata una vera

e propria analisi che utilizza oltre 20 diverse tecniche, esaminando tutti i campi del messaggio di posta, il corpo del messaggio e gli allegati. Importante, per esempio, l'analisi del testo, che consente di bloccare l'uscita di informazioni riservate al di fuori dell'azienda. Lo stesso dicasi per la capacità di document filtering del prodotto.

Con l'utilizzo di tecniche di analisi molto simili se non uguali a quelle impiegate per il filtraggio della posta, le soluzioni di IBM ISS si occupano di controllare i contenuti acceduti via Web, secondo le impostazioni definite dall'azienda.

Figura 2.7
Le tecniche di analisi per il filtraggio dei messaggi di posta elettronica



Anche per quanto riguarda gli spyware, IBM ISS adotta una strategia di sicurezza integrata per fornire una protezione pre-emptive. Le soluzioni antispyware di IBM ISS, in particolare, sono integrate all'interno delle appliance multifunzione Proventia e nella soluzione per la protezione degli endpoint, Proventia Desktop.
In particolare, IBM ISS ha implementato quattro metodi di protezione nel Proventia Desktop. Più precisamente, lo stesso VPS può bloccare i codici tipo hi-jacker e key logger, normalmente raccolti dal browser, mentre utilizzando l'application control, X.Force ha scritto diverse regole per bloccare applicazioni non autorizzate sulla rete e per identificare gli spyware più comuni. A questo si aggiunge, infine, il modulo di analisi dei protocolli del sistema IPS, cui è stato aggiunta la capacità di rilevazione e bloccaggio di pattern di installazione di ActiveX sospetti.
La soluzione di protezione IBM ISS impedisce agli utenti di installare inavvertitamente programmi sui propri sistemi, bloccando l'accesso ai siti Internet che li distribuiscono. I sistemi di Web filtering di IBM ISS sono aggiornati automaticamente, senza l'intervento dell'amministratore. Questo significa che quando compaiono nuovi siti, o quando i creatori degli spyware cambiano sito per non essere scoperti, i sistemi installati presso gli utilizzatori vengono aggiornati e rimangono protetti automaticamente.

Phishing e attacchi polimorfici

Man mano che le tecnologie di difesa automatiche si sono diffuse, facendosi nel contempo più accurate e difficili da superare, si è assistito a un progressivo cambio di strategie per l'attacco. Un sempre più alto numero di queste, infatti, si sono concentrate sul fattore umano, da sempre l'anello debole della catena. Anche se la sensibilità verso la sicurezza sta aumentando, resta ancora molto da fare se non si vuole che i propri sforzi nella definizione delle security policy aziendali vadano perduti.
Per sfruttare l'umano "errare", gli hacker adottano diverse tecniche, perlopiù catalogate come tipologie di "spoofing", per arrivare a raccogliere informazioni e dati sensibili in modo da rubare identità elettroniche, prendere possesso di computer remoti, penetrare in sistemi informativi protetti. Più precisamente, spoofing, che letteralmente significa "parodiare", corrisponde a una tecnica di mascheramento o simile. In pratica, l'attaccante "finge" di essere qualcos'altro o, meglio, cerca di far credere che un sito, un allegato di un'email o una richiesta d'accesso sembrano diversi da quello che sono in realtà, cioè un attacco (o una fase preliminare dello stesso, come un'intrusione).

La più nota frode online basata su tecniche di spoofing, in generale di tipo legato all'email e al Web, è il "phishing". Sono relativamente pochi a essere "pescati", circa il 5% secondo l'Anti-Phishing Working Group, ma considerati i volumi importanti di attacchi, si tratta di numeri significativi. Inoltre, dopo i primi allarmi, le tecniche sono state raffinate, dando anche origine a sottocategorie, come il "pharming", che fa riferimento alla manipolazione delle informazioni DNS (Domain Name Server) presenti all'interno di un pc o di un server al fine di reindirizzare l'utente in modo inconsapevole su siti Web falsi, lo "spear phishing", utilizzato per indicare attacchi indirizzati in modo molto mirato a specifici target, lo "smishing", che fa riferimento ad attacchi portati sfruttando i servizi SMS disponibili sui telefoni cellulari, e il "vishing", che deriva dalla contrazione di voice e phishing e rappresenta la pratica indirizzata a sfruttare le tecnologie di messaggistica vocale e, in particolare, il Voice over IP (VOIP) per indurre la vittima designata a fornire informazioni personali, finanziarie o riservate con l'obiettivo di ottenerne un vantaggio economico.

Il mascheramento è utilizzato anche per celare ai motori di controllo il codice maligno. Recentemente, Il concetto di malware morphing sta subendo ulteriori evoluzioni, con un'accelerazione preoccupante: per esempio su Web, gli hacker stanno ora modificando dinamicamente l'exploit offuscato ogni volta che una potenziale vittima visita la pagina Internet infetta, creando di fatto un exploit diverso per ogni diversa richiesta. Questo viene chiamato "exploit x-morphic" o polimorfico e produce exploit del tipo Web browser altamente nascosti e sempre differenti (one-of-a-kind). I motori x-morphic oscurano ulteriormente i loro attacchi utilizzando anche tecniche di personalizzazione avanzate, che creano sul sito Internet una "user experience" più dinamica.

Al primo sguardo la previsione non è delle più rosee. Si prevede che l'exploit polimorfico diventerà il metodo standard di attacchi su Internet e sostituirà i canali finora più specifici di impiego di exploit (di fatto, tentativi manuali per nulla coordinati) usati abitualmente dalle organizzazioni criminali. Tali canali sono destinati ad aumentare sempre di più, con sviluppatori di terze parti che forniranno contenuti specializzati a cui è possibile aderire con un semplice servizio di abbonamento.

Per combattere minacce dinamiche, dal phishing tradizionale all'exploit x-morphic è impossibile adoperare sistemi signature-based, perché non esistono oggetti da confrontare. Il controllo deve necessariamente incrociare più tipologie di analisi, come fanno gli oltre 20 moduli inseriti in Proventia Network Mail Security.

A questo si aggiungono le tecniche di anomaly detection e intrusion prevention, combinate con quelle basate sul comportamento.
Inoltre, per fronteggiare il crescente utilizzo di "shellcode" come metodo per sfruttare le vulnerabilità associate a diversi formati di file finora ritenuti affidabili (in pratica, viene inserito del codice all'interno di un exploit per svolgere uno specifico compito), IBM ISS ha sviluppato una nuova tecnologia, implementandola nei propri sistemi di protezione, capace di affrontare con successo il problema delle vulnerabilità associate ai formati di file e ai futuri protocolli di rete: la IBM ISS Shellcode Heuristics (SCH). Questa è stata progettata per identificare la relazione tra dati e, in base ai risultati di questa analisi, verificare che si tratti effettivamente di codice.

2.3.4 Le soluzioni Proventia di IBM ISS

Più volte citate nella descrizione delle tecnologie e dei sistemi per la protezione, le appliance e le soluzioni della gamma Proventia sono lo stato dell'arte per quanto riguarda la protezione multilivello e preventiva per la gestione delle minacce provenienti da Internet e dai moderni canali di comunicazione aziendale.
La gamma Proventia si espande orizzontalmente per tipologie di soluzioni e verticalmente per la scalabilità prestazionale che mette a disposizione delle imprese. Tutte le soluzioni sono completamente integrate tra loro, all'interno dell'Enterprise Security Platform, elemento principale della IBM ISS Protection Platform. Si tratta di un sistema strutturato, olistico ed estremamente articolato che consente di nascondere la complessità all'utente finale garantendo la prevenzione delle minacce note e anche non note, bloccando, con un approccio pre-emptive, i tentativi di attacco prima che possano impattare sul sistema aziendale.
La gamma IBM Proventia comprende: i Proventia Network Intrusion Prevention System (IPS) e il Proventia Network Intrusion Prevention System GX6116; i Proventia Network Multi-function Security (MFS); Proventia Server Intrusion Prevention System; Proventia Desktop Endpoint Security; Proventia Internet Scanner; Proventia Network Enterprise Scanner; Proventia Mail Filter; Proventia Network Mail Security System; Proventia Web Filter; Proventia Management SiteProtector, SiteProtector Reporting Module; SiteProtector SecurityFusion Module; SiteProtector Third Party Module.

2.4 La gestione degli eventi di sicurezza

Come è apparso chiaro nella descrizione delle varie tecnologie di protezione, inizialmente queste sono nate per rispondere a specifiche esigenze. In generale, l'approccio che si è sviluppato è quello di "silos" separati, che, se si vuole, in parte andavano a ricalcare l'organizzazione stessa dei sistemi informativi: ogni area facente storia a sé e sviluppata indipendentemente dalle altre o quasi. Nella realtà dei fatti, l'approccio "difensivo" è rimasto ancora lo stesso: ogni tipo di minaccia o metodo di attacco viene affrontato da una soluzione ad hoc, gestita separatamente dalle altre. Questo approccio è stato del resto favorito dalla sua corrispondenza con la logica del "best of breed" applicata tipicamente dalle grandi imprese.

Il nuovo scenario disegnato da minacce ibride e attacchi mirati rende questo il sistema dei silos inefficace, inefficiente e finanche del tutto inutile, pur rimanendo estremamente costoso. Non a caso, dunque, si è assistito al proliferare sul mercato di una nuova tipologia di prodotti e soluzioni, nota con l'etichetta di Unified Threat Management (UTM). Nella maggioranza dei casi, però, si tratta di "pure" operazioni di "make up", comunque in grado di apportare diversi vantaggi soprattutto per le piccole imprese, ma che non permettono di superare la limitazione dei silos.

IBM ISS è stata una delle prime società a immettere sul mercato un'appliance multifunzione e la prima a inserirvi le funzionalità di intrusion prevention reale, cioè con la capacità di bloccare automaticamente i flussi di traffico maligno, e la prima a garantire una pre-emptive protection gestita.

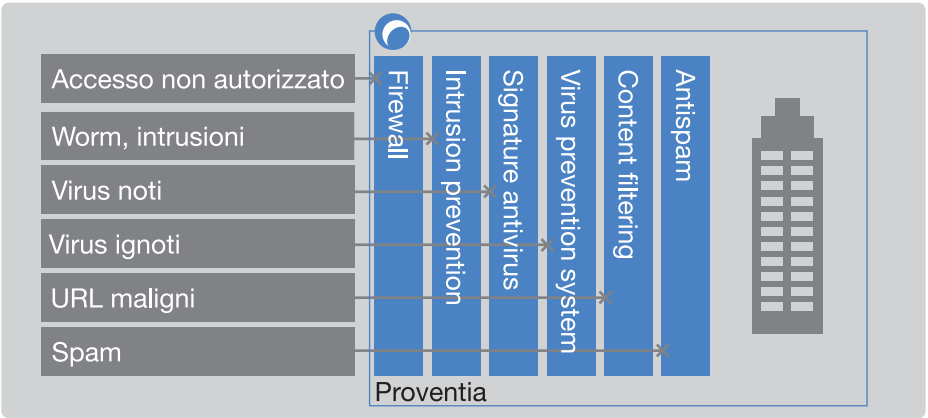


Figura 2.8
La protezione multilivello realizzata dall'UTM Proventia Network MFS di IBM ISS

Due gli elementi architetturali che costituiscono i punti di forza della soluzione: innanzitutto, il parallelismo dei controlli, che evita i continui disassemblaggi e riassemblaggi dei pacchetti salvaguardando le prestazioni pur con tutti i controlli attivi. In secondo luogo, ma non meno importante, l'appartenenza alla Enterprise Security Platform e, dunque, la disponibilità dell'intelligenza necessaria per rispondere alle sollecitazioni del sistema di gestione centrale, che analizza e corrrela in tempo reale tutte le informazioni registrate dall'apparato. Se per una piccola impresa l'UTM può essere sufficiente, il suo impiego in un sistema complesso risulta efficace ed efficiente e perfettamente integrato nel sistema di gestione degli eventi di sicurezza.

Quest'ultimo è il vero cuore di qualsiasi sistema di sicurezza, tanto più di un sistema integrato, come deve essere il modello attuale. Al centro di tutto, infatti, deve esserci una logica di gestione della sicurezza, che deve essere affidata a personale sempre più esperto, da un lato, e che deve essere supportata da strumenti intelligenti dall'altro. Per questo, le soluzioni appartenenti alla IBM ISS Protection Platform sono tutte gestibili dalla stessa console e, soprattutto, sono tutte dotate di intelligenza sufficiente a intervenire quando la situazione lo richiede.

Per aumentare ulteriormente il livello di sicurezza, IBM ISS offre tutto questo sotto forma di servizi, permettendo alle imprese di ogni dimensione di scegliere "on demand" il proprio sistema di sicurezza adattandolo dinamicamente alle esigenze del proprio business o alle mutevoli condizioni di sicurezza su Internet, grazie alla possibilità di aggiungere, togliere e modificare il paniere di servizi sottoscritti.

È questa logica dinamica e proattiva che fanno di IBM ISS un punto di riferimento per la sicurezza e la protezione dalle minacce di ieri, oggi e domani.

Sul fronte della gestione operativa, la complessità di un sistema per la sicurezza impone un management accurato e un'attività di controllo continua. Questo anche nel caso si attivino automatismi, auspicabili comunque per rispondere in tempo reale agli attacchi ormai rapidissimi, adeguando immediatamente il livello di protezione a fronte di una minaccia concreta. È evidente che in un simile contesto è pressoché d'obbligo implementare una gestione centralizzata della sicurezza. Attraverso un'unica console, preferibilmente Web based affinché sia svincolata da un luogo fisico e accessibile da una qualsiasi postazione, è possibile controllare tutto l'insieme di soluzioni e funzionalità distribuite ai vari livelli del sistema informativo. Solo in questo modo, del resto, è possibile raccoglie-

re tutte le informazioni in tempi appena accettabili per rispondere rapidamente a eventuali tentativi d'intrusione o ad altri problemi di sicurezza, impostando immediatamente nuove regole e privilegi applicabili a tutta la struttura aziendale.
La gestione centralizzata, dunque, deve consentire rapidi e appropriati interventi per modificare le impostazioni di sicurezza in relazione ai cambiamenti di esigenze. Una funzione che può essere attuata solo sulla base di un monitoraggio continuo e sulla flessibilità e semplicità nella definizione delle security policy. Quest'ultima, inoltre, deve essere abbinata a strumenti di enforcement, che ne garantiscano l'applicazione. Una gestione accurata della sicurezza permette anche di controllare i costi e ottimizzare l'utilizzo delle risorse, migliorando ulteriormente il TCO.
Altra caratteristica importante per un sistema centralizzato è quella di poter considerare le esigenze in modo flessibile: in altre parole, è opportuno poter considerare un approccio trasversale ai vari dipartimenti aziendali e uno puntuale per ciascuno di questi. I singoli dipartimenti, infatti, hanno propri specifici bisogni in termini di integrità, riservatezza e disponibilità dell'informazione. Nel gestire la sicurezza bisogna considerare tutti questi aspetti, ma anche seguire un approccio orientato all'amministrazione di risorse umane e tecnologiche, nonché logistiche ed economiche, per garantire un adeguato livello di protezione. In questo senso, per esempio, vanno le logiche di Protection on Demand di IBM ISS, che consentono di affidarsi a servizi MSS (Managed Security Service) in maniera assolutamente flessibile. È possibile recuperare le competenze che non si hanno in azienda o che è troppo costoso replicare, per effettuare un monitoraggio 24x7x365.
Gestire la sicurezza, con un approccio orientato a una vera e propria governance manageriale, peraltro, significa organizzare i processi legati alla sicurezza direttamente e indirettamente, affinché possano produrre informazioni significative e soprattutto servibili ai manager. A tal riguardo, per esempio, si consideri che un firewall è certamente in grado di registrare ogni evento di traffico, ma in un'azienda media questo si quantifica in decine di migliaia di eventi al giorno: un monitoraggio manuale diventa praticamente impossibile.
Gli aspetti che vanno in ogni caso considerati sono quattro:

- la gestione delle vulnerabilità (almeno per quanto riguarda i requisiti minimi su cosa fare quando per un sistema in produzione viene annunciata una vulnerabilità);

- la rilevazione degli eventi con uno standard che consenta di unificarne la gestione;
- la log retention, che significa potersi riservare anche in un secondo momento di controllare le registrazioni;
- le policy di incident response.

Tra l'altro, gli ultimi due punti sono fondamentali anche per quanto riguarda la compliance e relativi auditing e le eventuali esigenze d'indagine forense in caso d'incidente.
La logica d'impostazione legata alla governance deve necessariamente appoggiarsi a una console centralizzata, anche perché oggi non è possibile limitarsi a considerare solo gli aspetti legati al controllo degli accessi. Già questi devono essere protetti con l'integrazione di più strumenti quali firewall, anti-virus e i sistemi di rilevamento delle intrusioni, ma la visione sulla sicurezza deve essere ampliata e considerare anche altri strumenti, pure integrati per l'identity management, l'autenticazione dell'utilizzatore, il configuration management, la gestione degli eventi e delle vulnerabilità e la risposta agli incidenti.
Infine, un elemento fondamentale è la possibilità di misurare i risultati. Solo in questo modo, in particolare, si possono introdurre le migliorie eventualmente necessarie per adeguare il livello di protezione. La flessibilità degli strumenti per il management dei sistemi è cruciale in questo contesto: non basta infatti definire un livello di sicurezza e pensare che questo sia fissato e mantenuto inalterato nel tempo. Le condizioni esterne sono mutevoli e la protezione interna deve essere pronta ad adattarvisi. Gli strumenti di gestione devono essere efficaci ed efficienti per operare i cambiamenti necessari.

2.4.1 Security Management centralizzato

L'approccio agli aspetti gestionali di IBM è sempre stato molto avanzato. Già IBM ISS, sin dalla prime release di un sistema di management, realizzò un modulo per il supporto alle decisioni in tema di sicurezza. È infatti questo il nocciolo primario della questione: il log anche di un singolo sistema di sicurezza è faticoso da gestire, per un banale fattore quantitativo. Se si considera che la sicurezza deve prevedere l'integrazione di più dispositivi, s'intuisce che i log vengono istantaneamente moltiplicati per tanti quanti sono i sistemi attivi. Ma non solo: la natura ibrida delle minacce e l'utilizzo di più tecniche per sferrare gli attacchi impone che i singoli eventi vengano analizzati in maniera incrociata. In altre parole che siano correlati.

A questo problema, inoltre, si aggiunge la necessità di coprire due differenti punti di vista: da un lato occorre un cruscotto che fornisca in tempo reale la situazione in termini di risposta agli incidenti e livello di sicurezza, dall'altro è pure fondamentale avere con un colpo d'occhio il quadro relativo al rispetto della compliance. Grazie all'integrazione delle soluzioni per il security ed event management di IBM ISS e IBM Tivoli e, in particolare, grazie a Tivoli Security and Compliance Insight Offering, IBM permetterà di avere una gestione unificata e centralizzata di tutti gli aspetti legati alla sicurezza.
La soluzione di IBM ISS per la gestione, l'analisi e il monitoraggio della sicurezza è Proventia Management SiteProtector. Il primo immediato beneficio che apporta a una organizzazione consiste nel fatto che unifica la gestione delle soluzioni per la sicurezza distribuite su più livelli di un'infrastruttura informatica, dai gateway ai dispositivi di rete, agli host, dai sistemi di intrusion detection e prevention alle connessioni VPN.
Il secondo, non meno importante vantaggio, discende dalle funzionalità aggiunte dal modulo SiteProtector SecurityFusion, che, in sintesi, è il motore di correlazione degli eventi. In primo luogo, vengono raccolti tutti i log e gli eventi registrati collegati alla sicurezza, anche grazie all'integrazione trasparente con il software per la gestione IBM Tivoli Security Operations Manager (TSOM). Giunto alla versione 4.1, questo fornisce funzioni nuove e migliorate per gestire gli incidenti di sicurezza IT in modo più efficiente:

- Gestione e configurazione semplificate e miglioramenti di utilizzo per ridurre il tempo e le risorse necessarie per implementazioni e gestione tramite un'interfaccia dei dispositivi centralizzata e semplificata e una nuova funzione di configurazione automatica dell'origine degli eventi.
- Infrastruttura di correlazione e filtro degli eventi migliorata per offrire maggiore flessibilità con funzioni e prestazioni superiori.
- Attività di sicurezza migliorate, interfaccia utente dashboard con maggiore personalizzazione e nuove funzioni di analisi della sicurezza.
- Gestione dei casi ed etichettatura degli incidenti estese.
- Strumento di ricerca host migliorato per identificare e risolvere gli incidenti.
- Supporto di piattaforma esteso ed aggiornato, inclusi DB2, AIX e il supporto completo di globalizzazione e internazionalizzazione.
- Integrazione con Tivoli Compliance Insight Manager per fornire una soluzione completa SIEM (Security Information and Event Management).

2.5 I servizi per la sicurezza

La complessità dei sistemi di sicurezza e la necessità di mantenere il controllo 24 ore su 24 rendono la gestione dell'ICT Security un processo molto oneroso per le imprese. Soprattutto se si considerano gli alti costi di formazione di un personale qualificato e altamente specializzato, che deve mantenersi costantemente al passo con i tempi, magari confermando diverse certificazioni ogni anno. Sono questi alcuni dei driver che determinano il successo dei cosiddetti Managed Security Service. A rendere gli MSS appetibili per imprese di ogni dimensione, concorrono anche altri benefici aggiuntivi, come la garanzia di un livello sempre massimo dell'aggiornamento tecnologico e di una flessibilità del servizio. Fino all'estrema adattabilità della security on demand.

2.5.1 Il Virtual SOC e la Protection on Demand

Un manager responsabile e attento non discute sulla necessità di una sicurezza sofisticata ed efficiente, la dà per scontata. Questo a maggior ragione in presenza di leggi e regolamenti nazionali e internazionali che prescrivono l'obbligo ad adottare soluzioni di sicurezza per la protezione dei dati sensibili e la continuità del business, a fronte di precise responsabilità penali per i responsabili aziendali e di multe che, come nel settore finanziario, possono risultare anche molto severe. Resta il problema di come gestirne la complessità, il suo realizzarsi in pratica e la sua gestione e, soprattutto, del come ridurre tale complessità, prevenire gli attacchi e dimostrare al proprio interno e agli enti di certificazione quella che viene riferita come "due diligence".
La soluzione può consistere nell'adottare una politica focalizzata sui Managed Security Services, come quelli sviluppati da IBM Internet Security Systems, che permettono ad aziende grandi e piccole di disporre in modo rapido e immediato delle più sofisticate e aggiornate metodologie e livelli di protezione presenti sul mercato. Questo senza doversi dotare di un complesso know how o rimuovere preziosi collaboratori da altre attività interessanti il core business dell'azienda.
I servizi di IBM Internet Security Systems vengono erogati tramite diversi centri operativi distribuiti nel mondo in tutti i continenti, così da garantire l'assoluta disponibilità dei servizi anche in caso di disastri ambientali o terroristici particolarmente pesanti. All'utente, i centri si presentano come un unico e grande Security Operation Center (SOC) virtuale che ha il compito di erogare i servizi.

Il Virtual SOC rappresenta quindi il motore che sta alla base dei Managed Security Service e della piattaforma Protection on Demand e combina capacità evolute di analisi e di correlazione degli eventi, intelligenza artificiale, esperti nella sicurezza di levatura mondiale e il VIrtual SOC Portal, un portale appunto per la una gestione Web based dei servizi richiesti.
Dall'inizio del 2005, IBM Internet Security Systems ha esteso notevolmente l'offerta di servizi, aprendosi al mercato e ai sistemi di terze parti. In breve tempo, la percentuale di piattaforme gestite appartenenti ad aziende diverse da IBM ISS ha superato il 40% andando a coprire praticamente tutte le tecnologie di sicurezza e non solo firewall e intrusion detection. Per ampliare la portata dei propri servizi, IBM ha potenziato ulteriormente i propri SOC, che sono otto. Tutti i centri sono ridondati, autonomi ma interconnessi e operativi 24 ore al giorno per sette giorni la settimana, in modo da garantire la continuità del servizio e assicurare il livello di servizio previsto dal contratto, con il passaggio trasparente delle chiamate utente su un altro centro nel caso di congestione del traffico.

Uno dei vantaggi del Virtual SOC di IBM ISS è la possibilità di combinare tecnologie d'eccellenza per ottenere un sistema di sicurezza articolato per un elevato livello di protezione. In questo senso è un elemento costituente della piattaforma per la Protection on Demand. Altro elemento fondamentale di quest'ultima è l'Enterprise Security Platform e la possibilità, conferita da quest'ultima di attivare, per esempio, una particolare azione, come il blocco totale del traffico da parte di un firewall, in funzione di un allarme generato da un'analisi in tempo reale di più eventi registrati.
L'architettura aperta della piattaforma consente a IBM ISS di inserirvi anche prodotti di terze parti e di articolare i servizi in base alle specifiche esigenze di ciascuna impresa attraverso il Virtual SOC, cui chiedere i servizi che di volta in volta si ritengono necessari, tra l'altro con la possibilità di integrarlo con altri processi IT aziendali, quali il call center/help desk o il workflow management.
La grande potenzialità espressa dal Virtual SOC è frutto di una solida architettura basata su una rete estesa di sistemi intelligenti e processi che abilitano un'integrazione continua tra i Managed Security Service di IBM ISS e i Security Enablement Service erogati attraverso il Virtual SOC Portal. Questa integrazione fornisce alle imprese le informazioni, il supporto decisionale, gli strumenti e la capacità che necessitano per

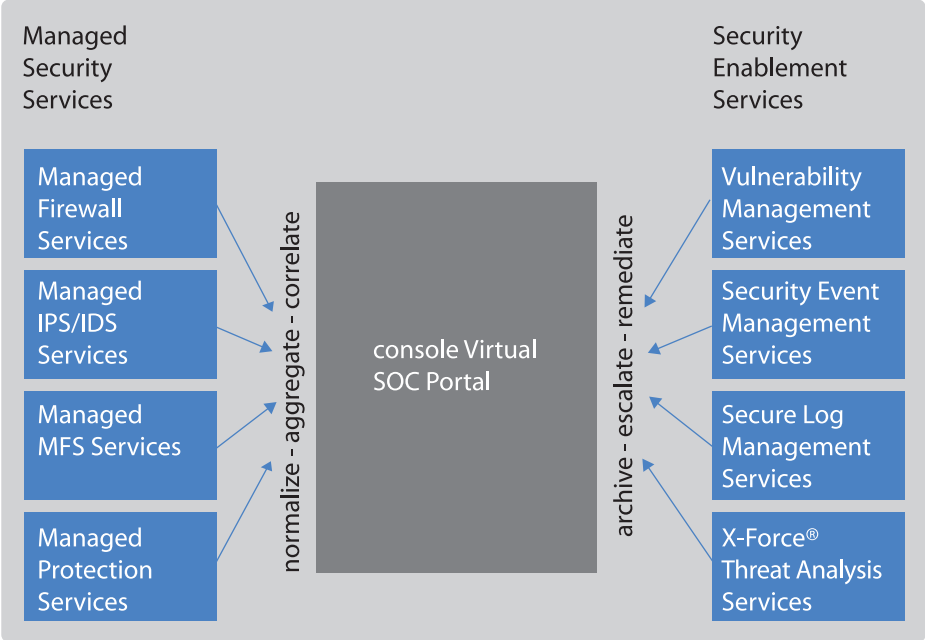


Figura 2.9
L'architettura del Virtual SOC di IBM Internet Security Systems

prendere decisioni in tempo reale richieste per attuare azioni immediate. Azioni che possono essere attivate in maniera automatica, sfruttando l'intelligenza delle soluzioni e dei servizi messi a disposizione da IBM ISS.

La flessibilità con cui possono essere richiesti i servizi è l'essenza della Protection on Demand ed è frutto dell'integrazione realizzata dalle funzionalità fornite con il Virtual SOC Portal. Il concetto di base è che l'eterogeneità dei diversi sistemi, che compongono e caratterizzano l'Open Vendor Architecture del Virtual SOC, viene uniformata dal portale: per esempio, l'insieme di log che in un sistema best of breed è necessario analizzare uno a uno, ciascuno impostato secondo la logica del produttore specifico e ciascuno attraverso l'interfaccia del proprio system manager, è presentato in maniera omogenea all'interno di un unico tool di analisi. Non solo, perché un potente motore di correlazione avrà già esaminato l'estesissima mole di informazioni, presentandole in funzione di una priorità reale, semplificando enormemente l'interpretazione. Inoltre, nel caso del servizio di Managed Protection erogato da IBM ISS, tali decisioni possono essere demandate a esperti costantemente davanti al monitor e, sfruttando l'intelligenza delle engine integrate nell'Enteprise Security Platform di IBM ISS, possono essere automatizzate (comunque in base a policy precise) perché rispondano in tempo reale ai cambiamenti delle condizioni di sicurezza sulla Rete.

Protection on Demand e flessibilità

La protezione su richiesta permette di:

- Selezionare esclusivamente la tecnologia e i servizi necessari
- Gestire solamente le problematiche desiderate, quando lo si desidera e nel modo più adatto alle proprie esigenze
- Avere un impegno economico esclusivamente per i servizi effettivamente utilizzati

Permette altresì di controllare la propria sicurezza e ottimizzare l'utilizzo delle risorse:

- In ogni momento: nell'ora di picco delle attività, nelle ore di normale attività, su base giornaliera, durante le ore notturne o nei fine settimana.
- In ogni modo: con modalità In-house, in outsourcing o con un mix di entrambe le modalità
- In ogni luogo: per aree e per dispositivi, globalmente, remotamente.

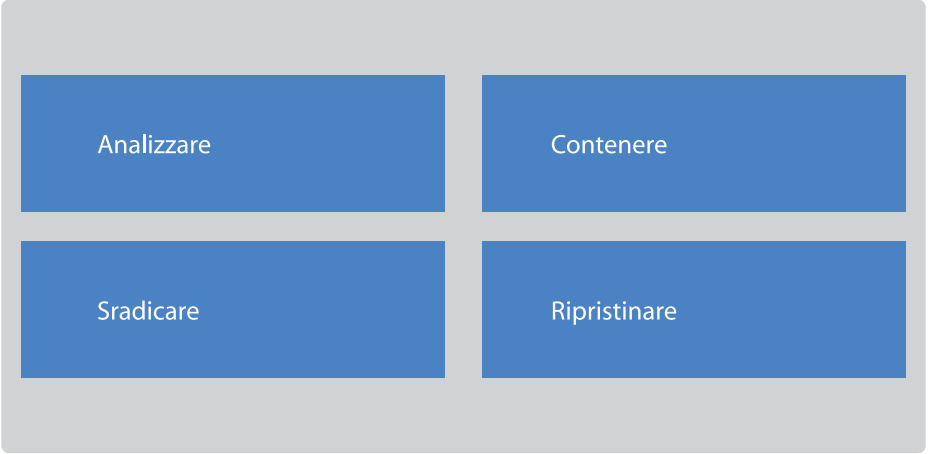
La Protection on Demand, dunque, fornisce una capacità di adattamento dei servizi che rende il sistema di sicurezza in grado di garantire risposte alle esigenze mutevoli di un'azienda. Per esempio, in termini di prestazioni, un simile approccio conferisce maggiore dinamicità, permettendo di adattare nel tempo le caratteristiche del sistema alla realtà aziendale. Con la Protection on Demand è facile verificare in dettaglio le prestazioni, riducendo inoltre il total cost of ownership.

2.5.2 I Managed Security Service di IBM Internet Security Systems

I servizi per la sicurezza offerti da IBM Internet Security Systems spaziano da quelli più tradizionali, quali la gestione e il monitoraggio di specifici prodotti, fino alla protezione completa di tutta la rete e i sistemi aziendali, applicando il concetto della Protection on Demand.
Servizi di base sono dunque Managed e Monitored Firewall Service e Managed Intrusion Detection e Prevention Service. Più avanzato e unico è il servizio X-FTAS (X-Force Threat Analysis Service): un servizio d'intelligence sulla sicurezza che fornisce informazioni personalizzate su una vasta gamma di minacce. In sostanza, si tratta di un servizio di advisor, il cui scopo è di contribuire alla protezione preven-

tiva delle reti aziendali tramite analisi dettagliate dello stato generale delle minacce online.
Una caratteristica essenziale del servizio X-FTAS è che è stato pensato in modo da essere facilmente adattabile al particolare ambiente aziendale. Ciò garantisce che gli utilizzatori del servizio ricevano esclusivamente le informazioni che risultano attinenti alla propria rete. Il servizio comprende anche la disponibilità di strumenti che consentono di specificare le piattaforme, i prodotti, le applicazioni, i settori di attività e le aree geografiche che interessano al cliente, così come il formato in cui desidera ricevere gli aggiornamenti quotidiani. Il servizio, oltre a far parte di numerose delle piattaforme comprese nei Managed Security Services è anche utilizzabile separatamente sottoscrivendo un abbonamento annuale.
Il Vulnerability Management Service, invece, è specificatamente pensato per fornire la gestione delle vulnerabilità, più precisamente, viene realizzato tramite un insieme di soluzioni che permettono di scoprire le vulnerabilità esistenti nelle applicazioni e nei processi aziendali, assegnare le priorità agli interventi in caso di attacchi, attuare le azioni di remediation, ottenere una protezione dinamica, verificare i risultati degli interventi di protezione, produrre report personalizzati. In particolare, è possibile disporre anche di rapporti personalizzabili atti a dimostrare la compliance con regolamenti industriali, nazionali o sovranazionali quali la Sarbanes-Oxley, HIPAA, SCADA, Gramm-Leach-Bliley o le normative più recenti quali lo standard Payment Card Industry (PCI) specifico del mondo finanziario.
Un insieme di servizi costituiscono la piattaforma “Security Event and Log Management” (SELM), che fornisce alle aziende gli strumenti atti a mantenere continuamente sotto controllo la sicurezza aziendale e che a tal fine comprende funzioni per la raccolta di dati ed eventi connessi alla sicurezza, per l’analisi di dati e per fornire una risposta rapida agli attacchi dell’asset dell’azienda.
Un ulteriore servizio è quello di risposta alle emergenze nell’ambito della sicurezza “Emergency Response Services” (ERS), che permette di rispondere in modo adeguato agli incidenti, di realizzare piani per fronteggiare gli attacchi e la conduzione di analisi forensi valide a fini legali. Il team ERS comprende esperti che adottano sofisticate e consolidate metodologie di intervento e di analisi e che sono disponibili, sia in base a sottoscrizione del relativo servizio che su richiesta, per rispondere molto rapidamente ad attacchi in atto ventiquattrore al giorno e per tutti i trecentosessantacinque giorni annui.

Figura 2.10
La strategia di risposta a un attacco dei team ERS di IBM ISS



I consulenti IBM ISS sono in grado di supportare in problematiche penali, civili e amministrative che derivino da falle nei propri sistemi di sicurezza. Il supporto include l'assistenza delle organizzazioni aziendali negli esami forensi di evidenze digitali o di media nelle seguenti aree: investigazioni su impiegati o interni; consultazioni ed esami preventivi; rilevamento di evidenze elettroniche; supporto testimoniale di esperti.

3
Identity and access management

L’identità elettronica di ciascun individuo assume un’importanza crescente nel Terzo Millennio. La sua gestione efficiente da parte delle imprese è un problema di ottimizzazione prima ancora che di sicurezza. Un approccio corretto prevede l’integrazione delle diverse aree dipartimentali coinvolte nel processo di definizione delle varie caratteristiche inserite nel profilo utente. È quindi necessario stabilire con precisione le responsabilità in termini di sicurezza per quanto concerne tali caratteristiche e i privilegi di accesso che devono essere riconosciuti a ciascun individuo.

3.1 Una gestione completa della protezione aziendale

La gamma di soluzioni software IBM Tivoli realizza un approccio consistente e unificato per rendere sicuri gli ambienti di e-business cross-enterprise. La strategia in base alla quale è stato sviluppato il software Tivoli interviene su più fronti per garantire alle aziende il raggiungimento di questi obiettivi.
Innanzitutto, le soluzioni di sicurezza Tivoli sono costruite su standard aperti che rappresentano l'elemento abilitante per un'integrazione sicura tra piattaforme eterogenee, multivendor e tra differenti organizzazioni enterprise.
Inoltre Tivoli dispone di un'offerta a supporto di tutti i meccanismi alla base dei servizi di identità e basati su Web Service, garantendo l'integrazione trasparente con una varietà di piattaforme per lo sviluppo e il deployment di Web Services come IBM WebSphere, Microsoft .NET e così via.
Le soluzioni software Tivoli sono pensate per innestarsi negli ambienti di sicurezza Web esistenti all'interno delle aziende, favorendo una rapida evoluzione indirizzata a consentire di trarre il massimo vantaggio dalle tecnologie dei Web Service e dagli standard federativi. Grazie a un approccio innovativo, le soluzioni Tivoli consentono di implementare una gestione efficace dell'identità e di costruire su di essa sofisticate soluzioni per la gestione dell'accesso extranet e per il *trust management*.
Le soluzioni Tivoli sono state sviluppate per affrontare in modo integrato tutte le aree che concorrono a garantire la protezione dell'azienda e dei suoi asset. L'approccio Tivoli prevede una fase di assessment indirizzata a verificare il livello di protezione presente in azienda, che favorisce la comprensione delle problematiche da affrontare e apre la strada all'implementazione di soluzioni per la protezione preventiva del perimetro aziendale.
Il controllo di accesso agli asset dell'organizzazione enterprise è un altro tassello fondamentale che viene garantito dalle soluzioni Tivoli, nell'ottica di una strategia per la protezione completa dell'azienda.
Attraverso uno dei più ampi portafogli di offerta IBM permette di implementare sofisticate soluzioni per la gestione e il controllo delle identità degli utenti e per i privilegi di cui dispongono. Inoltre, permette di estendere la gestione anche all'accesso alle risorse presenti in azienda e di prevedere la creazione e l'applicazione di sofisticate regole in base alle quali gestire in modo ottimale l'accesso ed esercitare un controllo puntuale verificando ruoli e privilegi.
Tutte queste attività sono sottoposte a pratiche di monitoraggio continuo che permettono di verificare che le misure di protezione adottate rispondano ai requisiti aziendali e siano conformi alle normative e di attuare, di conseguenza,

tutte le eventuali azioni correttive, in modo da realizzare un ciclo virtuoso indirizzato a predisporre un livello di protezione aziendale della massima efficacia.

3.2 Identity and access management

La diffusione attraverso il Web o le reti aziendali di dati ad alto valore, collegati a transazioni, all'accesso ad applicazioni e a processi di business che prevedono il trasferimento di informazioni sensibili, ha accresciuto l'importanza di possedere un'identità digitale sicura che consenta al security manager di esercitare un controllo efficace sull'accesso a informazioni e servizi senza penalizzare, peraltro, la produttività individuale.
La possibilità di gestire in modo rapido e semplice l'identità digitale degli utenti rappresenta il requisito necessario per poter esercitare un controllo sull'accesso alle risorse basato su policy e personalizzato in funzione dei diversi livelli di privilegio dell'utente.
L'importanza crescente per questo tipo di tecnologie e soluzioni è alimentato dalla presenza di informazioni critiche (in formato digitale) per il successo di un'azienda e dalla progressiva affermazione dei Web Service come modalità di erogazione di servizi on-demand.
Occuparsi di identity e access management non significa, pertanto, parlare di un prodotto, ma prevedere, invece, una serie di modalità, regole, processi che si appoggiano su tecnologie e architetture specifiche e su un'infrastruttura di supporto per la creazione, il mantenimento e l'utilizzo di identità digitali.
In alcuni casi l'identity management può diventare un vero e proprio business strategico, poiché permette di fornire una risposta a problemi fondamentali per la realizzazione e la distribuzione di risorse, informazioni e servizi ed è in grado di impattare direttamente su brand, modelli di business, riduzione dei rischi e profitti. D'altra parte, l'accesso non autorizzato alle informazioni aziendali rappresenta una minaccia crescente per la sicurezza aziendale le cui ripercussioni sul business diventano sempre più importanti.

3.3 Gestire il ciclo di vita dell'identità

La gestione dell'identità è un processo che richiede dedizione e che va affrontato e revisionato con continuità a livello operativo e strategico.
In un'ottica di conseguimento degli obiettivi di business la gestione dell'identità va, quindi, affrontata in un'ottica di gestione del suo intero ciclo di vita e di integrazione.

Per queste ragioni le organizzazioni devono avere risposte certe su “chi, cosa, quando e dove” in merito all’accesso alle risorse fisiche e logiche presenti sia all’interno sia all’esterno della struttura enterprise per tutto il tempo di validità delle informazioni e dei privilegi coinvolti nel processo.
Questo obiettivo è conseguibile unicamente attraverso una strategia unificata che preveda l’adozione di soluzioni di identity management e access control.
IBM ha predisposto una strategia unificata per l’enterprise security basata su soluzioni modulari, economiche e di semplice utilizzo per il controllo dell’accesso e l’identity management, grazie alle quali è possibile gestire l’intero ciclo di vita delle tematiche associate all’identità garantendo, nel contempo, la sicurezza e il rispetto della compliance e dei requisiti di business.
A supporto di questo approccio strategico IBM mette a disposizione tutte le soluzioni di sicurezza che permettono alle aziende di valutare il proprio livello di protezione e di coprire tutti gli aspetti a partire dall’analisi delle minacce fino al monitoraggio proattivo per eliminare possibili vulnerabilità.
Alle soluzioni software e alle tecnologie IBM aggiunge caratteristiche di competenza tecnica ed expertise uniche al mondo, potendo vantare una presenza globale di otre 3500 esperti nella sicurezza e privacy, cui si affianca una rete di Business Partner in grado di sostenere le aziende per rispondere in tempi rapidi e in modo appropriato a violazioni di sicurezza, minacce e obblighi di conformità.
IBM è anche protagonista nell’innovazione e dispone di oltre 100 brevetti in prodotti e tecnologie legati all’identity management.
Non da ultimo si avvale di competenze trasversali e allargate in praticamente ogni settore dell’IT potendo predisporre soluzioni per problematiche complesse che riguardano i più disparati segmenti di mercato e di azienda.
L’approccio perseguito da IBM mira a supportare la governance e il risk management allineando policy IT, processi e progetti con gli obiettivi di business.
Per farlo fornisce un insieme di servizi, software e hardware, che consentono di pianificare, eseguire e gestire iniziative di ogni tipo con un approccio modulare che si adatta alle esigenze di aziende di ogni dimensioni, aiutando i propri clienti a implementare la corretta soluzione IT per ottenere rapidi traguardi di business e diventare partner strategici nel processo di crescita e sviluppo del loro business.
La sinergia tra l’offerta software IBM Tivoli, gli IBM Identity and Access Management Services e l’attività degli IBM Business Partner, si concretizza in una gamma di soluzioni di sicurezza che forniscono funzioni integrate di identity management e access control le quali consentono di:

- ridurre i rischi di frode o furto
- favorire la collaborazione tra dipendenti, fornitori e partner
- ridurre i costi operativi legati alla gestione dell'identità e alla sicurezza
- massimizzare l'utilizzo e la profittabilità per il business e i partner
- semplificare i processi di audit e di compliance all'interno di ambienti eterogenei.

3.3.1 Identity proofing

L'Identity proofing consente di fornire un livello di protezione a commercianti e consumatori coinvolti in una transazione online.
Per questa ragione, sempre più spesso le banche e i retailer che operano online stanno incrementando il livello di utilizzo di questa tecnologia come metodo per la prevenzione delle frodi.
L'Identity proofing nasce dal concetto che, prima di fornire a qualcuno una password o di creare un account on line a suo nome sia necessario verificare che questi sia veramente chi afferma di essere. Questo momento di primo contatto rappresenta, in realtà, un grosso punto debole nella catena di autenticazione predisposta oggigiorno da molti retailer che operano online e da molte aziende che forniscono servizi finanziari. Attraverso le soluzioni Tivoli IBM permette di rispondere anche a problematiche di questo tipo.

3.4 Le soluzioni Tivoli per l'Identity and Access Management

All'interno del brand Tivoli, IBM mette a disposizione delle aziende una gamma di software per la gestione delle minacce, l'access management, la compliance, il provisioning automatico dei software e la Web security fornendo ai manager un unico centro di controllo per la gestione centralizzata degli account, l'impostazione delle regole di accesso e la definizione dei meccanismi di modifica.

IBM Tivoli Identity Manager

È la soluzione pensata per abilitare l'accesso sicuro e flessibile a dipendenti, clienti, business partner e fornitori. Questa soluzione software stabilisce un controllo dell'accesso centralizzato e basato su policy e consente di effettuare l'audit attraverso i principali sistemi presenti in azienda. Alle aziende enterprise, permette di automatizzare la creazione di nuovi "account" e di fornire all'utente finale funzioni autonome per la gestione delle identità.

IBM Tivoli Access Manager for e-business

È il software pensato per gestire la crescita e la complessità, controllare i costi associati e risolvere i problemi nell'implementare policy di sicurezza attraverso un'ampia gamma di risorse Web e applicazioni. Questa soluzione permette di definire e gestire l'autenticazione centralizzata e le policy di accesso e di audit per un'ampia serie di iniziative di business; inoltre provvede ad abilitare funzionalità di Single Sign-On (SSO) nei confronti di applicazioni Web che interagiscono su più siti o domini.

IBM Tivoli Access Manager for Enterprise Single Sign-On

La soluzione mette a disposizione funzionalità di autenticazione SSO attraverso le applicazioni in modo tale che l'utente non è più obbligato a memorizzare credenziali di accesso e password. Inoltre, permette di rafforzare la sicurezza aggirando eventuali comportamenti inefficaci o superficiali da parte dell'utente nella gestione delle sue credenziali e password. Questa soluzione contribuisce a ridurre i costi di help desk dell'IT riducendo il numero di chiamate per il reset delle password oltre a estendere le funzionalità di reporting e di audit. Quando opera congiuntamente a *IBM Identity and Access Management Services for Strong Authentication*, la soluzione contribuisce a valorizzare gli investimenti fatti dall'aziende nelle tecnologie di SSO. Tivoli Access Manager for Enterprise SSO è in grado di supportare differenti tipologie di autenticazione dell'utente che spaziano da password a smart card a soluzioni biometriche.

IBM Tivoli Access Manager for Operating Systems

È un sistema di sicurezza in grado di bloccare applicazioni business-critical, dati, files e piattaforme operative per prevenire l'accesso non autorizzato quando si verificano determinate condizioni. Questa soluzione è in grado di bloccare l'accesso ai dati da parte sia di chi accede dall'interno dell'azienda sia dall'esterno. Tivoli Access Manager for Operating Systems permette anche di inibire le modifiche alla configurazione di applicazioni chiave e controlla e tiene traccia dell'accesso alle altre applicazioni, in modo da consentire il controllo su qualsiasi eventuale modifica. Inoltre, garantisce funzioni di audit sulle attività svolte a livello applicativo e di piattaforma, combina sistemi di protezione di intrusion prevention, host-based firewall e fornisce funzioni di "Persistent Universal Auditing" per la compliance dei documenti rispetto alle normative e alle policy di livello corporate.

3.5 Gli IBM Identity and Access Management Service

Gli IBM Identity and Access Management Service comprendono servizi quali Identity Lifecycle Management e Access Management che sono stati sviluppati da IBM con l'obiettivo di assistere le aziende nello sfruttare in pieno le suite software IBM Tivoli dedicate alla gestione dell'identità e dell'acceso.

Questa offerta di servizi mette a disposizione una serie di soluzioni versatili per la risoluzione dei problemi di autenticazione e autorizzazione, che spaziano dalle funzionalità base di SSO fino al deployment di infrastrutture di sicurezza più complesse.

Gli IBM Identity and Access Management Services mettono a disposizione attività di consulenza, supporto e altri servizi per aiutare le aziende a gestire la complessità, controllare i costi e far fronte all'esigenza di implementare policy di sicurezza in ambienti distribuiti.

Questi servizi sono realizzati in modo da garantire la gestione dell'intero ciclo di vita delle identità in modalità end-to-end, consentendo di prevedere gestione automatizzata degli account e dei diritti di accesso lungo l'intero ciclo di vita e anche di realizzare scenari dimostrativi sull'impatto legato alle proposte di modifica delle policy.

Tabella 3.1
I principali prodotti che costituiscono l'offerta Tivoli per l'identity e access management

AREA DI INTERVENTO	PRODOTTO
Gestione del ciclo di vita dell'identità	IBM Tivoli Identity Manager IBM Tivoli Identity Manager Express
Gestione degli accessi e Single Sign-On in ambito Web	IBM Tivoli Access Manager for e-business
Federazione delle identità e gestione della sicurezza dei Web service	IBM Tivoli Federated Identity Manager IBM Tivoli Federated Identity Manager Business Gateway
Gestione del Single Sign-On per tutte le tipologie di applicazione (client, emulatore, Web)	IBM Tivoli Access Manager for Enterprise Single Sign-On
Gestione avanzata degli accessi ai sistemi operativi di tipo Linux e Unix	IBM Tivoli Access Manager for Operating Systems

Alcuni esempi degli ambiti in cui gli IBM Identity and Access Management Services intervengono in un'ottica di identity lifecycle management includono:

- Identity assessment and strategy
- Identity proofing
- Identity life-cycle management
- Directory services
- Access management
- Soluzioni di strong authentication

Gli IBM Identity and Access Management Services non si appoggiano unicamente sulla robusta offerta di IBM, ma anche su tecnologie avanzate messe a disposizione dagli IBM Business Partner che sono in grado di sviluppare specifiche funzionalità indirizzate all'identity management in grado di adattarsi a specifiche esigenze aziendali.

3.6 I Directory Services nell'offerta Tivoli

Le directory sono entità che contengono una raccolta di oggetti organizzati in una struttura ad albero e rappresentano uno strumento fondamentale per le operazioni IT e il deployment delle applicazioni di e-business all'interno di realtà di media e grande dimensione.
Per far fronte a queste esigenze IBM fornisce un supporto integrato per l'implementazione delle directory basato su industry standard e adatto per tutte le principali piattaforme, sia le proprie che quelle di altri vendor.

IBM Tivoli Directory Server

IBM Tivoli Directory Server implementa lo standard Lightweight Directory Access Protocol (LDAP) che il mercato ha fatto emergere rapidamente negli anni passati. LDAP definisce un metodo standard per accedere e aggiornare le informazioni contenute all'interno di una directory, a cui si accede utilizzando un modello di tipo client-server ottimizzato per l'accesso in lettura.
L'infrastruttura di identità LDAP messa a disposizione da *Tivoli Directory Server* costituisce la base per la distribuzione di applicazioni globali di gestione dell'identità e architetture software avanzate come i servizi Web.
In particolare è possibile evidenziare le seguenti caratteristiche di IBM Tivoli Directory Server:

- il supporto LDAP V3 che assicura la compatibilità con le applicazioni basate su LDAP standard nel settore;
- il motore affidabile IBM DB2 Universal Database V8.1, che fornisce scalabilità a decine di milioni di voci e a gruppi di centinaia di migliaia di membri;
- il supporto esteso delle piattaforma AIX, Solaris, Microsoft Windows, HP-UX, delle distribuzioni Linux per Intel e delle piattaforme server IBM;
- la capacità di replica per repliche master/dipendenti, di gateway, in sovrapposizione e peer-to-peer con dozzine di server master;
- la presenza della GUI Web Administration e delle funzioni Dynamic e Nested Groups, che facilita la gestione e l'utilizzo;
- la stretta integrazione con i sistemi operativi IBM, il middleware WebSphere e i prodotti di gestione identità e sicurezza Tivoli.

IBM Tivoli Directory Server è stato sviluppato con l'obiettivo di servire come base dati dell'identità per uno sviluppo e una distribuzione rapida delle applicazioni Web e delle iniziative di gestione identità incluse le funzioni di gestione, di replica e sicurezza. Con IBM Tivoli Directory Server è possibile scegliere la strategia di autenticazione, utilizzare un semplice ID utente e un'autenticazione password, oppure è possibile implementare la più sicura struttura digitale di autenticazione basata su certificati. IBM Tivoli Directory Server include anche un'interfaccia di plug in SASL (Simple Authentication Security Layer), inclusa l'autenticazione CRAM-MD5 (Challenge-Response Authentication Mechanism MD5) e Kerberos (opzionale).
Tivoli Directory Server rappresenta il directory server di default LDAP integrato con IBM Tivoli Access Manager (TAM) e può essere configurato sia come back-end server sia come proxy server. Tivoli Access Manager utilizza l'LDAP directory server come un registro utenti per memorizzare le proprie informazioni utenti e di gruppo.

IBM Directory Integrator

IBM Directory Integrator è una soluzione di metadirectory basata su un'architettura aperta per la sincronizzazione e lo scambio delle informazioni in tempo reale tra applicazioni o sorgenti di directory. Consente alle aziende di predisporre un'infrastruttura aggiornata e affidabile sui dati associati alle identità che funziona da piattaforma per la protezione dell'azienda e per le applicazioni basate su Web Service.

Questa soluzione software mette a disposizione delle aziende:

- un'architettura aperta grazie agli script Java;
- un ambiente di sviluppo connettori e connettori pre-integrati;
- meccanismi di gestione delle eccezioni e degli eventi;
- un'architettura flessibile e ottimizzata per le risorse basata sulla memorizzazione dei dati non permanenti.

Il funzionamento combinato di Tivoli Directory Integrator e Tivoli Identity Manager permette di automatizzare la creazione, la manutenzione e la cancellazione degli account degli utenti.
IBM Tivoli Directory Integrator sincronizza i dati di identità che risiedono all'interno di directory, database, sistemi di collaborazione, applicazioni utilizzate per le risorse umane (HR), Customer Relationship Management (CRM), Enterprise Resource Planning (ERP) e altre applicazioni aziendali.
Directory Integrator mette a disposizione uno strato di sincronizzazione flessibile, tra la struttura per l'identità di un'azienda e le sorgenti applicative dei dati di identità, eliminando l'esigenza di dover disporre di un unico contenitore centralizzato.
Per le imprese che scelgono di implementare una soluzione di enterprise directory, Directory Integrator può contribuire a facilitare il processo collegandosi ai dati di identità provenienti dai vari repository distribuiti attraverso l'organizzazione.

3.7 Modelli architetturali nell'uso di Tivoli Identity Manager e Tivoli Access Manager

Una soluzione di identity e access management permette di affrontare molti requisiti di business. In generale il requisito principale è quello di fornire una combinazione di processi di business e di tecnologie per gestire e garantire l'accesso sicuro alle informazioni e alle risorse all'interno dell'organizzazione.
Per raggiungere questo obiettivo una soluzione di identity e access management deve:

1. fornire un metodo per la concessione agli utenti dell'accesso alle applicazioni e ai sistemi (provisioning e de-provisioning) necessario per eseguire le loro funzioni lavorative, utilizzando le procedure di approvazione stabilite da parte delle imprese;

2. fornire la capacità di autorizzare i corretti livelli di accesso alle risorse in base alle policy aziendali;
3. consentire l'accesso alle risorse accessibili via Web come, per esempio, le applicazioni Web, e offrire un modo per l'autenticazione degli utenti alle risorse mediante Single Sign-On, dopo che l'accesso è stato concesso;
4. garantire un percorso di audit per assicurare il corretto funzionamento del sistema di identity e access management e verificare la compliance con le policy aziendali.

Naturalmente, vi è un rapporto di complementarietà tra gestione dell'accesso e dell'identità. Un soluzione integrata di Identity e Access Management prevede una combinazione di processi aziendali e tecnologie software per gestire e garantire l'accesso sicuro alle informazioni proprietarie all'interno di un'impresa.
Va ricordato che non si tratta solo di una corretta pratica di business, poiché molti settori industriali sono regolamentati attraverso obblighi di compliance che sono direttamente collegati alla soluzione di Identity e Access Management.

3.7.1 L'architettura di un sistema integrato per la gestione dell'identità e dell'accesso

Le soluzioni Tivoli Identity Manager, Tivoli Access Manager e i prodotti WebSphere Portal possono essere abbinati per realizzare un sistema integrato per la gestione dell'identità e dell'accesso.
Dal punto di vista dell'architettura logica, il punto di partenza del processo è rappresentato dall'utente, che interagisce con il sistema di gestione dell'identità e dell'accesso attraverso il proprio personal computer utilizzando un browser (o un client di posta elettronica), per accedere alle varie applicazioni Web che sono protette dal componente WebSEAL, presente nel prodotto Ibm Tivoli Access Manager for e-business.
Per accedere a queste applicazioni gli utenti utilizzano la user ID di Tivoli Access Manager, mentre WebSEAL garantisce il Single Sign-On. Alcune delle applicazioni protette da WebSEAL, come, per esempio, l'applicazione "self care" che consente a un'utente di gestire in autonomia le funzioni di identità, vengono eseguite all'interno di WebSphere Portal Server.
Tivoli Access Manager fornisce il servizio LDAP per il repository dei dati degli utenti, mentre Tivoli Access Manager Policy Server provvede a gestire le policy di controllo dell'accesso e a replicarle verso i punti in cui que-

ste regole vengono applicate da prodotti come Ibm Tivoli Access Manager for Operating System, che le utilizza per realizzare controlli di autorizzazione per l'accesso ai file e alle directory su sistemi UNIX.
Tivoli Identity Manager è utilizzato per gestire gli account di Tivoli Access Manager e anche quelli di altri sistemi. Identity Manager provvede a generare notifiche e-mail all'utente utilizzando un SMTP server e dispone di un proprio registro LDAP e di un proprio database relazionale.
Se si considera, invece, l'architettura dal punto di vista fisico, si può osservare che le richieste Web provenienti dagli utenti esterni passano attraverso un sistema di bilanciamento del carico prima di essere indirizzate verso l'Access Manager WebSEAL. Quest'ultimo è collocato all'interno di una zona separata (la cosiddetta zona demilitarizzata o DMZ), tra due firewall; Access Manager, Identity Manager, WebSphere Portal e i sistemi LDAP risiedono tutti nella intranet dietro il secondo firewall.
Dopo che l'utente ha effettuato il login (mediante la user ID di Access Manager, utilizzando WebSEAL) il componente Tivoli Access Manager Trust Association Interceptor (TAI++) viene utilizzato per creare le credenziali WebSphere per l'utente, che saranno poi utilizzate dalle applicazioni basate su WebSphere Portal.
Access Manager viene usato anche come provider di autorizzazione per WebSphere, sfruttando l' Access Manager Authorization Server.
Identity Manager è, invece, utilizzato per gestire gli account di Access Manager (o di altri sistemi analoghi) e viene rilasciato in un cluster di WebSphere per garantire l'alta disponibilità.

3.8 Esempi pratici di scenari di business con Tivoli Identity Manager e Tivoli Access Manager

Nelle pagine seguenti vengono illustrati diversi esempi in cui i prodotti IBM Tivoli Identity Manager e Access Manager possono essere integrati per fornire specifiche funzionalità orientate al business.

3.8.1 Assunzione di un nuovo dipendente

Il processo di provisioning è automatizzato in modo tale che, quando un nuovo dipendente viene inserito all'interno del sistema di gestione delle risorse umane (HRMS), i dati del nuovo impiegato attivano un processo automatizzato per la creazione dell'account e l'accesso. Questo consente di automatizzare il processo di accesso ai sistemi e alle applicazioni di cui il dipendente

ha bisogno per svolgere il proprio lavoro. La user identity del nuovo dipendente viene creata all'interno dell'ecosistema di Identity e Access Management come parte del processo di assunzione del dipendente.
Il "feed" fornito dal sistema dedicato alle risorse umane (HR) è costituito tipicamente da dati associati ai dipendenti, quali l'elenco dei nuovi dipendenti, quelli licenziati, le modifiche organizzative e così via, che sono inseriti nel sistema in varie forme, che possono prevedere l'importazione di file oppure connessioni programmate al sistema di gestione delle risorse umane, per esempio attraverso l'uso di IBM Tivoli Directory Integrator (ITDI Server).
I nuovi record delle risorse umane vengono elaborati all'interno di Tivoli Identity Manager e attraversano una serie di workflow operativi per rispondere alle specifiche esigenze di business delle diverse organizzazioni.
Questo workflow prevede attività quali:

- l'elaborazione di un nuovo record all'interno di Identity Manager;
- la valutazione e l'assegnazione di uno specifico ruolo in base a criteri configurati;
- l'applicazione di policy in base al ruolo svolto o all'organizzazione di appartenenza;
- la gestione delle approvazioni sulle policy di provisioning adottate;
- la creazione dell'account in Access Manager;
- l'invio di notifiche al dipendente una volta che gli account appropriati sono stati creati.

Un approccio di provisioning alternativo è quello di prevedere un processo di registrazione automatica da parte del dipendente, in cui l'utente è in grado di accedere a un'applicazione "self-care" per gestire autonomamente l'inserimento dei propri dati all'interno del sistema.

3.8.2 Modifica del ruolo di un dipendente

Il cambiamento del ruolo lavorativo di un dipendente viene notificato al sistema di identity e access management mediante un feed di dati proveniente dal sistema di gestione delle risorse umane al Tivoli Directory Integrator server. Il record modificato all'interno del sistema HR passa quindi attraverso una serie di flussi di lavoro all'interno di Tivoli Identity Manager che comprendono:

- valutazioni dinamiche del record modificato per l'assegnazione al nuovo ruolo organizzativo in base a opportuni criteri preconfigurati;
- applicazione delle policy;

- gestione delle approvazioni;
- creazione o modifica degli account;
- invio delle notifiche della creazione degli account.

3.8.3 Licenziamento di un dipendente

Il processo di de-provisioning è automatizzato in modo tale che, non appena un dipendente è rimosso dal sistema di gestione delle risorse umane, tutti gli account a esso associati vengono automaticamente cancellati.
La realizzazione di questa funzione prevede, innanzitutto, la notifica al sistema di identity e access management attraverso l'invio dei dati al Tivoli Directory Integrator server. Il record modificato attraversa poi una serie di flussi di lavoro specifici all'interno di Identity Manager che comprendono:

- modifica del record per impostare lo status come disattivato;
- invio delle notifiche di approvazione per la cancellazione dei privilegi;
- eliminazione/sospensione degli account appartenenti al dipendente.

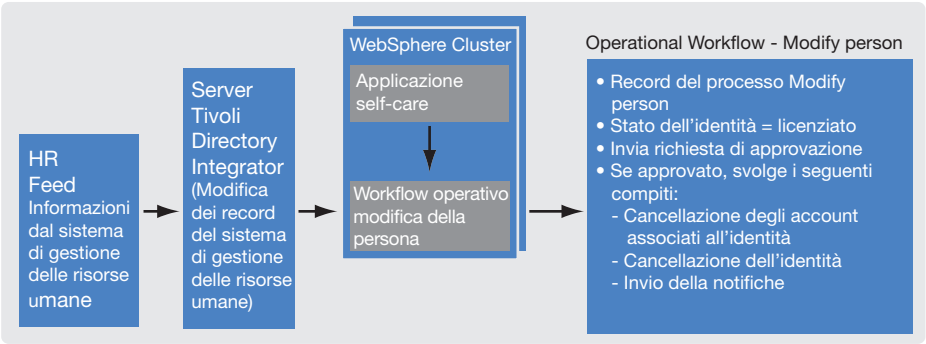


Figura 3.1
Gestione del licenziamento di un dipendente sfruttando Tivoli Identity Manager e Tivoli Access Manager

3.8.4 Gestione coerente della password

Eventi legati al ciclo di vita delle password come scadenza, modifica e reset possono essere gestiti coerentemente all'interno dell'ecosistema di identity e access management realizzato con le soluzioni Tivoli. Inoltre, policy associate alle password sono applicate in modo coerente attraverso tutti i sistemi che fanno parte dell'ecosistema, indipendentemente dal fatto che i dipendenti utilizzino un'interfaccia self-service o l'interfaccia nativa del sistema per eseguire le operazioni di modifica della password. La password che è stata reimpostata o modificata, successivamente alle opportune operazioni di convalida, viene sincronizzata attraverso tutti i sistemi. Questa funzione permette di migliorare l'esperienza dell'utente e rafforza la protezione.

Ci sono due modi in cui Tivoli Identity Manager è utilizzato per la centralizzazione di queste operazioni di gestione centralizzata.
Nel primo gli utenti accedono all'Identity Manager e cambiano la propria password. Viene verificato che la password modificata soddisfi le policy richieste e, in tal caso, viene sincronizzata con tutti gli endpoint, come per esempio Access Manager, Active Directory e così via.
Nella seconda modalità gli utenti accedono al sistema target che è configurato con il "reverse password synchronization module" di Identity Manager e cambiano la loro password. Questo modulo è un componente installabile che cattura eventi di modifiche della password su un sistema target e successivamente comunica con Tivoli Identity Manager per svolgere i seguenti compiti:

- verificare che la password soddisfi i requisiti di sicurezza richiesti dalle policy configurate su Identity Manager (per esempio lunghezza minima o inclusione di numeri);
- nel caso di superamento della verifica, memorizzare la nuova password centralmente nel repository di Identity Manager.

Il sistema di Identity and Access Management provvede ad applicare centralmente la gestione coerente delle password attraverso molteplici sistemi target.

3.8.5 Controllo di accesso basato su ruoli

Il controllo di accesso basato su ruoli è definito dalla realizzazione di un sistema automatizzato che prende le informazioni relative a una nuova assunzione presenti nel sistema HR e fornisce i corretti controlli di accesso a tutte le appropriate risorse attraverso l'intera organizzazione enterprise; il processo avviene sulla base delle informazioni di identità associate all'utente, senza richiedere alcuna azione da parte dell'amministratore.
Anche se questo è certamente l'obiettivo alla base di qualsiasi soluzione di identity e access management, nel mondo reale la granularità della gestione di accesso impedisce una diffusione tempestiva e conveniente di un reale controllo di accesso basato su ruoli (RBAC).
Tuttavia, l'auto-provisioning per selezionate applicazioni e/o sistemi target è realizzabile in un lasso di tempo ragionevole e la continua messa punto della soluzione di Identity and Access Management nel corso del tempo porta la soluzione sempre più vicina a un reale modello basato su ruoli.
La possibilità di ottenere la realizzazione di un RBAC deve passare attraverso la definizione e la configurazione dei ruoli organizzativa nella soluzione di identity e access management (in modo tale che specifiche informa-

zioni sull'identità utente siano raggruppate logicamente in corrispondenti livelli di controllo di accesso che si traducano nel provisioning dello user account su piattaforma adeguate), che insieme garantiscono il corretto controllo di accesso necessario per consentire all'utente di svolgere le proprie funzioni lavorative.
Per giungere all'obiettivo finale di configurare un controllo di accesso basato su ruoli è consigliabile procedere per fasi successive:

1. una gestione delle password mediante l'Identity Manager;
2. il provisioning manuale e la gestione di base dell'account con Identity Manager;
3. il provisioning automatizzato (combinando provisioning manuale e automatico);
4. il provisioning automatico ovvero il provisioning automatizzato per tutti gli endpoint gestiti, mediante meccanismi di approvazione configurati che richiedono piccole azioni da parte dell'amministratore;
5. un reale controllo di accesso basato su ruoli in cui si realizza il provisioning automatico di tutti gli account utente successivamente all'inserimento dei dati all'interno del sistema di gestione delle risorse umane (HRMS), senza che sia richiesto alcun compito di tipo amministrativo.

La procedura necessaria per ottenere una reale configurazione RBAC in Identity Manager richiede uno sforzo notevole, ma è utile per raggiungere gli obiettivi descritti nei punti precedenti.

3.8.6 Integrazione di un'applicazione

Quando vengono rilasciate nuove applicazioni all'interno dell'azienda enterprise la soluzione di identity e access management deve facilitare il loro inserimento all'interno dell'ecosistema di gestione dell'identità e dell'accesso, in modo tale che le operazioni di provisioning e di rafforzamento dell'accesso siano governate utilizzando i medesimi processi consistenti.

3.8.7 Audit della conformità e reporting

La soluzione di identity e access management deve essere in grado di effettuare operazioni di audit rispetto alla creazione, alla cancellazione e agli aggiornamenti dei profili legati all'identità e all'account dell'utente.

Inoltre, la soluzione deve poter tenere traccia sia dei tentativi riusciti quanto di quelli falliti di accesso alle risorse e questo per tutti i tipi di utenti inclusi gli amministratori. Gli auditor richiedono, infatti, il tracciamento di tutti gli accessi alle informazioni personali (non pubbliche) delle persone. Non solo viene richiesto di registrare ogni accesso a un record, ma anche qualsiasi trasferimento di dati, modifica e cancellazione.
Sia Identity Manager sia Access Manager sono configurati per la raccolta di eventi di audit di vario tipo. Per esempio, Access Manager è configurato per raccogliere eventi di audit per:

- autenticazione
- verifica del controllo di accesso
- operazioni di gestione dell'utente
- la creazione di gruppi
- aggiunta di utenti ai gruppi
- creazione e aggiornamento delle ACL
- fornire report per eventi di audit.

L'Identity Manager è configurato per generare eventi di audit per:

- elaborazione di flussi di lavoro
- provisioning
- ricertificazione dell'account
- fornire report per vari eventi di audit.

I report forniti da Identity Manager e Access Manager sono utilizzabili per varie esigenze e inoltre, gli eventi di audit provenienti da Identity Manager, Access Manager sono elaborati mediante Tivoli Compliance Insight Manager per verificare il rispetto delle policy di sicurezza e, nello stesso tempo, per valutare il livello di compliance garantito dalla soluzione di Identity e Access Management.

3.8.8 Auto-gestione del profilo utente e accesso alle risorse

Attraverso una singola interfaccia self-service, questa soluzione permette l'auto-gestione delle informazioni sul profilo dell'utente e la replica automatica dei dati di profilo verso i principali sistemi aziendali. L'interfaccia self-service mette a disposizione dell'utente la possibilità di chiedere, eliminare, approvare e modificare l'accesso a diverse applicazioni e anche di gestire le password da un'unica console.

Gli utenti che effettuano da soli la registrazione iniziale al sistema possono accedere all'applicazione di self-care come utenti non autenticati mediante un proxy Web di sicurezza (per esempio WebSEAL).
L'applicazione di self-care presenta l'auto-registrazione al repository di identità che è gestito da Tivoli Identity Manager.
Al completamento del processo di auto-registrazione, all'utente vengono inviati via e-mail un ID utente e le credenziali per l'accesso delle applicazioni.
Identity Manager gestisce la creazione dei diversi account necessari all'utente per accedere alle varie applicazioni, compresa la creazione dell'account utente di Access Manager.

3.8.9 Ripristino e reimpostazione di password dimenticate

La soluzione Tivoli permette agli utenti di recuperare una password dimenticata in modo sicuro attraverso varie modalità
In questo esempio, l'utente ha dimenticato la password utilizzata per autenticare WebSEAL. Al fine di facilitare il recupero della password dimenticata dall'utente, WebSEAL consente l'accesso non autenticato alle pagine dell'applicazione di self-care indirizzate a gestire uno scenario di password dimenticata.
L'utente digita il nome utente e seleziona il link per la password dimenticata, che porta l'utente all'applicazione self-care su una connessione non autenticata. All'utente vengono proposte una serie di domande di verifica precedentemente impostate con l'invito a fornire la risposta al sistema. Queste risposte sono convalidate dal sistema prima di lasciargli la possibilità di impostare una nuova password o effettuarne il reset.
In quest'ultimo caso viene solitamente generata una nuova password temporanea "monouso" che viene inviata via e-mail all'utente forzandolo a cambiarla al primo accesso.

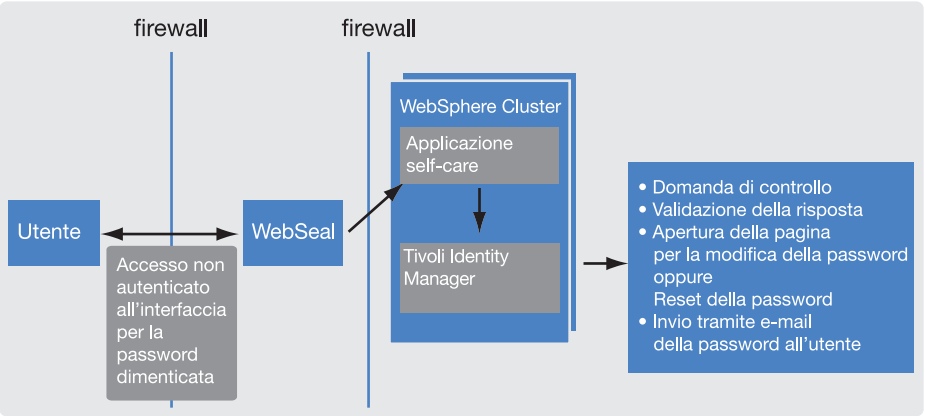


Figura 3.2
Gestione del ripristino e reimpostazione di password dimenticate sfruttando Tivoli Identity Manager e Tivoli Access Manager

3.9 Federated Identity and Trust Management

Condividere le informazioni di autenticazione e gli attributi degli utenti tra partner che hanno un reciproco rapporto di fiducia e attraverso Web Service rappresenta un desiderio crescente tra le organizzazioni. La possibilità di condividere queste informazioni con partner esterni o business unit interne permette, infatti, alle organizzazioni di fornire ai propri utenti un'esperienza notevolmente migliore e semplificata.
I driver che spingono le aziende verso questa direzione sono molteplici.
Il costo di gestire il ciclo di vita delle identità è molto alto e la maggior parte delle organizzazioni si trova, ormai, a dover amministrare, oltre alle identità dei propri dipendenti, anche quelle dei business partner e dei clienti. Se si considera che il rapporto tra il business e questi soggetti è una variabile che può mutare frequentemente e rapidamente, richiedendo una corrispondente azione di tipo amministrativo, si comprende facilmente come tutto diventi continuamente più complicato, insicuro e costoso.
Il raggiungimento di questi obiettivi definisce il concetto di "identity federation".
In un modello federato si stabilisce una relazione di partnership tra diverse organizzazioni; ognuna di queste mantiene il controllo delle informazioni di identità e delle preferenze dei propri utenti e concorda di riconoscere come valide le credenziali di utenti prodotte o autenticate dagli altri partner. Si crea, pertanto, un accordo di fiducia tra diversi enti (che gli anglosassoni chiamano circle of trust) che permette a un utente che dispone di credenziali ritenute valide da una struttura, di utilizzarle in modo inalterato anche per l'accesso a ogni applicazione resa disponibile dagli enti con essa federati.

3.9.1 Federated identity management

Parlare di federazione significa considerare un gruppo di due o più business partner che lavorano insieme e che decidono di attivare un'aggregazione finalizzata a migliorare l'esperienza dei rispettivi clienti e/o contribuire a ridurre i costi.
Per esempio, un'organizzazione di tipo finanziario potrebbe desiderare di fornire un accesso trasparente ai propri clienti primari a informazioni del mercato finanziario fornite da aziende indipendenti di analisi.
Oppure diversi enti governativi potrebbero voler collaborare per fornire al cittadino la possibilità di accede con un singolo *login* ai servizi forniti da entrambi. O, ancora, un piccolo negozio online potrebbe preferire evitare di dover gestire un gran numero di record e preferire affidarne la gestione a un'istituzione finanziaria partner.

Sono tutti esempi in cui le organizzazioni devono operare insieme per creare una business federation.
Le business federation vengono costruite su quelle che vengono chiamate relazioni di fiducia (trust relationship) che vengono create prevedendo preventivamente accordi legali tra i partecipanti.
Dopo che gli opportuni accordi sono stati predisposti è possibile avviare questa collaborazione avvalendosi di adeguati strumenti tecnologici a supporto, capaci di garantire funzioni di federazione, di gestione della fiducia e supporto per la crittografia; a questi si affianca l'implementazione di opportuni protocolli che consentono ai partner di operare in sicurezza sfruttando anche il canale Internet.
La gestione delle identità attraverso una federazione è il tema delle tecnologie di federated identity management che mirano a fornire sistemi standardizzati per semplificare la gestione delle identità attraverso differenti confini aziendali di influenza e pertinenza
Questo tipo di soluzioni e sistemi permette alle organizzazioni di distribuire o scaricare i costi di gestione dell'identità e dell'accesso sui business partner all'interno della federazione.
In pratica, l'adozione di una soluzione di gestione federata dell'identità consente a un membro di ricevere informazioni affidabili e sicure su un utente/cliente appartenente a un altro membro della federazione, senza che questo debba effettuare un nuovo processo di autenticazione e senza che l'azienda debba registrare quell'utente. Di conseguenza, una soluzione di federated identity management fornisce un beneficio diretto anche all'utente finale che opera all'interno di un federazione, che dovrà deve preoccuparsi unicamente di ricordare le credenziali con cui accede e si autentica all'interno della propria organizzazione per potersi autenticare anche presso le organizzazioni della federazione senza dover interagire direttamente con loro.
Questo processo non solo riduce il numero di credenziali che un utente deve tenere a mente ma diminuisce anche il numero di volte che tali credenziali devono essere fornite per accedere ai servizi aumentando il livello di sicurezza.
In questo processo un ruolo importante è svolto dai Web Service, una tecnologia che si è progressivamente affermata con le crescenti esigenze di integrazione cross-enterprise, cross-platform e cross-vendor.
I Web Service rappresentano una famiglia di tecnologie che abilitano in modo semplice l'interoperabilità tra servizi IT e l'integrazione di applicazioni all'interno dei processi di business. In altre parole permettono alle aziende di descrivere i servizi disponibili e di fornirne l'accesso utilizzando protocolli Internet standard.

Il processo di federated identity management prevede essenzialmente due tipologie di ruolo: l'identity provider e il service provider.
L'identity provider (a volte denominato anche account partner) garantisce l'identità dell'utente all'altra parte ed è responsabile per la gestione degli utenti e delle loro credenziali, per la fornitura delle credenziali, la gestione amministrativa dell'utente, l'autenticazione dell'utente.
Il service provider (indicato anche con il termine "relying party" o "resource partner") rappresenta la parte di validazione all'interno della transazione. Il service provider è responsabile di controllare l'accesso ai servizi, validare le informazioni di identità fornite dall'identity provider (tipicamente verificando una firma digitale), fornire accesso in relazione all'identità fornita e di gestire gli attributi di rilevanza locale (non l'intero profilo utente).

IBM Tivoli Federated Identity Manager

IBM Tivoli Federated Identity Manager è la soluzione che permette di svolgere operazioni di business che intervengono su ambienti diversificati e attraverso una pluralità di domini di sicurezza in modo protetto, flessibile ed efficiente.
Questa soluzione software sfrutta i principali standard di tipo federativo per garantire l'accesso degli utenti gestiti all'interno di un'organizzazione "trusted" in base alla loro identità e ruolo. Il risultato è la possibilità di sviluppare in modo più semplice servizi di terze parti da offrire ad altre organizzazioni così come di consentire ai propri utenti di avvantaggiarsi dei servizi di terze parti, senza obbligarli a dover navigare attraverso i siti della federazione e permettendo loro di spendere meno tempo dovendo effettuare le procedure di autenticazione in diversi ambienti e organizzazioni. Tivoli Federated Identity Manager permette di implementare funzioni di gestione dell'accesso sicuro ad applicazioni e servizi distribuiti come a mainframe, in ambienti SOA basati sull'utilizzo dei Web Service.
I vantaggi offerti da Tivoli Federated Identity Manager interessano la riduzione dei costi associati alla business integration, all'help-desk e all'amministrazione della sicurezza grazie alla possibilità di predisporre rapidamente una soluzione semplice di SSO; inoltre, l'uso di questo software contribuisce a minimizzare i costi necessari per creare e mantenere identità condivise attraverso molteplici business partner.
Infine contribuisce a migliorare la compliance grazie alle funzionalità di

tracciabilità e di auditing e permette di realizzare e condividere in modo molto rapido servizi Web-based con i propri business partner.
Alle organizzazione medie e piccole si indirizza, invece, **IBM Tivoli Federated Identity Manager Business Gateway**, che rappresenta una soluzione di tipo entry-point per cominciare a stabilire funzionalità federate di SSO su Web.

3.9.2 I protocolli di tipo federativo

Gli utenti si trovano solitamente nella condizione di disporre di un set differente di credenziali di autenticazione per ogni sito Web; questa fastidiosa situazione può diventare ancora più impegnativa e gravosa nel caso in cui il sito preveda anche una "strong authentication", per esempio basata sull'utilizzo di token. La medesima problematica, ribaltata dal lato enterprise, determina elevati costi per la gestione di questi account. Per superare queste difficoltà sono stati perciò sviluppati protocolli opportuni per consentire agli utenti di effettuare l'autenticazione un'unica volta all'interno di una federazione di siti Web cooperanti tra loro.
Essenzialmente è possibile ricondurre le tipologie di protocolli a due serie.
La prima di queste raggruppa protocolli focalizzati su modelli *enterprise-centrici* e comprende: Security Assertions Markup Language (SAML), Liberty e le specifiche Web services (WS) Federation. Questi protocolli di tipo federativo sono ormai in uso da svariati anni e sono ampiamente adottati.
Il secondo tipo è rappresentato dagli schemi di identità *user-centrici*. Si tratta di specifiche di più recente realizzazione che sono caratterizzate dal fatto di fornire agli utenti un maggiore livello di controllo sulle loro identità digitali.
Le diverse tipologie prevedono differenti relazioni di fiducia.
Nel caso dei modelli enterprise-centrici la trust relationship si realizza sempre tra due o più aziende che sono i business partner coinvolti nella federazione. Nei modelli user-centrici questo tipo di situazione è ancora praticabile ma è possibile anche che l'utente possa sviluppare autonomamente delle credenziali e possa utilizzarle in sostituzione delle password per superare alcuni dei problemi che si verificano nella gestione dell'identità per il sito Web.

3.10 Il Federated Single Sign-On

Il Federated Single Sign-On viene utilizzato in molti scenari basati sull'utilizzo del browser. Una soluzione di questo tipo consente a un utente di autenticarsi presso un sito Web (identity provider) per poi accedere ad altri siti Web (service provider) senza il bisogno di autenticarsi nuovamente. I service provider si affidano all'identity provider come garante per autenticare l'utente e accettare eventuali token di sicurezza emessi sempre dall'identity provider.
Il Federated Single Sign-On prevede un numero di funzioni di identità che include Single Sign-On/Sign-Off, il collegamento dell'account tra l'identity provider e il service provider, la possibilità di utilizzare alias per l'accesso invece della reale identità e di far fronte alla richiesta di attributi e informazioni sull'utente da parte dei service provider all'identity provider.
Il Federated single Sign-On rappresenta, pertanto, un caso particolare, all'interno di un modello più ampio di gestione federata dell'identità, focalizzato sulla gestione dell'identità tra aziende che cooperano tra loro attraverso il Web.
L'adozione di industry standard risulta particolarmente importante negli scenari di federated Single Sign-On poiché l'identity provider e i service provider sono solitamente aziende differenti che dispongono di ambienti IT diversi tra loro.

3.10.1 Gli standard per il SSO enterprise-centrici

Esistono tre principali standard per il supporto del federated Single Sign-On: SAML, Liberty e WS-Federation. IBM Tivoli Federated Identity Manager supporta tutte queste specifiche nelle diverse versioni disponibili sul mercato.

Security Assertions Markup Language (SAML)

Security Assertions Markup Language (SAML) è una specifica messa a punto per consentire l'interoperabilità tra le soluzioni di Single-Sign-On di differenti vendor. SAML è stato sviluppato da un consorzio di primarie aziende (inclusa IBM) e svolge due funzioni primarie.
La prima è quella di definire le Asserzioni (SAML assertion) che descrivono i token di sicurezza associati all'identità di un utente. Un'asserzione SAML è, di fatto, un token basato su XML che viene utilizzato per trasferire le informazioni sull'identità dell'utente da un identity provider verso un trusted service provider a complemento della richiesta di Single-Sign-On di un browser. In altre parole un'asserzione SAML mette a disposizione un metodo indipendente dal vendor con cui trasferire le informazione all'interno di una federazione di business partner.

La seconda funzione e quella di definire i profili e gli attributi SAML per un protocollo di Single Sign-On.
Come protocollo SAML è stato rilasciato in tre versioni: SAML 1.0, 1.1 e 2.0. Le prime due versioni sono focalizzate sulle funzionalità di Single Sign-On e vengono anche indicate nel loro insieme con la dicitura SAML 1.x. La versione 2.0 introduce in SAML un importante incremento di funzionalità perché tiene in considerazione una serie di aspetti legati al ciclo di vita dell'identità e affronta alcune problematiche correlate al rispetto della privacy all'interno di un ambiente federato.

Liberty

Liberty Alliance è un alleanza che raggruppa una serie di vendor (incluso IBM) e organizzazioni di utenti, nata per fornire e sostenere una soluzione di identità di rete federata che, inoltre, abiliti il Single Sign-On sia gli utenti del mondo consumer che per quelli business. All'interno di questo progetto sono state rilasciate le specifiche Liberty 1.2 che forniscono molte funzioni indirizzate al ciclo di vita dell'identità e che non erano originariamente state prese in considerazione da SAML 1.0 e 1.1. Questo protocollo è ancora utilizzato sebbene sia stato, di fatto, superato da SAML 2.0.

WS-Federation

WS-Federation è stato creato da un gruppo di vendor (incluso IBM) con l'obiettivo di fornire una risposta ai requisiti di identità richiesti sia dalle applicazioni Web sia dai Web Service. L'obiettivo di queste specifiche è, pertanto, quello di fornire un metodo comune in grado di supportare sia le applicazioni basate su browser sia quelle che si appoggiano ai Web Service. WS-Federation è strettamente allineato con gli standard appartenenti alla famiglia WS-Security. Attualmente sono state rilasciate due versioni delle specifiche WS-Federation siglate 1.0 e 1.1.

PROTOCOLLO	VERSIONI
SAML	1.0, 1.1, 2.0
Liberty	1.1, 1.2
WS-Federation	1.0

Tabella 3.2
Gli standard di single-Sign-On federato supportati da IBM Tivoli Federated Identity Manager

3.10.2 Il modello di gestione dell'identità "user-centrico"

Una delle critiche solitamente portate ai sistemi federati di Single Sign-On basati sui protocolli SAML, Liberty o Higgins è che questi protocolli sono progettati per rispondere alle esigenze delle strutture enterprise che si federano tra loro e che hanno bisogno di mantenere il controllo dell'informazione con l'identity provider e il service provider.
Agli utenti viene lasciato meno controllo di quello che desiderano avere rispetto a quali sono le informazioni richieste da identity e server provider, col risultato che si trovano spesso a fornire un numero di informazioni superiore a quello necessario per il completamento della transazione.
I sistemi user-centrici (a cui a volte si fa riferimento come Identity 2.0) rappresentano il tentativo di riportare il controllo nelle mani dell'utente.

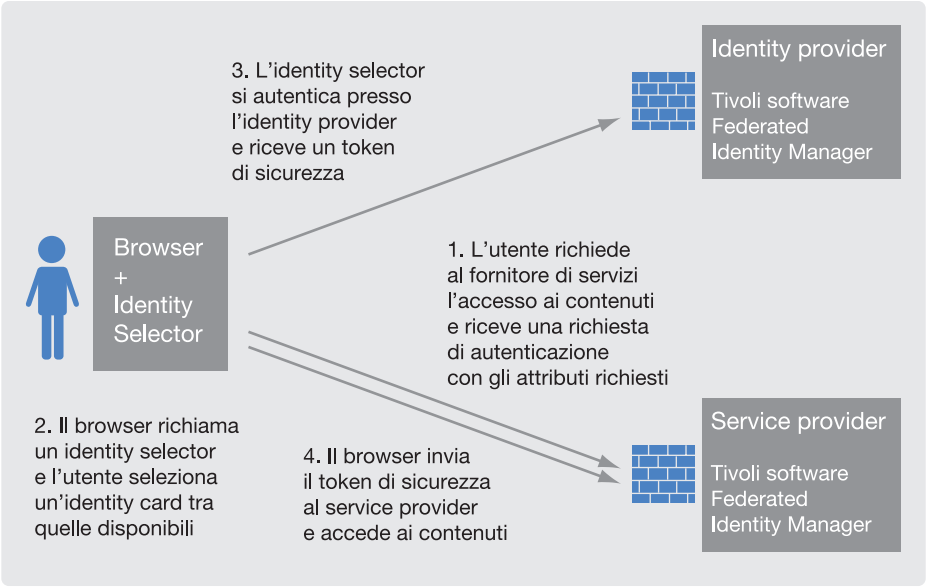


Figura 3.3
Un tipico esempio di single-Sign-On user-centrico in cui IBM Tivoli Federated Identity Manager è utilizzato sia dal lato dell'identity provider sia del relying party

Un altro beneficio offerto da questo tipo di sistemi è che possono consentire la realizzazione di relazioni debolmente accoppiate in cui la parte che eroga il servizio non deve necessariamente predisporre una relazione di fiducia preesistente con l'identity provider (sia che si tratti di un fornitore di identità gestita, sia nel caso in cui fornisca da solo le proprie credenziali).
IBM Tivoli Federated Identity Manager supporta due famiglie di protocolli di identità user-centrici: OpenID (con la possibilità di utilizzare selettori di identità quali Microsoft Windows CardSpace) ed Eclipse Higgins Project.

Microsoft Windows CardSpace è un metasistema per la gestione dell'identità digitale che introduce un componente visuale sul desktop dell'utente denominato identity selector. Questo selettore opera congiuntamente con l'applicazione client usata per l'accesso (per esempio il browser) per negoziare la richiesta di autenticazione attraverso una serie di schede (Information card) che rappresentano in modo visuale diverse identità associate all'utente; queste possono essere schede di informazioni personali fornite dall'utente in assenza di una validazione esterna oppure schede di informazioni gestite da un identity provider presso cui l'utente è registrato.
In un tipico scenario di utilizzo di CardSpace, gli utenti accedono a un sito che offre un servizio mediante il loro browser. La pagina di autenticazione del fornitore del servizio evidenzia, mediante un icona, che il sito supporta un sistema basato su Information card. Cliccando su questa icona viene inviato al browser dell'utente una richiesta di autenticazione che include gli attributi in termini di identità (claims) richiesti all'utente per accedere al servizio. A questo punto è lasciata facoltà all'utente di scegliere quale Information card intende utilizzare per autenticarsi. Poiché l'insieme di attributi di autenticazione richiesti viene visualizzato, l'utente ha la piena consapevolezza di quali informazioni vengono richieste (essenziali od opzionali) per l'erogazione del servizio desiderato. In questo modo l'utente detiene il controllo su quale Information card utilizzare e se, nel processo, vengono forniti anche degli attributi non strettamente necessari per l'erogazione del servizio richiesto. Dopo che è stata scelta un Information card gli utenti si autenticano presso il loro identity provider, mentre un token di sicurezza viene generato e inviato al browser e quindi al fornitore del servizio per completare il ciclo di autenticazione.

Higgins è un'implementazione open-source di un metasistema di identità di tipo user-centrico simile a quello offerto da Microsoft Windows CardSpace. Higgins fornisce tre differenti funzionalità per l'identità: un selettore di identità, servizi di identity provider/consumer Web-based e un servizio di attributi di identità.

PROTOCOLLO	VERSIONI
Identity selector (Microsoft Windows CardSpace)	1.0 (utilizzando WS-Trust 1.2)
Identity selector (Eclipse Higgins Project)	1.0
OpenID	Protocollo di Autenticazione 1.1 Simple Registration Extension 1.0

Tabella 3.3
Gli standard di Single-Sign-On "user centrici" supportati da IBM Tivoli Federated Identity Manager

OpenID è un framework "leggero" per un sistema di identità user-centrico derivante dalla comunità open source. Attraverso i protocolli OpenID l'identità di un utente viene rappresentata attraverso un URL dall'aspetto particolarmente familiare. OpenID si dimostra particolarmente adatto a situazioni in cui un service provider non ha l'esigenza o il desiderio di stabilire un rapporto particolarmente vincolato con un utente o un identity provider.

3.11 Il deployment della soluzione Tivoli per il single Sign-On federato

Nella Figura 3.4 è schematizzato il modello di deployment dei componenti di IBM Tivoli Federated Identity Manager per la realizzazione di un single Sign-On federato enterprise-centrico (SAML, Liberty o WS-Federation) o basato su OpenID o su un Identity Selector quale Microsoft Windows CardSpace o Eclipse Higgins.
La configurazione mostrata può essere considerata quella tipica per un sito Web che opera come un identity provider o un service provider all'interno di una federazione.
Facendo riferimento allo schema è possibile porre l'accento sui seguenti componenti:

- IBM Tivoli Access Manager for e-business WebSEAL: è utilizzato per il server Web che funge da punto di contatto; tutte le richieste del browser passano attraverso questo punto
- SSO Protocol Service: implementa i protocolli per SAML, Liberty e WS-Federation
- Security Token Service: un'implementazione di WS-Trust STS; gestisce I token per la creazione, la validazione e lo scambio all'interno delle varie federazioni
- IBM Tivoli Federated Identity Manager Management Service: un'applicazione Web-based per la configurazione delle caratteristiche federative
- IBM Tivoli Access Manager for e-business Policy Server: utilizzato per la gestione e la distribuzione delle policy di autenticazione/autorizzazione
- IBM Tivoli Access Manager for e-business Authorization Server: fornisce l'interazione con la directory LDAP dai componenti di autenticazione/autorizzazione dell'STS
- LDAP Registry: per memorizzare le identità degli utenti e gli alias.

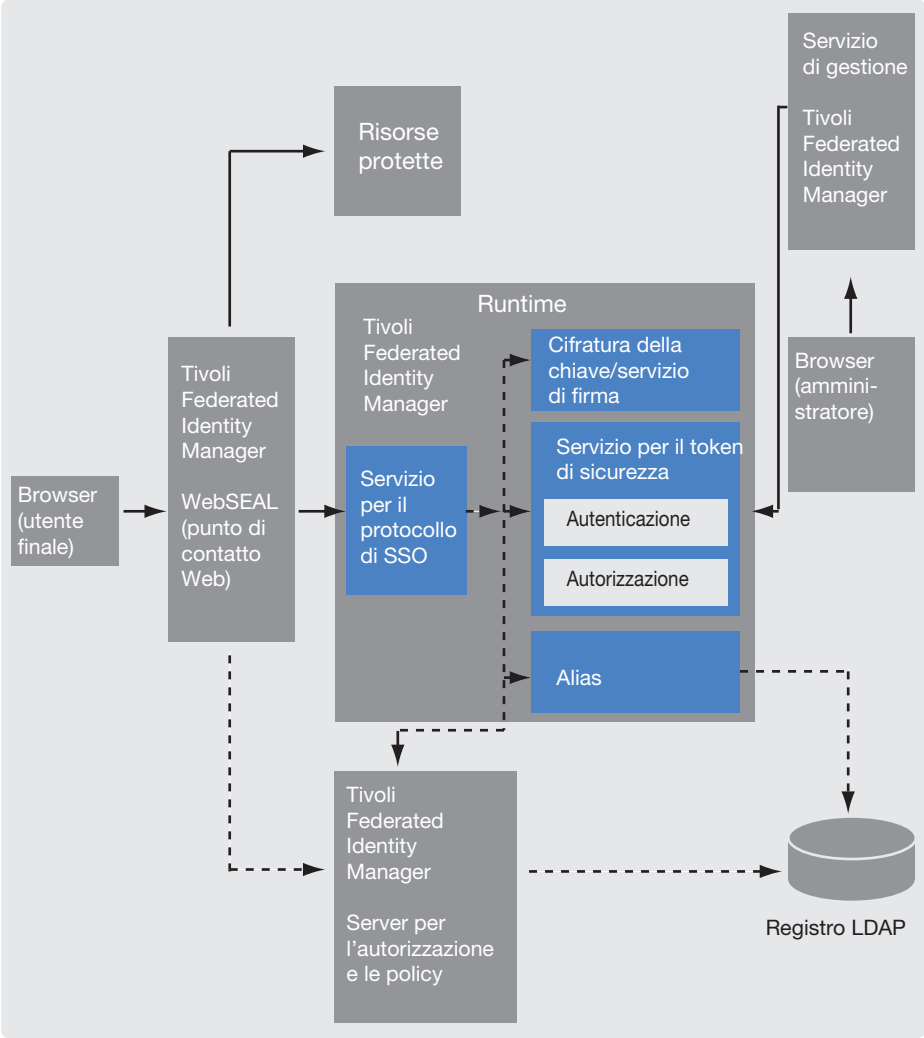


Figura 3.4
Deployment della soluzione Tivoli Federated Identity Manager per il Single Sign-On federato

IBM Tivoli Federated Identity Manager supporta anche un modello di deployment in cui i servizi di SSO possono essere integrati direttamente con Microsoft .NET e le applicazioni Ibm WebSphere senza che sia necessario utilizzare IBM Tivoli Access Manager for e-business.

Questo approccio risulta particolarmente indicato all'interno di ambienti in cui un'organizzazione enterprise dispone di una gestione dell'accesso di terze parti o è costituito da un business partner che richiede un modello di deployment per partecipare in una federazione utilizzando il Web application server come punto di contatto.

3.12 La gestione dell'identità e i Web Service

Un altro comune tipo di federazione può essere implementata utilizzando Web Service.
A differenza dello scenario del federated Single Sign-On che prevede un'interazione dell'utente per l'accesso alle applicazioni Web basata su browser, le federazioni dei Web Service sono basate sulla comunicazione tra applicazioni. Anche i Web Service dispongono di identità e, pertanto, a essi sono applicabili le medesime questioni legate alla federazione dell'identità e alla trust relationship esistente tra partner. Tuttavia, i protocolli e gli standard di sicurezza applicabili sono differenti e, in molti casi, potrebbe non essere possibile un'interazione diretta dell'utente per fornire le informazioni di autenticazione.
Parlare di Web Service significa realizzare una transizione da un modello focalizzato sui concetti di applicazioni e dati, verso uno orientato al servizio e alle operazioni.
Un Web service è costituito, di fatto, da un'applicazione modulare e autonoma, in grado di annunciarsi e di descrivere le proprie funzioni, che può essere pubblicata e richiesta attraverso la rete. Una volta che un'applicazione di questo tipo è stata rilasciata sul Web, altre applicazioni, oppure altri Web Service, sono in grado di richiamarla e di utilizzare il servizio da essa fornito.
I Web Service eseguono funzioni di business incapsulate, cha variano da una semplice richiesta di risposta fino a interazioni complete di processi di business. Una tipica applicazione Web service è costituita da un utilizzatore del servizio, un fornitore del servizio e, opzionalmente, da un registro in cui vengono memorizzate le definizioni dei Web Service.
Nell'ambito di un'architettura applicativa stratificata, un Web Service si traduce in una richiesta programmata di accesso a un servizio, che avviene attraverso un messaggio XML. La richiesta arriva a un livello di interfaccia esterno che propone le operazioni supportate dalla logica di business. Dopo essere passata per il Web server la richiesta XML viene convertita in una richiesta middleware e il risultato viene poi riconvertito in un messaggio XML che viene inviato come risposta.
L'adozione di un modello di architettura basato sui Web Service permette di costruire nuovi servizi in modo semplice, consentendo di elaborare nuovi modelli di business o di connettere in maniera più efficiente i tasselli che costituiscono la rete della catena del valore, realizzando relazioni più strette con i partner, i fornitori, i clienti e i dipendenti.

Le implementazioni dei Web Service sono in grado di sfruttare in modo ottimale i vantaggi offerti dalle risorse di federated identity management contribuendo al ROI aziendale.

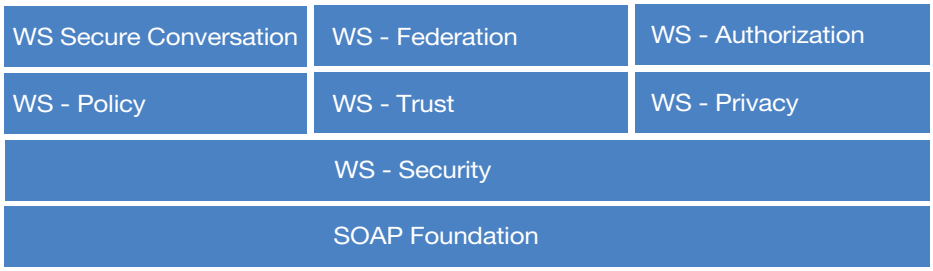
3.12.1 I protocolli dei Web Service

I Web services sono accessibili attraverso protocolli Internet standard che sono indipendenti dalle piattaforme e dai linguaggi di programmazione.
Il Web Services Description Language (WSDL) è un formato XML (utilizzato soprattutto dai service provider) che definisce una modalità per descrivere il formato delle richieste di Web Service su differenti protocolli o codifiche, ovvero per descrivere cosa può fare un determinato Web Service, dove si trova, chi lo eroga e come accedervi/invocarlo.
Il protocollo SOAP (Simple Object Access Protocol) è una specifica di descrizione dei messaggi per il loro trasporto sulla rete. Definisce un modo uniforme per trasferire dati codificati in XML e per eseguire RPC (Remote Procedure Call) utilizzando HTTP come protocollo di comunicazione sottostante. SOAP minimizza il problema dell'incompatibilità tra molteplici piattaforme nell'accesso ai dati.
WS-Policy è il tassello che fornisce una grammatica flessibile ed estensibile per rappresentare le funzionalità, i requisiti e le caratteristiche generali di entità all'interno di un sistema XML basato su Web Service. In altre parole, WS-Policy permette ai Web Service di specificare i loro requisiti di sicurezza verso potenziali client in modo interoperabile.

3.12.2 Le specifiche WS-Security

La progressiva diffusione dei Web Service porta con sé, inevitabilmente, la richiesta di condizioni sicure in cui operare. Per poter accedere ai servizi pubblicati sul Web si rende necessaria una fase di autenticazione a cui si aggiungono i requisiti indotti dai nuovi servizi che vengono creati per gestire l'identità in rete. Anche per i Web Service si rendono necessari i tradizionali requisiti di sicurezza quali audit, cifratura, autorizzazione, autenticazione e l'implementazione di policy e opportune procedure. Per far fronte a questi requisiti sono stati ratificati una serie di standard
La famiglia di specifiche Web Services Security (WS-Security) costituisce un insieme di standard individuali, tra loro correlati, che forniscono, nel loro complesso, un approccio stratificato per identificare e rendere sicuri i Web Service.

Figura 3.5
La famiglia di specifiche per la sicurezza dei Web Service



Di fatto, WS-Security rappresenta un set standard di estensioni SOAP, utilizzabili per la costruzione di Web Service sicuri al fine di implementare funzioni di integrità e confidenzialità.
WS-Security è stato progettato per rappresentare una base per la costruzione di un'ampia varietà di modelli di sicurezza inclusi Public Key Infrastructure (PKI), Kerberos e SSL. In modo più specifico, WS-Security fornisce il supporto per molteplici token di sicurezza, per "trust domain", per diversi formati di "signature" e tecnologie di cifratura.
Queste specifiche prevedono tre meccanismi principali: la propagazione di token di sicurezza, l'integrità del messaggio e la sua confidenzialità. Questi meccanismi da soli non garantiscono la completa sicurezza; WS-Security è, quindi, un tassello che può essere utilizzato congiuntamente ad altre estensioni dei Web Service e a protocolli di più alto livello, specifici per le applicazioni, per mettere a punto una varietà di modelli di sicurezza e di tecnologie di cifratura.
Rispetto a un sistema SSL il vantaggio che si ottiene con l'utilizzo di WS-Security è di fornire a livello di messaggio una protezione di tipo end-to-end. Questo significa che i messaggi sono protetti anche se attraversano una pluralità di nodi o intermediari. Inoltre, WS-Security è indipendente dal livello di protocollo di trasporto.

3.12.3 WS-Trust

Il Web Services Trust (WS-Trust) definisce un framework che utilizza il meccanismo per la sicurezza dei messaggi di WS-Security per definire una serie di estensioni per l'emissione, lo scambio e la validazione dei token di sicurezza; abilita, inoltre, l'emissione e la diffusione delle credenziali all'interno di domini trust.
Per realizzare una comunicazione sicura tra due parti, queste devono scambiare tra loro delle credenziali di sicurezza in modo diretto o indiretto. WS-Trust è l'estensione di WS-Security che consente alle due parti coinvolte in questo processo di verificare se si possono fidare delle credenziali fornite, grazie allo scambio di un token di sicurezza e alla definizione di modalità per stabilire e verificare la presenza di relazioni di fiducia.

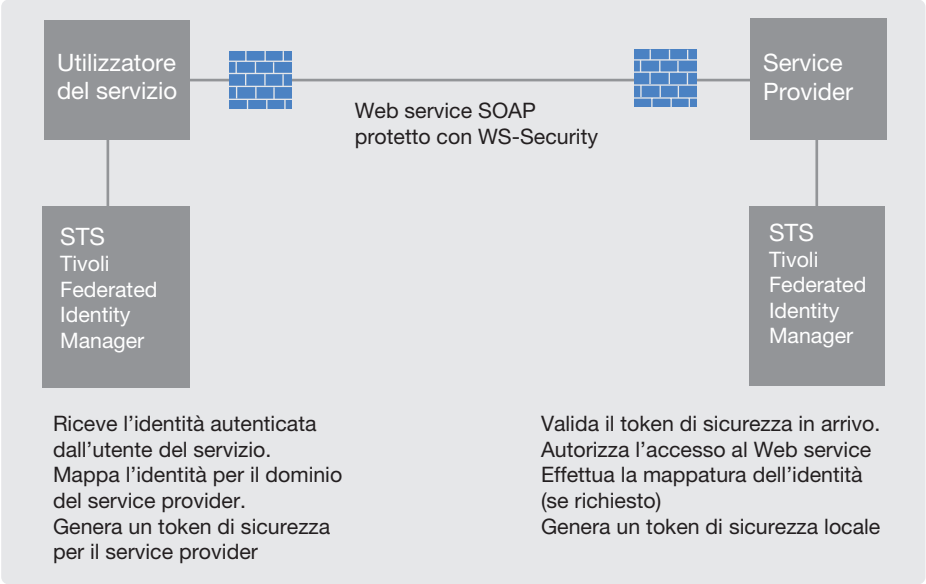


Figura 3.6
Una tipica implementazione di gestione dell'identità sicura basata su Web Service. L'utente del servizio Web manda la richiesta al service provider mediante un security token service utilizzando un messaggio WS-Trust. Il token viene trasmesso con la richiesta SOAP e trasporta informazioni sull'identità dell'utente (per esempio un'asserzione SAML)

3.13 La propagazione dell'identità in una SOA e il Security Token Service (STS)

Affinché le Service Oriented Architecture (SOA) risultino efficaci nel compito di allineare l'IT con il business, l'identità del richiedente del servizio deve poter attraversare tutti gli step di un'applicazione composta costituita da componenti debolmente accoppiati.
Poter stabilire l'identità del richiedente il servizio rappresenta un passo fondamentale per poter garantire l'implementazione di requisiti di business quali autorizzazione, audit e compliance. È perciò necessario predisporre servizi di identità all'interno di un'infrastruttura SOA in modo che i servizi possano essere facilmente interconnessi mentre le corrette identità sono propagate.
La propagazione delle identità all'interno della SOA deve essere considerata come una responsabilità dell'infrastruttura SOA e non delle applicazioni, se si vuole fornire il livello di flessibilità richiesto in un ambiente di business dinamico. Sulla base di questa premessa appare, pertanto, un logico passaggio che l'identità sia considerata come un servizio che possa essere invocato da varie piattaforme infrastrutturali SOA: per esempio gli application server o gli Enterprise Service Bus (ESB).
La specifica WS-Trust mette a disposizione un meccanismo basato su standard grazie al quale l'infrastruttura SOA è in grado di accedere a un servizio di identità per validare, trasformare e rilasciare token di sicurezza che rappresentano identità.

Un servizio che è in grado di rispondere a una richiesta WS-Trust viene chiamato *Security Token Service (STS)*. Detto in altri termini, questo significa che WS-Trust definisce meccanismi per delegare le operazioni di autenticazione, autorizzazione e gestione/mappatura dell'identità a un authority denominata Security Token Service (STS) all'interno di un processo di autenticazione che coinvolge i Web Service.

Nel caso in cui un Web Service client (WSC) effettui una richiesta di accesso a un Web Service provider (WSP) quest'ultimo può richiedergli una serie di informazioni (nome, ruolo, codice di autorizzazione e così via) che il WSC potrebbe non essere in grado di fornire direttamente. A questo punto interviene l'STS che opera come authority di intermediazione indipendente che fornisce le informazioni richieste al Web Service provider attraverso un token. Il Security Token Service che rilascia il token deve, però, avere relazioni di fiducia sia con il richiedente sia con il fornitore del servizio anche se questi non hanno relazioni tra loro.

IBM Tivoli Federated Identity Manager comprende tra le sue funzionalità fondamentali la possibilità di implementare un *Security Token Service* nelle modalità definite in WS-Trust. Questo servizio può essere utilizzato per creare, validare e scambiare i security token per WS-Security e WS-Federation e per fornire l'autorizzazione per le richieste dei Web Service.

Il Security Token Service fornito da IBM Tivoli Federated Identity rappresenta una soluzione di identità facilmente implementabile costruita utilizzando open standard e basata sui principi SOA che consentono di realizzare un'infrastruttura disaccoppiata dalla logica applicativa. Questo servizio è in grado di comprendere e operare con una varietà di formati di rappresentazione dell"identità ed è anche in grado di effettuare operazioni di mappatura a varie identità.

IBM Tivoli Federated Identity Manager STS prevede diverse configurazioni per la propagazione dell'identità (denominate *trust module chains*) che vengono accoppiate alle diverse richieste che arrivano all'STS all'interno di IBM Tivoli Federated Identity Manager, in base al valore di opportuni parametri (applicabilità, tipologia di token, "issuer" e così via). In questo modo la medesima istanza logica STS è in grado di supportare una varietà di requisiti di identità differenti.

Figura 3.7
Propagazione dell'identità all'interno di una SOA realizzata utilizzando WS-Trust e IBM Tivoli Federated Identity Manager STS

3.14 Il processo di autorizzazione del servizio nella SOA

La propagazione dell'identità rappresenta un aspetto certamente importante per la SOA, ma potrebbe non essere l'obiettivo finale. L'identità nella SOA è un fondamento sul quale è, infatti, possibile aggiungere un ulteriore valore di business.
A tal fine, l'utilizzo dell'identità rappresenta il requisito di base per abilitare servizi di:

- Autorizzazione, per determinare l'idoneità del richiedente di un servizio a potervi accedere e a utilizzarlo in base alle policy di sicurezza.
- Audit, per registrare il flusso di informazioni associate all'identità attraverso un'applicazione composta così come i risultati delle decisioni di autorizzazione del servizio.

IBM Tivoli Federated Identity Manager fornisce un meccanismo per estendere la propria soluzione di identità per la SOA in modo da includere il servizio di autorizzazione. Con IBM Tivoli Federated Identity Manager viene fornito un modulo di autorizzazione che è in grado di effettuare decisioni di autorizzazione utilizzando Tivoli Access Manager.
Il modulo di autorizzazione STS sfrutta le Tivoli Access Manager Java Authorization API per esaminare le decisioni di autorizzazione che sono determinate facendo una chiamata sicura al Tivoli Access Manager Authorization Server.

4
Applicazioni e sicurezza in ambienti SOA

La sicurezza delle applicazioni assume un'importanza fondamentale in un mondo sempre più connesso e complesso, in cui la disponibilità del servizio applicativo è la condizione per poter operare ed essere produttivi. Le architetture di nuova generazione, orientate ai servizi, o SOA, sono quelle che sin dall'inizio devono essere impostate con una sicurezza intrinseca e integrata.

Indipendentemente dal settore di attività, pubblico o privato, produttivo o finanziario, il mondo delle applicazioni sta diventando sempre più complesso e il fatto che l'operatività quotidiana dipenda da processi informatici rende la loro sicurezza un punto irrinunciabile di ogni strategia aziendale.
Un tale assunto vale ancora di più alla luce della diffusione di architetture informatiche quali la SOA (Service-Oriented Architecture), in cui le applicazioni possono operare liberamente, essere aggregate per formarne di nuove e interagire su scala planetaria tramite Internet o le reti di categoria pubbliche e private.
Se tutto ciò abilita un'elevata flessibilità e sofisticate possibilità applicative sinora impensabili, di assoluto rilievo è però il problema di come garantire la sicurezza delle applicazioni e delle architetture che ne permettono il funzionamento e la fruizione.
Per considerare le problematiche che si devono affrontare è utile far riferimento al settore bancario, assicurativo e finanziario, perché è tra i più competitivi e complessi. Presenta però il beneficio, per altri ambiti aziendali, di costituire la punta avanzata per quelle problematiche di sicurezza che poi finiscono con il coinvolgere progressivamente anche gli altri settori industriali. In sostanza, le esperienze in alcuni casi pionieristiche fatte in questo settore finiscono poi con l'essere esportate e applicate in buona parte del mondo produttivo e dei servizi pubblico o privato.
L'assioma di base di qualsiasi considerazione è che si tratta di un contesto con clienti esigenti e modelli di business che devono poter cambiare rapidamente in modo preciso.
Per avere successo, le aziende devono in particolare essere flessibili e quindi richiedere infrastrutture di Information Technology parimenti flessibili. È proprio ciò che conferiscono le architettura SOA ed è questo il motivo per cui si stanno progressivamente propagando nel mondo produttivo e finanziario. La diffusione di modelli di adozione come quelle sviluppate da IBM facilita l'ulteriore adozione da parte delle aziende di questo strumento che si sta rivelando estremamente utile ai fini competitivi perché mette a disposizione un'elevata flessibilità per quanto concerne proprio lo sviluppo di nuove applicazioni informatiche, che sono sempre più orientate a Internet e ai Web Service.

4.1 La criticità della sicurezza nelle architetture SOA

Il concetto SOA consiste essenzialmente in un metodo per convertire le applicazioni in componenti elementari del processo di business, denominati servizi.
Il vantaggio che ne deriva è che diventa possibile modificare rapidamente questi servizi, combinarli, aggiungerne nuovi e modificare i processi applicativi per rispondere alle specifiche esigenze di business, utilizzando i servizi creati in modo illimitato e ampiamente personalizzato.
Il processo di business, in sostanza, non risulta più vincolato da una specifica piattaforma o da un'applicazione, magari disponibile presso un solo fornitore, da cui dipendono i tempi di aggiornamento e le risorse in grado di apportare le modifiche necessarie.
Al contrario, un processo può essere considerato come un componente elementare, quindi riutilizzato o modificato, e può interagire o combinarsi con componenti sviluppati da altri fornitori.
La chiave interpretativa, dunque, è che si tratta di un approccio che permette la creazione di servizi in grado di definire le condizioni di business; in altre parole, un'architettura che conferisce flessibilità al business. In questo modo, SOA costituisce un programma, quasi il DNA, che abilita l'integrazione di business.
Dal punto di vista pratico, SOA fornisce un'architettura per i sistemi e l'integrazione aziendale che aumenta in modo molto consistente e altrimenti irrealizzabile se non a costi elevatissimi la flessibilità delle informazioni del sistema, rispondendo dinamicamente ai requisiti di business.
In un mondo sempre più globale e competitivo le aziende devono essere flessibili e poter rispondere rapidamente in base alle esigenze dei diversi settori industriali.
Per reggere a sfide globali molte aziende si associano o vengono acquisite o si fondono, in modo da poter meglio rispondere alle sfide del mercato, di una concorrenza agguerrita e di clienti esigenti.
Il processo che ha visto coinvolto il settore bancario è esemplificativo delle problematiche che in tal caso si devono affrontare.
Nel settore bancario, per esempio, a partire dal 1985, circa 50 banche primarie si sono consolidate in cinque e il processo sembra dover continuare. Si è trattato di acquisizioni in cui gli attori non condividevano gli stessi processi di business, le stesse soluzioni informatiche o applicazioni e ciò ha reso difficile la scelta e la reattività dei processi.

A queste sfide se ne sono aggiunte poi altre, come la necessità di rispondere alle nuove e rigorose normative pubbliche e di categoria per il trattamento dei dati e la loro riservatezza. Inoltre, quello che si è rivelato necessario è stato l'introdurre rapidamente nuovi servizi al fine di mantenere e conquistare nuovi clienti e soprattutto farlo contenendo i costi.
Nel complesso, sono sfide che hanno reso obbligatorio disporre a livello aziendale di un'estrema flessibilità e reattività, due obiettivi che si possono

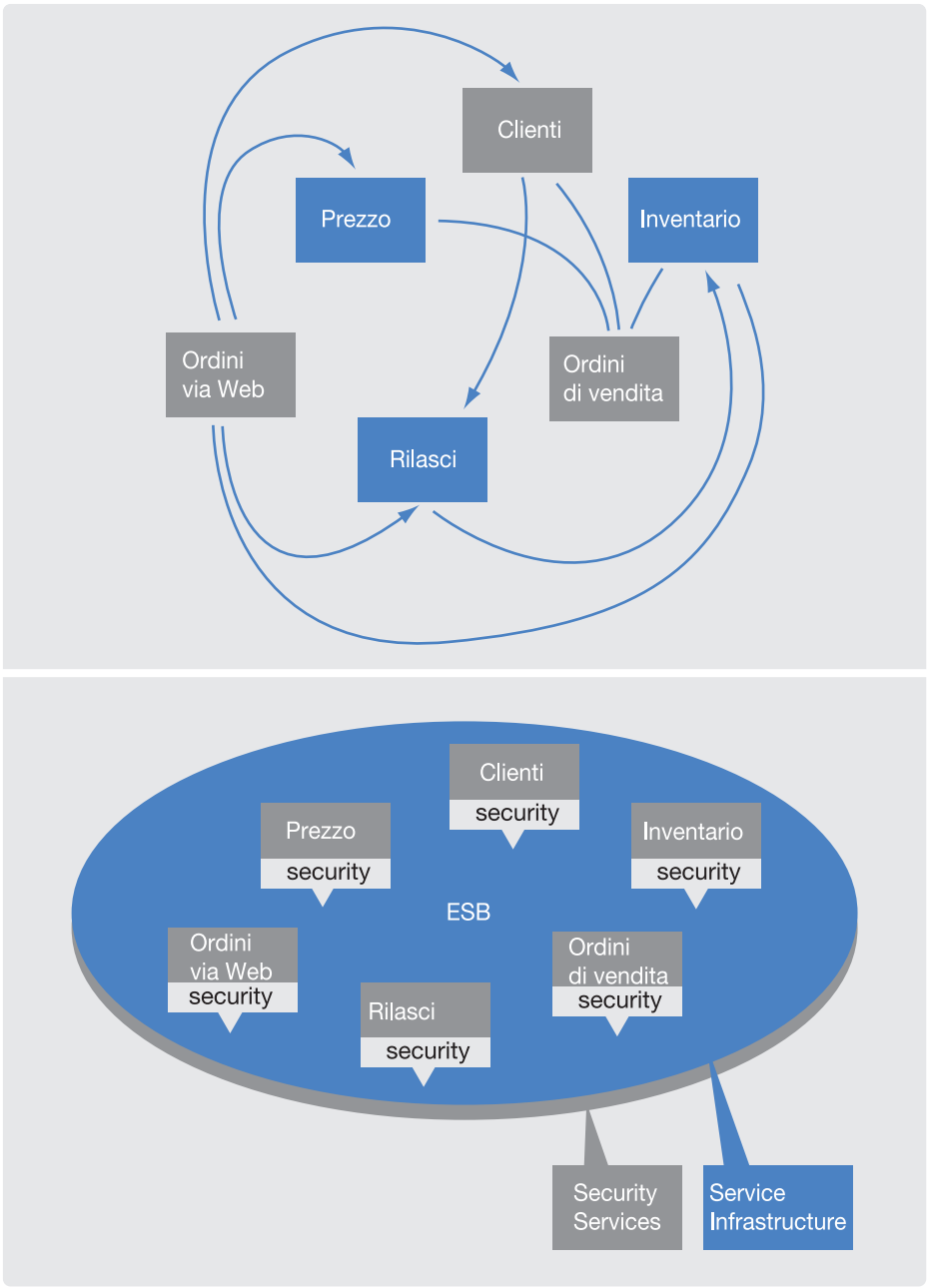


Figura 4.1
La semplificazione delle applicazioni nel passaggio da un modello disorganico a uno basato su SOA. Sopra: il modello usuale di relazione diretta tra servizi. Sotto: Il modello dei servizi basati su SOA

raggiungere solo se lo è parimenti anche l'infrastruttura di Information Technology e in particolare lo sono le applicazioni.
In questi casi e per queste esigenze la soluzione SOA è la risposta più adatta ed è particolarmente utile alle aziende con un portafoglio di applicazioni complesso come il mondo bancario.
Le banche hanno svariate filiali e diversi canali (bancomat, servizi online, per citarne un paio), che vanno supportati con una complessità di processi e applicazioni. Un problema che s'intensifica in caso di fusioni e acquisizioni. Inoltre, le attività di business devono sviluppare processi efficienti, sia internamente sia esternamente. I motivi per adottare SOA sono quindi svariati, ma una tale architettura non é utile esclusivamente al mondo finanziario. Anzi, è sempre più indispensabile anche per tutte quelle aziende che come caratteristiche e diffusione sul territorio hanno esigenze simili di flessibilità e dinamicità.

4.1.1 I vantaggi di business con l'integrazione dei servizi SOA

Per lo sviluppo di nuovi servizi, indipendentemente dal settore in cui opera la propria azienda, al CIO (Chief Information Officer) viene generalmente chiesto di conseguire due obiettivi principali: aumentare l'efficienza del business e ridurre i costi.
Allo stesso tempo gli viene chiesto di aumentare le opportunità di crescita del business tramite una maggiore reattività alle necessità dello stesso, anche se questo può dipendere da fattori esterni difficilmente prevedibili, per esempio atti terroristici, calamità naturali, crolli di borsa, mancanza di materie prime, decisioni governative o altro.
Sono obiettivi che sono perseguibili con un'infrastruttura informatica moderna, dinamica e con applicazioni basate su SOA.
Tuttavia, anche se in percentuale sempre più ridotta, persiste secondo Gartner un numero non trascurabile di manager che stentano a considerare l'Information Technology come uno strumento atto a facilitare il business e come tale indispensabile per raggiungere gli obiettivi aziendali. Una tale limitata visione fa si che le loro aziende non abbiano a disposizione l'integrazione e la flessibilità abilitata dal settore IT per supportare le esigenze di business. Non a caso, esiste una relazione diretta oramai ampiamente consolidata tra il successo di un'azienda e il suo grado di informatizzazione e in questa informatizzazione il ruolo di SOA sta continuamente crescendo.

Dal punto di vista pratico, quando si adotta un'architettura SOA, che è basata su standard internazionali ampiamente condivisi, si rimuovono le barriere sino a oggi presenti nel mondo dell'Information Technology, perché diventa possibile modificare i processi richiesti dai clienti senza dover cambiare anche la tecnologia di base. Contemporaneamente, è possibile migliorare la tecnologia di back end su cui si basano le applicazioni, senza dover intervenire anche a livello di front end, con un disaccoppiamento che facilita di volta in volta l'intervenire e aggiornare uno o l'altro dei due ambienti.
Quello che ne consegue, come già evidenziato, è una reattività di business molto elevata, che offre la possibilità di introdurre sul mercato nuovi prodotti e servizi rapidamente e con maggiori opportunità di guadagno.
Ma non si tratta solo di ottenere benefici esclusivamente interni di flessibilità nello sviluppo di applicazioni. Un altro grande vantaggio è che si possono utilizzare funzioni di integrazione che permettono di concentrarsi sulle best practice utili allo sviluppo di un'azienda.
Nel caso di acquisizioni, le aziende possono sfruttare le funzionalità rese disponibili da SOA per esportare rapidamente le best practice delle aziende acquisite, o, al contrario, applicare alle aziende acquisite quelle sviluppate in house. È possibile, per esempio, adottare i processi del ramo aziendale che ha saputo instaurare il rapporto migliore con i clienti o che ha saputo scegliere le migliori motivazioni per consigliare ai clienti l'utilizzo e prodotti come le carte di credito.
L'impatto positivo sulla flessibilità ha naturalmente un pari impatto benefico sui costi di struttura e operativi.
In un progetto basato su SOA realizzato da IBM per Bank of America la semplificazione che ne è derivata per la divisione dei servizi carte di credito ha consentito di ottenere un risparmio di 40 milioni di dollari in due anni. L'elemento di base è in tal caso consistito nello sviluppo di un modello di business basato sui componenti al fine di identificare le opportunità di business ed eliminare gli sprechi.
SOA e l'integrazione di business consentono quindi enormi risparmi nel settore dell'Information Technology e offrono la possibilità di creare, modificare e riutilizzare i servizi aumentando così in modo anche molto consistente l'efficienza aziendale.

4.2 La sicurezza delle applicazioni

Un numero crescente di imprese riconosce i vantaggi che derivano dall'impiego di componenti software riutilizzabili, basati su standard aperti, in un approccio di architettura orientata ai servizi. Questo perché adottare un tale approccio può tradursi in molti benefici: da un miglioramento delle transazioni finanziarie e degli acquisti online, a un'ottimizzazione del magazzino tra i vari fornitori, con conseguente risparmio di costi, a presentazioni multicanale e sincronizzate dei prodotti.
Allo stesso modo, adottare gli standard aperti, come quelli per i Web Service basati su XML, ha permesso a numerose aziende di migliorare la produttività, rispondere rapidamente all'evoluzione delle esigenze di business e cogliere le opportunità nel momento stesso in cui emergono.
Per sfruttare questo miglioramento nei processi di business, nella flessibilità e nell'efficienza dell'IT, prodotto dal passaggio alla SOA, le organizzazioni necessitano però di risolvere alcuni aspetti chiave quali:

- servizi e controlli scalabili e pervasivi;
- una solida sicurezza;
- un'elevata garanzia dei servizi nelle loro infrastrutture.

Oggi alcune organizzazioni si trovano in difficoltà nel far fronte a questi requisiti critici della SOA senza per questo dover sopportare costi sostenuti, complessità elevata e infrastrutture difficili da predisporre e gestire.
Affrontare contemporaneamente queste sfide richiede infatti un approccio pragmatico all'adozione di SOA. Un approccio in grado di prevedere e affrontare simultaneamente fattori quali:

- l'evoluzione degli standard;
- il valore degli investimenti esistenti in infrastrutture;
- le sfide della propria organizzazione;
- l'impatto sulle prestazioni tra le varie applicazioni.

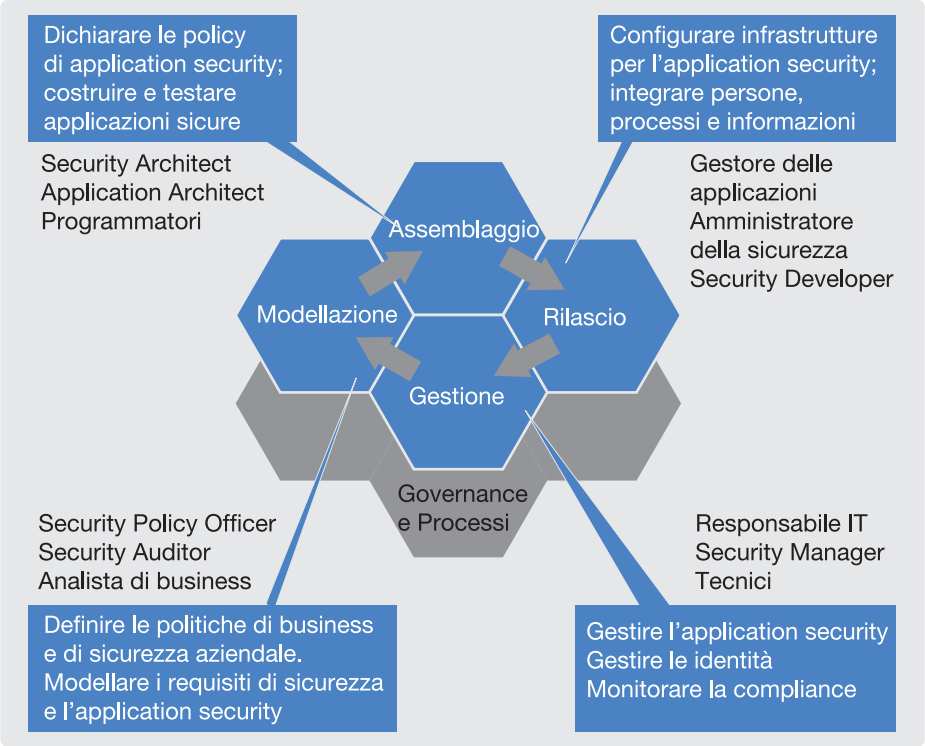
In tutto questo, come evidenziato, uno degli elementi fondamentali è la sicurezza, che interessa l'intero ciclo di vita di un'architettura SOA e delle applicazioni coinvolte.

4.2.1 Le esigenze di sicurezza di ambienti SOA

Garantire la sicurezza nell'accesso alle informazioni è un elemento fondamentale in ogni tipo o applicazione di business.
La sicurezza diventa ancora più importante e un fattore critico per implementazioni strutturate in accordo ai principi che sono alla base dell'architettura SOA, e questo come diretta conseguenza del lasco accoppiamento che esiste tra servizi e applicazioni e la loro interazione operativa al di sopra dei singoli confini organizzativi di un'azienda.
Un tale ambiente risulta, in sostanza, particolarmente esposto in termini di sicurezza, non ultimo anche per la sua naturale proiezione verso Internet e i Web Service.
In base alle osservazioni realizzate su un numero ampio di scenari e ai pattern che li caratterizzano è però possibile articolare le capacità richieste e creare un modello di riferimento che indirizzi specificatamente queste capacità.
Rendere sicuro un business necessita di una infrastruttura flessibile e customizzabile in base alle esigenze, così che essa possa adattarsi semplicemente a nuove necessità e regolamenti.
Assicurare la protezione del solo perimetro del sistema informativo relativo all'area in cui operano le applicazioni business mediante firewall e router non è sufficiente. Questo perché un business necessita di interazioni dinamiche che possono essere condotte con relazioni tra le entità coinvolte sicure e credibili, su ampi periodi di tempo e con il coinvolgimento continuo di partner industriali o di affari, clienti e dipendenti.
Per fornire una tale flessibilità, un business necessita di far leva su una infrastruttura di servizi di sicurezza adatta nonchè su una infrastruttura che sia basata su policy predefinite.
Qualora si vogliano raggiungere gli obiettivi di business prefissatisi mediante l'utilizzo estensivo di strumenti di Information Technology e in un modo che sia possibile sottoporre ad attività di auditing, è poi indispensabile prevedere nel ciclo di vita di una applicazione specifiche policy inerenti la sua sicurezza.
Se si esaminano le sfide poste dalla gestione della sicurezza dal punto di vista di chi disegna le applicazioni, il loro flusso e le loro interrelazione, in sostanza le architetta, per un ambiente orientato ai servizi si evidenziano svariate considerazioni:

- La necessità di disaccoppiare l'*Identità* del fruitore dal *Servizio* fruito. Tutte le entità in un'architettura SOA hanno una propria e unica identità, siano essi user o servizi o altro, identità che deve essere propriamente identificata in modo da poterle applicare i controlli di sicurezza

Figura 4.2
Il ciclo di vita di un'architettura SOA dal punto di vista della sicurezza



più adatti. Per esempio, il controllo delle impronte potrà essere applicato a un essere umano e non a una applicazione software.

- La necessità di potersi connettere in modo trasparente ad altre organizzazioni su base transazionale e in real-time.
- La necessità di assicurare che, per applicazioni composite, siano attivati per ogni servizio gli appropriati controlli di sicurezza così come lo debbono essere quando più servizi sono combinati tra loro.
- La necessità di gestire l'identità e la sicurezza attraverso un ampio range di sistemi e servizi che sono implementati con diverse combinazioni di tecnologie di vecchia o nuova generazione.
- La protezione dei dati sia quando sono in transito che quando sono residenti in un sistema.
- La capacità di dimostrare la compliance delle applicazioni e delle procedure con un numero crescente di standard regolatori di corporate, enti pubblici e privati e associazioni.

La gestione delle identità di user e servizi

Un'architettura SOA permette di creare ed erogare servizi che possono essere interconnessi tra loro e riutilizzati per rispondere alle esigenze di particolari processi di business. Ancor di più, questi servizi possono esser

connessi e implementati in una modalità sicura e controllabile da attività di auditing in base a policy di sicurezza predefinite.
L'identità gioca quindi in tutto questo un ruolo chiave e la figura 4.3 evidenzia le sfide che si devono affrontare al fine di garantire l'identità in un ambiente SOA.
Va osservato che l'Identità esiste sia per gli user che per i servizi, ed entrambe devono essere assoggettate ai medesimi controlli.
Può essere necessario che le identità possano essere propagate attraverso l'intero ambiente SOA.

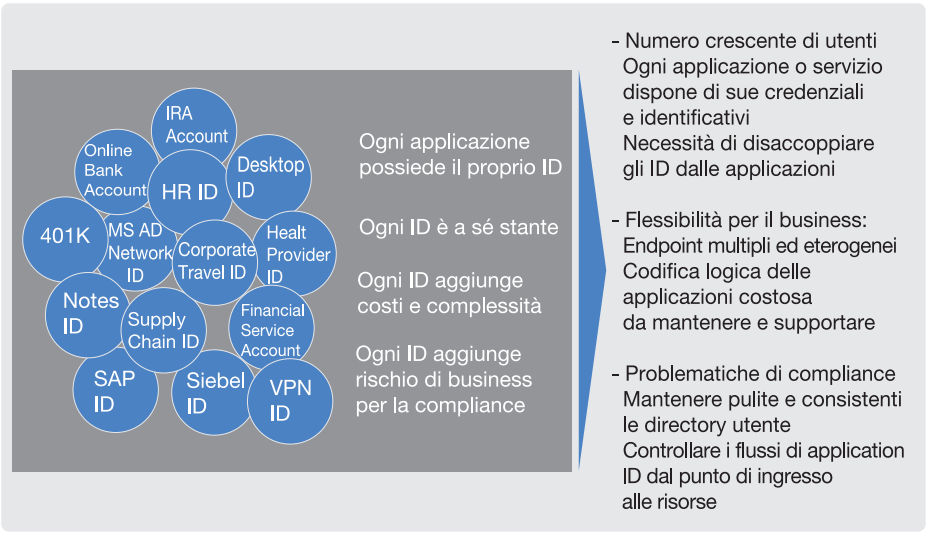


Figura 4.3
Le motivazioni per garantire l'Identità in un ambiente SOA

In molti casi, tuttavia, la modalità stessa di implementazione dei servizi può limitare le opzioni e i formati disponibili per la propagazione delle identità di un user verso o da un particolare servizio.
Agli "Identity Service" di una infrastruttura è quindi richiesto di poter far fronte a questi problemi, in modo da far sì che in ogni caso i servizi possano essere facilmente interconnessi senza che ci si debba preoccupare di come mappare e propagare la user identity di uno specifico utente da un servizio a un altro.
Un tale approccio e una tale flessibilità permette di ridurre consistentemente l'ammontare di nuovo codice software che deve essere scritto e di accelerare di conseguenza la velocità con cui viene sviluppato, e posto in produzione, un nuovo servizio.

Applicazioni composite

Le policy per la sicurezza includono le regole stabilite per permettere l'accesso ai servizi. Un utente o un servizio può però necessitare di disporre di specifici privilegi che gli permettano un tale accesso.

Quando i servizi sono combinati tra loro per fornire un servizio di livello superiore, per esempio un processo di business più complesso, e cioè vengono inseriti in una particolare coreografia, la combinazione dei servizi può richiedere un attento riesame delle policy di sicurezza.
Per esempio, un user può essere abilitato ad accedere al servizio A e al servizio B in modo indipendente ma può accadere che questi due servizi vengano inseriti nella medesima coreografia con altri servizi a cui l'user non è abilitato ad accedere.
In tal caso deve essere deciso se l'user può o meno mantenere i privilegi che lo caratterizzavano in precedenza, e se tali privilegi devono essere estesi o meno al nuovo servizio di livello superiore.
In sostanza, la complessità di un ambiente SOA consiste nel fatto che la policy per la sicurezza che caratterizza le coreografie dei servizi necessita che sia tenuto in attenta considerazione la combinazione e l'integrabilità dei servizi in differenti combinazioni, in funzione di quanto è richiesto dai cambiamenti inerenti i processi di business.
Ogni nuova coreografia, e cioè ogni nuova combinazione di servizi, può richiedere un riesame delle policy di sicurezza in modo da garantire che essa mantenga la sua validità anche nelle nuove associazioni.

La gestione della sicurezza attraverso ambienti diversi

Una tipica architettura SOA può presentare molti punti in cui una policy di sicurezza può essere erogata e implementata. Questi punti di "*erogazione*" della policy possono essere allocati sia a livello dei servizi di connettività così come all'interno delle implementazioni medesime dei servizi.
La gestione della policy attraverso questi punti di erogazione vari ed eterogenei fa sì che un amministratore debba disporre di diversi set di interfacce che abilitino una gestione centralizzata e una precisa associazione degli "oggetti" coinvolti nella sicurezza. Inoltre, è necessario che il tutto sia correlato da una apposita terminologia e semantica di policy di sicurezza.
Se però si vogliono, nell'ambito di una SOA, raggiungere gli obiettivi di flessibilità del business all'interno di un ambiente di governance e in modo da risultare compliant con i regolamenti, sia le definizione che le attività di gestione delle policy di sicurezza è opportuno che risultino il più possibile semplificate.
In sostanza, è opportuno che ci sia una terminologia e una semantica consistente e omogenea in ogni punto in cui la sicurezza interviene ed è erogata e che la cosa sia compresa in un apposito modello.

4.3 Il modello di riferimento per la sicurezza SOA di IBM

Per rispondere alle esigenze applicative, di management e di sicurezza connesse a un ambiente SOA, IBM ha sviluppato uno specifico modello di riferimento che risponde a tutte le esigenze che sono andate nel tempo esprimendosi a livello di utilizzatori e discusse nei paragrafi precedenti.
La definizione del modello trova le sue motivazioni nel fatto che un tale modello può aiutare nell'indirizzare i requirement e portare alla realizzazione di una architettura logica, e in fase successiva a una architettura fisica, in cui prodotti e tecnologie sono opportunamente mappati al fine di risolvere i problemi che via via si presentano nello sviluppo e nella gestione di applicazioni di business e, nello specifico, per quanto concerne gli aspetti connessi alla sicurezza di processi applicativi, dati e utilizzatori.
La security è applicabile a tutti i livelli di un modello SOA:

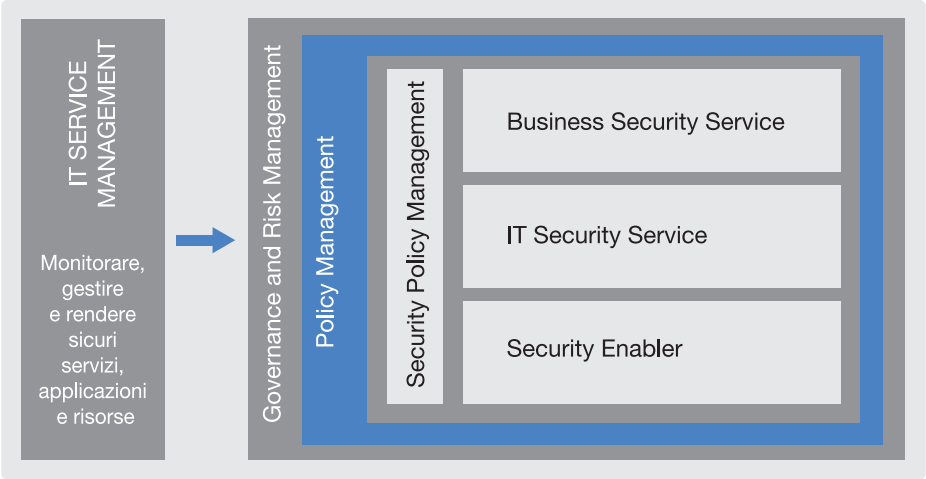
- a livello dell'intera infrastruttura;
- a livello delle applicazioni;
- a livello dei servizi di business;
- a livello dei servizi di sviluppo.

In quest'ottica e in base a quanto già considerato, il modello di riferimento può essere visto come suddiviso in diversi livelli di astrazione e precisamente in quelli di: Business Security Service, IT Security Service e Security Policy Management, cui va aggiunto un ulteriore livello, il "Security Enablers", che ha il compito di fornire le funzioni di sicurezza agli IT Security Service.
Le aree principali che compongono il modello sono le seguenti:

- *Business Security Service* - è inerente alla gestione delle esigenze e delle richieste del business, come per esempio il riconoscimento sicuro, la gestione di identità e accessi, la protezione dei dati scambiati tra le applicazioni e i servizi, la non ripudiazione e la sicurezza dei sistemi e della rete. Adottano la policy infrastrutturale comune a tutto l'ambiente SOA in modo da gestire le policy necessarie per soddisfare le esigenze del business.
- *IT Security Service* - descrive i blocchi di base per un'infrastruttura SOA e fornisce quanto è necessario al fine di rendere sicu-

Figura 4.4

Il modello di riferimento IBM per la sicurezza in ambienti SOA: le capacità di sicurezza all'interno dell'IT Service Management



ri i servizi e soddisfare le esigenze di applicazioni e infrastrutture erogando le stesse funzioni di sicurezza come se si trattasse a loro volta di servizi. Questi servizi includono la certificazione dell'identità, l'autenticazione mediante metodi sofisticati, l'autorizzazione, così come la confidenzialità, l'integrità dei dati e servizi di audit.

- *Security Enablers* - comprendono tecnologie quali la crittografia, directory e le aree dove sono mantenute le chiavi di cifratura che sono utilizzate dagli IT Security Service per realizzare i propri compiti.
- *Security Policy Management* - fa parte dell'omnicomprensivo e trasversale livello di Policy Management ed è inerente all'articolazione, alla gestione, alla messa in atto e al monitoraggio delle politiche di sicurezza. Questo include la capacità di definire policy per utenticare e autorizzare le entità che richiedono l'acceso a un particolare servizio, di propagare specifici contesti di sicurezza in base alle richieste dei richiedenti e alle caratteristiche del modello di credenziali adottato, effettuare l'audit degli eventi significativi e proteggere le informazioni. In sostanza, la funzionalità costituisce una parte essenziale nel fornire a una SOA le sue caratteristiche di sicurezza.
- *Governance e Risk Management* - fornisce i meccanismi che implementano e permettono di attuare le policy di sicurezza a livello dell'intero ambiente esteso interessato da SOA. La Governance supporta nel gestire la SOA a livello dell'intera organizzazione aziendale. Il Risk management si occupa dei processi di valutazione e di assessing del rischio nell'ambiente SOA e dello sviluppo delle strategie più adatte alla gestione di questi rischi.

Il modello di sicurezza per SOA non è però astratto dal contesto di business aziendale. Va osservato, infatti, che all'interno del modello IBM SOA Reference Model, il modello IBM SOA Security Reference Model costituisce un sotto elemento di IT Service Management, che rappresenta la visione omnicomprensiva di IBM per la gestione dei servizi per applicazioni business.

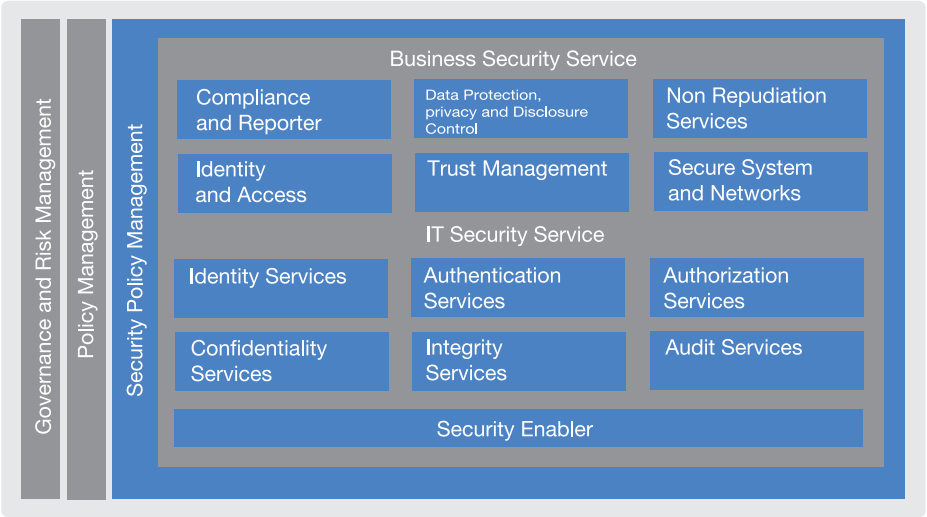


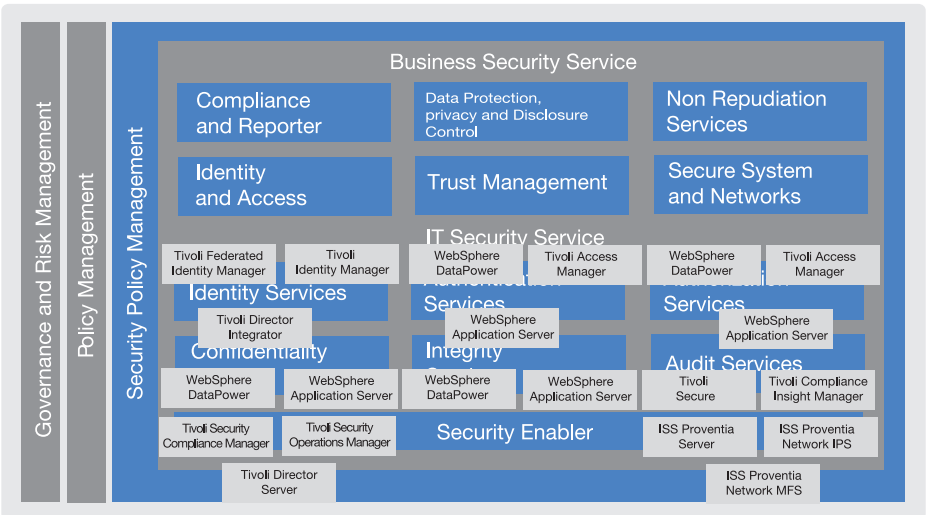
Figura 4.5
Il modello SOA Security Reference Model sviluppato da IBM

4.3.1 I prodotti e i servizi IBM per la sicurezza delle applicazioni

IBM ha sviluppato una serie molto ampia di prodotti che si mappano all'interno del suo modello di riferimento per la sicurezza IBM SOA Security Reference Model. Parte di questi prodotti sono stati descritti nei capitoli 2 e 3, laddove si vanno a indirizzare più in dettaglio le tematiche legate alla gestione degli eventi di sicurezza e quelle di federated identity management e di identity service. Per questi ultimi argomenti e la loro connessione con gli ambienti SOA, in particolare, rimandiamo alla lettura del paragrafo 3.13 del precedente capitolo, in cui sono descritte soluzioni appartenenti alla linea IBM Tivoli.
Le aziende hanno la possibilità di selezionare liberamente, in funzione delle loro necessità e pianificazioni di budget, nonché in base a un accurato approccio costo/benefici, uno o più di questi prodotti in modo da soddisfare le sue esigenze peculiari di sicurezza delle applicazioni e della loro fruizione da parte di altre applicazioni o di utenti interni ed esterni al proprio ambito aziendale.

Alcuni dei ruoli di un'organizzazione hanno il compito di contribuire alla creazione, alla definizione, alla messa punto, il monitoraggio, la verifica e il management delle policy inerenti la sicurezza per l'intero ciclo di vita di un'architettura orientata ai servizi.
Il motivo è semplice. SOA è per certi aspetti una sofisticata strategia di business che aiuta le aziende nel riutilizzare le tecnologie esistenti al fine di allineare in modo più intimo il proprio comportamento dal punto di vista applicativo con quelli che rappresentano gli obiettivi di business. Così facendo e mantenendo una continua attenzione agli elementi che compongono SOA e alle applicazioni, è possibile ottenere una maggiore efficienza, un risparmio sui costi, un miglior TCO, una maggiore agilità nei processi e una parimenti maggiore produttività individuale e complessiva.
Un elemento chiave della strategia IBM al fine di favorire l'ottenimento di questi goal è stato il rilascio di WebSphere Business Events, una soluzione che aiuta i professionisti dell'IT a identificare direttamente e analizzare in real-time le relazioni di causa-effetto tra i diversi eventi e nell'identificare e bloccare i possibili attacchi alla sicurezza al loro primo insorgere. Ciò viene realizzato tramite l'attivazione automatica di "trigger" quando si evidenziano dei trend anomali all'interno dei milioni di eventi casuali o schedulati che si verificano giornalmente all'interno delle applicazioni business di un'azienda.
Nel complesso, IBM mette a disposizione del mondo aziendale un ampio portafoglio pensato per effettuare automaticamente il tracciamento degli eventi e analizzare e reagire al cambiamento delle condi-

Figura 4.6
Il modello di riferimento per la sicurezza di IBM e i prodotti che ha reso disponibili

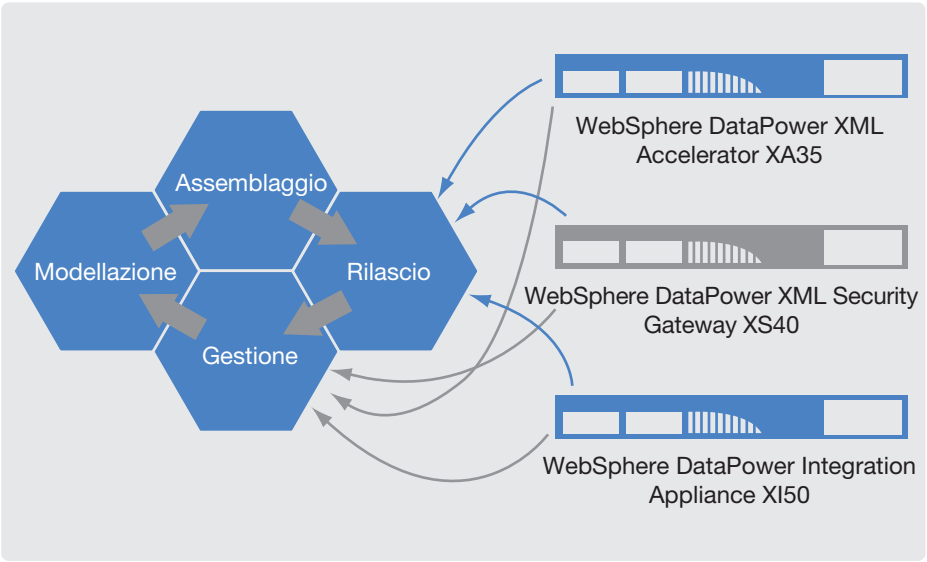


zioni di business sia in presenza di eventi pianificati che imprevisti. Molte delle soluzioni evidenziate nel modello sono già state citate nei primi tre capitoli, cui rimandiamo per brevi approfondimenti. In ogni caso, tutte le caratteristiche di prodotti e servizi IBM sono descritte in dettaglio sul sito della società.
IBM ha reso disponibile anche l'applicazione software WebSphere Virtual Enterprise, che permette alle aziende di qualsiasi dimensione di ridurre consistentemente gli onerosi costi operative e dell'energia associati con le applicazioni aziendali e l'ambiente SOA, ma incrementando allo stesso tempo la flessibilità del business e l'integrità dei processi applicativi.
I benefici sono ottenuti tramite la virtualizzazione dell'infrastruttura software che supporta le applicazioni e i servizi che risultano critici per i processi di business. Ma non basta. IBM ha espanso anche il framework del suo portafoglio di soluzioni per il mondo aziendale rilasciando IBM Banking Framework for Customer Care and Insight. Si tratta di un framework progettato al fine di aiutare il mondo bancario e del finance nel gestire e utilizzare con maggior profittabilità le informazioni inerenti i clienti in modo da aumentare il livello di fidelizzazione, i profitti, ridurre i rischi, migliorare l'efficienza operativa e incrementare la flessibilità in modo da supportare adeguatamente sia le esistenti che le nuove strategie di business.

IBM WebSphere DataPower

I dispositivi specializzati per la SOA IBM WebSphere DataPower rappresentano un modo evoluto per semplificare il rilascio, migliorare le prestazioni e potenziare la sicurezza delle implementazioni della SOA.
È un'ampia famiglia di prodotti che permette di far fronte alle varie esigenze aziendali ed é pensata come complemento dei prodotti specifici IBM o di altri, per supportare le varie fasi del ciclo di vita di un SOA.
I prodotti forniscono funzioni che aiutano nell'affrontare i problemi di accelerazione delle applicazioni, di sicurezza e di routing coinvolti nello sviluppo di una architettura SOA.
La tecnologia WebSphere DataPower è, in sostanza, in grado di soddisfare l'esigenza di un'elaborazione XML rapida e affidabile i cui apparati permettono di trasformare disparati formati di messaggi di back end in XML, applicando al contempo le politiche di servizi e di sicurezza a livello di messaggio.

Figura 4.7
I dispositivi specializzati WebSphere DataPower supportano le fasi di rilascio e gestione di SOA



Tramite WebSphere DataPower è possibile accelerare il rilascio della SOA in un ambiente a prova di sicurezza e con un dispositivo specializzato che richiede un ridotto intervento per la configurazione, personalizzazione e gestione.
È possibile inoltre accelerare l'integrazione delle applicazioni utilizzando un dispositivo WebSphere DataPower per ridurre al minimo il tempo necessario per implementare un'infrastruttura in grado di supportare in modo ottimale l'implementazione dell'IBM SOA Foundation.
Supportano inoltre nel proteggere il traffico della SOA e nell'implementare le funzioni di protezione dalle minacce relative all'XML e di sicurezza dei Web Service. Inoltre si integrano con il software di sicurezza e gestione delle identità, come per esempio il software IBM Tivoli.
I dispositivi specializzati per la SOA WebSphere DataPower hanno un fattore di forma adatto per rack standard. Il collegamento alla rete avviene tramite Ethernet.
I dispositivi integrano in un unico dispositivo molte delle funzioni chiave necessarie per l'adozione della SOA o dei Web Service. Sono progettati per essere installati con facilità in un ambiente esistente, come un dispositivo in-line in modalità proxy XML o parallelamente ai sistemi in modalità coprocessore.
I dispositivi, inoltre, supportano IBM Rational e altri ambienti di sviluppo integrato XML di uso comune, che aiutano a ridurre il tempo dedicato allo sviluppo e al debugging. È possibile inoltre utilizzare i dispositivi specializzati per la SOA WebSphere DataPower con IBM WebSphere Application Server, IBM WebSphere Process Server, IBM WebSphere

Portal, IBM WebSphere MQ, IBM WebSphere Enterprise Service Bus (ESB) e IBM WebSphere Message Broker, per elaborare le transazioni XML in modo più rapido, più sicuro e più semplice.
L'integrazione dei dispositivi WebSphere DataPower con IBM Tivoli Federated Identity Manager e IBM Tivoli Access Manager supporta nel realizzare ambienti SOA sicuri. Le soluzioni di gestione della sicurezza Tivoli consentono inoltre di gestire a livello centrale gli account e le credenziali degli utenti, di fissare le politiche della sicurezza e di controllare il traffico XML protetto dai dispositivi DataPower. L'integrazione con IBM Tivoli Composite Application Manager per la SOA consente un controllo centralizzato, la gestione dei livelli di servizio e il monitoraggio tramite cruscotti. La combinazione del software Tivoli e del gateway XML WebSphere DataPower fornisce, inoltre, le funzionalità per la sicurezza della SOA e la gestione dei Web Service richieste da un tipico ambito aziendale.

5
La sicurezza fisica

La sorveglianza dei propri asset, siano essi un piccolo negozio o l'agenzia di una banca può avvenire con maggiore efficacia e più flessibilità funzionale utilizzando un sistema video d'ultima generazione integrato con il resto del sistema per la sicurezza, abbassando contemporaneamente i costi, aumentando la protezione e prevenendo furti e truffe.

5.1 Le soluzioni integrate per la videosorveglianza

A prescindere dal settore in cui un'azienda opera, i sistemi di video controllo stanno assumendo un ruolo predominante nei processi di controllo per la sicurezza del business.
Anche apposite raccomandazioni governative richiedono alle imprese di fornire una maggiore documentazione video degli eventi. Inoltre l'utilizzo di tali tecnologie è enfatizzato dalla necessità di risolvere problematiche connesse alla sicurezza in generale, alla pubblica salvaguardia dei cittadini, alla prevenzione dei furti nonché al miglioramento della qualità del servizio offerto agli utenti.
Adottando tecnologie di video sorveglianza digitale è possibile, infatti, disporre di molti dati e informazioni contenute nelle immagini registrate e sovente le imprese non sono consapevoli delle enormi potenzialità messe a disposizione dall'utilizzo delle nuove soluzioni.
Le nuove tecnologie digitali sfruttano le reti aziendali basate sul protocollo Internet: in tal modo i dati possono essere utilizzati da diversi strumenti inclusi quelli che utilizzano la modalità d'accesso remota. Ciò porta a far sì che i responsabili IT delle aziende siano sempre più coinvolti nei programmi di sicurezza.
In parallelo, assume minore importanza l'archiviazione fisica in dispositivi di videoregistrazione a nastro e aumenta, invece, l'importanza delle problematiche legate all'archiviazione e gestione dei dati in formato elettronico. Grazie alla possibilità di indicizzare i dati digitali è possibile rivedere e ricercare i dati estratti dal video registrato con un determinato criterio, eliminando la necessità di dedicare un numero elevato di risorse e di tempo al controllo delle registrazioni stesse.
Tuttavia i benefici elencati rappresentano solo una piccola parte dei potenziali vantaggi derivanti dall'utilizzo delle nuove tecnologie.
Tutte le imprese, indipendentemente dal settore d'appartenenza, possono trarre benefici dall'utilizzo di tali tecnologie. Per esempio le forze dell'ordine possono utilizzare soluzioni di videosorveglianza al fine di prevenire o individuare le attività criminali e incrementare la salvaguardia dei cittadini e dei beni privati e pubblici. Allo stesso modo una banca può utilizzare tali tecnologie non solo ai fini di controllo e videosorveglianza, ma anche per migliorare la qualità del servizio offerto agli utenti gestendo in modo ottimale, per esempio, le code d'attesa agli sportelli.
Le aziende di distribuzione possono poi trarre vantaggio dall'adozione di tali tecnologie per prevenire le perdite o migliorare il servizio ai clienti, veri-

Figura 5.1
Un unico disegno architetturale integra le componenti di protezione ambientale, tecnologica e personale.

ficando anche se la disposizione dei prodotti sugli scaffali all'interno del negozio provoca o no l'attenzione della clientela.
Il punto fondamentale è in ogni caso che le imprese necessitano molto di più di un semplice insieme di dati video in archivio. Una necessità primaria è il dotarsi di sistemi che forniscono informazioni e risposte per migliorare le proprie attività di business e le proprie decisioni.
Il principale paradigma della sicurezza è che praticamente tutte le amministrazioni comunali, gli enti, le scuole, le aziende dei trasporti pubblici, gli istituti finanziari, le aziende di pubblico servizio e i centri medici devono tutelarsi dalle minacce e proteggere la sicurezza di dipendenti, clienti, cittadini, proprietà e infrastrutture IT. Non solo, perché al tempo stesso devono ridurre i costi operativi, migliorare la produttività e aumentare gli utili oltre che la soddisfazione dei clienti.
Esempi di rischi per la sicurezza e problematiche aziendali, che si possono gestire in modo più efficiente attraverso i metodi di videosorveglianza, sono:

- *Sicurezza e ordine pubblico*: le crescenti minacce spingono a utilizzare telecamere e sensori di videosorveglianza per il controllo degli ambienti che circondano le infrastrutture critiche, creando sistemi di "Situational Awareness" in grado di mostrare su schermo allarmi e video sulle situazioni critiche e posizionarle geograficamente.
- *Aeroporti, porti, stazioni ferroviarie*: le società e gli enti per il trasporto pubblico hanno la necessità di proteggere i passeggeri, il personale e le risorse fisiche da minacce terroristiche e violazioni della sicurezza, oltre che soddisfare i requisiti normativi.

- *Retail*: il monitoraggio degli esercizi commerciali permette di ridurre le frodi, i furti e gli errori amministrativi. I negozi al dettaglio utilizzano i video e le informazioni analitiche anche per determinare l'efficacia degli espositori promozionali e conteggiare le persone presenti nelle diverse aree al fine di ottimizzare l'assetto dei negozi e i livelli delle vendite.
- *Istituti finanziari*: molte banche dispongono di personale addetto alla vigilanza no-stop, per le operazioni all'interno e presso gli sportelli Bancomat. La sorveglianza e le analisi servono a ridurre le minacce di rapine e frodi. Inoltre molti operatori finanziari rafforzano i controlli di sicurezza nelle proprie filiali attraverso il monitoraggio delle informazioni video, audio e operative da un centro di comando e controllo unificato.

Sono alcuni esempi di casi in cui la videosorveglianza analogica ha già funzionato come deterrente contro i reati, oltre che come strumento per registrare le persone, i movimenti e gli eventi. Tuttavia, fattori quali i costi elevati, la scarsa qualità delle immagini e la ridotta capacità di trasmissione delle informazioni hanno fatto crescere l'esigenza di una tecnologia più evoluta.

5.1.1 L'evoluzione delle tecniche di sorveglianza

Per decenni le aziende hanno utilizzato le tecniche di videosorveglianza per contrastare attività criminali quali il furto, la frode e gli atti vandalici. Negli ultimi anni, si è sviluppata una tecnologia di sorveglianza che, oltre ad aiutare le aziende a riconoscere le minacce e reagire in modo più tempestivo, contribuisce a migliorare gli aspetti operativi dell'azienda stessa. A oggi, si è in presenza di tre generazioni tecniche di videosorveglianza: analogica, digitale e la videosorveglianza intelligente sviluppata da IBM.

Videosorveglianza analogica

Prevede videocamere analogiche posizionate in aree sensibili o strategiche di una data azienda, insieme a un televisore a circuito chiuso (TVCC) per il monitoraggio in diretta. Questo sistema non è solo un deterrente contro i reati, ma serve anche a registrare gli spostamenti delle persone e delle proprietà. Vengono spesso utilizzati per la registrazione degli eventi anche metodi di videosorveglianza mobili, come il montaggio di telecamere su autopattuglie, autobus e treni.
Il problema, o meglio, uno dei problemi, è che l'utilizzo di videocamere analogiche produce centinaia di nastri video che devono poi essere visionati dagli addetti alla sicurezza. Il costo del personale per il monitoraggio delle telecamere aggiunto a quello per l'archiviazione di un volume elevato

di nastri video, diventa proibitivo. Inoltre, i nastri video offrono una scarsa qualità delle immagini e si deteriorano nel tempo.
Per di più, alcuni studi hanno dimostrato che una persona incaricata di sedere di fronte a un monitor per molte ore al giorno e di prestare attenzione a determinati eventi rappresenta un sistema di protezione inefficace. Più precisamente, dopo appena 20 minuti di osservazione e valutazione degli schermi, l'attenzione della maggior parte delle persone scende molto sotto i livelli accettabili. Il monitoraggio dei video può produrre uno stato di noia e un effetto ipnotico. Inoltre, le ricerche manuali dei nastri possono richiedere tempi troppo lunghi rispetto quelli necessari per eventuali esigenze d'indagine.
Inoltre, spesso il video è visibile da un solo punto finale non condiviso. Ciò limita la capacità di distribuire le informazioni all'interno di un'impresa, capacità che potrebbe invece ridurre le minacce e gli allarmi in tutta l'azienda. Infine, i sistemi video analogici non sono in grado di estrarre informazioni dai dati registrati.

Videosorveglianza digitale

Il diffondersi di video digitali, videocamere IP, videoregistratori di rete, video Web, fotocamere di largo consumo e conoscenze sui video apre la strada a un'ampia gamma di applicazioni, che forniscono funzionalità avanzate e accrescono il valore aziendale.
La videosorveglianza digitale (DVS – Digital Video Surveillance) permette di definire strategie efficaci per il controllo del rischio, in grado di gestire e tutelare le informazioni aziendali e le risorse tecnologiche, anticipare le vulnerabilità e i pericoli, nonché conservare l'accesso tempestivo alle informazioni.
Molte aziende adottano però soluzioni frammentarie e sono messe alla prova da sistemi eterogenei che non comunicano fra loro. Spesso, la separazione fra sicurezza informatica e sicurezza fisica impedisce di sfruttare le infrastrutture e le applicazioni IT esistenti, come per esempio la gestione delle identità e le reti di trasmissione, che possono essere già presenti. Gestire sistemi totalmente separati significa impiegare una maggior quantità di manodopera, con conseguente aumento dei costi e riduzione dell'efficienza.
L'adozione di una soluzione DVS contribuisce a rimuovere non pochi dei limiti dei sistemi analogici basati su nastro e aiuta le aziende a ottenere un maggior ritorno dagli investimenti sulla sicurezza.
I motivi sono svariati:

- Consente il rilevamento in tempo reale e la potenziale prevenzione delle minacce attraverso una raccolta avanzata delle informazioni.

- Utilizza una visualizzazione basata sugli eventi a fini investigativi, eliminando la necessità di visionare cronologicamente i nastri video.
- Riduce la necessità di monitorare le videocamere e di sostituire i nastri.
- Aumenta la protezione dei prodotti attraverso la dissuasione dei potenziali taccheggiatori e il monitoraggio del personale.
- Offre prove contro le truffe.
- Aumenta la sicurezza interna ed esterna all'azienda.

Vantaggi e benefici che si traducono nel complesso in maggior sicurezza, flessibilità, un miglior ROI e un minor TCO.

Gli elementi salienti di un sistema integrato di sorveglianza

Il cuore di un sistema di Videosorveglianza è costituito dalle funzionalità di Video Management e Video Analisi.
La prima gestisce l'infrastruttura delle videocamere, i flussi audio e video, la codifica, la protezione dei dati sensibili, gli archivi e il trasporto dei dati. La seconda è invece complementare al sottosistema di Video Management e lo correda dell'intelligenza necessaria a rendere efficace l'intervento degli operatori di sicurezza, chiamati a intervenire solo al verificarsi di situazioni di potenziale pericolo.
Corollario della videosorveglianza sono altri sottosistemi, pure fondamentali per la sicurezza fisica aziendale.
I sistemi Anti-Intrusione sono generalmente preposti al controllo delle aree perimetrali e delle zone protette. I sensori maggiormente utilizzati in questo caso sono di diversi tipi:

- Volumetrico, per il rilevamento della variazione ambientale (microonde, infrarosso).
- Contatto magnetico, pulsante, bandella antirapina (per esempio una leva posizionata sotto la scrivania per la generazione di allarmi silenziosi).
- Cavo microfonico, cavo fessurato (utilizzabili per il controllo perimetrale dell'ambiente da proteggere).

I sistemi per il Controllo degli Accessi vengono utilizzati per la gestione degli accessi alle aree critiche e delle relative autorizzazioni. Esempi di sensori, in questo caso, sono:

- Lettori di badge a tecnologia magnetica.
- Lettori di badge a codice a barra.

- Lettori di badge con tecnologia laser (lettore ottico).
- Lettori smart-card (contatto, non a contatto, duali).

Anche se esistono diversi tipi di architetture per queste soluzioni, generalmente una o più centraline di raccolta sono collegate ai vari sensori di campo e traducono l'informazione per il software di gestione, installato e configurato su appositi sistemi.
I Sistemi Antincendio sono costituiti, tipicamente, da rilevatori in grado di percepire, segnalare ed eventualmente consentire un'estinzione automatica di ogni principio di incendio altrimenti devastante. Tali sistemi si basano su un'architettura composta, tipicamente, da una centrale di controllo, una serie di rilevatori automatici di fumo, fiamma o calore, una serie di pulsanti di segnalazione manuale e una serie di campane, targhe, sirene o avvisatori telefonici in grado di richiamare l'attenzione e indicare l'eventuale via di fuga alle persone coinvolte. Nei sistemi dove è prevista anche l'estinzione automatica, la centrale provvede a comandare la scarica dell'estintore adottato, sia esso a gas o acqua o polvere, per porre fine all'emergenza. In questo caso i sensori sono, generalmente:

- Rilevatori di fumo.
- Rilevatori di calore.
- Rilevatori di fiamma.
- Rilevatori di gas.
- Rilevatori di acqua.

5.1.2 La crescita delle esigenze aziendali

In generale si ritiene che le necessità del mondo bancario siano più complesse rispetto al resto dei settori economici in termini di sicurezza, ritenendo che le loro esigenze siano molto superiori. In realtà, si tratta di un esempio paradigmatico, che, tra l'altro, dimostra quanto la videosorveglianza e la capacità di esaminare rapidamente i dati archiviati siano d'aiuto nel garantire sicurezza e qualità del servizio. È molto probabile, inoltre, che anche a molti altri settori, soprattutto nell'ambito dei servizi pubblici e privati, saranno presto imposti i severi requisiti che assillano i responsabili della sicurezza nelle banche.
L'aggravarsi della criminalità e le normative legali sempre più stringenti costringono infatti le aziende ad assumere precise responsabilità nei confronti dei propri azionisti, spingendole a stringere accordi e relazioni commerciali con partner in grado di garantire sicurezza e affidabilità ai propri asset aziendali.

In particolare, con l'accordo di Basilea 2, si è evidenziato come la mancata gestione del rischio sottostante le operazioni aziendali (danneggiamenti, furti, mancanza di controllo), comporti la sensazione di un peggioramento dell'affidabilità aziendale e della sua capacità di stare sul mercato. Diventa quindi essenziale e irrinunciabile un'analisi attenta e aggiornata dei molteplici aspetti connessi al rischio. La sicurezza, infatti, non è un prodotto, ma un processo che si rinnova nel tempo e che deve essere costantemente monitorato alla luce degli sviluppi normativi e delle nuove strategie difensive che le imprese decidono di adottare. Risulta, dunque, indispensabile dotarsi di un sistema di controllo integrato che, coprendo tutta l'area operativa aziendale, non gravi eccessivamente sulle operazioni. Naturalmente, il rischio "rapina" rivolto al denaro circolante o ai clienti, è un problema che travalica il mondo bancario e coinvolge qualsiasi ambiente pubblico e privato in cui sia presente del denaro e degli avventori, dal supermercato, all'ufficio postale, al distributore di carburanti.
L'adozione di adeguate strategie per contrastare il fenomeno criminoso impone, inoltre, in linea con il decreto legislativo 81/2008, un'opportuna sensibilizzazione del personale al fine di prevenire e gestire gli eventi criminosi.
Le principali esigenze nei vari settori d'industria si possono quindi riassumere nei seguenti punti:

- Rispettare la conformità alle normative e alle responsabilità aziendali e sociali.
- Ridurre i costi di gestione della sicurezza.
- Migliorare l'efficienza dei processi di sicurezza.
- Stabilire standard e protocolli di comunicazione tra i vari sottosistemi di sicurezza eliminando la dipendenza da specifici fornitori.
- Realizzare una soluzione di sicurezza fisica integrata, in grado di accogliere differenti sistemi legacy (derivanti anche da nuove acquisizioni).
- Predisporre l'infrastruttura di videosorveglianza, anti-intrusione e controllo degli accessi in agenzia.
- Videoregistrare, memorizzare e conservare le immagini al fine di ricostruire e documentare a posteriori gli eventuali eventi criminosi.
- Predisporre la cifratura dell'archivio dei segnali video nel pieno rispetto di quanto stabilito dal Provvedimento Generale dell'Autorità garante per la protezione dei dati personali del 29 aprile 2004.
- Collegare le apparecchiature di erogazione del contante, Bancomat e contenitore passavalori al sistema di allarme.

Poiché il valore del sistema di sicurezza aumenta in modo proporzionale al suo livello di integrazione, ma ha un limite nel rapporto costi/benefici e nelle disponibilità di budget, occorre una soluzione di sicurezza fisica in grado di integrarsi alla sicurezza logica già presente in azienda, per salvaguardare gli investimenti fatti e per la protezione delle infrastrutture critiche.

5.1.3 Un modello di riferimento per l'integrazione dell'IT e della sicurezza fisica

In un tale scenario, l'evoluzione delle soluzioni di sicurezza fisica e delle tecnologie IT nel mercato enterprise ha posto le basi per realizzare modelli innovativi di governance e controllo delle agenzie bancarie e più in generale di ambienti aziendali con simili esigenze.
Sino a oggi i vari apparati di sicurezza fisica disponibili non erano integrati tra loro, nel senso che le informazioni generate da un sistema video, per esempio, non potevano essere correlate, visualizzate ed estratte insieme ai dati generati da un sistema di controllo di accesso.
Ovviamente una tale correlazione, se non impedisce la soluzione di problemi e i relativi interventi, perlomeno li ritarda molto e perde anche una parte della sua valenza ai fini preventivi di un crimine.
Mentre i vari sottosistemi si rendevano quindi sempre più autonomi e autoconsistenti, non esistevano protocolli e standard definiti a livello globale per la loro interoperabilità. Lo scenario attuale indica però una profonda trasformazione guidata dalla convergenza tra le soluzioni di sicurezza fisica e l'IT. Oggi, infatti, sono disponibili nuove soluzioni basate su linee guida applicabili sia al mondo IT sia a quello della sicurezza fisica. Ciò è ottenuto assicurando che le funzionalità di tutti i sistemi collegati tra loro siano omogenee e uniformi e che i responsabili della sicurezza possano utilizzarle per far fruttare i propri investimenti.
Un modello di riferimento che indirizza le principali caratteristiche funzionali connesse all'evolversi dei sistemi di sicurezza è quello sviluppato da IBM al fine di abilitare un approccio integrato e omogeneo, in grado di scalare in orizzontale (per esempio, il numero di agenzie bancarie gestite e i sottosistemi di sicurezza fisica gestiti per ciascuna agenzia) e in verticale (per esempio, il numero di servizi e di funzionalità resi disponibili per la sala di controllo).
Lo schema logico funzionale della figura illustra, seppur con una rappresentazione sintetica, il framework di riferimento. Si tratta di un modello che può essere rapidamente adattato ad altri ambienti industriali, del commercio o dei servizi pubblici o privati.

Figura 5.2
Framework di un evoluto sistema di sicurezza integrato

L'adozione di un modello di riferimento è importante per i processi di sicurezza, al fine di minimizzare l'impatto con l'operatività di gestione, poiché s'integra con le tecnologie pre-esistenti ed è in grado di far migrare facilmente le soluzioni verso un sistema di sicurezza evoluto e innovativo.
Nel trasformare in pratica un modello ideale le scelte che si possono fare sono svariate secondo il grado di copertura e di flessibilità che si desidera ottenere e mettere a disposizione degli utilizzatori.
Per esempio, proprio per garantire il massimo per entrambe le cose, per le componenti di Controllo Accessi, Anti-Intrusione, Anti-Incendio e Video Management IBM si basa su consolidate tecnologie di mercato.
In particolare, relativamente alla funzionalità di Video Management, IBM ha adottato due modalità:

- soluzione basata su appliance, adatta al livello di investimento che generalmente è previsto per gestire agenzie o sedi di piccole dimensioni, in termini di numero di telecamere e dispositivi di sicurezza;
- soluzione basata su server, in grado di far fronte all'esigenza di far crescere il numero di dispositivi per agenzia e che abilita: una maggiore flessibilità e scalabilità, in termini di funzionalità fornite, numero di dispositivi gestiti e tipo di servizi esportabili verso il centro; un miglior livello di gestione, in termini di standard gestiti a livello di sistema operativo e in termini di software di gestione che è possibile pre-caricare; un'estensione di funzionalità di alta affidabilità e Disaster Recovery;

una maggiore modularità, per permettere di aggiungere funzionalità di VideoAnalisi, non solo finalizzate all'individuazione di comportamenti sospetti, ma anche al supporto del business aziendale.

5.2 La soluzione IBM per una sorveglianza intelligente

Sorveglianza intelligente, videosorveglianza intelligente, analisi video, video intelligente e analisi intelligente sono tipiche espressioni che servono a descrivere il concetto dell'applicazione dell'analisi a segnale automatizzato e del riconoscimento morfologico alle videocamere e ai sensori, con l'obiettivo di estrapolare automaticamente le "informazioni utilizzabili" dai loro rispettivi flussi.
La soluzione IBM Analytic Surveillance Solution (IASS) aiuta a ottimizzare la sicurezza integrando l'hardware, il software e i servizi all'interno di un'azienda, permettendo così la convergenza della sicurezza fisica e informatica. Una parte integrante della soluzione IASS è costituita da un componente software, sviluppato da IBM Research e noto come IBM Smart Surveillance Analytics (SSA), in grado di consentire l'adozione di decisioni in tempo reale e la correlazione post-evento di persone e attività.
IBM Smart Surveillance Analytics dispone di funzionalità uniche che supportano nel gestire la sicurezza e a prevenire problemi:

- *Struttura aperta* - Un piano di protezione e sorveglianza può implicare eventi di varia natura catturati attraverso diverse tecnologie di analisi video, sensori non video e sistemi di gestione eventi come il TLOG in ambiente commerciale. SSA è stato progettato con una struttura aperta per consentire una vigilanza basata sugli eventi così da rendere più semplice e agevole la loro integrazione.
- *Creazione di profili comportamentali* - Molti produttori forniscono una serie di profili comportamentali, per esempio "veicolo grande e veloce" e "veicolo fermo". La progettazione di tali comportamenti è circoscritta a un ventaglio limitato di clienti. La capacità di notifica di SSA, basata su "metadati indicizzati al database" facenti riferimento a tutti gli eventi prodotti da una serie di telecamere, consente all'utente di personalizzare i comportamenti in base al contesto attraverso un'interfaccia di facile uso.
- *Ricerca attributi* - Il settore dei video intelligenti si è accostato alla sorveglianza in base a una gamma limitata di minacce note; da qui

l'enfasi posta su "dispositivi a superamento soglie e oggetti abbandonati" e le funzionalità estremamente ridotte nel supportare le indagini su "minacce ignote". SSA, mediante la sua innovativa ricerca di metadati, supporta un'ampia gamma di richieste su eventi che possono anche non essere stati precedentemente definiti come allarmi. Ciò è possibile perché SSA raccoglie i metadati sull'attività degli eventi e non solo sugli allarmi predefiniti.

- *Soluzioni personalizzate* - Numerosi sistemi "video-intelligenti" mettono a disposizione analisi e interfacce utenti di tipo limitato. Mentre le tecnologie analitiche di base sono pressoché identiche nei diversi settori di mercato e tra i vari clienti, i modelli di utilizzo variano enormemente secondo il settore. La struttura SSA consente un'agevole integrazione dei processi aziendali all'interno delle interfacce utente e offre soluzioni per diversi settori di mercato. Uno degli obiettivi chiave di SSA consiste nel supportare una rapida personalizzazione della struttura al fine di soddisfare le esigenze di specifici clienti e segmenti di mercato. La personalizzazione si estende sino a comprendere l'integrazione di soluzioni di Business Partner e degli eventi, con la parallela possibilità di un'ampia personalizzazione delle soluzioni e delle analisi.

Come evidenziato, conseguenza diretta della sua architettura, le funzionalità di SSA trovano applicazione in un'ampia gamma di segmenti di mercato, tra questi, ma non solo, amministrazioni comunali, aziende al dettaglio, istituti finanziari, agenzie di intelligence e settore pubblico. Dal punto di vista applicativo è possibile riunire queste soluzioni nelle seguenti categorie:

- *Soluzioni per la sicurezza* - Prevede l'utilizzo di SSA per fornire allarmi in tempo reale riferiti a "condizioni di minaccia" note e capacità d'indagine. Le aziende potenzialmente in grado di beneficiare di questa funzionalità sono le amministrazioni comunali, gli aeroporti, i porti, le stazioni ferroviarie, le installazioni critiche, le aziende al dettaglio e gli istituti finanziari.
- *Soluzioni di intelligence* - Le funzionalità di SSA consentono un repository indicizzato di eventi consolidati attraverso telecamere, utilizzabile per capire i modelli di attività all'interno di un'installazione o di una struttura e per individuare attività che deviano da questi modelli. Organizzazioni quali le università e le agenzie di pubblica sicurezza e di intelligence possono utilizzare questa funzionalità

unica, progettata per consentire l'utilizzo di eventi e modelli del passato per aiutare a prevedere le potenziali minacce.

- *Soluzioni operative* - La capacità della SSA di rilevare i movimenti umani viene utilizzata per studiare e migliorare l'efficienza operativa di un'installazione. Fra le possibili applicazioni vi sono il conteggio delle persone che entrano in un'area, la gestione dei tempi di attesa in una zona e la comprensione della struttura del traffico. Fra i possibili segmenti di mercato vi sono i negozi al dettaglio e gli aeroporti.
- *Soluzioni di trasporto* - La capacità della SSA di rilevare i veicoli in strada viene utilizzata per comprendere meglio l'affluenza del traffico, informare sui blocchi, fornire assistenza in tempo reale e supportare la pianificazione del traffico. Questa capacità può essere utilizzata per città, aeroporti e porti.
- *Soluzioni per l'intrattenimento* - Non ultimo, la funzionalità di rilevamento delle persone può essere utilizzata in occasione di eventi sportivi per generare statistiche avanzate, visualizzazioni e giochi interattivi. Fra i possibili clienti interessati vi sono case da gioco, club sportivi ed emittenti televisive.

5.2.1 L'architettura della soluzione IBM Analytic Surveillance Solution

Il componente software di IBM Analytic Surveillance Solution (IASS) è IBM Smart Surveillance Analytics (SSA), la cui struttura è costituita da due elementi di base:

- Middleware for Large Scale Surveillance (MILS).
- Smart Surveillance Engine (SSE).

IBM SSA ha il compito di eseguire analisi efficienti dei dati relativi alle sequenze video, sia in tempo reale sia registrate. Basata su middleware standard, la piattaforma software è progettata per consentire il monitoraggio e l'analisi di eventi del mondo reale attraverso vari sensori (come videocamere, radar o input sonori).
Tutte le funzionalità della SSA si basano sul Web, in modo da consentire un accesso potenziale "ovunque e in qualsiasi momento" sia ai dati in tempo reale sia a quelli storici del sistema.
Tramite le funzioni disponibili la soluzione IASS s'integra facilmente con le videocamere e i sistemi di registrazione esistenti in modo da fornire:

- Funzionalità di analisi di video e sensori.
- Una struttura per integrare le informazioni sugli eventi da molteplici fonti correlate.
- Una struttura per sviluppare soluzioni specifiche avvalendosi degli eventi registrati da video e sensori e integrandoli nel processo aziendale del cliente.

In particolare, IBM Smart Surveillance Analytics fornisce a un utente funzioni di allarmistica in tempo reale: gli utenti possono specificare "definizioni degli allarmi" che includono più condizioni e sono riferite a una telecamera o a sensore unici oppure a molteplici dispositivi. La SSA valuta gli eventi che si verificano nei sensori di riferimento rispetto alle definizioni di allarme. Ogni volta che si attiva la "definizione di allarme", la SSA è in grado di offrire all'utente una sollecita notifica dell'evento. Inoltre, gli utilizzatori (sia il personale sia le applicazioni) possono utilizzare SSA per effettuare ricerche sui contenuti tra i metadati degli eventi archiviati dalla componente SSA stessa. Per esempio, SSA può rintracciare tutti gli eventi registrati da una telecamera nei quali "un'auto rossa" si muoveva nel parcheggio.
L'architettura di SSA fornisce una serie di funzionalità sofisticate adatte a configurare, gestire e amministrare un sistema di grandi dimensioni, dotato di telecamere, sensori ed eventi provenienti da altri sistemi di trasmissione. La struttura supporta numerose tipologie di servizi:

- La gestione degli utenti offre la possibilità di aggiungere utenti nel sistema e fornisce un accesso selettivo alle telecamere.
- L'amministrazione dei sistemi include la possibilità di gestire le telecamere, i motori di analisi, le mappe e i contenuti dei metadati generati dalle analisi.
- L'indicizzazione dei metadati e servizi di ricerca sfrutta i metadati raccolti dagli Smart Surveillance Engine (SSE), analizza e inserisce i metadati in un database relazionale e fornisce alle applicazioni i servizi Web necessari alla ricerca e all'individuazione degli eventi dai metadati. Questo database diventa un indice completo non soltanto degli allarmi, ma del complesso degli eventi.
- I servizi di estendibilità consentono di estendere il modello base di dati al fine di integrare nuove fonti di informazioni, consentendo in tal modo un'agevole personalizzazione della SSA per soddisfare le esigenze dei clienti.

La soluzione IBM Analytic Surveillance Solution è molto innovativa e le sue potenzialità sono ulteriormente esaltate dal fatto di basarsi su un'architettura aperta (Service Oriented Architecture, Web Service), una piattaforma scalabile (Framework IBM WebSphere), protocolli standard (XML, J2EE, API, SDK). Le funzionalità fornite apportano un concreto valore al business in quanto s'integrano facilmente alle esistenti infrastrutture IT, sostenendo e facilitando le esigenze di crescita e di dinamicità dell'ambiente che ne fruisce .
L'implementazione della soluzione IBM Analytic Surveillance Solution, che comprende al suo interno la Smart Surveillance Analytics, offre molti vantaggi, fra cui la capacità di aumentare la redditività degli investimenti (ROI).
È possibile, per esempio, conseguire un ROI positivo grazie alla gestione dei rischi, l'aumento degli utili e la crescita dei ricavi. Il ROI, poi, presenta caratteristiche specifiche in funzione dei settori di mercato in cui un'azienda opera:

- *Retail* - Nel retail, la perdita della merce incide fortemente su utili e ricavi. A livello generale, a seguito di frodi da parte dei dipendenti, furti e danneggiamenti, la perdita incide mediamente per una quota compresa fra 1% e 3% su tutte le vendite al dettaglio. Ciò produce un impatto considerevole sui margini al dettaglio, specialmente per le attività che operano con un margine compreso fra 1% e 3%. La soluzione IASS può servire come strumento per prevenire le perdite, oltre che come fonte di dati intelligenti: può offrire tecnologia video per monitorare la contabilità dei registratori di cassa, l'area intorno ai registratori di cassa e tutto il negozio. I commercianti possono adottare la soluzione IASS per verificare l'efficacia di una promozione, monitorare le casse e contare le persone. Gli esercenti possono utilizzare la tecnologia per ridurre le perdite derivanti dalla mancata battitura in cassa di articoli dimenticati nel carrello. Un esercente ha ridotto queste perdite di oltre l'80%, integrando il riconoscimento ottico di IBM e un sistema POS dei business partner di IBM.
- *Sicurezza pubblica* - Le stazioni di polizia hanno utilizzato le soluzioni DVS per ridurre il numero di comparizioni nei tribunali, le spese legali e i tempi di redazione dei verbali. In molte città, sono stati installati video nell'abitacolo delle autopattuglie, con funzionalità wireless Wi-Fi che permettono di esaminare istantaneamente i video e di intervenire più rapidamente a potenziali reati. Nelle strutture scolastiche, i sistemi DVS offrono funzionalità a costi inferiori e più sicure rispetto ai tradizionali sistemi analogici.

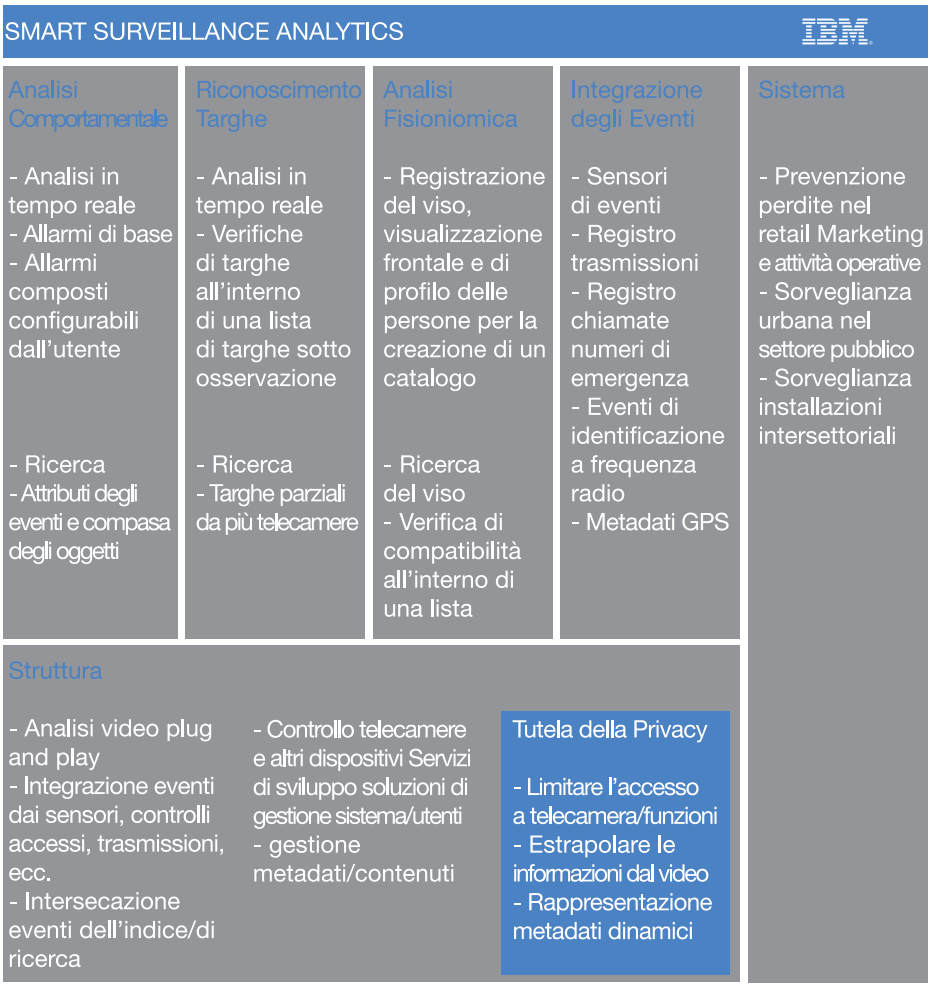
- *Settore bancario* - Nelle banche, l'integrazione di soluzioni DVS con sistemi di sicurezza esistenti (che includono controllo degli accessi, TVCC, DVR, NVR, sistemi anti-intrusione, prevenzione antincendio, dispositivi di riscaldamento, ventilazione e raffreddamento, pareti a proiezione video, allarmi, sistemi di gestione edifici e strumenti di analisi) può migliorare significativamente la gestione dei dati relativi alla sicurezza e, contemporaneamente, ridurre i costi operativi. Collegando i dati sulla sicurezza a quelli sulle operazioni commerciali, si possono ottenere vantaggi nelle seguenti attività bancarie: Bancomat/prevenzione di controllo frodi, monitoraggio posizione dei Bancomat, operazioni di conteggio del denaro, monitoraggio code ed efficacia dell'utilizzo dello spazio nelle filiali.
- *Trasporti ferroviari* - L'ispezione manuale delle vetture nei depositi ferroviari può essere ridotta fino alla metà attraverso l'implementazione di DVS per il controllo video. È possibile utilizzare le analisi DVS per eseguire controlli di sicurezza e per inviare allarmi quando viene rivelata la presenza di vetture non sicure.
- *Aeroporti* - Il ROI di un sistema DVS negli aeroporti è giustificato grazie al fatto che viene eliminato il controllo continuo dei monitor o la ricerca manuale di una ripresa fra centinaia di nastri video. Negli aeroporti, inoltre, ulteriori vantaggi derivano dal collegamento fra i dati sulla protezione e quelli sulle operazioni commerciali.

5.2.2 Le soluzioni di sorveglianza IBM per il mondo bancario

Per il mondo bancario, IBM Analytic Surveillance Solution, è in grado di effettuare un'analisi intelligente della scena, al fine di identificare e classificare gli oggetti (persone, autoveicoli), di corredarli di opportune informazioni (quali la direzione del moto, la dimensione, il colore, la velocità) rendendole disponibili in un database di metadati.
Il database permette di aggregare le suddette informazioni e renderle disponibili per indagini di tipo investigativo, sia durante un evento di crisi, sia durante un'analisi post-incidente.
Inoltre la possibilità di effettuare ricerche di tipo statistico sui dati, offre informazioni analitiche e reportistica a supporto dei servizi di business, quali:

- Monitoraggio del comportamento dei clienti in coda agli sportelli e ai circuiti ATM.
- Informazioni sulle utenze per un'adeguata distribuzione delle risorse nelle agenzie.

Figura 5.3
Le funzionalità Smart Surveillance Analytics all'interno della IBM Analytic Surveillance Solution



- Statistiche sul numero di persone in attesa (entrate/uscite).
- Integrazioni con le informazioni applicative, relative alle transazioni bancarie.
- Efficacia dei display e delle vetrine promozionali.

La soluzione abilita, infine, nella Sala di Controllo, l'integrazione dei vari sottosistemi appena descritti e assicura che le funzionalità di tali sottosistemi collegati tra loro siano utilizzate al meglio dai responsabili della sicurezza.
Va osservato che le Sale di Controllo devono processare una gran quantità di informazioni, provenienti dai vari sottosistemi, solitamente frammentate e non facilmente disponibili. La soluzione IBM è in grado di unificare la modalità di raccolta e la presentazione di tali informazioni al fine di renderle disponibili all'operatore che ne ha più bisogno, in un determinato momento, per risolvere un incidente.

Il Sistema Integrato IBM consente, inoltre, di estrarre questo tipo di informazioni dal sistema, al fine di fornire report e statistiche efficienti e puntuali sulle attività degli operatori stessi.
Per meglio identificare le reali situazioni di allarme è indispensabile far convergere e correlare informazioni provenienti dagli apparati fisici di campo delle diverse sorgenti. A tale scopo, la soluzione IBM è provvista di un "Engine" di correlazione in grado di integrare eventi provenienti da diverse sorgenti e di rispondere a determinate situazioni di allarme avviando procedure di reazione automatiche. Un database storico degli eventi, tiene traccia della tipologia e del numero degli eventi gestiti.
Il processo di integrazione dei sistemi comporta il collegamento tra diversi processi aziendali. IBM offre a tal fine uno strumento di controllo dei flussi operativi, in grado di implementare il processo di integrazione e fornire il totale controllo sull'esecuzione delle procedure, nel rispetto delle politiche di sicurezza aziendali. È infatti necessario conoscere da chi devono essere fornite le informazioni, quali operatori devono intervenire e che tipo di supporto devono fornire per gestire un determinato incidente.
Il controllo del flusso delle informazioni fornisce la struttura per un metodo più dinamico per la gestione delle Control Room. Le mansioni e gli eventi possono essere gestiti dalla risorsa disponibile più vicina piuttosto che da un ambiente statico in cui "l'operatore A deve essere alla stazione di lavoro B per svolgere questo ruolo".
La soluzione IBM permette agli operatori di agire in modo collaborativo, in modo da risolvere gli incidenti mentre accadono. Un processo flessibile può svolgersi dove gli operatori lavorano in modo cooperativo attraverso stazioni di lavoro multiple aumentando la visibilità e la qualità della risposta.

5.2.3 Le soluzioni per il Retail

Nel Retail mediamente si calcola un impatto dovuto alle perdite da taccheggio o danneggiamento per una percentuale che va dall'1% al 3% delle vendite. Per ridurre queste perdite, che corrispondono a enormi volumi di denaro, IBM Analytic Surveillance Solution utilizza tecniche automatiche per la comprensione delle immagini in modo da estrarre informazioni utili e immediatamente utilizzabili dai dati di sorveglianza. Il sistema adotta diversi algoritmi che processano i dati video e dei sensori, che estrapolano le informazioni per l'invio di allarmi in tempo reale o per funzionalità di ricerca statistica.

Le tecnologie di analisi sono:

- Analisi comportamentale: l'algoritmo rileva il movimento degli oggetti all'interno del campo visivo di una telecamera. Tali oggetti vengono classificati, registrati e corredati di informazioni, come per esempio il colore, la dimensione, la direzione del moto, la velocità. In base a tali attributi possono essere generati eventi, come per esempio superamento delle soglie, conteggio delle persone, oggetto rimosso o oggetto abbandonato e attivate ricerche statistiche, come per esempio il numero degli oggetti "veicoli rossi" rilevati nell'intervallo di tempo, la media di sosta degli oggetti/persone in una data zona, solo per citarne alcuni.
- Rilevamento volti: la funzionalità rileva automaticamente i volti umani nel video; key frame corredati di data e ora di rilevazione sono registrati nel sistema creando così un catalogo di volti di tutte le persone che sono apparse nel campo visivo di una telecamera.
- Integrazione degli eventi: la funzionalità consente di integrare gli eventi prodotti dall'analisi di altri sensori, come i sensori antintrusione delle porte allarmate, dispositivi di riscaldamento, ventilazione, raffreddamento, dispositivi sonori, con il flusso di eventi prodotti dai sistemi IT, quali log delle transazioni di acquisto, entrate in un varco con il controlli accessi. Infine una volta integrate, le informazioni sugli eventi possono essere intersecate agli eventi basati su video come l'analisi comportamentale e il rilevamento dei volti.

La maggior parte dei sistemi di video analisi è concentrata esclusivamente sull'aspetto legato all'estrazione delle informazioni, mentre il sistema IBM esplora l'uso delle informazioni estratte nel contesto della ricerca, del recupero delle informazioni, della gestione dei dati e dell'indagine. Il maggior valore si ottiene quando è possibile correlare le diverse tipologie di informazioni, come per esempio l'identificazione di una coda alle casse troppo lunga, la conoscenza del numero di persone presenti nel magazzino e davanti a quale scaffale hanno maggiormente sostato, la percezione dell'efficacia di una promozione e ancora il tasso di conversione, ovvero il numero di visitatori su quello degli effettivi compratori.
Il registratore di cassa è poi il luogo dove è più probabile che si verifichi un furto, anche, in non rari casi, da parte di impiegati infedeli. Osservando la zona e interpretando correttamente i dati, è possibile integrare la videoanalisi con il log delle transazioni di cassa e confermare le eventuali attività fraudolente.

Associando la transazione con il movimento del cassiere è possibile infatti rilevare oggetti non scannerizzati, verificare le eccezioni, gli sconti. La combinazione di video e log delle transazioni elimina in sostanza ogni possibile errore.
Per contrastare situazioni di taccheggio, la soluzione IBM Loss Prevention usa la tecnologia "oggetto rimosso" di IBM Analytic Surveillance Solution per tenere traccia di oggetti multipli e del relativo movimento. L'indicizzazione del video non si basa sulle frame, ma sugli oggetti all'interno della frame, sulla generazione degli indici basata sulla descrizione del movimento, della forma e del colore. Tutte queste informazioni costituiscono il bagaglio di dati utili a individuare un oggetto, quando è stato rimosso da uno scaffale e tenerne traccia all'interno del magazzino ed eventualmente anche fuori: tutto in real time. È inoltre possibile configurare un allarme se s'intercetta un oggetto lasciato abbandonato.
Oltre a individuare comportamenti sospetti all'interno dei negozi, la stessa infrastruttura tecnologica IBM Analytic Surveillance Solution può fornire valore ai servizi commerciali ed efficacia alle iniziative di marketing. La funzionalità di conteggio delle persone non permette semplicemente di contare le persone che entrano nel magazzino attraversando per esempio una linea immaginaria lungo l'entrata: le persone, o gruppi di persone, vengono tracciate durante tutto il loro percorso, anche se si distribuiscono in piccoli gruppi o in singole persone tra gli scaffali, fino al momento in cui si riuniscono (coppie, famiglie che scelgono diversi reparti merceologici) effettuando infine un singolo acquisto della merce scelta. Gli scenari descritti sono inoltre atti ad analizzare il comportamento dei consumatori all'interno del punto vendita.

5.2.4 Le soluzioni per ambienti portuali e di campus

Come conseguenza degli attentati terroristici dell'11 Settembre 2001, il problema della sicurezza nel mondo dei trasporti è diventato un elemento imprescindibile con cui confrontarsi. Una struttura portuale, e in genere aree di campus connesse a servizi di trasporto, devono essere in grado di controllare il proprio perimetro per difendersi da intrusioni, che possono essere perpetrate a scopo di sabotaggio o furto, ma, a volte, effettuate anche da parte di persone che accedono per scopi ludici (pesca, osservazione navi, ecc.); in secondo luogo deve essere in grado di controllare che la circolazione di mezzi e persone all'interno dell'area portuale sia in linea con le direttive di "safety & security". Inoltre, l'accesso stesso alle varie zone dell'area portuale deve essere consentito in base a un corretto controllo delle identità e delle credenziali per l'autorizzazione.
Per soddisfare queste esigenze, IBM ha affiancato alla sua tradizionale linea di prodotti e servizi nell'area della cosiddetta sicurezza logica (pro-

tezione delle informazioni e dei sistemi ICT), una proposizione fatta di best practice, prodotti e servizi di system integration per la protezione delle infrastrutture critiche.
La soluzione IBM Analytic Surveillance Solution (IASS) contribuisce, in questo caso, a ottimizzare la sicurezza integrando l'hardware, il software e i servizi all'interno di un'azienda, rendendo possibile così la convergenza della sicurezza fisica e informatica. Una parte integrante della soluzione IASS è costituita dalla componente software IBM Smart Surveillance Analytics (SSA), in grado di consentire l'adozione di decisioni in tempo reale e la correlazione post-evento di persone e attività.
IBM è in grado di offrire un'ampia gamma di soluzioni specifiche grazie alle esperienze fatte in varie strutture di trasporti nel mondo, sulle diverse problematiche di logistica e sicurezza, attraverso l'adozione delle più moderne tecnologie.
L'elemento qualificante è un approccio alla sicurezza di tipo integrato che comprende: controllo perimetrale, controllo accessi, controllo area e zone portuali, unico sistema di comando e controllo, protezione dei sistemi e delle informazioni, tracking di persone e mezzi nelle aree pericolose.
A questo possono essere abbinate delle integrazioni con i sistemi di logistica e di emissione biglietti per le operazioni di imbarco e sbarco e carico e scarico merci, in modo da riutilizzare al massimo le tecnologie impiegate e automatizzare le operazioni innalzando il livello di sicurezza, velocizzando il servizio e massimizzando il ritorno degli investimenti.
Per esempio, è possibile automatizzare il controllo del check-in/check-out di camion e container, diminuendo i tempi di attesa e incrementando, nel contempo, la sicurezza, leggendo le targhe e gli identificavi dei container, controllandone la corretta associazione con l'identità del conducente e i dati comunicati al porto; inoltre è possibile rilasciare automaticamente le indicazioni di direzione e associare le immagini relative allo stato del container per le successive verifiche alla consegna.
Il sistema di videoanalisi, oltre a fornire le informazioni per la sicurezza, è in grado di fornire informazioni in tempo reale o statistiche per gestire le file agli sportelli o ai punti d'imbarco, informazioni sui flussi percorsi all'interno delle varie aree e sulla maggiore o minore permanenza in alcune di loro; informazioni quindi estremamente utili per ottimizzare l'utilizzo delle aree di servizio e modificare la disposizione dei servizi.
Oppure i sistemi basati su RFID e smart-card possono consentire di automatizzare il controllo degli accessi nelle varie aree, rendendo più veloci i flussi e le operazioni ma anche fornendo servizi aggiuntivi agli utenti: fidelity card, fast-track, fast check-in, borsellino elettronico per i parcheggi.

Appendice
Ridurre i rischi e aumentare l'efficienza con la suite IBM Tivoli zSecure

Ogni organizzazione dispone di una serie di dati “mission-critical” da proteggere. Gli errori e i malfunzionamenti in materia di sicurezza non costituiscono delle semplici interruzioni ma possono essere eventi catastrofici con conseguenze che si ripercuotono sull’intera organizzazione. Gli errori involontari degli utenti privilegiati possono determinare danni per valori pari a milioni di dollari, a causa di errori di configurazione non intenzionali o comandi di sicurezza eseguiti senza prestare attenzione. Danni ancora maggiori possono essere causati da utenti dolosi con accesso autorizzato.

Se consideriamo che il 70% dei dati critici aziendali risiede su mainframe, si capisce come gli amministratori della sicurezza affrontino sfide impegnative per proteggere i dati sensibili dell’azienda. Il personale IT deve fornire una documentazione di audit e di controllo dettagliata e, contemporaneamente, essere in grado di far fronte alle richieste crescenti dovute a fusioni, riorganizzazioni e altri cambiamenti. Molte organizzazioni non dispongono di un numero di amministratori esperti in sicurezza del mainframe sufficiente a soddisfare le richieste; inoltre aumentare le competenze del personale più giovane su tecnologie di sicurezza tipiche del mainframe può richiedere molto tempo.

Malgrado, quindi, i server System z siano “security-rich by design” e dispongano tradizionalmente di una soluzione leader di mercato come

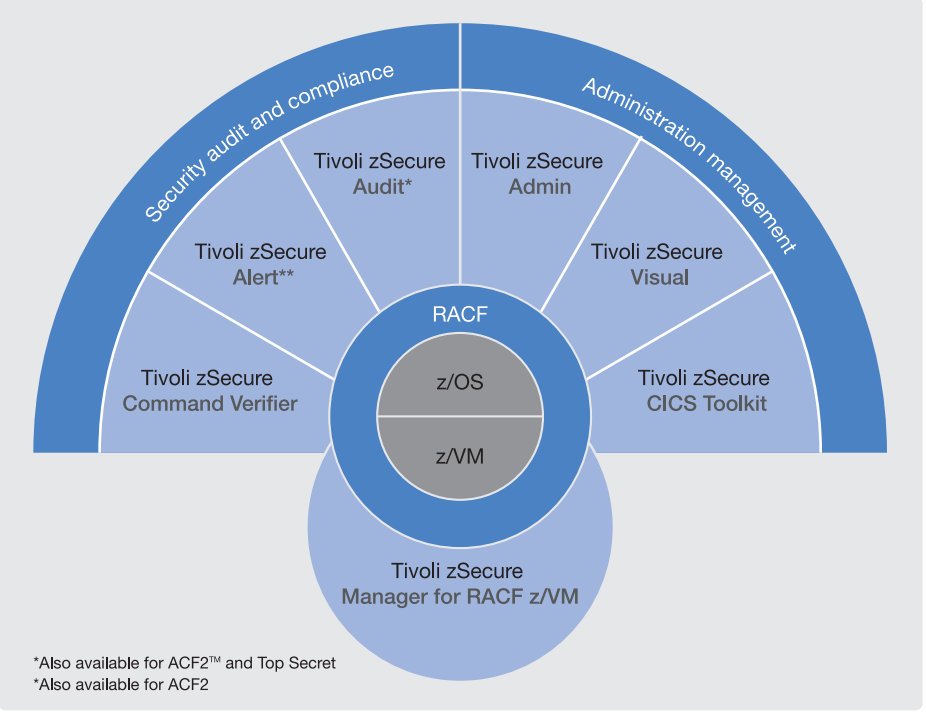


Figura A.1
La suite Tivoli zSecure

il Security Server for z/OS (RACF), a inizio del 2007 IBM ha deciso di acquisire la società Consul Risk Management International, considerata da anni leader nell'amministrazione della sicurezza e nelle attvità di auditing per il mainframe con un'estensione in profondità in tutta l'impresa.

La suite specializzata sulla piattaforma mainframe è denominata Tivoli zSecure e comprende i seguenti moduli:

- zSecure Admin: amministrazione RACF e query via TSO o batch;
- zSecure Audit: rilevazione e reporting degli eventi sul mainframe, con analisi delle esposizioni di sicurezza;
- zSecure Alert: rilevazione delle condizioni di alert (rilevazione delle intrusioni) legate alla sicurezza su z, con notifica al supporto appropriato (WTO, Dataset, e-mail, cellulare e così via);
- zSecure Command Verifier: tool di security compliance RACF per l'applicazione delle politiche sui comandi RACF;
- zSecure Visual: amministrazione e query RACF di base, utilizzando l'interfaccia di Windows Client a RACF;
- zSecure CICS Toolkit: amministrazione RACF di base via CICS.

A questi moduli, per i clienti che hanno RACF su z/VM, si aggiunge zSecure Manager for RACF z/VM, che realizza amministrazione RACF e query via TSO o batch in ambiente z/VM

zSecure fornisce un significativo valore aggiunto in termini d'innovazione, che saranno illustrati più in dettaglio nel seguito.
Il primo beneficio è legato al problema del sovraccarico di lavoro degli amministratori. zSecure Admin è stato progettato per essere un meccanismo efficiente nel gestire l'amministrazione della sicurezza di RACF, usando molte meno risorse umane, meno tempo e meno risorse di sistema di quanto richiesto dai tool tradizionali. Il vantaggio chiave è che mostra le informazioni di profilo RACF in modo da consentire agli amministratori di prendere decisioni informate, mostrando il contesto dei profili RACF, riducendo al minimo gli errori e con un enorme risparmio di tempo. Solo per fare un esempio, consideriamo attività come la clonazione di una regione CICS o la duplicazione di tutte le definizioni RACF relative a un'applicazione di una grande azienda. Di norma, attività di questo tipo potrebbero richiedere un'in-

tera giornata di lavoro agli amministratori RACF, se si vuole fare tutto nel modo giusto, considerando ogni circostanza e risolvendo ogni problema. Con zSecure Admin possono essere completate nel giro di qualche minuto. Con i normali comandi RACF, un amministratore della sicurezza dovrebbe fare un comando di "list" che fa scorrere le righe di output attraverso il suo terminale. Una volta premuto "Invio", le righe di output precedenti spariscono. Con zSecure Admin, dispone invece di un'interfaccia che dà al database RACF l'aspetto di una pagina di dati a scorrimento, che si può editare senza dare alcun comando. Come l'editor ISPF, può sovrascrivere i campi e apportare le modifiche in modalità WYSIWYG10. Se si apporta una modifica e si preme "Invio", il comando RACF viene generato automaticamente. Ciò comporta un enorme risparmio di costi, perché prevenire gli errori nell'amministrazione della sicurezza è un'attività che può essere molto onerosa, determinando downtime del sistema ed esposizioni a vulnerabilità. Oltre che con la metodologia ISPF, il sovraccarico di lavoro degli amministratori della sicurezza mainframe può essere semplificato, in diversi casi, anche decentralizzando le attività amministrative con tecnologie maggiormente "user-friendly", come quelle fornite da CICS e Windows. A tale scopo, possono essere installati e utilizzati i moduli zSecure CICS Toolkit e zSecure Visual, a seconda del tipo di competenze dell'amministratore della sicurezza e del reparto.

Un altro valore innovativo apportato dalla suite riguarda la sempre crescente preoccupazione in materia di normative e audit. Uno dei problemi maggiori per i reparti di auditing è la grande quantità di parametri e profili da controllare per stabilire se una certa azienda rispetta i regolamenti di sicurezza nello svolgimento delle sue attività quotidiane. I responsabili di tali verifiche, in particolare, devono identificare tutte le possibili esposizioni al rischio. Un compito molto difficile e oneroso quando la fonte dell'informazione è molto ampia, come nel caso di un archivio SMF. zSecure Audit, che può essere considerato attualmente uno dei migliori tool di auditing per z/OS presenti sul mercato, è stato progettato proprio per risolvere questi problemi di audit della sicurezza per il mainframe. Si concentra su due aspetti molto interessanti, che lo rendono particolarmente allettante per il reparto auditing. Il primo riguarda proprio gli aspetti legati alle esposizioni, che il tool identifica insieme alle vulnerabilità nel più breve tempo possibile, anche se la mole di informazioni arriva da archivi di

enormi dimensioni quali SMF. Lo strumento consente di raccogliere informazioni sui record SMF in tempo reale, mettendo a disposizione i risultati di auditing subito dopo il verificarsi di eventi di sicurezza nel mainframe. zSecure Audit permette inoltre di analizzare la configurazione di System z I/O, ottenuta direttamente dal core di z/OS, correlando il rispettivo contenuto alle informazioni RACF e creando trasparenza delle definizioni che controllano la sicurezza del mainframe. Il secondo aspetto molto importante su cui si concentra zSecure Audit è la facilità di interpretazione di questa mole di informazioni per i responsabili dell'auditing. Una sfida ancora più grande in questo caso è rendere System z più familiare e facile da capire attraverso la sicurezza, quindi per chi si occupa tipicamente di auditing e di norma non ha a che fare con il mainframe nella propria vita professionale. Una semplificazione resa possibile e caratterizzata da potenti funzioni di reporting, analisi e valutazione. Queste sono valide non solo per RACF ma anche per altri sottosistemi z/OS e possono essere ottenute in qualsiasi tipo di formato, dal classico e potente ISPF al facile e user-friendly formato XML, esportabile in HTML, Microsoft Excel, Lotus 123 e in qualsiasi altro formato elettronico.

Infine, è importante sottolineare che l'utilizzatore può verificare i propri sistemi, rilevare esposizioni e quindi eseguire un audit di stato, non solo quando confronta le informazioni disponibili con le normative di sicurezza in vigore, ma anche quando desidera confrontare tali informazioni con le regole di sicurezza interne.

La tecnologia di auditing di zSecure è estremamente flessibile e può essere resa oltre che efficace ache molto efficiente per il singolo cliente, con l'aiuto di un consulente, che potrà modellare le funzioni del tool in base a qualsiasi esigenza di audit del mainframe. È facile comprendere l'utilità di questa tecnologia semplificata per i clienti mainframe, soprattutto perché le nuove normative in merito alla protezione dei dati personali impongono agli amministratori di sistema di dover essere sempre pronti a fornire in qualsiasi momento informazioni su tutti i dati a cui ognuno ha avuto accesso, includendo il tipo di accesso e la protezione a esso associata. I log SMF, che contengono le informazioni sugli accessi avvenuti e che sono tipici del mainframe, hanno un formato grezzo, di lettura e interpretazione estremamente complicate. Tutte queste informazioni diventano invece facilmente ricavabili e interpratabili tramite zSecure Audit, coadiuvato da zSecure Admin.

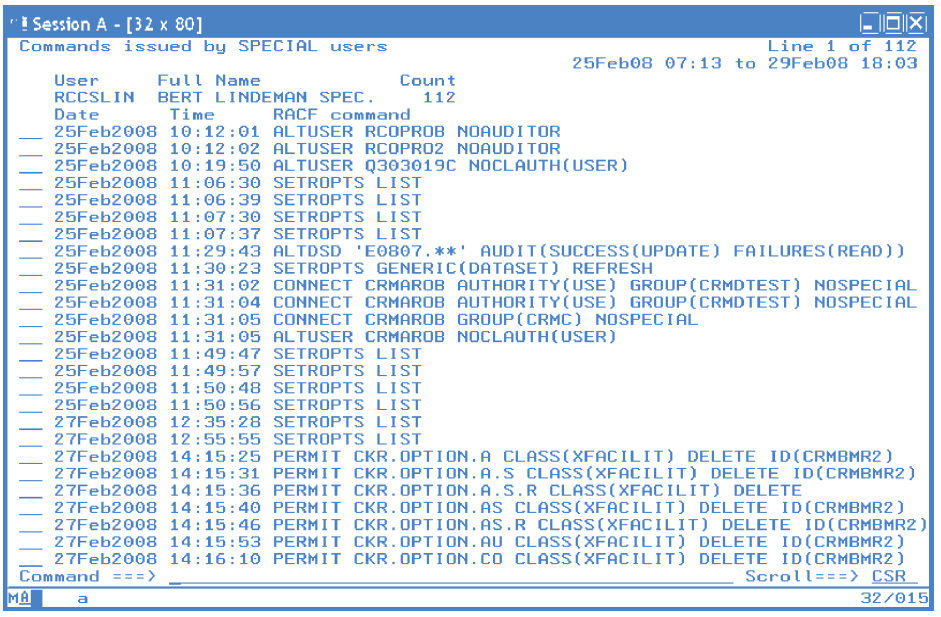


Figura A.2
Lista dei comandi RACF eseguiti, ottenuta tramite zSecure Audit

L'ultimo valore aggiunto della suite zSecure in termini di innovazione riguarda i problemi legati ai rischi per la sicurezza provenienti dall'interno. Questi rischi derivano spesso dal grande potere che gli amministratori della sicurezza devono necessariamente avere, ma che rappresenta un rischio sia in caso di errori sia, a maggior ragione, se sussistono intenti fraudolenti. Non a caso, con un provvedimento pubblicato sulla Gazzetta ufficiale del 24 dicembre 2008, il Garante ha imposto precise regole per il controllo degli amministratori di tutti i sistemi (non solo quelli preposti alla sicurezza). Di grande efficacia è il tool zSecure Command Verifier. Si può considerare un tool di "security compliance", studiato per garantire che tutte le attività RACF siano eseguite con la logica, o meglio con i criteri, accettati dall'azienda. Questi criteri possono essere determinati da diversi fattori, come le norme comuni in materia di security compliance (per esempio quelle previste all'interno della legge Sarbanes-Oxley), o come gli standard interni aziendali (per esempio la regola per riconoscere un utente RACF interno da uno esterno). Una spiegazione tecnica al riguardo può essere fornita dicendo semplicemente che molti comandi, che sarebbero normalmente accettati ed eseguiti da RACF, potrebbero non seguire le regole di security compliance o gli standard aziendali, e per questa ragione dovrebbero essere respinti.
Poiché RACF non può decidere da solo quali comandi accettare e quali respingere, anche perché i criteri possono variare da un'azienda all'altra, la suite dispone del tool zSecure Command Verifier, che consente di defi-

nire criteri propri di sicurezza. Esempi di questi criteri possono essere convenzioni di denominazione da seguire, valori obbligatori da specificare, valori di default in caso di valori mancanti nella definizione di un oggetto, evitare l'attribuzione di autorità superiori o altro.
Oltre a zSecure Command Verifier, i rischi sopra citati possono essere ridotti anche con l'ultimo modulo della suite chiamato zSecure Alert. Questo tool fornisce un meccanismo in tempo reale che monitora gli eventi su z/OS e li confronta alle politiche di sicurezza preimpostate. Inoltre identifica le minacce al sistema in generale, o a un'applicazione in particolare, ed è in grado di monitorare set di dati sensibili, per esempio i dati della contabilità. In particolare, zSecure Alert può monitorare tramite i record SMF che non si verifichi nessun accesso a questi data set della contabilità. Quando si verifica un accesso, quando uno degli utenti privilegiati utilizza effettivamente tale privilegio, può essere inviato un alert al responsabile della sicurezza dei dati o al responsabile della compliance. Questi può quindi verificare se il privilegio è stato usato correttamente oppure può intervenire immediatamente, rintracciare l'origine dell'evento e cercare di limitare l'impatto dell'esposizione dei dati. Questi alert possono essere registrati ovunque, inviati via e-mail o anche forniti a una console degli eventi di gestione della sicurezza, come Tivoli Security Operation Manager.
I moduli zSecure Audit e Alert sono nativamente integrati con la soluzione, sempre di provenienza Consul, Tivoli Compliance Insight Manager, un tool di analisi della security compliance che fornisce una dashboard semplice, in grado di mappare i dati dei log della sicurezza tra le varie piattaforme e di fornire report di facile comprensione, con tutte le esposizioni di sicurezza rilevate dai log sopracitati confrontati con una o più normative in materia di sicurezza. Questa dashboard può essere sfruttata anche per analizzare i dati di sicurezza del mainframe per ottenere una visione crossplatform ed End to End della conformità delle applicazioni critiche aziendali.

Testi a cura di Reportec srl, Milano

Stampato a cura di Laser Copy, Milano
Finito di stampare nel mese di marzo 2009

IBM Italia S.p.A.
Circonvallazione Idroscalo
20090 Segrate (Milano)
Per ulteriori informazioni:
http://www-935.ibm.com/services/it/index.wss/offerfamily/igs/g1025846