# Un pianeta più intelligente è anche più sicuro

Realizzato da Reportec srl
www.reportec.it

# Prefazione

Stiamo assistendo a grandi cambiamenti nel mondo: organizzazioni di ogni tipo stanno investendo in nuove tecnologie e nuovi processi che le rendono più efficienti, agili e competitive. Il mondo sta diventando uno "Smarter Planet", un pianeta che, in maniera ubiqua, è tecnologico, interconnesso e intelligente.

Tecnologico, in quanto ricco di sensori e dispositivi elettronici vari che vengono integrati ovunque: nelle auto, sulle strade, nei gasdotti, nei macchinari.

Sempre più interconnesso, perché le statistiche dimostrano che presto supereremo i 2 miliardi di utenti Internet e i 4 miliardi di abbonati alla telefonia mobile, mentre le macchine dotate dei suddetti sensori stanno determinando un'esplosione di comunicazioni tra le macchine stesse e le persone, che presto porterà a un miliardo di miliardi di interconnessioni!

Intelligente, nel senso che la tecnologia e le interconnessioni stanno determinando un'esplosione di dati. Sistemi potenti per l'analisi e l'utilizzo di questi dati forniranno al mondo un nuovo tipo d'intelligenza: un'intelligenza che non solo permetterà di sviluppare il business, ma ci aiuterà a risparmiare energia, a migliorare il rendimento dell'agricoltura e a ridurre l'impatto dei disastri naturali.

IBM ha lanciato una sfida: creare un Pianeta più intelligente. Ma "Smarter Planet" non è semplicemente un'idea di IBM: è una visione per IBM e per i propri clienti. Significa che è possibile lavorare insieme per rendere il mondo un posto migliore in cui vivere, lavorare e giocare.

Più strumenti, quindi maggior profondità di analisi e predizione, più interconnessioni e più intelligenza sviluppano nuove possibilità, ma aprono anche a nuovi rischi, a cominciare dai problemi di privacy e sicurezza della grande quantità di nuovi dati che vengono creati, per continuare con l'esigenza di proteggere nuove infrastrutture e nuove sorgenti di dati. Così come per i criminali si aprono nuovi fronti d'attacco, per esempio nuovi

servizi che possono essere bloccati o nuovi tipi di frodi che possono essere perpetrate. Le informazioni e la tecnologia, in altre parole, possono essere utilizzate per rendere il Pianeta più intelligente, cioè per migliorare la vita dei cittadini, i servizi della pubblica amministrazione, i processi delle aziende. Ma un Pianeta più intelligente, dove tutto e tutti sono interconnessi e dove crescono ogni giorno i mezzi tecnologici a disposizione, deve essere anche più sicuro.

## La sicurezza aziendale by design

In azienda, questo non significa "semplicemente" proteggere l'IT, ma realizzare un'infrastruttura sicura e "resiliente", considerando quindi anche la continuità dei processi e delle operazioni di business. Significa progettare i servizi IT, a partire dalle applicazioni per esempio, affinché siano intrinsecamente sicuri: una sicurezza by design che si può raggiungere non solo nelle nuove organizzazioni, ma si può impostare come approccio evolutivo dell'IT. Ma significa anche che tutti i processi di business, lo sviluppo dei prodotti e le attività operative quotidiane devono essere progettate per essere sicure.

Si otterrà la tranquillità necessaria per adottare in sicurezza recenti forme di tecnologia o nuovi modelli di business, che permetteranno di ottimizzare i costi, innovare prodotti o processi e ridurre il time to market.

IBM è continuamente alla ricerca di elementi innovativi nelle piattaforme hardware integrate, nelle tecniche di crittografia, nell'analisi del rischio e nelle architetture di sicurezza. Forniamo strumenti per esaminare, identificare e assegnare priorità ai rischi di sicurezza relativi alle applicazioni Web, in ambienti di pre-produzione, per aiutare a sviluppare il codice in maniera sicura.

IBM introduce tecnologie di sicurezza nel "fabric" di hardware, software e servizi che fornisce. Ma più in generale, IBM ha implementato al proprio interno una sicurezza intrinseca in processi, prodotti e operazioni sin dalla progettazione, non aggiunta a cose fatte. Tanto che per supportare la filosofia del Security By Design, in IBM è stato introdotto un Security Architecture Board e un Security Executive Board.

Disponiamo quindi di una grande esperienza da condividere con clienti e business partner e ci troviamo, pertanto, in una posizione unica per aiutare le aziende a valutare le proprie esigenze di sicurezza, fornire loro le soluzioni adeguate e supportarle per garantire una corretta implementa-

zione. In IBM, infatti, abbiamo X-Force, uno dei massimi team di ricerca e sviluppo sulla sicurezza e migliaia di ricercatori, sviluppatori, consulenti ed esperti della materia; forniamo consulenza e supporto nella realizzazione per migliaia di progetti sulla sicurezza; possediamo una visione d'insieme dalle strategie e la governance della sicurezza sino alle tecnologie per la sicurezza di mainframe, desktop, reti e ogni elemento dell'infrastruttura IT; conosciamo le dinamiche dei diversi settori industriali in cui operano i nostri clienti (forniamo soluzioni di sicurezza su misura per ambienti verticali); gestiamo sicurezza e privacy dei nostri 400mila dipendenti nel mondo e i nostri team gestiscono oltre 7 miliardi di "eventi" di sicurezza ogni giorno; ci occupiamo di sicurezza IT da oltre trent'anni; c'è una grande comunità di nostri business partner che implementa le nostre soluzioni e le integra con un'offerta complementare; i nostri consulenti di sicurezza possono suggerire le architetture e le tecnologie più appropriate di IBM o di propri partner, per assistere i clienti nella creazione della migliore soluzione per il loro ambiente. Realizziamo progetti per la sicurezza del territorio e per la protezione delle infrastrutture critiche sfruttando "l'intelligenza" prodotta dalle nuove tecnologie.

## Il governo del rischio

Il futuro riserva alle aziende molte opportunità, per sfruttare le quali se ne devono comprendere i rischi e imparare a gestirli con gli strumenti adeguati e in maniera integrata, valutando accuratamente l'impatto che i cambiamenti e le decisioni di business hanno sul livello di sicurezza e di conformità a leggi e normative.
In passato le aziende gestivano i diversi rischi con strutture separate che usavano metodologie di analisi e metodi di misura differenti. Un approccio a silos che non è più efficace, perché non dà una reale visibilità del livello di rischio aziendale e determina una duplicazione dei costi, con attività ripetute e ridondanti. È necessario passare a una gestione del rischio basata su un approccio integrato. In pratica, lo impongono le normative stesse, perché molte insistono sugli stessi elementi e chiedono le stesse garanzie, in termini di misure per la sicurezza o valutazione del rischio, per esempio. Con un approccio integrato si evitano ridondanze nei controlli e si persegue l'obiettivo di ridurre i costi, ma sono molteplici i fattori che spingono per una gestione integrata e convergente del rischio:

Meno costi e più efficacia: si ottimizzano gli investimenti tramite infrastrutture di sicurezza più efficaci ed efficienti e si riducono al minimo le conseguenze degli incidenti.
Pressioni del mercato: Investitori e clienti si aspettano che le aziende adottino un approccio integrato alla gestione del rischio, e che ne dimostrino i benefici ottenuti. Vogliono sapere qual è l'esposizione al rischio dell'azienda.
Benefici organizzativi: Una visione integrata del rischio consente all'azienda di cogliere opportunità di business più affidabili e di ottenere vantaggi consolidando le strutture organizzative. Come ha evidenziato uno studio del Politecnico di Milano, è importante adottare una struttura integrata anche a livello organizzativo per indirizzare i vari aspetti della gestione del rischio, viceversa il management avrebbe difficilmente una visione chiara.
Leggi e regolamenti: Il crescente numero di leggi e regolamenti orientati alla gestione del rischio d'impresa spinge ad adottare un approccio integrato.

## Dall'IT al business

Per supportare il cambio di approccio alla gestione del rischio, IBM ha quindi studiato e sviluppato modelli di governo e appositi strumenti. Da un lato, ha definito una metodologia di Enterprise Risk Management, che considera tutte le linee di business, non parte dall'IT, bensì dai processi di business per arrivare ai problemi tecnologici. Quindi la sicurezza vista come un processo da gestire con continuità e con un'organizzazione che sia in grado di definirlo e mantenerlo sempre allineato alle necessità dell'azienda. Non più solo sicurezza ICT, ma anche resilienza, che vuol dire creare un'infrastruttura capace di adattarsi ai cambiamenti e di garantire la continuità delle operazioni, coerentemente con le esigenze delle linee di business. In sintesi, un passaggio dall'IT al Risk Governance.
Da un altro lato, IBM ha sviluppato un modello di Compliance Management, che considera anche i requisiti del corporate audit, oltre alle normative che arrivano dall'esterno (leggi o regolamenti industriali). Tale modello comprende metodologie e sistemi per il Security Risk Management, finalizzati a rendere sicure tutte le infrastrutture che servono per conseguire gli obiettivi di business: persone, tecnologie, informazioni e processi. Solo garantendo che tutti questi elementi rispettano i requisiti di sicurezza stabiliti dall'azienda, è possibile dimostrare che l'azienda stessa ha una postura di sicurezza coerente con i propri obiettivi.

IBM ha anche sviluppato dei modelli per tradurre nel concreto il passaggio dalla security governance alla corporate governance. Il primo è l'IBM Security Framework che fornisce una vista a livello di business, seguito dalla IBM Security Blueprint, che dà una vista tecnologica, e, infine, l'offerta di prodotti, soluzioni e servizi di IBM insieme alle capacità ed esperienze dei suoi consulenti permettono di definire in dettaglio un'architettura dei sistemi che occorrono per ottenere i livelli di sicurezza e continuità operativa necessari per la propria azienda. Il framework per la sicurezza recepisce quanto previsto da standard internazionali, esperienze progettuali di IBM e best practice di settore, fornendo una visione di business e identificando le aree coinvolte nei processi di Security Governance, Risk Management e Compliance: Persone e Identità, Dati e informazioni, applicazioni e processi; applicazioni e processi; rete, server ed endpoint; infrastruttura fisica. Attraverso i professional service, i Managed Service e le proprie soluzioni hardware e software, trasversali alle suddette aree, IBM copre tutte le esigenze di sicurezza

A questo si aggiungono una serie di Red Book che aiutano a "tradurre" la visione di business in quella IT della sicurezza.

## Il supporto di IBM

Noi supportiamo i nostri clienti, sia direttamente sia attraverso i nostri partner, permettendo alle aziende di ottenere il desiderato livello di sicurezza, riducendo i costi di gestione e, soprattutto, rendendo questi ultimi prevedibili con certezza. Un altro elemento importante della nostra visione è la formazione, tesa, in particolare, a far crescere il livello di sensibilità alla sicurezza degli utilizzatori. L'abbiamo in primo luogo sperimentata internamente con documentazione, materiale e corsi sull'intranet.

Questo volume vuole essere una sintesi delle strategie, tecnologie, soluzioni, servizi di consulenza e servizi gestiti che IBM può mettere a disposizione dei propri clienti. Indubbiamente una sintesi articolata, ma che tocca comunque rapidamente i molteplici aspetti riguardanti la sicurezza e di cui IBM, come detto, vanta una vasta e lunga esperienza. Ognuno potrà essere interessato a una o a un'altra problematica, trovare notizie e nozioni sconosciute, gradire alcuni approfondimenti. Chiunque, però, potrà comunque contare sui consulenti IBM per qualsiasi dubbio, perplessità o "semplicemente" per avere una risposta alle proprie esigenze di sicurezza.

# Indice

# Un pianeta più intelligente è anche più sicuro

# 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. Ma i vantaggi maggiori si ottengono con una sicurezza "by design", cioè progettata sin dall'inizio in tutti i processi aziendali, nello sviluppo di prodotti e servizi, nelle attività quotidiane.

## 1.1 La security by design e un approccio olistico

IBM condivide una visione con i propri clienti: quella di uno Smarter Planet. Un pianeta in cui un crescente numero di strumenti e di interconnessioni crea grandi quantità di dati che potenti sistemi d'elaborazione trasformeranno in una nuova generazione d'intelligenza, in grado di migliorare la vita delle persone, i servizi della Pubblica Amministrazione, i processi delle aziende.

Grandi opportunità che comportano sfide sul fronte della sicurezza. Per quanto riguarda le imprese, l'esperienza fatta da IBM con migliaia di clienti dimostra che sono tre i fattori che spingono a investire in sicurezza: la complessità, i costi e la conformità a leggi, normative internazionali e standard (cioè la "compliance", volendo usare una sola parola con dizione inglese).

La complessità cresce ogni giorno sotto i nostri occhi, insieme alla quantità di informazioni che produciamo e raccogliamo: i dati continuano a raddoppiare in volume ogni 18 mesi. Tecnologie emergenti come la virtualizzazione o il cloud computing aumentano la complessità dell'infrastruttura, mentre le applicazioni Web 2.0 e SOA introducono nuovi problemi e vulnerabilità. Per rispondere alle esigenze di business, a quelle di disaster recovery e così via, storage, sicurezza e discovery delle informazioni sono sempre più importanti. Anche la mobility porta vantaggi, ma propone nuovi strumenti di accesso e identificazione, per i quali le tecnologie di sicurezza sono molto indietro rispetto a quelle utilizzate per i pc. Aumenta la complessità nella gestione della data security end to end lungo la catena del valore, mentre le aziende investono per migliorare il livello di collaboration con i propri clienti/utenti, anche attraverso i social network.

"Di più con meno" è un imperativo per la gestione dei costi, ma, anche a causa della maggiore complessità, la carenza di competenze tecniche dovuta tipicamente a staff ridotti all'osso crea problemi di sicurezza.

La pressione sulla compliance è in crescita. Prima ancora che imposta dalla legge, la privacy è richiesta dai clienti e dai dipendenti, che pretendono la riservatezza dei propri dati personali. Per garantirla è necessario integrare la sicurezza in infrastrutture, processi e applicazioni. Inoltre, la globalizzazione rende complessa e costosa l'attività di compliance, anche solo per il numero di normative che ogni azienda è chiamata a soddisfare.

I responsabili d'impresa devono dunque 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 relativo alla sicurezza e tutte le sfide sopra riportate ne fanno parte, viene tipicamente impostato un approccio tecnologico.

Secondo la visione di IBM è giunto il momento di pensarla in modo completamente diverso: introducendo la sicurezza in azienda "by design", cioè security e privacy devono essere inseriti nei processi di business, nei prodotti e nelle attività operative di ogni giorno sin dall'inizio. La sicurezza deve essere progettata e non aggiunta dopo.

IBM si propone come partner "trusted" per aiutare le imprese a implementare la sicurezza by design, avendo essa stessa sperimentato questo approccio: tecnologie di sicurezza sono infatti integrate nel fabric dei dispositivi hardware, nel codice del software e negli elementi caratterizzanti i servizi che fornisce. Inoltre, per supportare tale filosofia, IBM ha lanciato la Secure By Design Initiative, che, al proprio interno, ha portato alla costituzione in IBM di un Security Architecture Board e un Security Executive Board.

All'esterno, invece, l'iniziativa continua con lo sviluppo di prodotti e servizi che aiutano le imprese a ridurre i costi e i rischi, facilitando l'integrazione della sicurezza sin dalla fase di progettazione. Più precisamente: nuovi modelli di erogazione e distribuzione dei servizi, non ultimo il cloud computing, permettono alle organizzazioni di fornire accesso sicuro a server e applicazioni; servizi di test del software consentono di verificare se il codice sorgente contiene vulnerabilità e se rispetta la compliance, sin dalle prime fasi di sviluppo, in modo da aiutare a produrre applicazioni e processi sicuri; servizi di valutazione del codice esistente, che forniscono raccomandazioni per apportare modifiche e intraprendere azioni correttive.

A monte di tutto ciò, IBM mette a disposizione la propria esperienza, con servizi di consulenza relativi alla sicurezza by design, sia per gli aspetti organizzativi sia per quelli tecnologici, in particolare relativamente allo sviluppo di codice sicuro.

## 1.2 L'Information Security Governance

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. 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.

La sicurezza dell'impresa, in un senso più ampio è sempre stata una priorità del business e così deve essere anche per l'Information Security, che va fatta rientrare in una strategia più ampia di Enterprise Risk Management. Con questa logica, le spese diventano investimenti, la gestione della sicurezza sarà continua e integrata e non a intermittenza, mentre l'approccio sarà basato sui processi. Inoltre, questo significa anche che all'interno del dipartimento IT si dovrà spostare l'attenzione dall'Information Security a un concetto più ampio di resilienza dell'infrastruttura, cui si chiede di supportare i cambiamenti e garantire la continuità operativa. Obiettivi che coincidono con quelli di Compliance Management, altra tematica che, in un senso più ampio, riguarda il business, a partire dall'ufficio legale, prima ancora che il fronte operativo.

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 possa 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.

### 1.2.1 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.

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 avendo 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

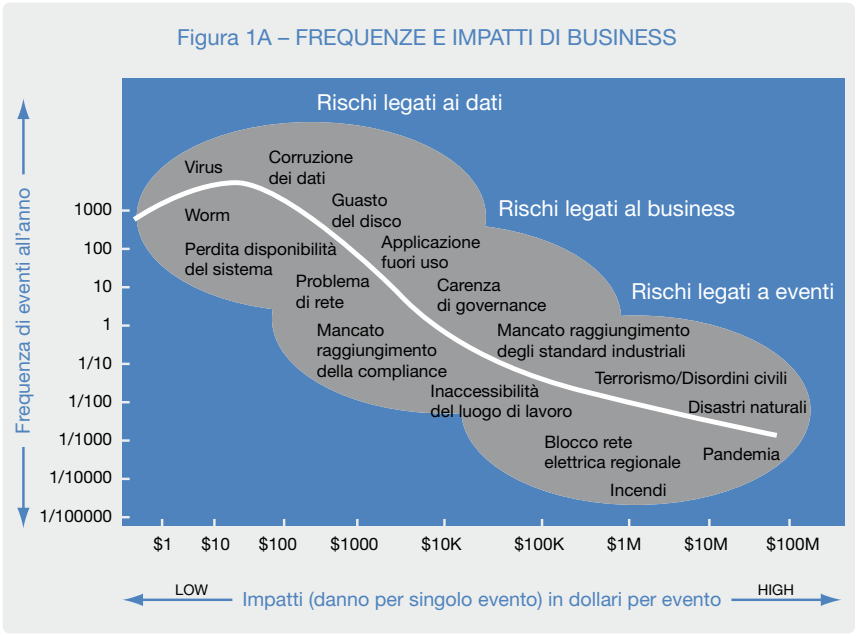



Figura 1.1
Frequenze e impatti di business

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 tipo data, business ed event driven. In generale, si possono identificare cinque macro aree chiave, che corrispondono, in pratica a quelle dell'IBM Security Framework e 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 nello svolgimento dei 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 strumenti 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 confrontate 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 sui sistemi, sui personal computer o più genericamente sugli end point 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 disponibilità 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.

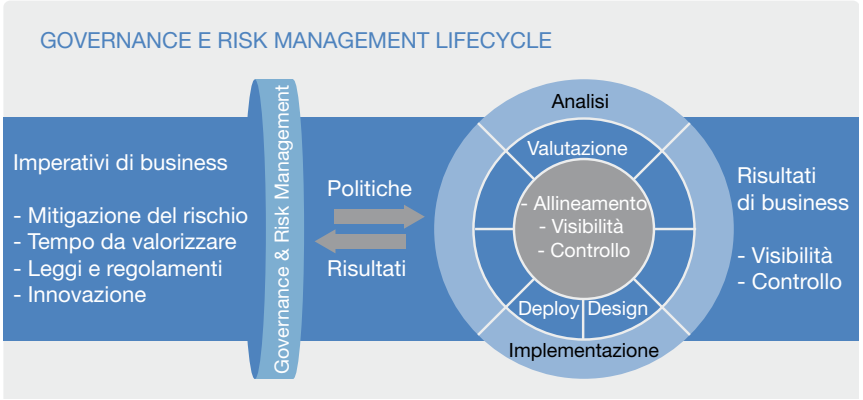
### 1.2.2 La strategia per l'Information Security Governance

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 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.

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

Figura 1.2
Governance e Risk Management Lifecycle

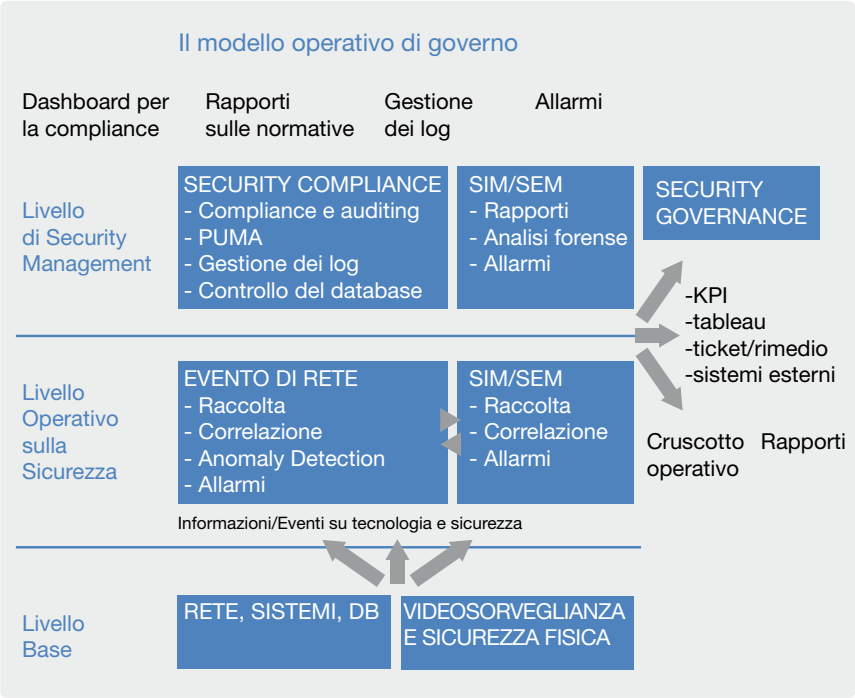


modo da soddisfare aspettative ampiamente riconosciute dal mercato. Queste aspettative sono stabilite da regole sociali, obblighi, norme per l'uso responsabile di Internet, codici etici aziendali e professionali e un insieme crescente di leggi nazionali e internazionali che richiedono la compliance da 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 tocca il tema del Security Information & Event Management, processo fondamentale per consentire di operare valutazioni e azioni in funzione del livello di responsabilità in una organizzazione, attraverso il monitoraggio e controllo della sicurezza. A partire dai controlli implementati a livello tecnologico sul campo, attra-

Figura 1.3
Il modello operativo di governo




verso opportune aggregazioni, correlazioni e analisi è possibile controllare gli indicatori di qualità della sicurezza in essere e intervenire con azioni di miglioramento.
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 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 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.

### 1.3.1 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 organiz-

zativa, 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.

### 1.3.2 Il supporto di IBM per la compliance alle normative sulla sicurezza

IBM 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.

Per le esigenze tecnologiche d'Information Security Compliance, accanto alle IBM Security Solutions, 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 framework 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'infrastruttura 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.

## Soluzione per l'Audit e il Monitoraggio della Sicurezza)

La proposta IBM per la realizzazione del Sistema di Audit e Monitoraggio della Sicurezza permette di rilevare e gestire le informazioni rilevanti 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 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 proposta da IBM è realizzata tramite l'utilizzo e la completa integrazione dei seguenti moduli:

- IBM Security Operation Manager;
- IBM Security Information and Event Manager.

## IBM Security Operation Manager

IBM Security Operations Manager 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 Security Operation Manager 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, Security Operation Manager 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 Security Information and Event Manager

IBM Security Information and Event Manager 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 IBM Security Information and Event Manager 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. IBM Security Information and Event Manager 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 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 sette 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.

### 1.3.3 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 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 portato a rivolgersi ad altri enti finanziari. Con il rischio di emulazione da parte anche di altri proprietari del medesimo tipo di carta. 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 cioè 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 e JCB. Lo standard definisce definiti requisiti o "requirements", concede 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 o service provider che memorizzano, elaborano o trasmettono in qualsiasi modo i dati delle carte 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.

Ad 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 le 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 busi-

ness, hanno già adottato criteri di sicurezza particolarmente robusti, come quelli derivanti da altri standard, quale l'ISO 27001, 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.

## 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 alle 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:

**Costruire e mantenere una rete protetta**

- Requirement 1: Installare e mantenere una configurazione con firewall per proteggere i dati dei titolari delle carte
- Requirement 2: Non utilizzare password di sistema predefinite o altri parametri di sicurezza impostati dai fornitori

**Proteggere i dati dei titolari delle carte**

- Requirement 3: Proteggere i dati dei titolari delle carte memorizzati
- Requirement 4: Cifrare i dati dei titolari delle carte quando vengono trasmessi attraverso reti pubbliche aperte

**Rispettare un programma per la gestione delle vulnerabilità**

- Requirement 5: Utilizzare e aggiornare con regolarità il software antivirus
- Requirement 6: Sviluppare e mantenere applicazioni e sistemi protetti

**Implementare misure forti per il controllo dell'accesso**

- Requirement 7: Limitare l'accesso ai dati dei titolari delle carte solo se effettivamente indispensabili per lo svolgimento dell'attività commerciale
- Requirement 8: Assegnare un ID univoco a ogni utente che ha accesso ai computer
- Requirement 9: Limitare la possibilità di accesso fisico ai dati dei titolari delle carte

**Monitorare e testare le reti con regolarità**

- Requirement 10: Monitorare e tenere traccia di tutti gli accessi effettuati alle risorse della rete e ai dati dei titolari delle carte
- Requirement 11: Eseguire test periodici dei processi e dei sistemi di protezione

**Adottare una politica di sicurezza**

- Requirement 12: Adottare una politica di sicurezza

Come accennato, molti dei punti elencati trovano risposta e formulazione nello standard ISO/IEC 27001, 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 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 è in grado di realizzare permettono di rispondere in modo adeguato ai requirement dello standard e a eliminare le conseguenze 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.

## Il supporto di IBM 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 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 coinvolto con esperti IBM Security Service, 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

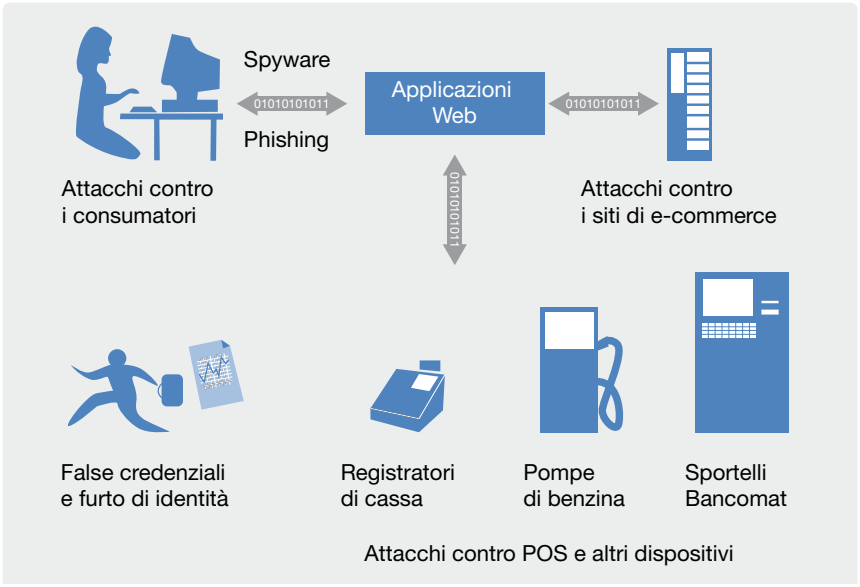



Figura 1.4

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

esigenze di compliance di un'azienda di qualsiasi dimensione prevede tre diversi interventi: assessment, remediation e certification. In particolare, quest'ultima fase, è supportata dagli esperti di IBM, che sono "Globally Certified" per realizzare i servizi PCI, possedendo certificazioni Qualified Security Assessor (QSA), Approved Scanning Vendor (ASV), Payment Application Qualified Security Company (PA-QSA).

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 Security Service 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

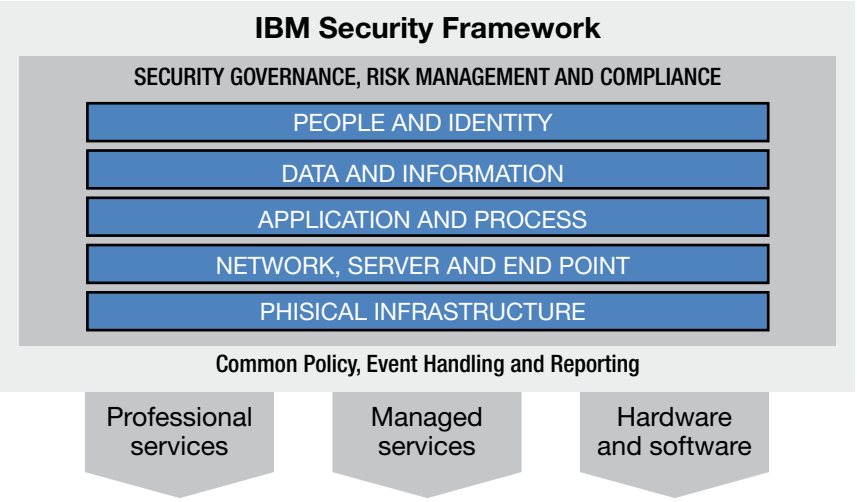
Le soluzioni IBM indirizzano l'intero insieme dei requirement stabiliti dallo standard PCI. Le soluzioni sviluppate, peraltro, rispondono alle esigenze di sicurezza basandosi su solide considerazioni sia economiche sia tecnologiche. Analisi da parte di primarie società di ricerca evidenziano infatti 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 Security indirizzano nel complesso tutti e sei i diversi temi che raggruppano i requirement previsti dallo standard PCI.

## 1.4 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.
L'ampiezza della strategia e la value proposition di IBM sono ben sintetizzate nell'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 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 innanzitutto una visione di business della sicurezza e, anche grazie ad altri modelli complementari, traccia un approccio 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).
Il framework per la sicurezza recepisce quanto previsto da standard internazionali, esperienze progettuali di IBM e best practice di settore, fornendo una visione di business e identificando le aree coinvolte nei processi di Security Governance, Risk Management e Compliance: Persone e Identità, Dati e informazioni, applicazioni e processi; rete, server ed endpoint; infrastruttura fisica. Attraverso i professional service, i managed service e le

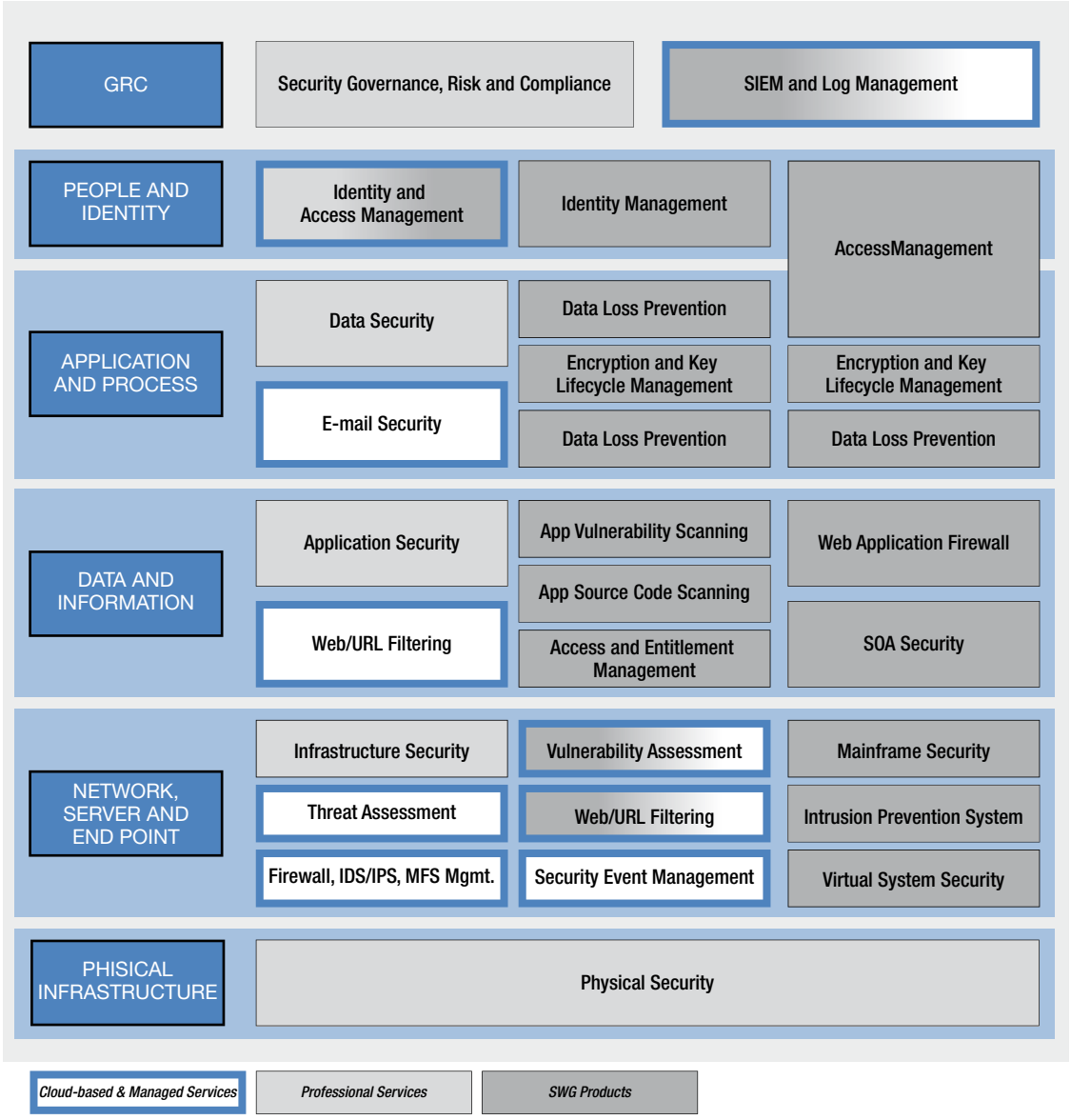
Figura 1.5
IBM Information Security Framework




proprie soluzioni hardware e software, trasversali alle suddette aree, IBM copre tutte le esigenze di sicurezza.
IBM ha inoltre creato modelli complementari, raccolti nell'IBM Security Blueprint, per favorire la convergenza della prospettiva di business della sicurezza con quella tecnologica.
All'interno dell'IBM Security Blueprint, il Foundational Security Management Services descrive i principali servizi di gestione che sono necessari per raggiungere le funzionalità descritte nell'IBM Security Framework: viene così creato un collegamento tra il requisito di business, identificato nel framework e il servizio IT proposto a soddisfarlo. La Common Security Infrastructure, a sua volta, contiene gli elementi infrastrutturali e i servizi che sono utilizzati dai servizi di alto livello descritti tra i Foundational Security Management Services.
Entrambi gli elementi della IBM Security Blueprint sono basati su standard e tecnologie aperte, che, insieme all'IBM Security Framework, possono essere utilizzate per progettare un'architettura che comprende piattaforme, componenti e configurazioni, basate su principi e pratiche aziendali per la sicurezza.
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

Figura 1.6
L'offerta di soluzioni e servizi IBM Security



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.

## Persone e identità

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 in azienda. Sempre più si tende a coinvolgere il responsabile delle risorse umane e dell'organizzazione 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. L'offerta di soluzioni e servizi di IBM in tale area consente di ottenere benefici quali:

- ridurre il costo, migliorare l'efficienza e abilitare l'audit-ability della gestione del flusso di utenti che entrano, lavorano e lasciano l'azienda;
- diminuire il rischio di frodi interne, perdita dati o interruzioni;
- supportare la centralizzazione delle operazioni;
- favorire il passaggio da una gestione tradizionale alla fornitura di servizi di gestione da remoto liberando risorse umane e capitali presso i clienti e i partner;
- migliorare l'esperienza dell'end user con applicazioni di business Web based abilitando il single sign-on;
- favorire lo sviluppo di servizi in ambiente federato.

## Dati e informazioni

La confidenzialità di informazioni e dati è un elemento fondamentale nella gestione del rischio aziendale. Ancora di più in un'epoca caratterizzata dalla globalizzazione dei mercati, da un lato, e delle comunicazioni, dall'altro. Le

soluzioni per la Data Loss Prevention, a partire dall'encryption per continuare con il controllo degli accessi ai dati e alla loro gestione consentono ai clienti IBM di ottenere i seguenti vantaggi:

- ridurre i costi;
- aumentare la capacità di soddisfare requisiti di auditing e di conformità;
- disporre di un metodo cost-effective per rispondere ai requisiti legali e per conservare e gestire le evidenze;
- assicurare la disponibilità dei dati alle persone giuste nei tempi giusti;
- assicurare che i dati non possano essere, volontariamente o inavvertitamente, persi, sottratti, modificati o distrutti;
- diminuire il numero e la complessità dei controlli aziendali.

## Applicazioni e processi

La sicurezza deve essere applicata a tutto il ciclo di vita delle applicazioni, dal loro disegno, 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 che consente di verificare in modo continuo e automatico le applicazioni Web, di risolvere alcuni problemi di sicurezza e di creare report con suggerimenti per semplificare il processo di correzione dei difetti nel codice. 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 e che è ovviamente coperta in termini di sicurezza dalle soluzioni IBM Security. Inoltre, IBM ha sviluppato soluzioni e servizi anche per la sicurezza delle applicazioni negli emergenti ambienti di cloud computing.

Le soluzioni IBM Security in tale ambito portano i seguenti benefici:

- ridurre il rischio di indisponibilità, defacement o furto di dati associati alle applicazioni Web;
- verificare e monitorare la conformità con le politiche di sicurezza a livello enterprise;
- migliorare la conformità con le normative e gli standard di settore (per esempio, PCI, Data Privacy, SOX e altre);
- migliorare la sicurezza nell'integrazione delle applicazioni business critical;
- riduzione dei costi di sicurezza nel lungo periodo tramite l'automazione del testing e la gestione dei requisiti della sicurezza in tutto il ciclo di vita del software.

## Mitigazione delle minacce all'infrastruttura IT (reti, server ed endpoint)

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.

Tra i punti di forza dell'offerta IBM Security, le soluzioni e i servizi per la mitigazione dalle minacce portano vantaggi quali:

- ridurre il costo della gestione quotidiana della sicurezza;
- migliorare la disponibilità dei servizi di gestione e assicurare prestazioni allineate ai service level agreement garantiti dai managed protection service;
- migliorare la produttività tramite la riduzione dei rischi di virus, worm e diffusione di codice maligno;
- diminuire il volume di posta indesiderata (incoming spam);
- investigare dettagliatamente specifiche violazioni per indirizzare rapidamente le soluzioni;
- mostrare rapidamente lo stato di allineamento rispetto alle principali normative.

## La sicurezza delle infrastrutture fisiche

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. In quest'ambito l'offerta di IBM è in continua crescita e già consente di ottenere benefici come:

- ridurre il rischio di interruzione o furto di dati associato al malfunzionamento o perdita di asset fisici critici;
- rispondere alle minacce più velocemente, rispetto a quanto avviene in ambienti monitorati a vista, riducendo i costi e i rischi di perdite, grazie a una strategia di sorveglianza e sicurezza fisica integrata, che permette di estrarre dati "intelligenti" da molteplici sorgenti.

### 1.4.2 Gli IBM Managed Security Service

All'interno dei framework IBM sono elencate best practice che sono supportate dalle soluzioni e servizi di IBM. Di fatto, IBM lascia un'ampia scelta al cliente, grazie a un'offerta vasta di servizi gestiti, su cui IBM Security Service vanta una lunga esperienza.
L'architettura open-vendor consente a IBM di gestire e monitorare piattaforme multivendor e di fornire una vista integrata dello stato della sicurezza tramite un'unica interfaccia Web-based disponibile sul portale di gestione, lasciando all'azienda la possibilità di controllare la sicurezza della propria infrastruttura. D'altro canto, la gestione operativa, molto costosa perché richiede un'elevata competenza, può essere demandata a chi d'esperienza ne ha "da vendere", concentrandosi sul proprio core business. Gli IBM Managed Security Service rispondono in questo modo all'esigenza di ridurre i costi di gestione e, nel contempo, di aumentare l'efficacia delle misure di sicurezza.

### 1.4.3 La formazione degli utenti e la cultura della sicurezza

Gli IBM Security Service forniscono servizi di consulenza per la valutazione, progettazione e implementazione della sicurezza aziendale per realizzare soluzioni efficaci per la sicurezza delle informazioni, riducendo le minacce alle risorse essenziali per il business.
Tra i servizi di consulenza peculiari ci sono anche quelli sulla formazione del personale e sull'organizzazione della sicurezza. La formazione è infatti un elemento importante per la strategia di sicurezza aziendale e IBM ne ha fatto un punto fondante della propria visione. Implicito nel concetto stesso di "Security by Design", infatti, vi è anche quello della formazione: se si vuole adottare un approccio innovativo alla sicurezza orientato al business, cioè basato sulla gestione dei rischi, non si può dimenticare l'importanza della cultura aziendale. Una sicurezza integrata nei processi di business e nelle attività operative quotidiane, infatti, impone prima la crescita della sensibilità verso la sicurezza da parte degli utenti.
IBM ne è talmente consapevole che ha varato specifiche iniziative in tal senso, per esempio, dedicando un'intera settimana alla sicurezza sull'intranet aziendale e diffondendo documentazione di vario tipo, per far crescere la consapevolezza sulla tematica.

#### IBM Institute for Advanced Security

Esperti globali, membri delle pubbliche amministrazioni, dell'industria, dell'università e di organizzazioni non governative provenienti da tutto il

mondo hanno individuato nelle minacce alla cyber-security un potenziale rischio per la pace e la stabilità internazionale, invocando la creazione di un'agenzia per la cyber-sicurezza, con l'obiettivo di intensificare la collaborazione tra settore pubblico e privato e sensibilizzare i leader globali sulle problematiche legate alla sicurezza del Web. Per affrontare queste problematiche, IBM ha costituito l'Institute for Advanced Security: un'iniziativa volta a supportare aziende, università e partner a comprendere, affrontare e mitigare più agevolmente i problemi associati alla protezione del cyberspazio.

L'istituto, con sede nella capitale statunitense, Washington D.C., collaborerà con dirigenti del settore pubblico e privato e permetterà l'accesso a una vasta gamma di risorse, per aiutare la pubblica amministrazione a proteggere in modo più efficiente ed efficace le informazioni e le infrastrutture critiche, su cui incombono dal cyberspazio minacce sempre più pericolose e onerose. Esperti IBM di ogni divisione aziendale collaboreranno con l'Istituto per aiutare i clienti ad affrontare le sfide esistenti ed emergenti, utilizzando le tecnologie, i servizi e le soluzioni più avanzate per prevedere, prevenire e mitigare il crescente rischio, e il potenziale impatto economico, di un cyber attacco. Per esempio, la U.S. Air Force ha scelto IBM per progettare e realizzare un'infrastruttura di cloud computing altamente sicura, in grado di supportare le reti di difesa e di intelligence.

L'Istituto ha inoltre aperto un forum per consentire ai clienti di comprendere meglio come i risultati della ricerca IBM (per esempio la rivoluzionaria crittografia totalmente omomorfica) possano aiutarli a operare in modo più efficace, proteggendo al contempo la privacy e la sicurezza delle informazioni critiche.

Al centro del supporto degli esperti IBM vi sarà il "Security by Design", come approccio ritenuto vincente, rispetto ai modelli tradizionali "aggiuntivi", che si occupano di sicurezza solo dopo il verificarsi di un evento e che vengono scelti spesso con il solo metro del veloce ROI (Return On Investment).

Con oltre 3.000 brevetti in materia di sicurezza e gestione del rischio e uno dei più completi database del mondo sulle minacce e vulnerabilità, IBM si avvarrà dell'IBM Institute for Advanced Security per applicare le capacità e l'esperienza dei suoi 15mila esperti in sicurezza a una vasta gamma di sfide per la cybersecurity e la privacy.

## 1.5 La ricerca e sviluppo di IBM a tutela della sicurezza

La visione olistica della sicurezza professata da IBM si riflette anche negli sforzi di ricerca e sviluppo. Sono nove e distribuiti in varie parti del Globo i centri R&D di IBM dedicati alla sicurezza: 3 negli Stati Uniti, Almaden, TJ Watson (Hawthorne) e Atlanta; uno in Canada a Ottawa; uno in Europa a Zurigo in Svizzera; due in Israele, Haifa ed Herzliya; uno a Nuova Delhi, in India; uno a Tokyo in Giappone. 24 ore su 24, dunque, ci sono esperti di IBM impegnati nello sviluppo di nuove soluzioni e tecnologie per la sicurezza in tutti i suoi aspetti: crittografia, smart card, biometrica, vulnerabilità, analisi del malware e altre tecniche di contrasto alle minacce Internet, PKI, antivirus, antispamming e altro ancora.

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 dalla pericolosità espressa dalle nuove forme di attacco, dall'altro. Ma 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 acquisito da IBM con 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 IBM Security, nonché educare i media e le comunità di utilizzatori su tali problematiche emergenti.
Non a caso X-Force rappresenta una delle ragioni che hanno portato alla nomina di Internet Security Systems come security provider dell'Information Technology Information Sharing and Analysis Center (IT-ISAC) nel 2000, all'atto della sua fondazione.
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.

### 1.5.1 L'intelligenza "virtuosa" della ricerca X-Force

Il ciclo di vita della ricerca e sviluppo attuata da X-Force, si avvale di un meccanismo virtuoso, innescato dalle migliaia di dispositivi per la sicurezza monitorati da IBM X-Force. Questi comprendono gli apparati targati IBM Security che sono stati installati negli anni presso i clienti, ma anche dispositivi di terze parti, la cui gestione è comunque affidata agli IBM Managed Security Service. La quantità di dati che viene raccolta viene utilizzata ai fini della ricerca, quindi per meglio comprendere cosa sta accadendo sul fronte delle minacce e per meglio sviluppare il codice d'analisi per i moduli della piattaforma di protezione IBM Protocol Analysis Module. Ovviamente ciò accade con il consenso dei clienti: consenso che praticamente nessuno nega, non solo per la garanzia di riservatezza, ma soprattutto perché i risultati di questo lavoro ritornano immediatamente sotto forma di una protezione più accurata ed efficiente.
Alla grande quantità di dati raccolti dai dispositivi e analizzati nell'erogazione dei Managed Security Service, nonché di quelli che arrivano dalle sonde d'intrusion prevention e dagli altri dispositivi di sicurezza IBM Security, X-Force conduce la propria analisi dettagliata dei possibili exploit o dei siti

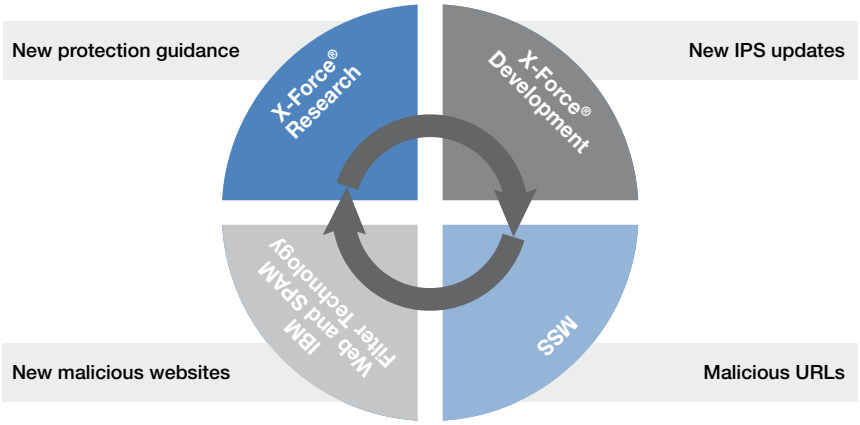



Figura 1.7
Il ciclo virtuoso della ricerca e sviluppo di IBM X-Force

compromessi e ne ricavi orientamenti e linee guida per lo sviluppo della sicurezza. I risultati della ricerca, peraltro, utilizzano anche dati provenienti da altre molteplici fonti, come quelle degli enti e delle società che partecipano ai programmi di "information sharing", le collaborazioni, le organizzazioni industriali o, semplicemente, attraverso i contatti online degli stessi ricercatori.
Nella fase di sviluppo questi risultati vengono messi in atto nella realizzazione degli aggiornamenti per i dispositivi di sicurezza. Grazie alla formula di distribuzione X-Press Update (XPU), inoltre, le nuove protezioni arrivano tempestivamente alle soluzioni IBM Security, che continueranno a essere monitorate, chiudendo il ciclo.
Sono circa 7mila le vulnerabilità annunciate ogni anno, IBM X-Force le analizza tutte e di ognuna viene valutato l'impatto e la gravità, in base a vari fattori, come il tipo di vulnerabilità, l'effetto prodotto, la diffusione del sistema vulnerabile, le condizioni dell'exploit perpetrato.

## 1.5.2 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 50mila vulnerabilità catalogate a partire dagli anni Novanta, con continui aggiornamenti. Ogni trimestre 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 analizzano 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.
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 è storicamente uno tra quelli che scoprono il maggior numero di vulnerabilità, in particolarità delle vulnerabilità ad alto rischio.
I Security Operation Center di IBM, 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. 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 sul sito di IBM per la sicurezza, www-03.ibm.com/security, 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 e di emergenza per la protezione.
Un aspetto importante del lavoro di X-Force è rappresentato dall’attenzione che viene riservata alla qualità nella scrittura del codice e nella validazione del software prodotto, elementi alla base del “secure by design”. 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 analogo a quello 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. Considerando che alcuni protocolli chiave sono proprietari e quindi non documentati (come per esempio RPC di Microsoft), ciò non è semplice e un aspetto fondamentale è controllare, una volta che il parser sia stato scritto, che sia effettivamente capace di rilevare tutte le varianti di utilizzo del protocollo. Inoltre, occorre verificare che 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 "severi", non rappresentano la completezza mondo reale, e conducono attività importanti in collaborazione con partner fidati.

## 1.6 La sicurezza del mainframe con la suite 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 del valore di 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 della 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 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 attività di auditing per il

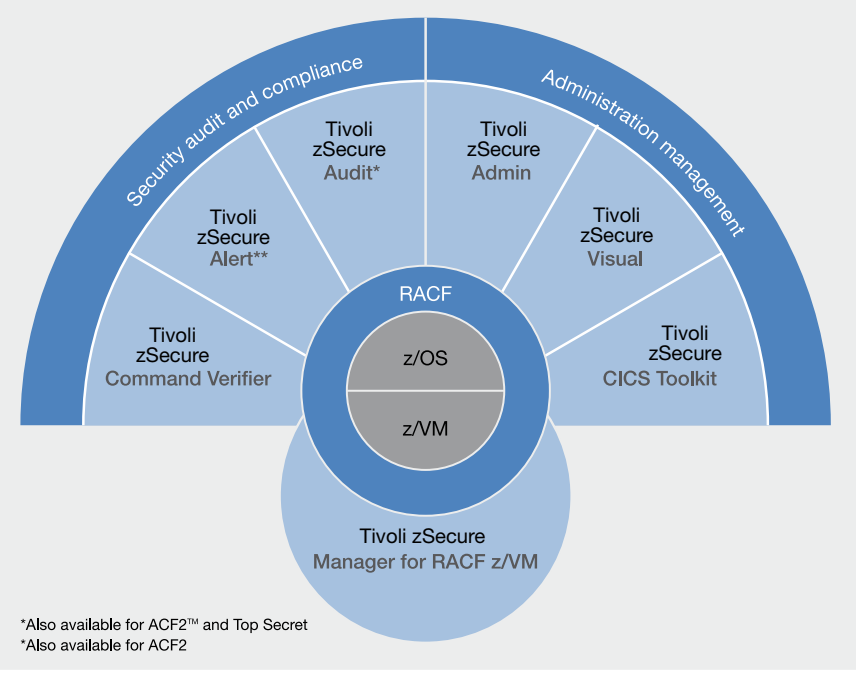
mainframe con un'estensione in profondità in tutta l'impresa.
La suite specializzata sulla piattaforma mainframe è denominata Tivoli zSecure e comprende i seguenti moduli:

- Tivoli zSecure Admin: amministrazione RACF e query via TSO o batch
- Tivoli zSecure Audit: rilevazione e reporting degli eventi sul mainframe, con analisi delle esposizioni di sicurezza
- Tivoli 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, ecc.)
- Tivoli zSecure Command Verifier: tool di security compliance RACF per l'applicazione delle politiche sui comandi RACF
- Tivoli zSecure Visual: amministrazione e query RACF di base, utilizzando l'interfaccia di Windows Client a RACF
- Tivoli zSecure CICS Toolkit: amministrazione RACF di base via CICS

A questi moduli, per i clienti che hanno RACF su z/VM, si aggiunge il modulo

- Tivoli zSecure Manager for RACF z/VM: amministrazione RACF e query via TSO o batch in ambiente z/VM

Figura 1.8
La suite Tivoli zSecure



### 1.6.1 Admin

Vediamo in dettaglio i valori in termini di innovazione apportati dalla sopracitata suite. Il primo è legato al problema del sovraccarico di lavoro degli amministratori. Tivoli zSecure Admin è stato progettato per essere un meccanismo efficiente per 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'intera giornata di lavoro agli amministratori RACF, se si vuole fare tutto nel modo giusto, considerando ogni circostanza e risolvendo ogni problema. Con Tivoli 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 Tivoli 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 WYIWYG10. Se si apporta una modifica e si preme Invio, il comando RACF viene generato automaticamente. Ciò rappresenta ovviamente un enorme risparmio di costi, perché prevenire gli errori nell'amministrazione della sicurezza è un'attività che può essere molto onerosa, per il downtime del sistema e le esposizioni di sicurezza. Oltre alla 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 Tivoli zSecure CICS Toolkit e Tivoli zSecure Visual, a seconda del tipo di competenze dell'amministratore della sicurezza e del reparto.

### 1.6.2 Audit e compliance

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 control-

lare per stabilire se una certa azienda rispetta i regolamenti di sicurezza nello svolgimento delle sue attività quotidiane. Ciò significa per i responsabili di tali verifiche identificare tutte le possibili esposizioni di sicurezza, un compito enorme e difficile quando la fonte dell'informazione è molto ampia, come nel caso di un archivio SMF. Tivoli 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 il punto dolente dei clienti a cui accennavamo in precedenza, relativamente a System z. Il tool è infatti in grado di identificare le esposizioni e le vulnerabilità della sicurezza nel più breve tempo possibile, anche se la mole di informazioni arriva da archivi di enormi dimensioni quali SMF. 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. Il tool consente 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 Tivoli 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. Questo aspetto di semplificazione è caratterizzato da potenti funzioni di reporting, analisi e valutazione, valide non solo per RACF ma anche per altri sottosistemi z/OS, che 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. Ma non è l'unico vantaggio. L'ultima cosa da dire che è un cliente 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 accettate dal cliente per il proprio ambiente. Questa tecnologia di audit è estremamente flessibile e può essere resa più efficiente per un cliente con l'aiuto di un consulente della sicurezza, che potrà modellare le funzioni del tool in base a qualsiasi esigenza di audit del mainframe del cliente. È facile comprendere l'utilità di questa tecnologia semplificata per i clienti mainframe, soprattutto perché le nuove normative in merito alla protezione

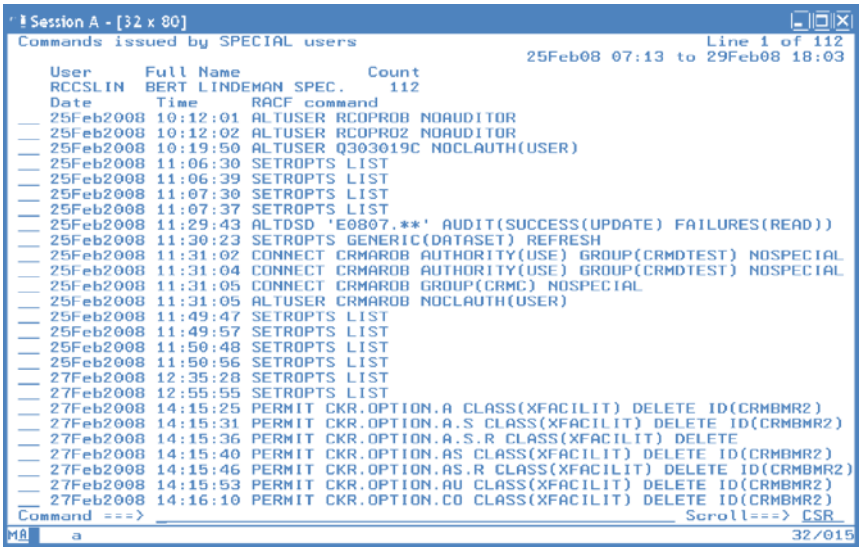



Figura 1.9
Lista dei comandi RACF eseguiti, ottenuta tramire Tivoli zSecure Audit

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 come si sa un formato grezzo, di lettura e interpretazione estremamente complicate. Tutte queste informazioni diventano invece facilmente ricavabili e interpretabili tramite Tivoli zSecure Audit, coadiuvato da Tivoli zSecure Admin, come si può vedere dalla figura successiva che fornisce una tipica query mainframe di lettura decisamente più semplice.

L'ultimo valore aggiunto della suite Tivoli 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, e che può causare errori involontari e talvolta attacchi interni fraudolenti. Di grande efficacia è il tool Tivoli 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 normal-

mente 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 Tivoli zSecure Command Verifier, che consente di definire criteri propri di sicurezza. Esempi di questi criteri possono essere convenzioni di dominazione 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, ecc. Oltre a Tivoli zSecure Command Verifier, i rischi sopra citati possono essere ridotti anche con l'ultimo modulo della suite chiamato Tivoli 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. Identifica le minacce al sistema in generale, o a un'applicazione in particolare. È in grado di monitorare set di dati sensibili, per esempio i dati della contabilità. Supponiamo di avere le nostre informazioni sanitarie che contengono molti database della contabilità. Dobbiamo assicurare che nessuno dei nostri utenti privilegiati copi o modifichi questi dati. È qui che entra in gioco Tivoli zSecure Alert, che 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 IBM Security Operation Manager, completandone le funzionalità.

I moduli Tivoli zSecure Audit e Alert sono nativamente integrati con la soluzione, sempre di provenienza Consul, IBM Security Information and Event 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.

# 2
# La mitigazione delle minacce all'infrastruttura IT

**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 una Smart Protection. 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 e browser, 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 Security Solutions, 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 dimostrativa né tanto meno goliardica, bensì spinti dal desiderio di profitto o, peggio ancora, dall'odio o dalla ven-

Tabella 2.1

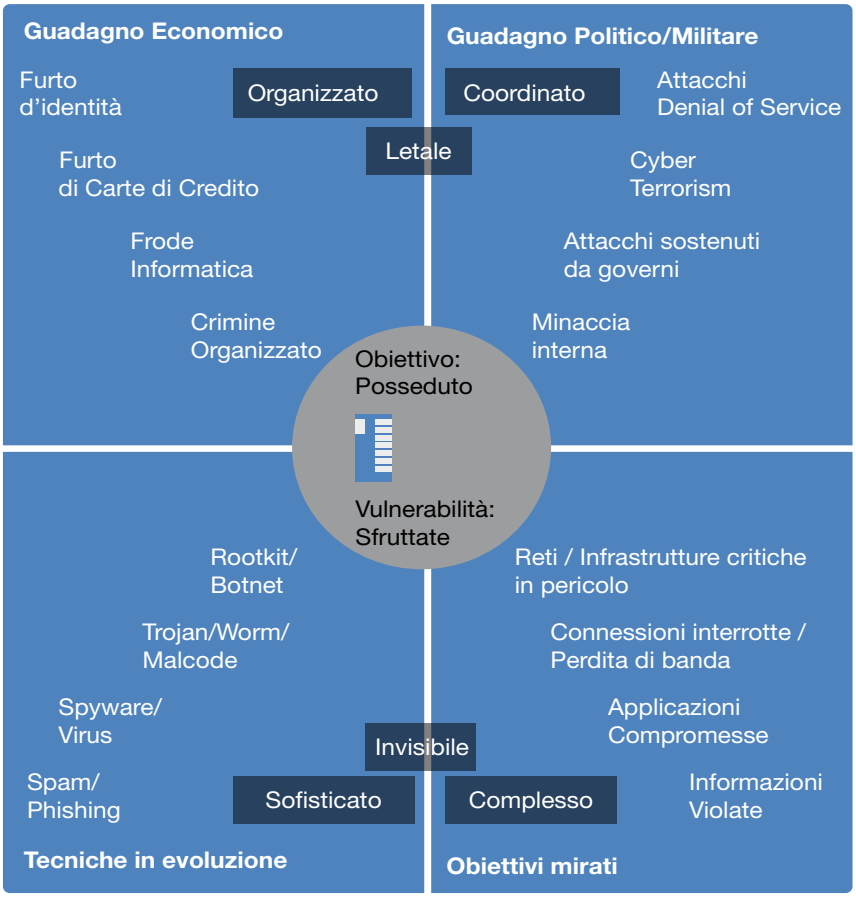
Come sono cambiate le caratteristiche degli attacchi dalla prima alla seconda decade di Internet

| 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 |

detta. 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. Molte di queste truffe, inoltre, sono orchestrate con scopi molto precisi da parte di associazioni

criminali di vario tipo, anche di stampo mafioso, per il riciclaggio di denaro proveniente da attività illecite.
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. Non si deve peraltro credere che il rischio sia relegato in questo tipo di siti, perché ormai circa il 50% delle vulnerabilità si trova nel mondo delle applicazioni Web. Anche pagine insospettabili vengono manomesse, in modo da annidarvi malware che viene scaricato sul computer dell'ignaro visitatore. Le applicazioni che vengono offerte agli utenti, di fatto, vengono sfruttate dagli hacker. Per questo le aziende che intendono sviluppare opportunità di business online devono dotarsi di adeguati sistemi di sicurezza.
Intanto, 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 quanto riguarda la protezione dalle minacce, IBM propone i servizi, le soluzioni e le tecnologie best of breed IBM Security Solutions.
IBM Security è stata la prima a sviluppare un sistema di vulnerability assessment e la prima a commercializzare un sistema di Network Intrusion Prevention. 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, sviluppati in chiave "cloud". In quest'ottica, la filosofia per la protezione dalle minacce s'integra appieno con quella di approccio integrato e olistico di IBM.

Figura 2.1
Le forze dinamiche nell'evoluzione delle minacce




## 2.2 L'approccio olistico basato sull'IBM Security Framework

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. È quindi necessario che la sicurezza sia affrontata ad alto livello, con un taglio strategico. Per questo, IBM ha sviluppato il Security Framework i cui pilastri fondamentali sono security governance, risk management e compliance management. Qualsiasi aspetto riguardante la sicurezza aziendale deve partire da problematiche di tipo strategico, definendo l'insieme di regole che consentono di governare la sicurezza in base alle esigenze di business e di gestire il rischio dell'intera organizzazione, nonché assicurare la compliance (si veda il capitolo 1).

Il discorso vale in generale per tutto il sistema di security aziendale, ma anche, in particolare, per quel che concerne la mitigazione delle minacce all'infrastruttura IT e la data security. Prima degli aspetti tecnologici, infatti, è necessario affrontare questioni 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 Security Solutions, 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 Security 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 Security 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 IBM Security 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 Security si riferisce a questo modo di operare con il termine di "Preemptive Protection" o protezione preventiva. Una volta che si è stabilita la priorità degli interventi e si sono messe in campo le misure di sicurezza addizionali ritenute necessarie, giunge il momento di verificare se le azioni intraprese abbiano una reale efficacia. Le risposte le forniscono, anche in questo caso, le IBM Security Solutions

## 2.3 IBM Protocol Analysis Modular Technology

L'infrastruttura IT è costituita da quegli elementi, server, storage, rete ed endpoint, che rappresentano la piattaforma di elaborazione a supporto dei processi aziendali. In tale veste è spesso l'obiettivo di attacchi da parte

degli hacker. È quindi fondamentale garantire che l'infrastruttura sia protetta affinché i servizi e le applicazioni che vi si appoggino funzionino rispettando le condizioni operative previste (in altre parole, si devono garantire i Service Level Agreement). È bene osservare che buona parte dei disservizi sono riconducibili a errori di configurazione da parte degli amministratori di sistemi o a processi di change management mal impostati. Addirittura l'87% degli incidenti interni è causato dagli utenti "privilegiati". Con una gestione efficace non solo è possibile ridurre il rischio in questi casi, ma anche diminuire sensibilmente il total cost of ownership delle risorse. In particolare, secondo quanto affermato da Gartner, il TCO di un desktop sicuro può essere ridotto del 42%.

IBM dispone di strategie, soluzioni e servizi che consentono di gestire diverse forme di rischio in più modi, proteggendo server, endpoint, reti e mainframe, attraverso un'offerta completa per la sicurezza dell'infrastruttura. La Smart Protection Platform di IBM Security fornisce una 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, basati sul lavoro di IBM X-Force: un team di ricerca costantemente in anticipo sulle minacce, bloccandole prima che abbiano impatto sull'organizzazione.


Figura 2.3
Gli elementi che costituiscono la IBM Security Solutions Smart Protection

Figura 2.4

Una visione dei prodotti e servizi IBM Security per la Smart Protection dell'infrastruttura IT

**BUSINESS VALUE**

Massimizzare la disponibilità del servizio mitigando il rischio, ottimizzando esperienza, tecnologia e processi

| | **Protezione dei server** | **Protezione degli endpoint** | **Protezione delle reti** | **Protezione dei mainframe** |
|---|---|---|---|---|
| Business Challange | Mitigare minacce rivolte ai server; prevenire la perdita dei dati (Data Loss Prevention) | Una gestione efficace può tagliare del 42% i costi di possesso di un desktop sicuro (fonte Gartner) | Mitigare minacce basate sulla rete; prevenire la perdita dei dati (Data Loss Prevention) | Mitigare le minacce rivolte ai mainframe; protezione delle vulnerabilità di configurazione; contenere i privilegi per gli utenti |
| Software | Server Protection, Server Protection for WMWare | Desktop security platform; encryption | Network Intrusion Prevention System (IPS) | Tivoli zSecure suite |
| Professional Services | Server security, data security assessment services | Desktop security, data security assessment services | Network security assessment services | |
| Managed Services | Managed IDS, Privileged User Mgmt | Managed Desktop security platform | Managed Network IPS | |

Alla base della piattaforma di protezione intelligente c'è un meccanismo virtuoso, tale per cui immediatamente tutti i dati raccolti dai prodotti installati presso migliaia di clienti o registrati dai Managed Security Service vengono analizzati e correlati, in modo da alimentare l'attività di ricerca e, al tempo stesso, al fine di mantenere sempre aggiornate le soluzioni e i servizi di prevenzione.

Grazie a questi presupposti la IBM Security Solutions Smart Protection 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 Security Solutions: evitare 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 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 Smart Protection sono tutte

gestibili dalla stessa console (IBM Security SiteProtector integrata con IBM Security Incident and Event Management) e, soprattutto, sono tutti dotati di intelligenza sufficiente a intervenire quando la situazione lo richiede. Per aumentare ulteriormente il livello di sicurezza, IBM Security offre tutto questo sotto forma di servizi, permettendo alle imprese 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 fa di IBM Security un punto di riferimento per la sicurezza e la protezione dalle minacce di ieri, oggi e domani.

Alla base di questa strategia preventiva vi è l'IBM Protocol Analysis Module (PAM), un engine di protezione verso un'estesa varietà di minacce, frutto della ricerca e sviluppo portata avanti negli anni da IBM X-Force. Grazie alla sua struttura modulare, PAM è in continua evoluzione e blocca anche le ultime minacce, senza bisogno di aggiungere ulteriori punti di protezione o soluzioni dedicate, così come si faceva in passato nelle architetture di sicurezza a "silos". In maniera automatica, X-Force aggiorna i moduli del motore di analisi per assicurare sempre la protezione allo stato dell'arte.

Gli elementi dell'IBM PAM comprendono:

- Virtual Patch – È uno scudo che impedisce gli exploit delle vulnerabilità, anche senza che siano state installate le patch per le stesse.
- Client side Application Protection – Protegge gli utilizzatori dagli attacchi mirati alle applicazioni di uso quotidiano, come i pacchetti office, i Web browser, eccetera.
- Web Application Protection – Protegge i Web server da attacchi sofisticati come SQL Injection, XSS (Cross Site Scripting), PHP file-includes, CSRF (Cross-site request forgery).
- Threat Prevention – Rileva e previene intere classi di minacce relative a specifici exploit o vulnerabilità.
- Data Security – Monitorizza e identifica informazioni personali (PII – Personally Identifiable Information) e altre informazioni confidenziali per impedirne la divulgazione non autorizzata. Fornisce anche la capacità di esplorare i flussi di dati attraverso la rete e aiuta a determinare potenziali rischi.
- Application Control – Permette di controllare applicazioni non autorizzate o a rischio, all'interno di specifici segmenti di rete, per esempio bloccando l'esecuzione di Active X fingerprint o di applicazioni peer to peer, instant messaging o tunneling.

PAM, inoltre, combina e utilizza molteplici tecnologie per la prevenzione di minacce, tra cui quelle base sulla content analysis, ispezione del traffico e assemblaggio dei flussi, analisi dei protcolli, stateful ispection e altri, tra cui una premiata tecnologia di Shellcode Heuristics.
Per indirizzare tutte le diverse categorie di attacchi, PAM impiega diverse tecnologie per l'intrusion prevention. 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.
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 "Day 0", perché è da qui che si comincia a calcolare quanto tempo ci mettono le comunità di hacker a ideare un exploit. Ma, ormai, si tratta di un tempo che andrà misurato in ore piuttosto che in giorni. Infatti, si è praticamente arrivati allo "zero day threat": è pari all'80% la percentuale di vulnerabilità di cui viene effettuato un exploit entro 24 ore dal loro annuncio. Peraltro, nella migliore delle ipotesi, quest'ultimo viene effettuato contestualmente al rilascio della patch, ma, soprattutto a livello enterprise, è impossibile riuscire a installare una patch e portarla in produzione istantaneamente: stime accurate mostrano tempi medi di un anno per il patching. Non sempre, poi, quando viene annunciata una vulnerabilità è già disponibile la patch. Per questo, PAM risponde con tecnologie d'avanguardia, come Virtual Patch e Shellcode Heuristics, per fornire la "0 Day protection".

### 2.3.1 L'intrusion pre-emption

L'evoluzione delle minacce presenta vari 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 intera-

zione 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 considerino, per esempio, informazioni, foto, video e altri dati privati pubblicati sui siti di social networking come Facebook, Twitter, YouTube, LinkedIn e altri. Questi rappresentano 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.

Partendo dai propri punti di forza tradizionali, vulnerability assessment e intrusion Prevention, IBM Security Solutions 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, cioè gli errori di "iper-sensibilità", che potrebbero determinare impatti negativi sulla rete. D'altro canto, è altrettanto se non più importante evitare i falsi negativi, cioè gli errori di "ipo-sensibilità", in seguito ai quali un attacco passa inosservato. Trovare il bilanciamento ottimale è il lavoro continuo svolto da sviluppatori e ricercatori nell'ambito della qualità del prodotto.

Gli esperti di IBM Security Solutions hanno 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 prevention (IPS) è la piattaforma di gestione rappresentata dalla suite SiteProtector di IBM Security Solutions. 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 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 ha da tempo messo in interazione il sistema di vulnerability assessment e l'IPS, 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, peraltro, non si limita a estrapolare dati: perché 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 messa al servizio dei clienti.

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 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 Security Solutions è innanzitutto rappresentata dall'avanzata tecnologia di scansione e controllo della rete e degli host. La tecnologia di intrusion Prevention, sul lato rete, comprende un'analisi dei protocolli molto raffinata, estesa su tutti i 7 livelli della pila OSI. In particolare, le tecnologie di protezione attuate dai sistemi di intrusion prevention di IBM Security Solutions 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.
Nelle reti convergenti di nuova generazione, inoltre, si presentano problematiche di sicurezza particolari. Le tecnologie di analisi IPS di IBM Security 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 Virtual Patch

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 e, in un mercato estremamente competitivo, la priorità è sempre stata l'accelerazione del time to market.
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, crescevano 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. Infine, best practice indicate da più normative impongono che le patch siano installate prima in ambienti di test e solo successivamente in produzione: la compliance impedisce, perciò, di accelerare i tempi.
Per questo, IBM 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 la Virtual Patch, trade mark registrato da IBM che per prima ha sviluppato questo meccanismo. La Virtual Patch garantisce una protezione attraverso una sorta di "aggiornamento" virtuale dei sistemi vulnerabili. Quando gli esperti di X-Force rilevano una vulnerabilità e identificano un modo in cui questa può essere sfruttata, studiano quali sono le caratteristiche necessarie e sufficienti per sfruttare la vulnerabilità anche se non esistono ancora 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). Fatto questo sviluppano un codice per il modulo Virtual Patch dell'IBM PAM, che è così allertato e potrà bloccare il traffico maligno con il quale si sta tentando l'attacco. La soluzione IBM Security, in pratica, protegge l'infrastruttura come se fossero state installate le patch. Così, almeno, sembrerà all'hacker, 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 Patch è dunque preventiva, perché prima che sia stato sferrato l'attacco la protezione è già in essere. Poiché, nella maggior parte dei casi, è IBM 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, per ragioni varie, le

vulnerabilità non sono immediatamente disponibili. Talvolta, ma solo ed esclusivamente se esiste un attacco contro una vulnerabilità ed è necessario avvisare gli utenti, può accadere che IBM decida di annunciare la vulnerabilità in contrasto con il produttore del sistema. In taluni casi, quando sono varianti di vulnerabilità già scoperte, la Virtual Patch è già disponibile e, anzi, grazie al servizio XPU di distribuzione automatica degli aggiornamenti, la protezione è pro-attivamente installata presso i clienti.

### 2.3.3 Shellcode Heuristics

Per la "0 Day protection" potrebbe non bastare Virtual Patch, in particolare per gli attacchi che sfruttano il payload dei pacchetti, attraverso il cosiddetto "shellcode": in sintesi si tratta di "pezzi" di codice incapsulati in payload di pacchetti "insospettabili", come quelli degli editor o dei viewer. Preso singolarmente, tale codice sembra innocuo, ma giunto a destinazione si ricompone (suscitando immagini da Transformers o affini), preparando exploit o svolgendo un compito preciso, come guadagnare il controllo di una macchina. Per fronteggiare il crescente utilizzo di shellcode come metodo per sfruttare le vulnerabilità associate a diversi formati di file finora ritenuti affidabili, IBM Security ha sviluppato una nuova tecnologia, compresa in PAM, capace di affrontare con successo anche il problema delle vulnerabilità associate ai futuri protocolli di rete: la IBM Security Solutions 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.
Più precisamente, Shellcode Heuristics rileva l'utilizzo di shellcode in tre forme di payload: Web browser attack payload; contenuto shellcode grezzo (in file dall'estensione comune come .doc, .pdf, .ppt, .xls, .dot, .pwz e altri); comuni protocolli di rete (come Dns, Radius, http, ftp, Rpc, Imap e altri).
Il browser è l'applicazione prescelta per gli hacker, visto che è utilizzato da tutti gli utilizzatori e spesso non è considerato critico dalle aziende: si può dire che per gli attacker massimizzi il ROI. Con IBM Security SCH si prevengono gli exploit dei Web browser, sia quelli basati su shellcode sia quelli di offuscamento, proteggendoli da centinaia di vulnerabilità.

### 2.3.4 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.

## 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 legale, 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 moduli software e specifici servizi per la content security.

Il primo punto di forza della tecnologia di content filtering IBM Security è

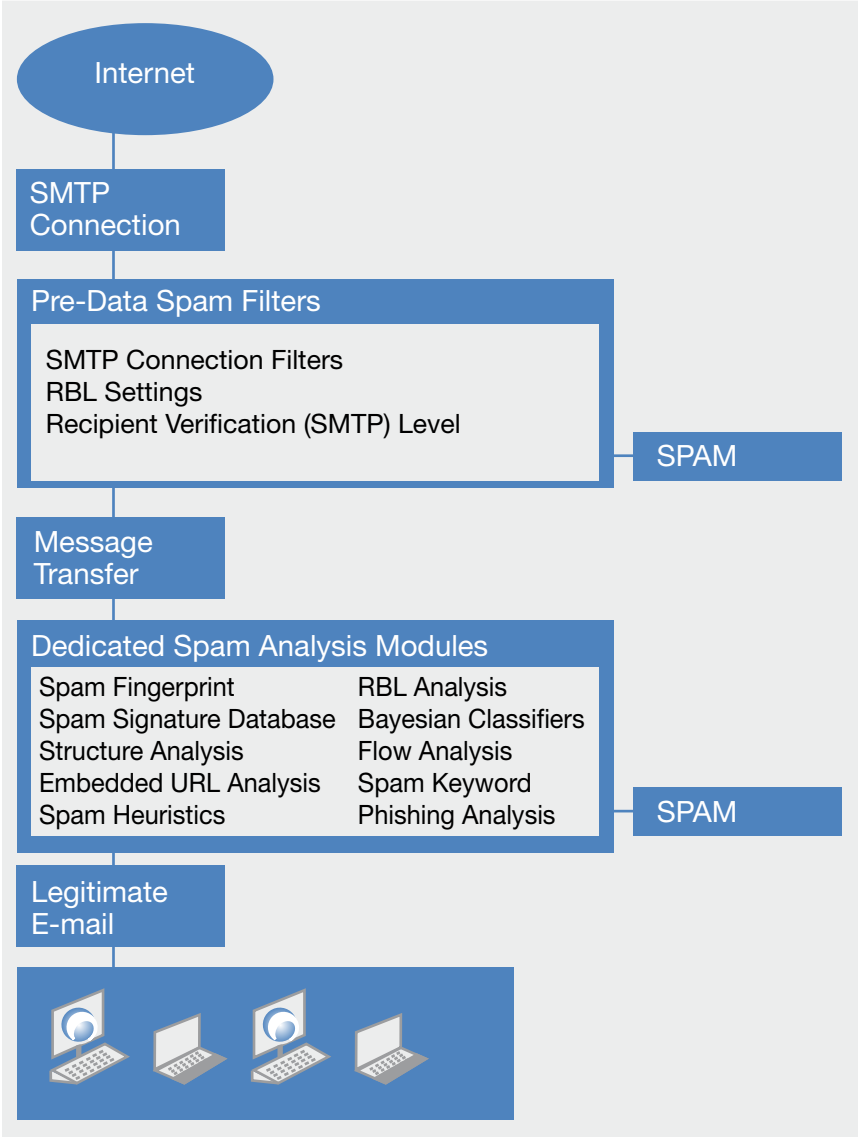



Figura 2.5

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

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 al 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 Security si occupano di controllare i contenuti acceduti via Web, secondo le impostazioni definite dall'azienda.
Anche per quanto riguarda gli spyware, IBM adotta una strategia di sicurezza integrata per fornire una protezione pre-emptive. Le soluzioni antispyware IBM Security, in particolare, sono integrate all'interno delle appliance multifunzione IBM Security e nella soluzione per la protezione degli endpoint, IBM Security Desktop. La soluzione di protezione IBM Security 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 Security 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 le soluzioni per la protezione della posta elettronica di IBM Security.

### 2.3.5 La sicurezza dei server virtuali

La virtualizzazione dell'IT ha registrato un successo notevole, perché è il modo più immediato e diretto per ottenere una serie di benefici economici e funzionali. Economici perché permette di ridurre il numero di macchine fisiche utilizzando meglio quelle che già esistono in azienda: per esempio, dati medi rilevati sul campo indicano che è possibile incrementare lo sfruttamento dei server dal 20-25% al 70-80%, un livello che sinora era garantito solo dai mainframe di fascia più elevata. Altrettanto validi sono i benefici funzionali, che, per esempio, consistono nel rendere semplice spostare un server virtuale da una macchina fisica a un'altra, nella stessa sede o in una sede diversa, in modo da far fronte a accresciute esigenze di calcolo o di sicurezza applicativa. In sostanza, un IT virtuale costituisce in modo nativo un ambiente che si caratterizza per un elevatissimo grado di ridondanza e che permette di operare, anche se in modo progressivamente ridotto, sino a che uno dei server disponibili a livello fisico rimane operativo.

Il rovescio della medaglia è rappresentato dalla sicurezza del sistema. Garantire la sicurezza di un server e delle applicazioni che vi risiedono è relativamente facile quando si tratta di un ambiente IT non virtualizzato. Il server può essere protetto in un data center, può essere isolato all'interno di un sistema di protezione altamente affidabile, le applicazioni che vi risiedono possono essere facilmente controllate, il personale può essere scelto in modo oculato in base alle esigenze e alle garanzie che deve offrire, gli interventi tecnici possono essere effettuati e organizzati in modo tale che i tecnici non abbiano accesso a parti della macchina o a dati sensibili, eccetera.

Tutto questo però cambia quando si opera in un ambiente virtuale. Un problema ancora più grande se, oltre all'ambiente, cambia anche il modello di business. In una realtà virtuale il server fisco oggi può risiedere su una macchina fisica allocata presso una sede e domani su un'altra macchina allocata su una sede diversa, gestita da personale diverso e su cui coesistono anche altri server virtuali. Garantire un livello di sicurezza adeguato in un tale scenario, in cui la mobilità di applicazioni e server è elevata, richiede un approccio alla sicurezza di tipo globale, automatico e, in sostanza,

anch'esso virtualizzato e in grado di seguire passo passo il modo di fruizione dei server virtuali. Quando si trasferisce un server virtuale vanno, in pratica, trasferite anche tutte quelle condizioni di sicurezza che lo devono caratterizzare. Quindi devono essere disponibili funzioni, servizi e competenze tecniche che permettono di ricreare automaticamente un ambiente di utilizzo dotato degli stessi privilegi di sicurezza e che corrisponda sia alle esigenze del server virtuale sia delle applicazioni che vi girano. Inoltre, servono anche funzionalità e servizi di gestione che permettano di effettuare il costante auditing dell'ambiente virtuale e di verificare che il grado di sicurezza rimanga invariato, sia quando un server virtuale viene trasferito da una macchina all'altra sia nel corso della sua usuale operatività dal punto di vista applicativo.
Operare in ambiente virtuale richiede quindi che la sicurezza operi al massimo dei suoi livelli qualitativi ed è questo quello che Ibm ha reso possibile tramite le sue applicazioni dalla suite IBM Security e un approccio progettuale che concepisce la "security by design".

## IBM Virtual Server Security for VMware

Per questo, IBM ha sviluppato IBM Virtual Server Security for VMware , un prodotto software progettato per aiutare le organizzazioni a mettere al sicuro e proteggere la propria infrastruttura server virtuale. Il software fornisce alle imprese un percorso più sicuro per spostare le risorse critiche su data center aziendali virtuali, completando le già disponibili e potenti funzionalità IBM per la protezione dell'ambiente virtuale, quali il controllo degli accessi e il monitoraggio dei privilegi.
La velocità di adozione della virtualizzazione aumenta man mano che le aziende consolidano i propri data center. IBM lavora con i clienti per gestire questa transizione strategica e semplificare e ottimizzare le loro infrastrutture. Se da un lato la migrazione verso ambienti virtuali mette a disposizione molti vantaggi, dall'altro impone alle aziende di adottare misure straordinarie per combattere la prossima generazione di minacce alla sicurezza e di sfide in termini di compliance. Queste misure sono necessarie a causa della minore visibilità e controllo derivanti dall'aggiunta di ulteriori "strati" IT.
Alla luce dei cambiamenti dinamici che interessano il data center, la capacità di gestire, controllare e verificare le azioni di utenti e amministratori di sistemi privilegiati e potenti, tra ambienti tradizionali e virtuali, diventa ancora più critica. Tutte le funzionalità di protezione automatica contenute nella soluzione di IBM Security possono aiutare i clienti a soddisfare più facilmente gli standard di conformità e i requisiti di legge.

Dato questo scenario in evoluzione, la sicurezza tradizionale concepita per gli ambienti di calcolo fisici risulta inadeguata come unica soluzione. IBM Virtual Server Security for VMware aiuta ad affrontare questi timori, fornendo protezione per ogni strato dell'infrastruttura virtuale, compresi hypervisor, sistema operativo, rete, applicazioni, desktop virtuali basati su server, macchina virtuale e traffico tra le macchine virtuali. Integrandosi con la tecnologia Vmsafe di VMware, la soluzione di IBM Security fornisce ai clienti migliore visibilità, sicurezza granulare e scalabile nei loro data center virtuali in espansione.
Le funzionalità di protezione automatica comprendono:

- Virtual Network Access Control (VNAC), per limitare l'accesso alla rete da un server virtuale fino all'avvenuta conferma della condizione di sicurezza;
- rilevamento e prevenzione dei rootkit, per aumentare l'uptime e la disponibilità del server virtuale;
- monitoraggio e reporting dell'infrastruttura virtuale per identificare le vulnerabilità;
- autodiscovery e protezione del segmento di rete virtuale, per fornire visibilità e controllo sull'infrastruttura virtuale.

IBM può contare su un'esperienza quarantennale sulla virtualizzazione, che per prima ha introdotto sui mainframe, e ha quindi sfruttato tale patrimonio nella ricerca, sistemi e software, per realizzare un'integrazione tra il mondo fisico e quello virtuale e creare ambienti leader per la sicurezza della virtualizzazione, anche grazie ai feedback ricevuti da centinaia di clienti.

## 2.4 La gestione centralizzata 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 il sistema dei silos inefficace, inefficiente e finanche del tutto inutile, pur rimanendo estremamente costoso. 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 Security Solutions, 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, antivirus 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, 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 Security Solutions e, in particolare, grazie a IBM Security SIEM (Security Information and Event Management), IBM permette di avere una gestione unificata e centralizzata di tutti gli aspetti legati alla sicurezza. Il primo immediato beneficio che la soluzione IBM Security Solutions per la gestione apporta a un'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 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 Security Operations Manager (TSOM). 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 IBM Security Compliance Insight Manager per fornire una soluzione completa SIEM.

## 2.5 La data security

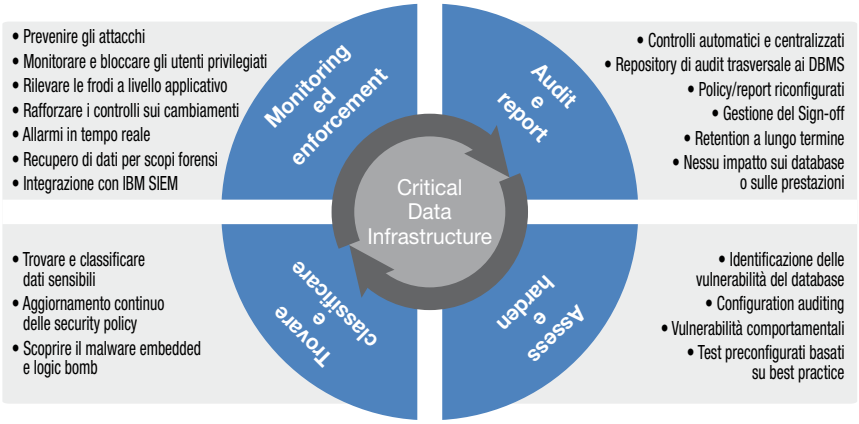
Un elemento sempre più critico riguarda la protezione dei dati. Come accennato più volte, gli attacchi sono diventati mirati e il dato è il loro target finale. Per questo IBM ha sviluppato una strategia indirizzata alla Data Security attraverso soprattutto due aree di sviluppo: la sicurezza dei database e quella dei dati personali distribuiti in azienda (dati non strutturati).

### 2.5.1 Sicurezza e compliance dei database durante il loro ciclo di vita

La sicurezza dei database è un elemento fondamentale per la compliance a numerose normative e leggi, oltre che, ovviamente, per la continuità del business e la sua protezione.
Uno degli aspetti importanti da considerare riguarda le attività non autorizzate o sospette da parte di utenti dotati di privilegi d'accesso particolari, con il relativo rischio di abusi da parte di personale interno e hacker. Inoltre, l'accesso ai database da parte delle applicazioni di business, dagli ERP alla Business Intelligence, aprono la porta a utenti malintenzionati che potrebbero commettere delle frodi. Per questo IBM Security propone una piattaforma che è in grado d'impedire tutto questo. Più precisamente IBM Guardium 7 è forse l'unica soluzione, costruita attorno a una singola console unificata,un data store di back end e un sistema di automazione del work

Figura 2.6

L'architettura per la sicurezza e la compliance dei database




flow, che fornisce una famiglia di moduli integrati per gestire la sicurezza e la compliance dell'intero database per tutto il ciclo di vita dello stesso.
La soluzione permette di:

- localizzare e classificare le informazioni sensibili contenute nei database aziendali;
- identificare le vulnerabilità e i difetti di configurazione dei database;
- bloccare le configurazioni una volta che i cambiamenti raccomandati sono stati implementati;
- ottenere una visibilità totale e una granularità completa delle transazioni all'interno dei database, attraverso qualsiasi piattaforma o protocollo, con un sistema di tracciamento sicuro, a prova di manomissioni e che supporta la separazione di responsabilità;
- monitorare e imporre le policy per gli accessi ai dati sensibili, le azioni degli utenti privilegiati, il controllo dei cambiamenti, le attività degli applicativi utente e le eccezioni di sicurezza, come i login falliti;
- automatizzare l'intero processo di auditing per la compliance, comprese la distribuzione dei report ai diversi team coinvolti, la sigla finale e l'eventuale escalation, con rapporti preconfigurati per la conformità alla SOX, al PCI DSS e altre normative;
- creare un singolo centralizzato repository di audit per il reporting di conformità inerenti l'intera organizzazione aziendale, per finalità di ottimizzazione delle prestazioni, scopi investigativi e legali;
- scalare facilmente dal salvaguardare un singolo database a proteggere migliaia di database in data center distribuiti in tutto il mondo.

## Trovare e classificare

Scovare le informazioni e classificarle è un grosso crescente problema per le organizzazioni, che devono gestire volumi enormi e in costante aumento

di informazioni. Senza contare le complicazioni delle aziende che devono gestire integrazioni dopo una fusione o un'acquisizione. In generale, la difficoltà più comune è quella di individuare tutti i database contenenti informazioni sensibili e comprendere chi o cosa e come vi può accedere (amministratori, sviluppatori, applicazioni per il business, processi batch e così via). È evidente che diventa difficile proteggere le informazioni, se non si sa quanto siano sensibili e ancora di più lo diventerà gestire il rischio. Un problema, poi, è capire cosa è soggetto a compliance. Tutti problemi risolti dalle funzioni di auto-discovery  e classificazione fornite da IBM Guardium. È anche possibile programmare scansioni periodiche del sistema informativo, per prevenire l'installazione di database server fuori controllo.

## Assess e harden

IBM Guardium risulta particolarmente utile anche per effettuare un costante assessment delle vulnerabilità, delle configurazioni e del comportamento d'utilizzo dei database. Viene fornita la postura di sicurezza per ciascun database, attraverso una valutazione basata sia sui dati storici sia su quelli in real-time. Sono disponibili test preconfigurati, ma è possibile definirne di propri. I test sul comportamento monitorizzano tutto il traffico e mettono in evidenza abusi e situazioni sospette, come l'esecuzione di comandi amministrativi da parte di utenti "semplici", login fuori orario di lavoro e così via.
Dopo l'assessment vengono fornite raccomandazioni per riconfigurare i database. Viene così stabilita una configurazione di riferimento. Il Guardium Configuration Audit System (CAS) monitorizza i successivi cambiamenti e avvisa nel caso ci siano scostamenti dal riferimento, in modo da individuare i comportamenti scorretti.

## Monitoring ed Enforcement

Il monitoraggio e l'enforcement sono due delle caratteristiche vincenti di IBM Guardium, sia per assicurare il rispetto delle policy di sicurezza sia per controllare i cambiamenti. Stare dietro a questi ultimi può essere un problema importante per molte organizzazioni. Il tutto, inoltre, senza dover necessariamente coinvolgere i manager dei diversi database.
L'analisi continua del traffico e di ogni singola transazione SQL minimizza i falsi positivi e quelli negativi, fornendo un livello di controllo elevato come mai prima. Definendo un modello di riferimento, è possibile, inoltre, rilevare comportamenti scorretti e automatizzare le politiche da adottare.
Attraverso una nutrita serie di controlli in real time, poi, la soluzione risponde proattivamente ai comportamenti non autorizzati o comunque anomali.

Gli incidenti possono non solo essere tracciati, ma anche risolti attraverso un'interfaccia utente che consente interventi rapidi e mirati, grazie a informazioni dettagliate e accurate.

### Audit e Report

Soprattutto, ma non solo, ai fini della compliance, le funzionalità di auditing e reporting di IBM Guardium sono molto apprezzate. L'audit trial finemente granulare che viene creato continuamente, permette di valutare costantemente lo stato dei database e della loro sicurezza.
La documentazione prodotta fornisce una visibilità accurata e dettagliata delle attività attorno al database, permettendo di dimostrare la compliance.

## 2.5.2 La protezione dei dati confidenziali in ambienti non di produzione

La privacy dei dati è un tema caldo ancora oggi per tutte le organizzazioni, anche considerando gli investimenti già effettuati per assicurarsi la compliance rispetto alle applicazioni di uso quotidiano. Il problema, peraltro, si presenta quando si considerano le strategie di protezione per gli ambienti non di produzione, come quelli di test, di sviluppo o di formazione, troppo spesso trascurati.
La questione delicata riguarda il modo in cui i database per tali ambienti vengono creati. Normalmente, infatti, vengono copiati database reali, contenenti dati confidenziali. I dati reali, infatti, rendono più consistente il lavoro di test e sviluppo e più semplici da capire sono i risultati di questi lavori. Ma, nella realtà, si potrebbero utilizzare dati "camuffati", che non presentano problemi di sicurezza, ma mantengono una verosimiglianza che è quanto basta per le finalità di collaudatori e programmatori.
IBM Optim Data Privacy Solution trasforma gli elementi confidenziali dei dati concernenti segreti commerciali o informazioni sensibili in modo da creare database realistici ma finti.
Il concetto è semplice, ma l'esecuzione non è banale perché la maggior parte delle organizzazioni opera con ambienti eterogenei e complessi, applicazioni e database correlati. La soluzione consente di utilizzare diverse tecniche di mascheramento, ottenendo database singoli o multipli perfettamente trasformati in ambienti realistici e consistenti con il contesto di produzione reale, ma dai quali non è assolutamente possibile risalire ai dati originali. In questo modo, gli ambienti non di produzione potranno utilizzare questi database che non necessitano di essere protetti.

# 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.

La sicurezza end-to-end rappresenta un punto focale nel garantire i processi di business nel contesto dell'economia odierna sempre più globalizzata. Sicurezza e adeguate credenziali sono la condizione sine qua non per stabilire durature, sicure e proficue relazioni di business.
Le sfide che si devono affrontare per l'espansione del proprio business sono però svariate e soprattutto costose. Per esempio, attivare nuovi utenti su tutti i sistemi aziendali richiede in media due settimane e quasi il 30% delle chiamate all'help desk sono relative al reset delle password. Consistenti sono anche i costi per garantire la sicurezza delle applicazioni. Una conosciuta azienda del settore finanziario ha speso una media di 60mila dollari per garantire la sicurezza di ognuna delle sue 400 applicazioni.
A queste e altre problematiche IBM risponde con un approccio che coinvolge i tre elementi cardine di un'efficace politica aziendale per la sicurezza, volta a incrementare la sicurezza nell'identificare gli utenti su base end to end e a stabilire relazioni "trusted" tra le diverse entità coinvolte in un processo di business globale. L'approccio affronta e risolve efficacemente i problemi connessi a:

- il costo e la complessità della gestione delle identità;
- la sicurezza nell'accesso alle applicazioni;
- l'auditing, il reporting e la gestione degli accessi alle risorse.

| | Costi e complessità per la gestione delle identità | Accesso trusted alle applicazioni | Auditing, reporting e gestione degli accessi alle risorse |
|---|---|---|---|
| Software | IBM Security Identity and Access Assurance, Tivoli zSecure suite | IBM Security Access Manager, IBM Security Federated Identity Manager, IBM Security Policy Manager | IBM Security Identity and Access Assurance, IBM Security Information and Event Manager |
| Professional Service | Identity and Access Management Professional Services | Identity and Access Management Professional Services | Compliance Assessment Services, Privileged Identity Management |
| Managed Service | Managed Identity and Access Management | Managed Identity and Access Management | Managed User Monitoring and Log Management |

Tabella 3.1
Le soluzioni per l'identity management

I tre punti sono affrontati con un insieme ottimale di applicazioni software specifiche, servizi professionali e servizi gestiti che è possibile combinare in base alle specifiche esigenze in modo da ottimizzare i costi e i benefici per l'azienda e garantire l'accesso sicuro e trusted alle applicazioni business e la identità degli utilizzatori.
I paragrafi seguenti entrano in dettaglio dei numerosi strumenti che IBM ha posto a disposizione delle aziende, sia come applicazione che come Professional Services o Managed Services. Si tratta di servizi ritagliabili su misura che permettono a un cliente sia di disporre di strumenti di assoluto rilievo nell'assicurare la gestione dell'identità che di demandare in toto la gestione delle identità e dell'assessment a IBM, liberando così risorse da dedicare al proprio core business.
La tabella 3.1 riporta gli elementi più significativi della strategia IBM per la garanzia e la gestione dell'identità su base end-to-end.

## 3.1 Una gestione completa delle identità a protezione dell'azienda

Uno degli elementi cardine di una strategia integrata di sicurezza riguarda la gestione delle identità e il controllo degli accessi. A tal riguardo, Ibm dispone di un'ampia gamma di soluzioni e servizi per l'Identity e Access Management. Questi consentono di realizzare una politica di provisioning accurata, per mantenere il controllo sulle identità ed evitare il proliferare di anagrafiche e coordinate di accesso alle diverse risorse logiche e fisiche aziendali. In altre parole, permettono di sviluppare e implementare un sistema completo per la gestione delle identità e degli accessi alle risorse in base al ciclo di vita dell'identità e alla tipologia di contesto e applicazione del controllo. Più precisamente, la visione di Ibm comprende soluzioni e servizi: per l'identity assessment e le strategie di identity management, per lo user provisioning, il Web access management, l'enterprise single sign-on, la gestione del "lifecycle" delle identità, l'autenticazione, la registrazione delle attività utente per la compliance.
La suite software IBM Security realizza un approccio consistente e unificato che permette di rendere sicuri gli ambienti di e-business cross-enterprise. Le soluzioni sono basate su standard aperti che permettono una semplice e sicura integrazione tra piattaforme eterogenee, multivendor e tra differenti organizzazioni enterprise. Inoltre, supportano tutti i meccanismi

alla base dei servizi di identità e basati su Web Service, garantendo così l'integrazione trasparente con una varietà di piattaforme per lo sviluppo e il deployment di Web Services.
Una delle principali considerazioni nello sviluppo della suite di sicurezza è che 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 quindi un 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.
In un tale scenario evolutivo le soluzioni IBM permettono non solo di trarre il massimo beneficio dalle tecnologie dei Web Service e dagli standard federativi ma anche, grazie a un approccio innovativo, 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.
L'ampia suite di prodotti permette di implementare sofisticate soluzioni per la gestione e il controllo delle identità degli utenti e dei 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.
L'insieme di queste attività è sottoposto a un continuo monitoraggio che permette 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.
Nell'affrontare il problema della gestione degli accessi e delle identità una soluzione deve però rispondere ad alcune esigenze primarie quali:

- Fornire la capacità di autorizzare i corretti livelli di accesso alle risorse in base alle policy aziendali.
- 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.

- Garantire un percorso di audit al fine di 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. Una soluzione integrata di Identity e Access Management deve necessariamente prevedere una combinazione di processi aziendali e tecnologie software per gestire e garantire l'accesso sicuro alle informazioni proprietarie all'interno di un'impresa. È un approccio che, se attuato con gli strumenti adeguati, permette di rispondere non solo a quanto richiesto da una corretta pratica di business aziendale, ma anche di essere compliant con le regolamentazioni di categoria, come per esempio per l'ambito bancario, o nel trattamento di informazioni confidenziali e sensibili di clienti o cittadini.

## 3.2 Gestire il ciclo di vita dell'identità

La gestione dell'identità è un processo che richiede molta attenzione e che va affrontato e revisionato con continuità a livello operativo e strategico. Per conseguire gli obiettivi di business la gestione dell'identità va affrontata considerando tutti gli aspetti correlati al 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.

Per rispondere a una tale esigenza IBM ha ideato 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, certificate da una

presenza globale di otre 3500 esperti nella sicurezza nella privacy, cui si affianca una rete di Business Partner in grado di sostenere le aziende nel 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 ogni settore dell'IT ed è in grado di predisporre soluzioni per problematiche complesse inerenti i più disparati segmenti di mercato e di aziende.
L'approccio adottato da IBM supporta la governance e il risk management e allinea policy IT, processi e progetti con gli obiettivi di business.
È un approccio che si è concretizzato in un insieme di servizi, software e hardware che consente di pianificare, eseguire e gestire iniziative di ogni tipo con un approccio modulare che si adatta alle esigenze di aziende di ogni dimensioni.
Le soluzioni che fanno parte della proposizione ***IBM Security Solutions*** pongono a disposizione, tra le numerosissime altre, funzioni integrate di identity management e access control che 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 la profittabilità per il business e i partner.
- Semplificare i processi di audit e di compliance all'interno di ambienti eterogenei.

Una funzione che sta acquisendo crescente importanza è anche l'identity proofing, che consente di fornire un livello di protezione a fornitori di servizi coinvolti in una transazione online.
L'Identity proofing deriva dalla considerazione che, prima di fornire a qualcuno una password o di creare un account online a suo nome è 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 IBM Security Solutions, IBM dà una risposta anche a questa complessa e critica necessità.
Quanto segue illustra le caratteristiche salienti della suite IBM Security Solutions per il controllo degli accessi e delle identità

## 3.3 Le soluzioni IBM per la gestione delle identità e degli accessi

La gestione dell'acceso è uno degli aspetti più critici al fine di garantire la sicurezza dei dati e di un sistema. La suite di soluzioni IBM affronta i numerosissimi aspetti che si presentano tramite una ampia gamma di soluzioni software che permettono di gestire e controllare efficacemente l'accesso, il controllo della compliance, il provisioning automatico dei software e la Web security. Il tutto può essere fatto dai manager tramite un unico centro di controllo da cui gestire gli account e impostare le regole di accesso. Numerosi I prodotti IBM per il controllo dell'accesso:

### IBM Security Identity Manager

È il prodotto IBM che abilita 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 Security Access Manager for e-business

È il software che permette di gestire la crescita e la complessità, controllare i costi associati e risolvere i problemi che si presentano quando si implementano policy di sicurezza attraverso un'ampia gamma di risorse Web e applicazioni. La 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.

### IBM Security Access Manager for Enterprise Single Sign-On

La soluzione mette a disposizione funzionalità di autenticazione single sign on (SSO) in modo tale che l'utente non sia 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. Security 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 Security Access Manager for Operating Systems

È un sistema di sicurezza in grado di proteggere le applicazioni business critical, dati, file 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 che dall'esterno.

Security 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.

## 3.4 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 Security 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 la 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. 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 solida 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.

## 3.5 I Directory Services

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. La suite IBM security mette a disposizione per la gestione delle directory due sofisticati strumenti:

- IBM Security Directory Server è un'applicazione che implementa lo standard LDAP che mette a disposizione numerose funzioni, tra cui il supporto LDAP V3, la possibilità di gestire decine di milioni di voci e gruppi di centinaia di migliaia di membri; il supporto delle piattaforma AIX, Solaris, Microsoft Windows, HP-UX, delle distribuzioni Linux per Intel e delle piattaforme server IBM.
- IBM Security Directory Integrator è invece una soluzione per la gestione di metadirectory per la sincronizzazione e lo scambio delle informazioni in tempo reale tra applicazioni o sorgenti di directory. Consente di predisporre un'infrastruttura affidabile sui dati associati alle identità che funziona da piattaforma per la protezione dell'azienda e per le applicazioni basate su Web Service.

In sostanza, IBM Security Directory Integrator permette di disporre di 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.

## 3.6 Esempi pratici di scenari di business con IBM Security Identity Manager e Access Manager

I benefici che derivano dall'adozione di prodotti quali IBM Security Identity Manager e IBM Security Access Manager sono numerosi.
I paragrafi seguenti prendono in esame alcuni casi comuni e come le due soluzioni possono essere integrate nei processi di business per garantirne una elevata sicurezza.

### Assunzione di un nuovo dipendente

Quando viene assunto un nuovo dipendente il software IBM permette di automatizzare il processo di provisioning. Appena i dati del dipendente sono inseriti all'interno del sistema di gestione delle risorse umane si attiva un processo automatizzato per la creazione dei relativi account.
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 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, e che possono prevedere l'importazione di file oppure connessioni programmate al sistema di gestione delle risorse umane, per esempio attraverso l'uso di IBM Security Directory Integrator.
I nuovi record generati delle risorse umane vengono elaborati all'interno di IBM Security Identity Manager e attraversano una serie di workflow operativi in modo da rispondere alle specifiche esigenze di business delle diverse organizzazioni. Nell'ambito di questo percorso è possibile stabilire, per esempio

- La valutazione e l'assegnazione di uno specifico ruolo.
- L'applicazione di policy in base al ruolo svolto o all'organizzazione di appartenenza.

- La gestione delle approvazioni per le policy di provisioning.
- La creazione dell'account in IBM Security Access Manager.
- L'invio di notifiche al dipendente una volta che gli account appropriati sono stati creati.

Un approccio di provisioning alternativo consiste nel 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.

### Modifica del ruolo di un dipendente

Tramite il software IBM il cambiamento del ruolo lavorativo di un dipendente viene notificato al sistema di identity e access management mediante un feed di dati originati dal sistema di gestione delle risorse umane e inoltrati all'applicazione IBM Security Directory Integrator. Il record, dopo essere stato modificato all'interno del sistema HR, passa successivamente attraverso una serie di flussi di lavoro all'interno di IBM Security Identity Manager che comprendono:

- Valutazioni dinamiche del record modificato per l'assegnazione al nuovo ruolo organizzativo.
- L'applicazione delle nuove policy.
- La gestione delle approvazioni.
- La creazione o modifica degli account.
- L'invio delle notifiche della creazione degli account.

### Licenziamento di un dipendente

Il software IBM permette di automatizzare il processo di licenziamento (de-provisioning), eliminando così il rischio che possano rimanere attivi dei privilegi che potrebbero permettere al dipendente di accedere a dati o aree aziendali sensibili. Non appena un dipendente è rimosso dal sistema di gestione delle risorse umane, tutti gli account a esso associati vengono automaticamente cancellati o disabilitati. La realizzazione di questa funzione prevede, innanzitutto, la notifica al sistema di identity e access management attraverso l'invio dei dati a IBM Security Directory Integrator. Il record da esso modificato attraversa poi una serie di flussi di lavoro specifici all'interno di IBM Security Identity Manager che comprendono:

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

## Gestione coerente della password

I prodotti IBM permettono di gestire automaticamente gli eventi legati al ciclo di vita delle password quali la loro scadenza, la modifica o il reset. Sono eventi che possono essere gestiti in modo coerente all'interno dell'ecosistema di identity e access management realizzato con le soluzioni IBM Security.

È anche possibile applicare specifiche policy alle password 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. Ciò non solo rafforza la protezione ma migliorare anche la user experience.

Due sono i modi in cui IBM Security Identity Manager può essere utilizzato per la centralizzazione di queste operazioni di gestione.

Nel primo gli utenti accedono all'Identity Manager e cambiano la propria password. L'applicazione verifica 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 configurato con il "reverse password synchronization module" di Identity Manager e cambiano la loro password. Questo modulo cattura eventi di modifiche della password su un sistema target e successivamente comunica con IBM Security Identity Manager per svolgere automaticamente 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 verifica positiva provvede a memorizzare la nuova password nel repository di Identity Manager.

## Controllo dell'accesso basato su ruoli

Il controllo di accesso basato su ruoli è usualmente costituito da un sistema automatizzato che colleziona le informazioni relative a una nuova assunzione presenti nel sistema di gestione delle risorse umane (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, nella realtà la intrinseca granularità della gestione di accesso impedisce una diffusione tempestiva delle informazioni necessarie per un immediato controllo di accesso basato su ruoli (RBAC).
Va osservato che un efficace RBAC richiede la definizione e la configurazione dei ruoli organizzativi nella soluzione di identity e access management. Ciò permette di far si che specifiche informazioni sull'identità del'utente vengano raggruppate logicamente in corrispondenti livelli di controllo di accesso.
Un modo per disporre di un controllo dell'accesso basato su ruoli può consistere nel passare attraverso le seguenti fasi successive:

- Gestione delle password mediante IBM Security Identity Manager.
- Realizzare il provisioning manuale e la gestione di base dell'account con Identity Manager.
- Realizzare il provisioning automatizzato (combinando provisioning manuale e automatico).
- Realizzare il provisioning automatico ovvero il provisioning automatizzato per tutti gli endpoint gestiti, mediante meccanismi di approvazione che richiedono ridotti interventi da parte dell'amministratore.
- Attivare 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, senza che sia richiesto alcun compito di tipo amministrativo.

Quello RBAC non è, naturalmente, l'unico modello possibile e IBM Security Identity Manager, che è uno strumento molto flessibile, opera bene anche in altri contesti più convenzionali, come quelli basati sul modello request based, e offre benefici anche in presenza di contesti misti.

## Integrazione di un'applicazione

La soluzione IBM di identity e access management fornisce concreti benefici anche quando in azienda vengono passate in produzione nuove applicazioni . Il software ne semplifica l'inserimento all'interno dell'ecosistema di gestione dell'identità e dell'accesso e garantisce che le operazioni di provisioning e di rafforzamento dell'accesso siano governate utilizzando in modo consistente i medesimi processi.

## Audit della conformità e reporting

Una 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.

Deve anche 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 stessi 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.
Per soddisfare queste esigenze sia la soluzione Ibm di Identity Manager che di Access Manager sono configurate per abilitare la raccolta di eventi di audit di vario tipo. Per esempio, IBM Security Access Manager è configurato per raccogliere eventi di audit per:

- Autenticazione e verifica del controllo di accesso.
- Operazioni di gestione dell'utente,
- La creazione di gruppi e l'aggiunta di utenti ai gruppi.
- La creazione e aggiornamento delle ACL.
- Fornire report per eventi di audit.

IBM Security Identity Manager permette invece di 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 IBM Security Identity Manager e da IBM Security Access Manager sono utilizzabili per varie esigenze e, inoltre, gli eventi di audit provenienti dai due prodotti possono essere elaborati mediante IBM Security Information and Event 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.

## 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

IBM Security 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.

## Ripristino e reimpostazione di password dimenticate

IBM Security mette a disposizione degli utenti varie modalità di recupero di una password dimenticata.

Un caso comune è, per esempio, un utente che 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.

A questo punto 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.

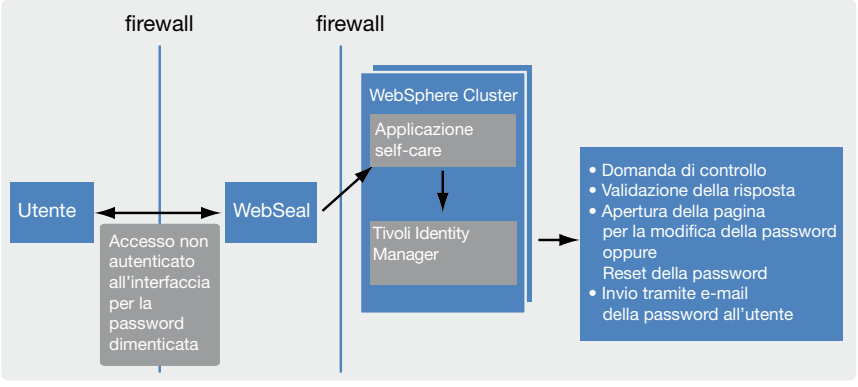



Figura 3.1
Gestione del ripristino e reimpostazione di password tramite IBM Security Identity Manager e IBM Security Access Manager

## 3.7 Federated Identity and Trust Management

Una necessità sempre più irrinunciabile in ambito aziendale è condividere con i partner, in modo sicuro e attraverso Web Service, le informazioni di autenticazione e gli attributi degli utenti.
La possibilità di condividere queste informazioni con partner esterni o business unit interne permette alle organizzazioni di fornire ai propri utenti una migliore e più semplice user experience.
I driver che spingono le aziende in questa direzione sono molteplici. per esempio, il costo di gestione del 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.

### 3.7.1 La gestione federata delle identità

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.
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.
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, 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 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 rappresenta la parte di validazione all'interno della transazione. È responsabile del controllo dell'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).
In un contesto federato esiste però il problema di come le diverse entità si parlano e del protocollo di dialogo adottato
Gli utenti di solito dispongono di un set differente di credenziali di autenticazione per ogni sito Web. La medesima problematica, ribaltata dal lato enterprise, determina elevati costi per la gestione di questi account. Per superare queste difficoltà sono stati sviluppati protocolli che consentono agli utenti di effettuare l'autenticazione un'unica volta all'interno di una federazione di siti Web cooperanti tra loro. Due sono le tipologie di protocolli adottate. La prima raggruppa protocolli focalizzati su modelli enterprise-centrici e comprende: Security Assertions Markup Language (SAML), Liberty e le specifiche Web services (WS) Federation. Sono protocolli di tipo federativo ampiamente adottati. Il secondo tipo è rappresentato dagli schemi di identità user-centrici. Si tratta di protocolli di più recente realizzazione che forniscono agli utenti un maggiore livello di controllo sulle loro identità digitali. Creare un ambiente sicuro e federato in grado di supportare i diversi tipi di protocolli esistenti è quanto permette di fare la soluzione IBM Security Federated Identity Manager.

### 3.7.2 IBM Security Federated Identity Manager

IBM Security Federated Identity Manager permette di svolgere in modo protetto, flessibile, efficiente e attraverso una pluralità di domini di sicurezza, operazioni di business che intervengono su ambienti diversificati. La soluzione software sfrutta i principali standard di tipo federativo al fine di garan-

tire 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 navigare attraverso i siti della federazione per effettuare le procedure di autenticazione nei singoli ambienti e organizzazioni.
In sostanza, IBM Security Federated Identity Manager permette di implementare funzioni di gestione dell'accesso sicuro ad applicazioni e servizi distribuiti.
Grazie alla possibilità di predisporre rapidamente una soluzione federata, IBM Securityi Federated Identity Manager abilita una forte riduzione dei costi associati alla business integration, all'help-desk e all'amministrazione della sicurezza. Inoltre, il suo utilizzo contribuisce a minimizzare i costi necessari per creare e mantenere identità condivise attraverso molteplici business partner. Non ultimo, 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.

## 3.8 Il Federated Single Sign-On

Il Federated Single Sign-On viene utilizzato in molti scenari basati sull'utilizzo di 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 il Single Sign-On/Sign-Off, il collegamento dell'account tra l'identity provider e il service provider e la possibilità di utilizzare alias per l'accesso invece della reale identità. A questo va aggiunta la possibilità all'identity provider di far fronte alla richiesta di attributi e informazioni sull'utente da parte dei service 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.

### 3.8.1 Il modello di gestione dell'identità "user-centric"

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. Un altro beneficio offerto da questo tipo di sistemi è che possono consentire la realizzazione di relazioni lascamente 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 Security Federated Identity Manager supporta due famiglie di protocolli di identità user-centrici: OpenID e Information Card Profile (con la possibilità di utilizzare selettori di identità quali Microsoft Windows CardSpace ed Eclipse Higgins Project).

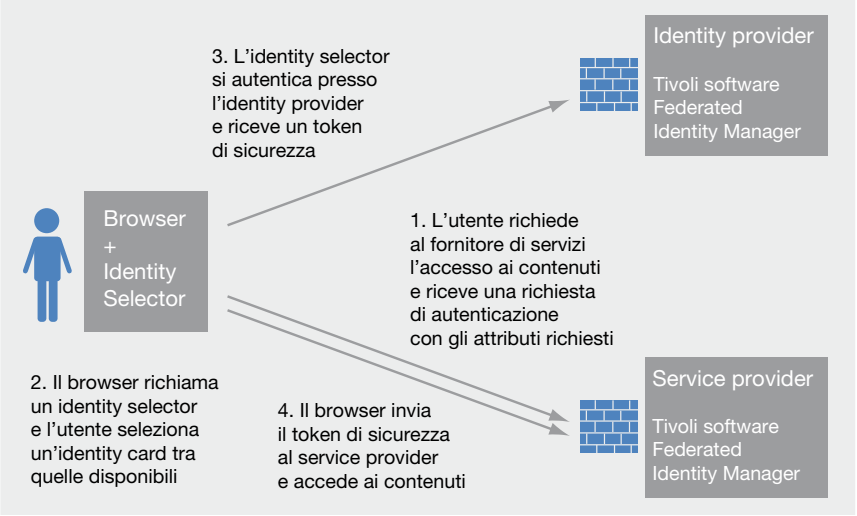



Figura 3.2

Un tipico esempio di single sign on user-centrico in cui IBM Security Federated Identity Manager è utilizzato sia dal lato dell'identity provider sia del relying party

## 3.9 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 permettono di sfruttare in modo ottimale i vantaggi offerti dalle risorse di federated identity e di avere impatti molto positivi intermini di ROI aziendale.

## 3.10 La propagazione dell'identità in una SOA

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 lascamente accoppiati.
Per stabilire l'identità del richiedente il servizio è 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.
Se si vuole fornire il livello di flessibilità richiesto in un ambiente di business dinamico la propagazione delle identità all'interno della SOA deve essere considerata come una responsabilità dell'infrastruttura SOA e non delle applicazioni. 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


Figura 3.3
Propagazione dell'identità in una una SOA utilizzando WS-Trust e IBM Security Federated Identity Manager STS

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 Security 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 Security 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.

Il 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 Security 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 Security 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.

## 3.11 L” autorizzazione tramite IBM Security Policy Manager

La gestione delle policy ha un ruolo chiave nell’abilitare la governance di ambienti SOA. Le policy sono il mezzo mediante il quale i servizi descrivono le condizioni in base alle quali possono essere usati e in base alle quali gestiscono il comportamento delle infrastruttura che li supportano. Aggiungere policy che sono esterne al servizio medesimo aggiunge ulteriori punti di controllo, rende l’ambiente SOA più fruibile e facilita l’adozione di soluzioni SOA.

È questo uno degli obiettivi, assieme a molti altri, che è possibile raggiungere con IBM Security Policy Manager, una soluzione basata su standard per la sicurezza delle applicazioni. Tra gli elementi che lo caratterizzano:

- Abilita una gestione centralizzata delle applicazioni.
- Semplifica e rafforza la gestione delle policy per la sicurezza in ambienti SOA.
- Abilita l’erogazione della sicurezza come servizio run-time che rafforza il controllo degli accessi per nuove applicazioni e servizi.

IBM Security Policy Manager permette ai proprietari delle applicazioni e agli amministratori di esternalizzare la sicurezza e di semplificare la gestione di complesse policy di autorizzazione sia per applicazioni già esistenti che di nuova concezione, incluso tra queste applicazioni personalizzate in funzione del cliente.

I benefici che permette di ottenere comprendono: la capacità di rispondere rapidamente ai cambiamenti delle esigenze del business tramite la definizione di ruoli controllati centralmente; il controllo delle abilitazioni e delle autorizzazioni per l’accesso ai dati; il miglioramento della compliance e della gestione della sicurezza mediante il controllo dei diritti di accesso basato su regole, ruoli e attributi.

Inoltre, IBM Security Policy Manager offre ai designer dell’architettura dei processi aziendali e ai team per la sicurezza la possibilità di gestire centralmente e rafforzare le policy di sicurezza nell’utilizzo di servizi Web, per esempio tramite le appliance WebSphere DataPower SOA.

La loro adozione permette di ridurre gli oneri connessi alla gestione manuale delle policy per la sicurezza, costosa, sovente poco consistente e time-consuming e offre la possibilità di delegare la governance operativa e le attività di audit.

In sostanza, IBM Security Policy Manager permette di disporre di un servizio centralizzato di alto profilo per la gestione delle policy inerenti la sicurez-

za. Permette altresì di definire il modello, le autorizzazioni, il rafforzamento e il monitoraggio delle policy per la sicurezza.
Non ultimo, attraverso la sua centralizzazione e l'erogazione di funzioni di controllo che operano su base end-to-end è un'applicazione che riduce i rischi e i costi digestione.
IBM Security Policy Manager è stata progettata in modo da potersi integrare con altri prodotti IBM per la governance e il provisioning. Il discovery di servizi Web può essere, per esempio, realizzato tramite
WebSphere Service Registry.

# 4
# La sicurezza delle applicazioni

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 operare ed essere produttivi. Le soluzioni IBM permettono di gestire la sicurezza in tutte le fasi di sviluppo e di esercizio di un'applicazione e ottimizzano la sicurezza per il suo intero ciclo di vita. Sono soluzioni che affrontano il problema della sicurezza delle applicazioni non solo nei normali ambienti di utilizzo aziendale o Web 2.0, ma anche in presenza di architetture innovative e complesse come SOA.

## 4.1 Secure by design

Le minacce e il numero di attacchi che quotidianamente vengono portati alle applicazioni Web sono in costante crescita. Ma questo costituisce solo una parte del problema che deve affrontare chi ha in carico la sicurezza aziendale dei dati e delle applicazioni business.
Un'altra parte deriva dal fatto che i dati non solo possono essere trafugati e originare, quindi, una perdita d'immagine o avere implicazioni legali anche molto onerose nei confronti dei clienti che all'azienda avevano affidato dati sensibili, ma possono anche essere alterati per portare ad analisi aziendali sbagliate o a errati processi produttivi. In un caso e nell'altro i danni sono potenzialmente enormi, come hanno già sfortunatamente sperimentato numerose aziende, anche di primo piano nel mondo finanziario e dei servizi, di diversi settori industriali sparse per il mondo.
Per garantire il corretto funzionamento aziendale, l'attenzione va quindi allargata sino a comprendere la protezione dei processi aziendali critici e non solo dell'asset esistente.
Ma per far questo non è sufficiente il software di sicurezza e i modelli di suo utilizzo sinora disponibili. Quello che necessita è un nuovo approccio che permetta sia di controllare la sicurezza delle applicazioni business o Web già esistenti sia di approcciare in modo innovativo lo sviluppo delle nuove applicazioni. Per queste ultime va tenuto conto della crescente esposizione delle applicazioni, man mano che se ne diffonde l'uso via Web, o del fatto che in azienda s'introducono nuovi modelli per l'IT, come per esempio SOA o il Cloud Computing, che proprio su Web si basa per la sua fruizione come modello di business.

### 4.1.1 Applicazioni sicure per l'intero ciclo di vita

Per rispondere a questa esigenza primaria per la prosecuzione dei processi di business IBM ha ideato un approccio innovativo, riferito come "Secure by Design", che consiste nel progettare le applicazioni, sin dalla fase di sviluppo iniziale, in modo sicuro, dando per scontato che le medesime, sia in ambito aziendali sia in ambito web, saranno soggette a continui e sempre più sofisticati attacchi. È un approccio che risponde non solo alla crescita delle minacce ma anche alle esigenze di un IT in rapida evoluzione e all'adozione di nuovi paradigmi di calcolo come il citato Cloud Computing. Garantire le applicazioni in modo nativo con un progetto adeguato e una sicurezza intrinseca è un'esigenza che non discrimina nessuna azienda. Sia le piccole sia le grandi aziende o le maggiori corporate sovranazionali, che

i settori pubblici o i service provider, stanno investendo in nuove tecnologie per fronteggiare le sfide del mercato, la concorrenza dei paesi emergenti, la globalizzazione, e hanno bisogno di infrastrutture IT e produttive, nuove, agili e flessibili.
Tuttavia, queste nuove tecnologie generano anche nuovi rischi, che compromettono le infrastrutture critiche, la privacy e l'identità e impongono alle organizzazioni di ripensare al modo di confrontarsi con la conformità, la gestione del rischio e la protezione dei dati.
È per questo che l'elemento centrale nell'approccio di IBM per affrontare le attuali e future sfide di sicurezza dei clienti consiste nello spostamento dell'attenzione dalla protezione degli asset alla protezione dei servizi critici.
L'iniziativa Secure by Design (Secure By Design initiative) di IBM Security Solutions, ha il beneficio di aiutare i clienti a incorporare la sicurezza nel tessuto stesso dei servizi offerti, rendendola intrinseca rispetto ai propri processi di business, allo sviluppo dei prodotti e alle attività operative quotidiane e affrontando al contempo i concetti emergenti di conformità.
L'iniziativa Secure by Design non è la sola che IBM ha attuato. Al fine di garantire la massima protezione possibile delle applicazioni dei clienti, ha sviluppato anche le best practices per progettare prodotti software sicuri.
Per aiutare i clienti, le aziende IT e il mondo accademico a implementare un approccio sicuro end-to-end alla fornitura dei propri prodotti, IBM ha realizzato e messo a disposizione il framework "Security in Development: The IBM Secure Engineering Framework".
Il framework suggerisce le best practices in tema di sicurezza, che rappresentano sempre più un requisito fondamentale per lo sviluppo di prodotti e applicazioni che girano nell'infrastruttura digitale mondiale.
L'attenzione alla sicurezza è richiesta, infatti, sia nella catena delle forniture globali che nei processi di sviluppo, per fornire prodotti dotati delle giuste caratteristiche di sicurezza e di resistenza alle vulnerabilità.
L'obiettivo di questo framework è consentire una maggiore collaborazione tra tutti gli attori del settore, gli enti normativi e le pubbliche amministrazioni di tutto il mondo al fine di perfezionare l'approccio delle organizzazioni alla sicurezza. Quello che serve quindi è una sicurezza intrinseca e che le applicazioni siano progettate considerando gli aspetti di sicurezza per il loro intero ciclo di vita.

## Applicazioni sicure per l'intero life cycle

Lo sviluppo e l'esercizio delle applicazioni software sono suddivisibili in diverse fasi, da quella di progetto sino a quella di produzione.

Per garantire la sicurezza nell'intero ciclo di vita e nelle diverse fasi sia i requirement sia l'architettura devono essere ideati avendo in mente il problema della sicurezza. In caso contrario un'applicazione può presentare un'intrinseca debolezza per quanto concerne la sua sicurezza e purtroppo questa è la realtà per molte delle applicazioni business esistenti. Un esempio può aiutare a capire meglio il problema, quello di come sin dall'origine di uno sviluppo software sia opportuno prevedere le modalità di selezione della password da parte di un utente. Recenti ricerche hanno evidenziato che il 10% delle persone utilizzano una delle 500 password più comuni e che una ogni 50 utilizza una delle 20 password più comuni.
Consideriamo più in dettaglio quali sono le fasi di sviluppo di un'applicazione e le correlate esigenze di sicurezza a cui rispondono le soluzioni IBM:

**Fase di design**

La fase di design è quella in cui vanno tenuti in considerazione i requisiti di sicurezza dell'applicazione e le problematiche connesse alle modalità da adottare per garantire che il livello di sicurezza nel tempo non diminuisca, per esempio perché l'utilizzatore adotta una password semplice da individuare o non la cambia con la frequenza necessaria. È una fase in cui, inoltre, i controlli necessari e le best practice devono essere documentate alla stessa stregua dei requisiti funzionali.
Ad esempio, è opportuno impedire sin dalla fase di progetto che un utente possa adottare le password contenute nella lista delle top 500 o delle top 20, che peraltro può essere variabile nel tempo, o che possa adottare password troppo semplici, per esempio che coincidano con la propria data di nascita, dei familiari, eccetera.

**Fase di development**

Nella fase di development l'applicazione viene scritta, costruita e testata. È un passaggio critico, perché sotto la pressione dei tempi di sviluppo un analista o un programmatore può essere tentato di usare moduli software non adeguatamente verificati per quanto concerne la sicurezza. Una volta incorporato nel prodotto finale la vulnerabilità persisterà per l'intero ciclo di vita dell'applicazione. Con la diffusione di Web 2.0 e architetture SOA, che sul riutilizzo di moduli software pongono uno dei motivi del loro successo, il problema è molto critico e impone un diverso approccio per quanto concerne la sicurezza. L'organizzazione deve quindi assumere come dato di base che un utente proverà intenzionalmente a utilizzare in modo fraudolento un'applicazione e cercare di trarne beneficio.

Per evitare di incorrere nelle problematiche esposte che possono ridurre il livello di sicurezza, nella fase di sviluppo è quindi indispensabile controllare accuratamente il software durante la sua codifica in modo da:

- Eliminare le possibili vulnerabilità derivanti da errori di implementazione.
- Verificare la conformità ai requisiti di sicurezza.

**Fase di Build&Test**

Chi pensasse che avendo applicato tutte le possibili best practice e l'attenzione alla sicurezza nella fase di progetto e nella successiva di sviluppo si può stare tranquilli, corre il rischio di una grossa delusione.

Le applicazioni progettate e sviluppate nel modo più sicuro possibile smettono in non pochi casi di esserlo nella fase di delivery, quando cioè passano in produzione perché non sono state in precedenza efficientemente testata dal punto di vista della sicurezza in relazione al futuro ambiente di loro reale utilizzo.

In sostanza, non basta sviluppare un'applicazione con un approccio "maniacale" alla sicurezza, ma lo stesso approccio si deve avere in relazione all'ambiente fisico e IT in cui verrà rilasciata e utilizzata e ciò richiede una pari attenzione quando si effettua il test prima del rilascio definitivo. In particolare, due sono le attività da compiere in questa fase del ciclo di vita di una applicazione:

- Un accurato testing delle applicazioni alla ricerca di errori e al fine di verificare la conformità ai requisiti di sicurezza per l'intera applicazione.
- La realizzazione di test che verifichino o no la penetrabilità delle applicazioni in ambienti di deployment.

**Fase di deployment**

Il deployment di un'applicazione in produzione è un momento particolarmente critico del ciclo di vita, perché permette di verificare in reali condizioni di utilizzo il grado di sicurezza di un applicazione.

Richiede strumenti adeguati e best practice che permettano non solo di verificare la validità delle applicazioni per quanto concerne la sicurezza, ma che aiutino anche nell'adeguare l'ambiente che ospita l'applicazione.

Ad esempio, non sempre la sicurezza dipende dalla sola applicazione. In alcuni casi può essere necessario rafforzare e proteggere le infrastrutture, proteggere i dati utilizzati mentre viaggiano in rete, difendere l'ambiente di produzione, definire strategie di aggiornamento e di diffusione e installazione delle patch sicure, sino al supporto e al controllo in modo sicuro dei sistemi operativi e dei singoli componenti di uno stack IT, infrastruttura di

virtualizzazione compresa. Spesso, per esempio, ci si dimentica di configurare il Web Server affinché neghi l'accesso ai non autorizzati alla struttura della directory, cosa che apre la strada all'accesso fraudolento a informazioni sensibili e a codice applicativo.

**Fase operativa**

Un ambiente di produzione non è mai una realtà congelata nel tempo ma è continuamente soggetta a modifiche in base alle esigenze della produzione, del business, del tipo di attività svolte dalla specifica divisione aziendale, eccetera.

In sostanza, si tratta di un ambiente fortemente dinamico caratterizzato da parametri che, cambiando in modo difficilmente prevedibile, possono incidere sulla vulnerabilità di una applicazione e sulla sua sicurezza complessiva. In sostanza, se si vuole mantenere costante il livello di sicurezza in presenza di un mutare delle condizioni ambientali di utilizzo in produzione, è necessario monitorare costantemente le applicazioni per verificarne il corretto uso, le vulnerabilità e difenderle contro gli attacchi.

Quello che si rende indispensabile è quindi realizzare una costante attività di audit, con gli strumenti adeguati, in modo da scoprire immediatamente riduzioni della sicurezza o il crearsi di particolari vulnus che potrebbero ridurre l'efficacia degli strumenti adottati o sviluppati al fine di rendere sicura un'applicazione in produzione.

### 4.1.2 Tecniche e strumenti IBM per garantire la sicurezza per il lifecycle delle applicazioni

IBM ha sviluppato strumenti adeguati e sofisticati, che permettono nel complesso di garantire il massimo della sicurezza e garantirla nel tempo per l'intero ciclo di vita di una applicazione. Sono strumenti che rispondono a per tre diverse necessità di utilizzo:

- Strumenti per la "White box analysis"
- Strumenti per la "Black box analysis"
- Strumenti per la "Gray box analysis"

La suddivisione deriva dall'ammontare di dati e informazioni sul sistema e sul software che è disponibile per lo strumento quando viene realizzata l'analisi e dipende anche dalla fase del ciclo di vita in cui ci si trova.

#### La White box analysis

La White box analysis analizza la sicurezza dell'architettura, del codice sorgente e del codice binario e permette di:

- Verificare tutte le informazioni rilevanti per la sicurezza.
- Individuare i punti logici critici.
- Documentare in modo semplice l'area e la sua dimensione su cui potrebbe svilupparsi l'attacco.
- Trovare facilmente errori di programmazione.

Inoltre, risolve anche aspetti connessi al fatto che in alcuni casi non è facile realizzare il test del software in ambienti distribuiti o accedere alle specifiche di progetto o di codice sorgente. Un esempio di utilizzo di una analisi effettuata tramite i tool White box consiste nell'effettuare la scansione del codice sorgente durante la fase di sviluppo.

## La Black box analysis

La Black box analysis prevede tool che permettono di esaminare il software senza la conoscenza dell'ambiente in cui verrà utilizzato. In sostanza, è un tipo di analisi molto simile a quella che un malintenzionato che accede dall'esterno può realizzare.

Lo strumento utilizza metodi automatici e tecniche manuali, analizza ed evidenzia le possibili aree di attacco e la loro ampiezza. Inoltre, effettua il testing del sistema per individuare quali sono le informazioni rilevanti e il loro grado di esposizione. L'analisi, oltre a utilizzare la tecnica di vulnerability scanning, come per la White Box Analysis, utilizza anche la Dynamic analysis.

La prima si basa sull'uso di un data base che contiene le vulnerabilità conosciute al fine di verificare la vulnerabilità da parte degli worm delle applicazioni. La seconda, riferita anche come Web application scanning, verifica in modo automatico l'ampiezza dell'area di attacco, effettua il test delle applicazioni tramite la tecnica di "fault injecton" e determina l'esistenza di eventuali vulnerabilità in base alla risposta del sistema. È una tecnica che, rispetto alla prima, permette di scoprire vulnerabilità non conosciute.

La Black box analysis permette di:

- Realizzare il test di software in produzione in modo da avere una maggior confidenza della sua sicurezza, sia dell'applicazione sia dell'ambiente.
- Nessuna necessità di accedere alle specifiche di progetto o al codice sorgente.
- Possibilità di test in ambito di rete.

## La Gray box analysis

Il terzo tipo di tecnica è la Gray box analysis, che combina in modo estremamente efficace i metodi sia della White box sia della Black box e permette di mettere a fattor comune i benefici di entrambi i tipi di strumento

minimizzando il rischio di omettere nel controllo aspetti importanti ai fini della sicurezza delle applicazioni. In pratica, gli strumenti devono garantire di poter applicare tecniche sia di white box sia di black box, andando a incrociare i risultati per avere una maggior copertura delle vulnerabilità e allo stesso tempo ridurre il numero di falsi positivi.

## 4.2 La sicurezza delle applicazioni Web

IBM Rational AppScan è una suite do prodotti per il test di applicazioni Web che sono utilizzabili per automatizzare la scansione delle applicazione e individuarne le loro vulnerabilità.
Il campo di utilizzo include l'identificazione delle vulnerabilità classificate dal Web Application Security Consortium (WASC) e dall'Open Web Application Security Project. I paragrafi seguenti illustrano gli elementi salienti della suite in correlazione alla specifica fase del ciclo di vita di una applicazione.

### Rational AppScan Standard Edition e Express Edition

Rational AppScan Standard Edition è uno strumento per la sicurezza che risponde alle esigenze del security auditor che deve verificare il comportamento di un'applicazione al termine del suo sviluppo e prima che venga passata in produzione. Il software automatizza la realizzazione dei test e supporta le più recenti tecnologie Web 2.0.
Tra queste: il parsing e l'esecuzione di script Java e applicazioni Flash Adobe, JavaScript e XML (AJAX), Adobe-Lex, JavaScript Object Notation, Action Message Format (AMF) e SOAP.
A questi aggiunge anche il supporto e l'analisi dei complessi ambienti SOA. La soluzione affronta anche il problema della remediation e produce una lista in ordine di priorità delle vulnerabilità rilevate nel corso dell'analisi in modo che si possano affrontare per prime le criticità principali.
IBM Rational AppScan Express Edition è invece la versione del prodotto che IBM ha sviluppato per rispondere alle esigenze delle medie imprese. Anche in tale contesto aziendale consente il test automatico e completo per le vulnerabilità delle applicazioni Web, la scansione di malware e la riduzione della necessità di costosi test manuali. Come per la versione standard consente la scansione automatica delle applicazioni Web complesse utilizzando tecnologie Web 2.0 come Adobe Flash, Javascript e AJAX e di rispettare gli standard di conformità principali come Payment Card Industry

Data Security Standard (PCI DSS), Payment Application Data Security (PA-DSS) (nuovo) e ISO 27001 e ISO 27002. Supporta il sistema operativo Microsoft Windows.

### Rational AppScan Reporting Console

AppScan Reporting Console permette di consolidare i dati e i risultati delle analisi di vulnerabilità effettuate, con i tool di analisi statica e dinamica, in un sito centralizzato. Inoltre gestisce l'accesso e la profilazione degli utenti e dei gruppi di lavoro. Offre la possibilità di comunicare e condividere i risultati tra i diversi team di sviluppo, e di facilitare la comunicazione tra i responsabili delle aree applicative e la funzione di Sicurezza. Esso offre anche la possibilità di creare report e dashboard che possono essere distribuite a utenti diversi in funzione del loro ruolo e dello storico: report che mostrano gli andamenti rispetto numero e tipologia di problemi riscontrati nelle diverse fasi, quali indicatori della qualità del codice prodotto.

### Rational AppScan Source Edition

È un prodotto aggiuntosi di recente alla suite Rational che ha ulteriormente potenziato il portfolio per la sicurezza e che deriva dalla acquisizione di Ounce Labs. Fornisce una soluzione completa per le organizzazioni interessate a correggere le vulnerabilità delle applicazioni prima che esse diventino operative ed è in grado di eseguire la scansione del codice sorgente del software e identificare le potenziali vulnerabilità di sicurezza e conformità sin dai primissimi stadi di sviluppo del software stesso, quando le correzioni sono meno onerose da apportare.

Per le organizzazioni che non dispongono internamente di competenze per la sicurezza delle applicazioni, o che preferiscono affidare all'esterno tali valutazioni, IBM ha reso disponibile Application Source Code Security Assessment, un servizio progettato per aiutare i clienti a capire e migliorare la propria conformità normativa e a ridurre il rischio, fornendo una valutazione iniziale del codice sorgente delle applicazioni, per favorire l'incorporazione della sicurezza nel ciclo di vita di sviluppo del software (SDLC).

Grazie a questo nuovo servizio, i consulenti IBM possono realizzare il test delle applicazioni per i clienti, identificare le vulnerabilità per la sicurezza e fornire raccomandazioni per la prioritizzazione e le misure di rimedio dettagliate per risolvere tali vulnerabilità.

Tra le diverse modalità di licencing, c'è anche la possibilità di avere una soluzione per realizzare la scansione avanzata di sicurezza delle applicazioni Web che consente di automatizzare le valutazioni della loro vulnerabilità.

Presenta il beneficio di ridurre notevolmente i costi associati alle attività di test manuali delle vulnerabilità e consente di proteggere gli ambienti dalle minacce di attacchi di hacker, automatizzando le analisi di sicurezza al fine di rilevare le vulnerabilità.

## 4.3 La 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.

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.

Per sfruttare in tutta tranquillità i benefici di SOA nei processi di business, nella flessibilità e nell'efficienza dell'IT, 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.

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 personalizzabile 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 nonché su una infrastruttura che sia basata su policy predefinite.

Qualora si vogliano raggiungere gli obiettivi di business prefissatisi median-

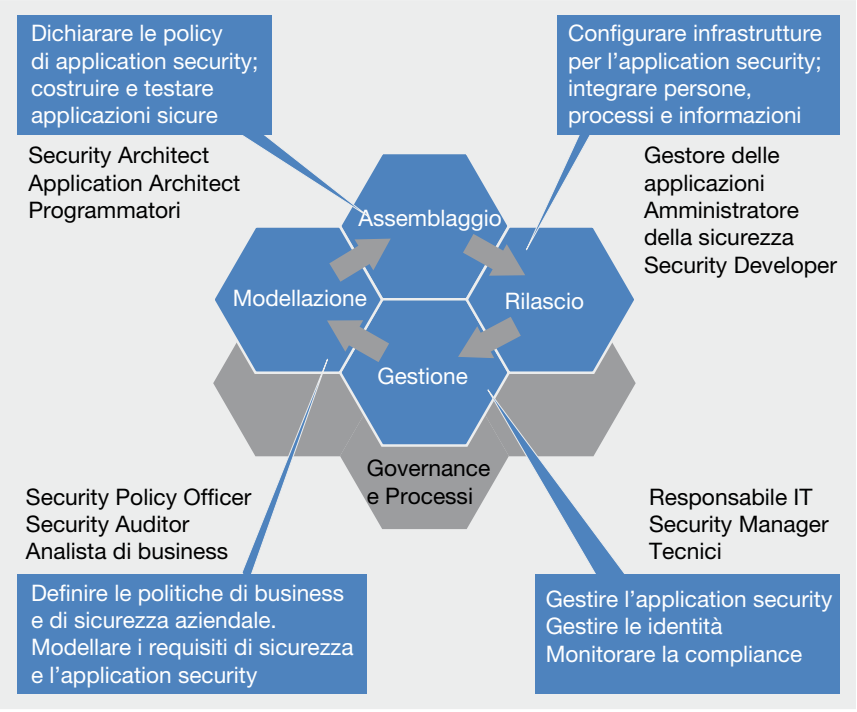



Figura 4.1
Il ciclo di vita di un'architettura SOA dal punto di vista della sicurezza

te 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 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 sia 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 corpo-rate, 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.

Va osservato che l'Identità esiste sia per gli user sia 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.

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.
Il problema della policy è enfatizzato dall'esigenza di gestire la 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 definizioni sia 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.

### 4.3.1 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 esso può aiutare nell'indirizzare i requirement e portare alla realizzazione di un'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 scam-

biati tra le applicazioni e i servizi, la non ripudiabilità 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 sicuri 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 autenticare e autorizzare le entità che richiedono l'accesso 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 sup-

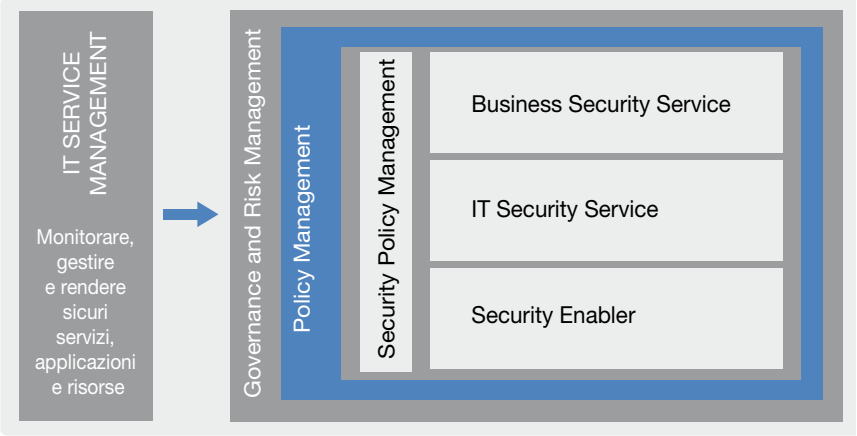



Figura 4.2

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

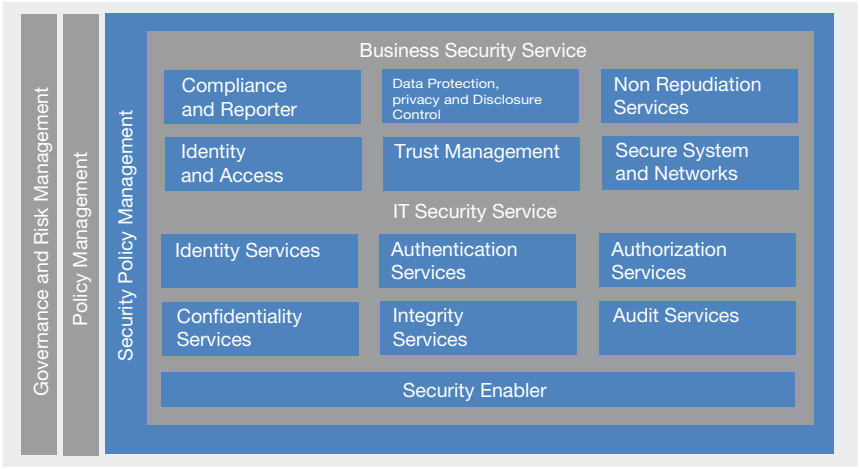



Figura 4.3
Il modello SOA Security Reference Model sviluppato da IBM

porta 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.

### 4.3.2 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, si rimanda al precedente capitolo. 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 obiettivi è 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.

IBM ha 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.

A queste soluzioni si aggiunge IBM Banking Framework for Customer Care and Insight. Si tratta di un framework che permette al mondo bancario e del finance di 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 sia le nuove strategie di business.

# 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, verificando 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

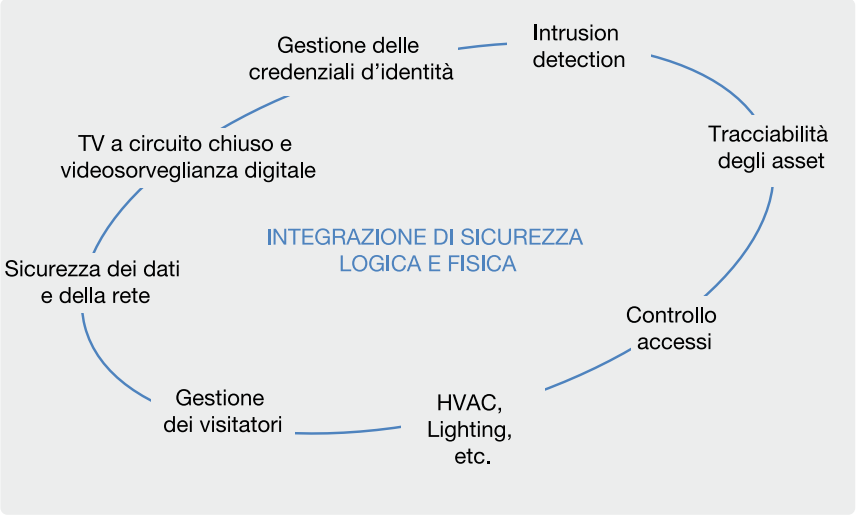



Figura 5.1
Un unico disegno architetturale integra le componenti di protezione ambientale, tecnologica e personale.

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 attenzio-

ne 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 auto-consistenti, 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.
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 facil-

Figura 5.2
Framework di un evoluto sistema di sicurezza integrato

mente 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 sorveglianza intelligente con IBM Smart Vision Suite

IBM collabora con enti governativi, società e istituzioni a livello mondiale e favorisce l'adozione di open standard per rafforzare i protocolli aziendali e implementare un approccio olistico alla sicurezza che consente ai propri clienti di proteggere sistemi informatici, dispositivi, edifici, dipendenti e risorse intellettuali.
Per quanto riguarda la sicurezza fisica l'elemento centrale della strategia IBM è rappresentato dalla "IBM Smart Vision Suite", che capitalizza il know how IBM in tema di hardware, software, ricerca e servizi per permettere l'accesso alle informazioni critiche per la sicurezza e fornire alle aziende la capacità di individuare in tempo reale i comportamenti anomali o sospetti e di fare ricerche mirate per particolari attributi sulle immagini video registrate.

La sicurezza fisica è particolarmente importante nel settore pubblico, per la protezione in ambiti quali i trasporti, la sicurezza urbana e altre realtà vitali per il Paese, ma è parimenti importante anche presso le aziende che abbiano siti critici da proteggere, a partire dalle banche per arrivare ai centri commerciali o ai negozi.
La soluzione Ibm Smart Vision Suite rimuove i limiti tipici della videosorveglianza analogica, che imponeva la presenza di personale attento e dedicato davanti ai monitor per la generazione di allarmi e che, per il resto del tempo, si limitava a registrare ore di video su nastri di lenta consultazione, quando possibile.
Con la soluzione Smart Vision le riprese sono invece indicizzate come contenuto XML, che consente di generare allarmi e facilita la ricerca di informazioni post-evento. Per esempio, è possibile effettuare una ricerca chiedendo al sistema di selezionare tutti i video ripresi da "n" specifiche telecamere poste in altrettanti incroci stradali, in cui è registrato il passaggio di un automezzo bianco in un determinato arco temporale. Le possibilità sono quindi molteplici e aiutano a potenziare la consapevolezza della situazione, su più scale spaziali e temporali.

### 5.2.1 Una risposta di alto profilo alle esigenze di sorveglianza pubblica

La consapevolezza della situazione rappresenta la chiave per la sicurezza e necessita di informazioni variegate: un analista della sicurezza deve tenere traccia dell'identità (cioè chi sono le persone e oggetti, come i veicoli ma non solo, in uno spazio), della posizione (cioè dove si trovano le persone e gli oggetti in uno spazio) e dell'attività (cioè che cosa fanno le persone e gli oggetti in uno spazio).
Dopodiché occorre confrontare il comportamento di tali elementi rispetto a un contesto storico o atteso: per esempio, il fatto che un furgone portavalori sia in anticipo sull'orario previsto genera sospetti e fa innalzare la soglia di attenzione.
La possibilità di associare attributi specifici ai video, in sostanza, consente a Ibm Smart Vision Suite d'individuare in tempo reale i comportamenti anomali o sospetti e far scattare allarmi o segnalazioni per successive indagini.
La suite IBM Smart Vision Suite permette non solo di monitorare automaticamente una scena, ma anche di gestire i dati di sorveglianza, effettuare il recupero dei dati sulla base degli eventi, ricevere alert degli eventi in tempo reale attraverso l'infrastruttura web ed estrarre modelli statistici di attività a lungo termine.

Grazie alle sue funzioni di analisi comportamentale basate su video, di allarme in tempo reale e controllo a eventi "pre-programmati", aiuta a comprendere meglio i potenziali modelli di violazione e consente di sviluppare strategie di sicurezza più intelligenti.
La chiave dei benefici offerto dalla Smart Vision Suite di IBM è costituita dal fatto che adotta un approccio object-oriented al video. Non si limitra a registrare, ma interpreta e capisce il video stream, scomponendolo in persone, oggetti e aree di interesse. Ha inoltre incorporato nella sua progettazione diversi modi per tutelare la privacy delle persone nello spazio controllato.
La soluzione si basa su una tecnologia per la sicurezza assolutamente innovativa, creata dai laboratori di ricerca IBM. ed è l'unica tecnologia in grado di fornire le funzionalità per effettuare efficaci analisi dati su sequenze video, sia in tempo reale che registrate.
Basata su standard aperti, permette di monitorare e analizzare eventi reali mediante sensori multipli, tra cui video camere, radar, sensori chimici o ingressi audio, ed è predisposta per integrare le principali tecnologie disponibili sul mercato.
IBM Smart Vision Suite permette di accedere in tempo reale alle informazioni critiche per la sicurezza e fornisce la capacità di individuare immediatamente i comportamenti anomali o sospetti o di fare ricerche mirate per particolari attributi sulle immagini video registrate.
La concezione modulare della soluzione consente l'integrazione dei sistemi legacy e l'uso di funzionalità tecnologiche avanzate e future, quali l'identificazione biometrica, il tracking di oggetti, la gestione degli eventi, il comando e controllo centralizzato e il riconoscimento dei modelli.

### 5.2.2 I benefici di Smart Vision Suite

Rispetto ai sistemi di video sorveglianza tradizionali, Smart Vision Suite si caratterizza per la risposta positiva che dà a esigenze primarie, quali:

- la capacità di supportare le attività di prevenzione degli incidenti: è realizzata attraverso allarmi in tempo reale che segnalano i comportamenti sospetti; il potenziamento delle funzioni di indagine scientifica e il recupero di video basato sui contenuti.
- la consapevolezza della situazione: è realizzata attraverso la consapevolezza congiunta di posizione, identità e attività degli oggetti nello spazio monitorato.

Inoltre, Smart Vision Suite è in grado di acquisire un numero elevatissimo di dati video e di conservarli per periodi prolungati e permette un accesso immediato al materiale video in real-time e di archivio per gli utenti in sedi distribuite.

La soluzione, basata sulla rete e abilitata da sensori, permette di estendere i componenti di sicurezza esistenti, fornendo inoltre migliore accesso e maggiori funzionalità, tra cui l'automazione delle attività quotidiane di acquisizione, indicizzazione e archiviazione di contenuti video.
I vari reparti aziendali possono poi avere accesso al sistema, previa l'autenticazione delle password, per collaborare e rispondere in caso di emergenza, furto o frode.
La soluzione è continuamente aggiornata con funzionalità sempre più avanzate di sorveglianza intelligente ed è in grado di integrare sistemi per il riconoscimento biometrico, per esempio il riconoscimento del volto, che potrebbe essere implementata per avvisare automaticamente il personale di sicurezza quando compare un autore di un reato noto alle forze dell'ordine.
La soluzione è basata su standard aperti, rendendo quindi possibile l'integrazione tra i componenti attualmente utilizzati e i potenziamenti futuri man mano che si renderanno disponibili. Si tratta quindi di una soluzione modulare, flessibile e in grado di crescere di pari passo con l'evoluzione delle esigenze.
Tramite la collaborazione con fornitori leader nel campo della video sorveglianza digitale e all'integrazione dei loro prodotti hardware e software nelle soluzioni IBM, è possibile risparmiare tempo prezioso eliminando la necessità di riesaminare, testare e valutare continuamente nuovi prodotti.
In sintesi, la soluzione IBM Smart Vision Suite è studiata per prevenire le perdite, riducendo rischi e responsabilità e permette di:

- Sfruttare gli investimenti esistenti in telecamere, reti e altra tecnologia per aiutare a ridurre i costi di implementazione.
- Impiegare tecnologia basata sugli standard, per accogliere e integrare facilmente strumenti e tecnologie futuri.
- Aiutare a ridurre i tempi e le spese di amministrazione, con il controllo centralizzato su un'infrastruttura consolidata.
- Automatizzare operazioni quali digitalizzazione, indicizzazione, gestione e recupero dati.
- Incorporare, nella progettazione, diversi modi per tutelare la privacy delle persone nello spazio monitorato.

### 5.2.3 L'utilizzo della Smart Vision Suite

Smart Vision Suite permette di eseguire analisi efficienti dei dati relativi alle sequenze video, sia in tempo reale sia registrate. Basata su middleware standard, la suite software è progettata per consentire il monitoraggio e l'analisi di eventi del mondo reale attraverso vari sensori (come video-

camere, radar o input sonori). Tutte le funzionalità della suite 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 si 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, Smart Vision Suite 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. Il software valuta gli eventi che si verificano nei sensori di riferimento rispetto alle definizioni di allarme. Ogni volta che si attiva la "definizione di allarme", il software è in grado di offrire all'utente una sollecita notifica dell'evento. Inoltre, gli utilizzatori (sia il personale sia le applicazioni) possono utilizzare le funzioni per effettuare ricerche sui contenuti tra i metadati degli eventi archiviati.
Per esempio, è possibile rintracciare tutti gli eventi registrati da una telecamera nei quali "un'auto rossa" si muoveva nel parcheggio. L'architettura 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. L'architettura funzionale supporta numerose tipologie di servizi. In particolare:

- 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, 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 per soddisfare le esigenze dei clienti e dei diversi ambiti applicativi.

Va poi osservato che Smart Vision Suite è una soluzione IBM 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 permette di ottenere molti benefici, 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 Smart Vision Suite 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 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 di sicurezza IBM 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 IBM offrono funzionalità a costi inferiori e più sicure rispetto ai tradizionali sistemi analogici.

- ***Settore bancario*** - Nelle banche, l'integrazione di soluzioni IBM 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 soluzioni IBM per il controllo video. È possibile utilizzare le analisi per eseguire controlli di sicurezza e per inviare allarmi quando viene rivelata la presenza di vetture non sicure.
- ***Aeroporti*** - Il ROI di un sistema di controllo video IBM 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.
- ***Ambienti urbani*** - La soluzione Smart Vision Suite permette di realizzare sistemi a largo raggio e grado di copertura in grado di incrementare enormemente la sicurezza urbana e di accelerare gli interventi delle forze dell'ordine, rintracciare automezzi e malintenzionati correlando dati provenienti da diversi sottosistemi ed eseguendo analisi in real time che permettono rapidità di intervento e maggior soddisfazione del cittadino.

## 5.3 Le soluzioni verticali

Le soluzioni di sicurezza IBM affrontano e risolvono i problemi per la sicurezza di numerosi settori verticali:

### 5.3.1 Le soluzioni di sorveglianza IBM per il mondo bancario

Per il mondo bancario, la Smart Vision Suite permette 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.
- 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 una funzione 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".

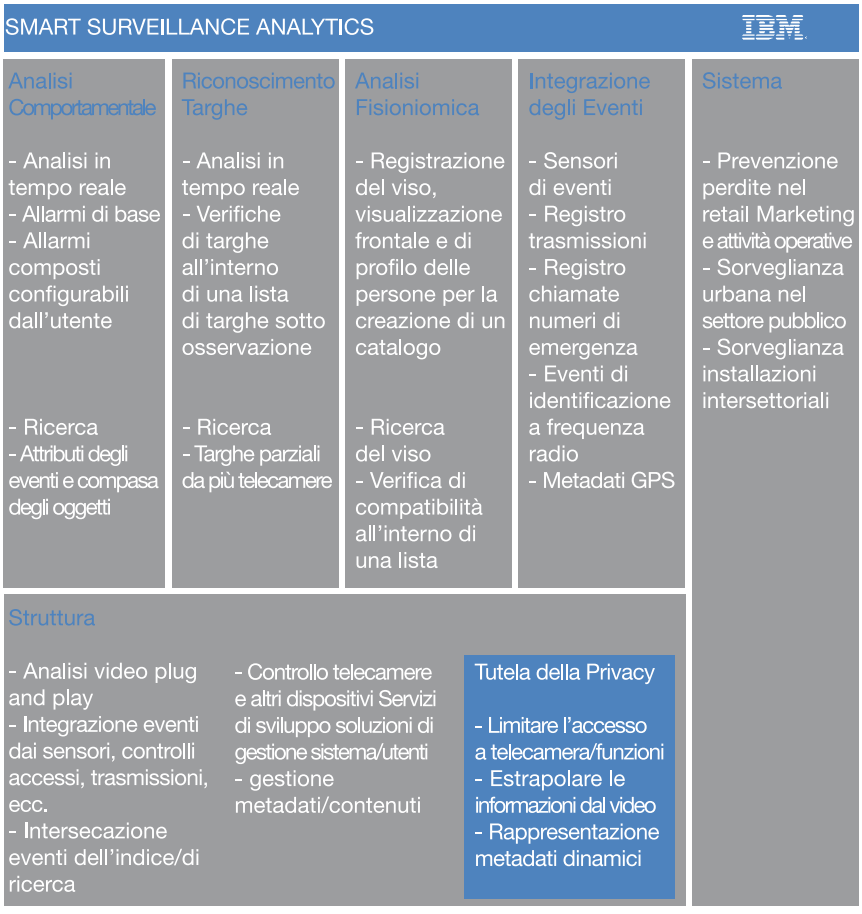



Figura 5.3
Funzionalità di analisi disponibili nella Smart Vision Suite di IBM

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.

### 5.3.2 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 (protezione delle informazioni e dei sistemi ICT), una proposizione fatta di best practice, prodotti e servizi di system integration per la protezione delle infrastrutture critiche.
L'elemento qualificante della sua piattaforma 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.

### 5.3.3 Le soluzioni per la sicurezza urbana e i trasporti pubblici

Le soluzioni IBM per la sicurezza fisica in ambito urbano permettono di rendere più sicuro l'ambiente medesimo nel suo complesso, soprattutto in quegli orari di fruizione di mezzi pubblici e nelle aree urbane dove maggiormente la sicurezza del cittadino o dei mezzi potrebbe essere messa a rischio. Per questo, le soluzioni IBM e le funzionalità della Smart Vision Suite indirizzano espressamente due precise tematiche:

- La sicurezza urbana.
- La sicurezza dei trasporti pubblici.

Al fine di garantire al cittadino la migliore sicurezza urbana possibile e farlo sentire confidente con l'ambiente e il servizio pubblico, nelle soluzioni e nella suite IBM per la sicurezza sono presi in considerazione e affrontati aspetti quali:

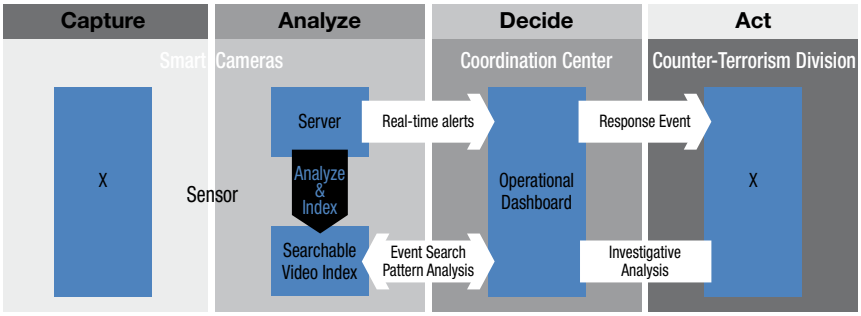
- Interventi di antiterrorismo
- L'analisi forense di crimini
- Prevenzione dei crimini e della microcriminalità
- La protezione di obiettivi di alto valore materiale e simbolico (uffici pubblici, rappresentanze diplomatiche, musei, chiese, ecc.).
- Gestione degli eventi e organizzazione delle contromisure.

Per quanto concerne la sicurezza nel trasporto pubblico IBM rende disponibili soluzioni per il controllo e la prevenzione dei crimini per:

- Le infrastrutture di accesso ai sistemi di trasporto.
- Le stazioni.
- I tunnel.
- Le officine di manutenzione dei mezzi.
- Le centrali di alimentazione elettrica o di rifornimento di carburante.

La soluzione IBM per la video sorveglianza urbana affronta e risolve nume-

Fig. 5.4
Le applicazioni Smart Vision Suite per l'ambiente urbano




rosi dei problemi che rendono poco efficienti le soluzioni convenzionali, come, per esempio:

- i tempi di fuori servizio.
- i lunghi tempi di analisi delle registrazioni che impediscono interventi rapidi e risolutivi.
- le aree di copertura.
- la difficoltà nel correlare i dati tra sottosistemi diversi di fornitori diversi.
- le complessità nella gestione mediante un'applicazione centrale comune.

A questo si aggiunge il problema di come gestire i dati oramai datati ma che è difficile capire se siano ancora utili o meno, come eliminare automaticamente i dati non necessari per non saturare il sistema di archiviazione e rendere in accettabilmente lunghi i tempi di ricerca, come registrare e correlare milioni di eventi trasformati in metadati.

Sono tutti problemi che possono rendere altamente inefficiente una soluzione costata alla comunità milioni di euro.

La soluzione di IBM basata su Smart Vision Suite e un controllo del territorio che fa largo uso di video analytics, supporta il personale nell'analizzare rapidamente enormi volumi di registrazioni video e permette loro di soffermarsi ed esaminare esclusivamente quelli realmente utili per interpretare quanto sta avvenendo e decidere rapidamente gli interventi da attivare.

Ad esempio, senza gli strumenti IBM un operatore deve monitorare continuamente le video camere o visionare personalmente i video archiviati per supportare una investigazione in corso. Si tratta di attività che richiedono tempo da parte dell'operatore e che distolgono personale dalle loro attività principali.

Con le soluzioni Ibm e le informazioni filtrate, organizzate ed evidenziate che gli vengono presentate a video l'operatore può invece valutare eventi in tempo reale, mentre stanno avvenendo, e decidere così quale sia l'ap-

propriata risposta. Inoltre, può lanciare ricerche e poi valutare i risultati una volta che il sistema gli ha preparato l'elenco delle informazioni richieste senza che però nel frattempo sia stato obbligato a rimanere innanzi ala console.
Non ultimo, tramite la soluzione Ibm e gli analytics che mette a disposizione, l'operatore ha la possibilità di identificare pattern nel comportamento di eventi (mezzi, persone) che molto probabilmente passerebbero non notati a causa della difficoltà mentale di correlare eventi tra molti altri, a distanza di ore o di giorni tra loro.

# 6
# I Managed Security Service

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, oltre ad altri benefici aggiuntivi, come la garanzia di un livello sempre massimo dell'aggiornamento tecnologico e di una flessibilità del servizio.

## 6.1 Il ricorso ai Managed Security Service

Spesso le aziende si trovano nella condizione di imporre alle proprie divisioni riduzioni di costo a breve termine. Nell'ambito IT, ma non solo, questo si accompagna sovente al supporto di cambi strutturali.
In pratica, mentre si bloccano le assunzioni, si riducono i budget per nuovi progetti, si chiudono contratti con subfornitori, si danno buone uscite e si preme per prepensionamenti, contemporaneamente si cerca di trasformare costi fissi in costi variabili.
Questo si ottiene tipicamente trasferendo risorse/applicazioni, centralizzando la governance dell'IT, ridefinendo strategie e priorità, ottimizzando i processi.
IBM può aiutare le imprese ad aumentare l'efficienza operativa e la capacità di gestione IT, il che si traduce in risparmio e in un possibile aumento degli investimenti in nuove tecnologie. Questo grazie ai Managed Security Service, il ricorso ai quali permette di abbassare i costi operativi e di trasformare i Capex (acquisto di dispositivi e software) in Opex (canone per i servizi e pay per use). In molti casi, IBM ha potuto dimostrare la possibilità di ridurre i costi del 55% passando da una gestione in house della sicurezza all'outsourcing presso IBM.
Fin qui si è analizzato il lato che sta forse più a cuore al business manager, del resto 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".
Peraltro, il vantaggio principale derivante dall'adozione dei servizi gestiti di sicurezza IBM Security consiste in un aumento del livello di sicurezza. Poche aziende infatti sono in grado di reggere il ritmo dei continui cambiamenti sul fronte delle minacce, con conseguenti rischi per l'operatività e finanche il business stesso. In un mondo costantemente connesso, la sicurezza deve essere perseguita 24 ore su 24 e comprende molteplici attività, dal patch management alla gestione dei dispositivi, dal monitoraggio degli

eventi al consolidamento delle politiche per la sicurezza. Occorre personale competente, costantemente aggiornato e, magari, numeroso.
Secondo IBM, inoltre, la sicurezza si deve considerare come un elemento abilitante del business e, per questo, deve essere concepita già nella fase di progettazione dei servizi IT e dei processi aziendali. Ma questo implica ulteriori complessità organizzative e oneri per lo staff IT. Peraltro, una cattiva gestione della sicurezza equivale all'insicurezza o può avere impatti sull'operatività, per esempio bloccando transazioni legittime in seguito a un falso positivo mal interpretato. Gli IBM Managed Security Service forniscono un'alternativa alla dispendiosa gestione operativa in house della sicurezza, permettendo di riguadagnare il controllo sul sistema di sicurezza nella sua interezza, compresi tutti i dispositivi managed o unmanaged, indipendentemente dal produttore.
I servizi di gestione, in particolare, possono essere sottoscritti in diverse modalità, lasciando la scelta ai clienti: dal monitoraggio 24 x 7 x 365 a un servizio complementare all'attività in proprio, per esempio solo per le ore notturne, secondo un modello chiamato di Protection on Demand.

### 6.1.1 Protection on Demand e flessibilità

Grazie alla tecnologia e alle infrastrutture possedute da IBM è possibile acquistare i servizi secondo la massima flessibilità garantita dalla formula Protection on Demand. 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 adat-

tare 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.

### 6.1.2 L'esperienza negli MSS e il valore della ricerca

IBM vanta più di dieci anni d'esperienza nei Managed Security Service che fornisce ad aziende di ogni dimensione.
Riconosciuta tra i leader del settore a livello mondiale da tutte le principali società di ricerca, IBM ha investito molto per costruire un'infrastruttura estesa e all'avanguardia. In particolare, per garantire una totale copertura oraria, per il disaster recovery, ma soprattutto per avere una visibilità costante in ogni parte del Pianeta, IBM ha costituito 9 Security Operations Center (SOC) distribuiti in tutto il mondo: Toronto, in Canada; Boulder, Detroit, Atlanta, negli USA; San Paolo, in Brasile; Bruxelles, in Belgio; Bangalore, in India, Tokyo, in Giappone; Brisbane, in Australia. 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.
IBM continua a investire in talenti, tecnologie e infrastrutture, ma il valore che vuole trasferire ai propri clienti consiste nella capacità di riduzione dei costi e in quella di salvaguardia dalle minacce e mitigazione del rischio.
A tal proposito, è importante sottolineare come l'esperienza maturata dagli specialisti degli IBM Security Service si riflette in una maggiore sicurezza per i clienti attraverso un meccanismo automatico. L'enorme quantità di eventi registrati dai nove SOC viene analizzata dai motori di analisi e correlazione di IBM Security Services e va a costituire una base per la ricerca da parte dei team di esperti, come IBM X-Force. Il risultato di tale ricerca, dunque, è il frutto delle informazioni raccolte non semplicemente presso il singolo cliente (che ciascuno potrebbe registrare sulla propria infrastruttura), ma di quelle relative agli eventi in tutto il mondo. Data la globalizzazione di alcuni attacchi e le modalità di propagazione degli stessi, questa visibilità è fondamentale per sviluppare gli opportuni aggiornamenti per i dispositivi di prevention installati a protezione delle reti dei clienti. Questi ultimi, dunque, beneficiano della visione globale in tempo reale.
Tre sono gli elementi differenzianti dei Managed Security Service targati IBM: il Virtual SOC Portal, il Virtual-SOC X-Force Protection System e X-Force Security Intelligence (per quest'ultima si veda al riguardo il capitolo 1).

## 6.2 Il Virtual SOC di IBM Security Service

Gli IBM Security Service 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 X-Force Protection System rappresenta quindi il motore che sta alla base dei Managed Security Service 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 gestione Web based dei servizi richiesti. IBM Security Service 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 ha superato il 60% andando a coprire praticamente tutte le tecnologie di sicurezza e non solo firewall e intrusion detection.

### 6.2.1 Il Virtual-SOC X-Force Protection System

Il Virtual-SOC X-Force Protection System o più semplicemente XPS è un'architettura proprietaria che utilizza sistemi d'intelligenza artificiale e tecnologie avanzate per creare una visione unitaria e completa della postura di sicurezza per ogni azienda cliente. XPS fornisce informazioni traducibili rapidamente in azioni. Più in dettaglio, l'architettura d'integrazione importa in tempo reale tutti i dati relativi alla grande mole di eventi registrati dai vari sistemi di sicurezza multivendor installati presso il cliente. Una volta raccolti nel Virtual SOC i dati vengono autenticati, cifrati, verificati e normalizzati. Quindi gli eventi così codificati sono archiviati nel data warehouse degli MSS di IBM, dove un sistema proprietario di IBM per il data mining li ricerca per analizzarli, correlarli e assegnargli una priorità.
Quando il sistema rileva una minaccia, l'evento viene identificato e segnalato come evento di sicurezza agli analisti di IBM, i quali analizzano questo tipo di eventi e, quando necessario, contattano il cliente di cui stanno gestendo l'infrastruttura si sicurezza per suggerire azioni di contenimento dell'incidente rilevato.
L'architettura aperta del Virtual-SOC X-Force Protection System consente a IBM Security Service di inserirvi anche prodotti di terze parti e di articolare i servizi in base alle specifiche esigenze di ciascuna impresa. Al Virtual SOC, inoltre, sarà possibile chiedere i servizi che di volta in volta si ritengono

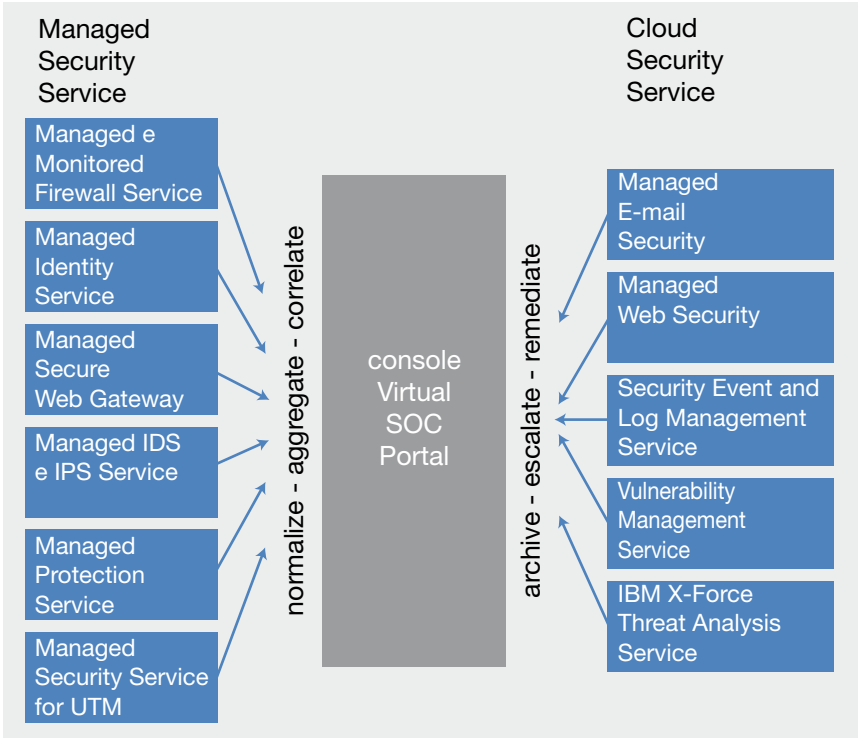



Figura 6.1
L'architettura del Virtual SOC di IBM Internet Security Systems

necessari, tra l'altro con la possibilità di integrarli 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 Security Service e i Security Enablement Service erogati attraverso il Virtual SOC Portal. Quest'integrazione fornisce alle imprese le informazioni, il supporto decisionale, gli strumenti e la capacità che necessitano per 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 Security Service.

### 6.2.1 Il Virtual SOC Portal

La flessibilità con cui possono essere richiesti i servizi 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 Security Service, tali decisioni possono essere demandate a esperti costantemente davanti al monitor e, sfruttando l'intelligenza delle engine integrate di IBM Security Service, possono essere automatizzate (comunque in base a policy precise) perché rispondano in tempo reale ai cambiamenti delle condizioni di sicurezza sulla Rete.
In pratica, attraverso il Virtual SOC Portal, il cliente potrà gestire in maniera autonoma il proprio sistema di sicurezza, sfruttando tutta la potenza del motore architetturale messo a disposizione dal Virtual SOC. Si ha, in altre parole, piena evidenza del livello di sicurezza della propria organizzazione e si possono tenere costantemente sotto controllo il profilo delle minacce e lo stato degli attacchi.

## 6.3 Gli IBM Security Service

I servizi per la sicurezza offerti da IBM Security Service 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.
L'offerta è in continua evoluzione e comprende molte proposte innovative, anche in chiave cloud computing, secondo le tendenze emergenti. In generale, si possono distinguere due portafogli di servizi: gli IBM Managed Security Service e gli IBM Cloud Security Service.
I primi sono quelli che prevedono di affidare la gestione operativa della propria infrastruttura agli esperti IBM, che forniscono quindi un servizio di monitoraggio e management continuo 24 x 7 x 365. Servizi gestiti tradizionali di base sono dunque Managed e Monitored Firewall Service, Managed Identity Service, Managed IPS Service, Managed Protection Service for Networks, Servers and Desktops.
Gli IBM Cloud Security Service, invece, permettono di sfruttare tutta la potenza delle soluzioni cloud sviluppate da IBM e del motore di analisi e correlazione di IBM X-Force per proteggere la propria infrastruttura attraverso servizi remoti, che richiedono investimenti contenuti in dispositivi e

manutenzione o non ne richiedono affatto, consentendo una massiccia riduzione del total cost of ownership.
Tra i servizi Cloud figurano i seguenti servizi: Managed E-mail Security, Managed Web Security, Security Event and Log Management Service, vulnerability Management Service, IBM X-Force Threat Analysis Service (X-FTAS).
Quest'ultimo è 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 preventiva 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.

# 7
# La sicurezza IBM per il Cloud Computing

**Il cloud computing abilita una concreta riduzione di Capex e Opex, ma per ottenere questo beneficio è necessario poter operare in un ambiente "trusted", in cui tutti gli enti che vi partecipano, fornitori dei servizi e fruitori dei medesimi, siano sicuri che i dati scambiati in rete non possano essere intercettati, carpiti o modificati in modo fraudolento.**

## 7.1 La sicurezza come elemento abilitante del Cloud Computing

Il Cloud è un emergente modello di consumo e distribuzione per i servizi IT in cui l'utente vede solo il servizio e non ha bisogno di conoscere la tecnologia o l'implementazione su cui esso si basa. IBM è fortemente impegnata nel rendere disponibili tecnologie, applicazioni e servizi che rendano fruibile per le aziende tale innovativo sistema di utilizzo delle risorse IT. Questo permette di ottimizzare sia Capex che Opex e avviare in azienda una politica volta a sensibilizzare gli utilizzatori sul valore dell'IT, tramite politiche di tariffazione in base all'uso che ne viene effettivamente fatto.
In questo contesto la "Cloud Security" concerne la confidenzialità, l'integrità e la disponibilità degli asset IT critici per il business, conservati o elaborati su una piattaforma di cloud computing.
Quest'ultima, intesa come insieme ed evoluzione dei paradigmi IT più o meno recenti, quali lo strategic e il global outsourcing, il grid computing, la Service Oriented Architecture e la virtualizzazione, è soggetta ai rischi impliciti in ognuno di essi e non solo. Si devono dunque impiegare varie tecnologie di protezione, processi, procedure, leggi e modelli Trust per rendere sicuro il cloud.
Il problema della sicurezza nel cloud è molto critico. Studi recenti del team di ricerca e sviluppo IBM X-Force indicano che il panorama delle minacce continua a evolversi rapidamente e che i moderni hacker adottano approcci sempre più sofisticati nei loro attacchi alle imprese pubbliche e private. Un rapporto realizzato da IBM X-Force evidenzia tre minacce principali, che dimostrano come gli aggressori abbiano utilizzato Internet a scopo di lucro o per il furto di dati. Infatti, nello scorso anno, il numero di nuovi link "malevoli" sul web è aumentato vertiginosamente, così come è cresciuta l'attività di phishing e la vulnerabilità per i "document reader" e per gli strumenti di editing, in particolare per quanto riguarda i documenti in Portable Document Format (PDF).

### 7.1.1 L'approccio di IBM per la Cloud Security

I nuovi modelli di business e di fruizione dell'IT, in primis il cloud computing, richiedono alle aziende di ripensare al modo di trattare la conformità, la gestione del rischio e la protezione dei dati: l'elemento centrale nell'approccio IBM per affrontare le sfide di sicurezza dei clienti è uno spostamento dell'attenzione, dalla protezione degli asset alla protezione dei servizi critici.

Grazie a soluzioni integrate, ovvero tool che possono fungere da monitor sulle attività operative e sulle potenziali aree di rischio, IBM può aiutare a progettare la sicurezza nel tessuto dei servizi che essi forniscono, rendendola così un elemento intrinseco dei processi di business, dello sviluppo dei prodotti e delle attività quotidiane.

La criticità di ambienti cloud deriva anche da uno dei suoi elementi fondamentali, la virtualizzazione. La velocità di adozione di questa tecnologia di ottimizzazione e di efficientamento dell'IT e di ambienti cloud aumenta man mano che le aziende consolidano i propri data center. Se da un lato la migrazione verso ambienti virtuali offre molti vantaggi, dall'altro impone alle aziende di adottare misure straordinarie per combattere la prossima generazione di minacce alla sicurezza e di sfide in termini di conformità. Queste misure sono necessarie a causa della minore visibilità e controllo derivanti dall'aggiunta di ulteriori "strati" d'information technology.

Tutto questo ha portato IBM a realizzare una strategia di prodotto che assicura, in ambito di cloud sia privato sia pubblico, l'adeguato ambiente di sicurezza nell'erogare i servizi o nell'attribuire l'uso delle risorse aziendali ad aree specifiche, divisioni o persone.

L'impegno di IBM è quindi di alto e ampio livello e tale da garantire il massimo dei benefici e della sicurezza nella realizzazione e nella fruizione di ambienti cloud. Più precisamente, IBM è fortemente impegnata nel garantire la sicurezza cloud in tre fondamentali modalità:

- La consulenza sulla cloud security, per aiutare i clienti a capire come proteggere un ambiente cloud, attraverso anche la fornitura di alcuni servizi (tra cui, per esempio, il penetration testing, l'Information security assessment e lo sviluppo di policy e standard per la protezione).
- I prodotti per la sicurezza nel cloud, tra cui l'ampio portafoglio di soluzioni che già oggi proteggono le infrastrutture di migliaia di aziende, cui si aggiungono funzionalità specifiche per ambienti cloud e ambienti virtualizzati in particolare, come Virtual appliance e solu-

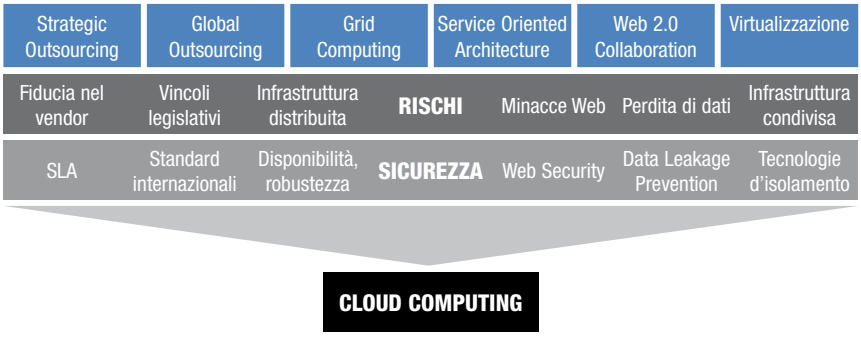



Figura 7.1

L'approccio IBM per la sicurezza in ambienti cloud fa proprie tutte le esigenze espresse nel tempo dagli ambienti che nel cloud sono confluiti

zioni per l'integrated virtualization security, compresa la soluzione IBM Security Virtual Security Server, realizzata in collaborazione con VMware, che protegge a più livelli gli ambienti virtuali.

- Gli Smart Business Security Services, che, oltre a comprendere una vasta offerta di managed service, si possono, in taluni casi, connotare come Security as a Service. Tra questi, per esempio quelli relativi alla posta elettronica. Si tratta di servizi cloud che prevedono la pulizia o la sicurezza della posta, scalabili con SLA (Service Level Agreement) garantiti molto elevati in termini sia di disponibilità sia di prestazioni, per esempio, nel blocco dello spam.

## 7.2 L'IBM Security Framework e i prodotti per la sicurezza nel Cloud

Per poter passare da una situazione in cui un'azienda ha il pieno controllo dell'infrastruttura e dei suoi servizi al cloud computing, essa deve innanzitutto ottenere le risposte a una serie di domande:

- Chi ha il controllo del sistema e da dove lo esercita?
- Dov'è situato il server che eroga le applicazioni?
- Dove sono memorizzati i dati delle applicazioni e come sono conservati?
- Chi effettua il backup e con che modalità?
- Chi controlla gli accessi e con quali strumenti?
- Quanto è robusto il servizio nel suo complesso e che SLA supporta?
- Cosa rende disponibile per gli auditor?
- Come può essere coinvolto il team per la sicurezza aziendale?

Sono domande che sottintendono tutta una serie di problemi e rischi collegati in termini di perdita di controllo, affidabilità, protezione dei dati, gestione della sicurezza e compliance. La cloud security è dunque un requisito fondamentale da parte delle aziende e un potenziale elemento di differenziazione per gli operatori sul mercato.

In quest'ambito, come e ancor più che nelle architetture tradizionali, è necessario un approccio globale alla sicurezza. Per questo IBM ha impostato la propria strategia di security governance sul rischio complessivo dell'azienda e sulla gestione della compliance.

Con questi due obiettivi al centro, IBM ha poi impostato e realizzato un

proprio Security Framework che abbraccia ogni aspetto della sicurezza, per ciascuno dei quali IBM fornisce soluzioni e servizi, schierando circa 15mila ricercatori sulla sicurezza, annoverando oltre 3mila brevetti e centinaia di clienti, investendo circa 1,5 miliardi di dollari per la sicurezza e gestendo più di 4 miliardi di security event per conto dei clienti.
L'IBM Security Framework identifica cinque "aree" da proteggere: persone e identità; dati e informazioni; applicazioni e processi; rete, server ed end point; infrastruttura fisica.
Attraverso i professional service, i managed service e le soluzioni hardware e software di IBM, trasversali alle aree citate, sono coperte tutte le esigenze di sicurezza nel cloud che Gartner, per esempio, identifica in: privilegi d'accesso degli utenti, data segregation; data recovery; supporto investigativo; compliance; data location, disaster recovery.
I paragrafi seguenti esaminano le principali aree protette da IBM e illustrano le soluzioni che sono disponibili per garantire la sicurezza aziendale in ambito Cloud.

### 7.2.1 Persone e identità: Access Manager

IBM Security Access Manager è una soluzione che fornisce la validazione e l'elaborazione delle credenziali e indirizza il bisogno di autenticazione degli utenti nell'ecosistema cloud garantendo la assoluta separazione tra chi è un semplice utente del servizio erogato e chi svolge funzioni di amministrazione del sistema e dei servizi forniti in ambito cloud.
IBM Security Federated Identity Manager permette invece di federare il processo di autenticazione abilitando la connessione degli utenti a più domini in ambito cloud caratterizzati da massive infrastrutture di calcolo parallelo.
IBM Security Federated Identity Manager, per esempio, permette di stabilire una relazione trusted tra ambienti applicativi basati su SOA (Service Oriented Architecture) e di connettere gli utenti ai servizi attraverso più domini di business. Aiuta inoltre le aziende nel rafforzare e automatizzare la concessione dei diritti di accesso agli utenti.
Quelli citati sono solo due esempi di come le soluzioni IBM già oggi forniscano protezione all'interno del cloud. Per quanto riguarda la protezione dei dati, poi, non vanno dimenticate le caratteristiche di sicurezza appartenenti ai sistemi e allo storage di IBM o quelle dei servizi IBM Protection Services di backup e recovery.

### 7.2.2 Applicazioni e processi: Rational AppScan e Security Vunerability Assessment Log management

Nell'ambito delle applicazioni e processi, il focus delle attività atte a garantire la sicurezza di una infrastruttura Cloud sono svolte da:

- IBM Rational AppScan
- IBM Security Vulnerability Assessment,

IBM Rational AppScan è una soluzione che esegue la scansione ed effettua il test di vulnerabilità delle applicazioni web. Tra i test svolti vi sono quelli di QL-Injection, Cross-Site Scripting e di Buffer Overflow.

IBM Security Vulnerability Assessment è invece un servizio che realizza la scansione automatica dell'ambiente al fine di identificare i sistemi operative, le applicazioni attive e il loro rispettivo grado di vulnerabilità ad attacchi esterni o interni.

In sostanza, si tratta di soluzioni che permettono di effettuare il testing interno o esterno di applicazioni cloud e della infrastruttura IT tramite la quale sono erogate. Aspetto qualificante è che possono essere utilizzate sia come componente di base integrate nella soluzione cloud che come servizio hosted erogabile tramite cloud.

### 7.2.3 Rete, server e endpoint: Enterprise Security Solutions

Network, server ed end point sono tutti elementi di una infrastruttura IT basata su Cloud di estrema importanza perché entrano tutti in gioco quando si estende a un ambiente cloud l'infrastruttura IT esistente.

Tutti questi elementi possono sono efficacemente protetti tramite le soluzioni ibm Security, WebSphere, Lotus, Rational e quelle di IBM Information

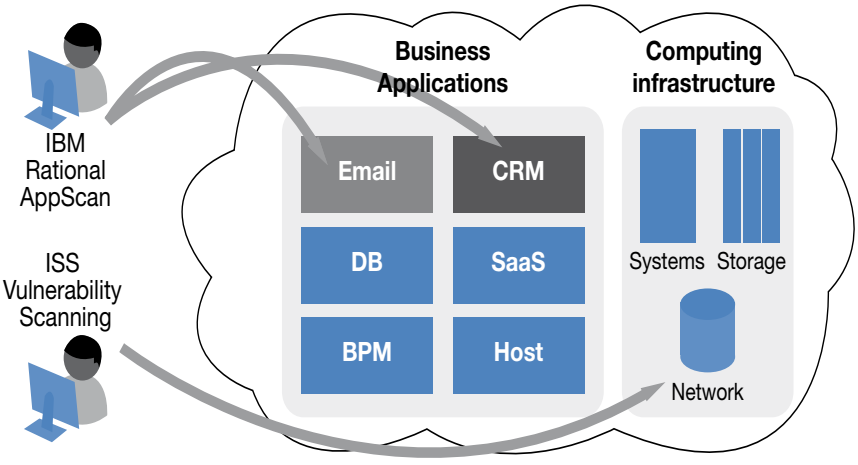



Figura 7.2
IBM Rational AppScan esegue la continua scansione delle applicazioni per scoprire eventuali vulnerabilità.

Management, oltre che dalle tecnologie hardware e software per l'Enterprise Security.
In particolare, le soluzioni "IBM Security Products and Services", il "Security Software" e i sistemi IBM operano in modo sinergico al fine di rendere disponibile un ambiente di calcolo di elevatissima sicurezza che riduce al minimo i potenziali rischi posti da attacchi alla sicurezza.
In sostanza, le soluzioni end-to-end sviluppate da IBM permettono di realizzare sistemi complessi di cloud computing in grado di fronteggiare efficacemente le sfide che si stanno già ponendo fornitori di servizi e loro fruitori.
Alle "Enterprise Security Solutions" si aggiungono, per quanto concerne la protezione di ambienti virtuali, la suite di soluzioni "IBM Virtualization Security". La sicurezza di ambienti virtuali è irrinunciabile al fine di abilitare un rapido e sicuro provisioning di risorse attraverso un insieme eterogeneo di server e hypervisor come usualmente si riscontra in ambienti cloud pubblici o privati.
La suite di soluzioni IBM comprende un ampio set di capability per la virtualizzazione che deriva da una quarantennale esperienza nel campo della sicurezza e che comprende tecnologie per rendere sicura la virtualizzazione. Sono soluzioni articolate in un ampio portafoglio di prodotti che aiutano a costruire un'infrastruttura cloud sicura, mediante applicazioni e soluzioni che vanno dall'Intrusion prevention ai Firewall, dalla protezione di applicazioni Web alla realizzazione di VPN sicure, dalla sicurezza del Messaging alla protezione degli Host (server e desktop).
Per quanto concerne in particolare la protezione delle applicazioni Web va osservato che per l'utilizzatore il cloud è di fatto costituito da un'interfaccia Web, e cioè una singola connessione che può consentire di costruire e amministrare un intero data center virtuale.
Le applicazioni Web, peraltro, sono da tempo oggetto di continui attacchi, anche perché risultano spesso deboli: il team di ricerca IBM X-force, per esempio, ha osservato che il 50,4% delle vulnerabilità individuate nella prima metà del 2009 è relativo a questo tipo di applicazioni, con l'SQL Injection e il Cross-Site scripting che si contendono il primo posto.
Elemento saliente dell'approccio adottato da IBM è che le piattaforme di virtualizzazione sono progettate avendo la sicurezza tra i propri requirement e non come un add-on successivo.
Soluzioni come Proventia "Server and Virtual Appliances", per esempio, rafforzano enormemente la capacità di difesa ed eliminano potenziali e aggiuntive minacce per l'ambiente Cloud.

## 7.3 Security Service

IBM ha disponibili un ampio insieme di servizi per esercire e gestire in modo sicuro ed efficiente ambienti cloud.

### 7.3.1 IBM Vulnerability Management

IBM Vulnerability Management è una suite di servizi chiavi in mano per medie e grandi aziende che permette di ridurre i rischi complessivi e la complessità di una soluzione cloud. Mette a disposizione funzioni per la scoperta delle vulnerabilità, la protezione dinamica, la prioritizzazione, il reporting personalizzato. Tra i benefici che permette di ottenere:

- Riduzione dei tempi di fuori servizio.
- Dimostrabilità dell'aderenza alle compliance.
- Minor esposizione a worm, virus e altre vulnerabilità.
- Maggior sicurezza complessiva.
- Incremento della produttività e dell'efficienza operativa.
- Riduzione del Total Cost of Ownership
- Integrazione trasparente con altri Managed Security Services

Il servizio di gestione delle vulnerabilità combina servizi di scansione gestita con la gestione esperta dei flussi di lavoro e la gestione delle diverse casistiche che si possono verificare.

Quello che ne risulta è un forte potenziamento delle capacità di protezione delle infrastrutture di rete da intrusioni che potrebbero causare profondi e costosi disservizi.

Inoltre, i report altamente personalizzabili mettono in grado di dimostrare la compliance con i regolamenti nazionali e internazionali quali Sarbanes-Oxley, HIPAA, SCADA e Gramm-Leach-Bliley.

### 7.3.2 IBM Managed Email Security e Managed Web Security

I servizi IBM Managed Email e Web Security proteggono dai problemi causati da spam, virus, worm, spyware e contenuti non desiderati. Contribuiscono quindi in modo molto efficiente a eliminare il rischio di costosi interventi di manutenzione software e hardware o di sovradimensionamenti non necessari della banda trasmissiva di rete.

IBM Managed Email Security comprende una suite di servizi che intercettano e scartano la posta dannosa prima che possa raggiungere la rete e permette di adottare le opzioni di sicurezza più adatte al proprio contesto scegliendole tra: antivirus, anti spam, controllo delle immagini, controllo dei contenuti.

La suite è particolarmente adatta per aziende di medie dimensioni che desiderano incrementare la sicurezza del loro ambiente di posta elettronica ed è un servizio che può essere sottoscritto sulla base del singolo utente. Tra le caratteristiche principali:

- Facilità d'uso e nessuna necessità di installare hardware o software aggiuntivo.
- Gestione h24.
- Posta sospetta messa in quarantena al di fuori della propria rete.
- Rimozione delle immagini e dei contenuti inaccettabili in base alla policy prestabilita.
- Comprende il supporto dell'help desk IBM

Il servizio IBM Managed Web Security risponde invece all'esigenza che hanno le medie aziende di proteggere investimenti e produttività diminuendo i rischi derivanti da spyware e virus che possono entrare nella propria rete tramite Web. Permette inoltre di rafforzare la politica di sicurezza aziendale limitando l'accesso a URL non appropriati o potenzialmente pericolosi. Il servizio permette di selezionare le opzioni desiderate scegliendole tra: anti-virus e anti-spyware; URL filtering; Antivirus, anti-spyware e URL filtering.
Tra le caratteristiche e i benefici principali del servizio:

- Scansione in tempo reale del traffico per individuare virus e spyware
- Disponibilità di semplici strumenti di amministrazione via Web per definire il proprio profilo e le policy di sicurezza.
- Filtraggio del traffico in accordo alla policy prestabilita e blocco del traffico indesiderato.
- Inoltro del traffico permesso senza apparente ritardo nella consegna in rete al destinatario.
- Comprende il supporto dell'help desk IBM

### 7.3.3 IBM Security Event & Log Management

IBM Security Event & Log Management è un servizio che permette di ridurre i rischi e migliorare il livello di sicurezza mediante la collezione, l'analisi e il reporting degli eventi che interessano la sicurezza e la rete. Tra i principali benefici:

- Disponibilità di una suite di prodotti per la gestione degli eventi connessi alla sicurezza senza dover investire in costose soluzioni in conto capitale e per la gestione.
- Incremento della visibilità degli eventi che interessano la rete.
- Potenziale riduzione dei costi di analisi e di log di soluzioni multivendor, complesse da gestire e da integrare.

- Supporto nel rispondere a richieste di compliance e ad analisi forensi.
- Integrabilità trasparente con altri servizi di sicurezza gestita di IBM.
- Fa parte della piattaforma di servizi on-demand di IBM.

IBM Security Event and & Log Management Service offre anche la possibilità di realizzare query sui log effettuati tramite un'unica interfaccia. È un approccio che migliora enormemente la rapidità con cui è possibile condurre investigazioni inerenti la sicurezza. Inoltre, è possibile archiviare in modo sicuro dati con valenza forense, ammissibili come prove in sede di giudizio per un periodo di sino a sette anni.

## 7.4 Un programma per la validazione del cloud

Per facilitare l'adozione del cloud computing, IBM ha reso disponibile un programma per validare la resilienza delle aziende che forniscono applicazioni o servizi ai clienti in ambiente cloud. I clienti possono così identificare rapidamente e facilmente i fornitori che, superando una rigorosa valutazione, risultano più affidabili e fruire in tutta tranquillità i vantaggi di business offerti dai servizi cloud.

Il programma, riferito come IBM "Resilient Cloud Validation" consente alle aziende che collaborano con IBM, rispettando un sistema rigoroso, coerente e collaudato di benchmarking e validazione della progettazione, di utilizzare il logo IBM: "Resilient Cloud" nella commercializzazione dei loro servizi.

Gestendo il maggior numero di data center nel mondo, IBM fornisce da decenni servizi di tecnologia remota ai clienti, sviluppando standard severi di qualità del servizio: dalla progettazione dell'infrastruttura all'eccellenza dei processi.

Grazie al nuovo programma Resilient Cloud Validation, l'unità IBM Business Continuity and Resiliency Services, forte di 40 anni di esperienza nell'eliminazione di downtime negli ambienti di business più impegnativi, supporta i provider di servizi cloud a soddisfare i più elevati standard di resilienza. Inoltre la Ricerca IBM ha sviluppato strumenti che individuano e valutano l'impatto che l'ottimizzazione e la migrazione verso ambienti cloud virtualizzati ha sulla infrastruttura e in termini di ritorno dell'investimento.

I Business Continuity and Resiliency Services di IBM sono erogati tramite 155 data center sparsi per il mondo e offrono un'ampia gamma di funziona-

lità, che vanno dai servizi di consulenza a infrastrutture resilienti completamente gestite. Questi team sono disponibili per valutare le architetture cloud attuali rispetto alle best practices di resilienza, per identificare, quantificare e prioritizzare lacune e rischi, e fornire quindi assistenza costante in fase di progettazione e competenza di gestione per infrastrutture più resilienti.

## 7.5 I servizi professionali IBM per la sicurezza del Cloud

Per supportare le aziende nell'affrontare correttamente il problema della sicurezza nell'evoluzione da una infrastruttura IT convenzionale a una basata sul cloud, IBM ha sviluppato due tipologie di servizi professionali, il "Cloud Security Assessment" e il "Cloud Security Strategy Roadmap".

### 7.5.1 Il servizio di Cloud Security Assessment

Affrontare il problema della sicurezza in ambito cloud è complesso perché non solo richiede metodologie appositamente definite ma anche, elemento ancora più critico per poter rapidamente godere dei benefici di un cloud sicuro, personale altamente specializzato e in grado di utilizzare i sofisticati strumenti oggi disponibili nell'ampia offerta di IBM. Per far si che anche le aziende che non hanno la possibilità di dotarsi rapidamente di un tale skill possano godere dei benefici del cloud, IBM ha reso disponibile il servizio di Cloud Security Assessment, che assiste i clienti nel valutare la robustezza delle architetture, delle policy e delle practice della loro soluzione cloud. Inoltre, il servizio è in grado di realizzare il test e valutare la reale efficienza dei controlli di sicurezza implementati al fine di prevenire sia gli attacchi interni o esterni che una non corretta applicazione delle misure di sicurezza. Il servizio di security assessment di IBM risponde a tre diverse esigenze:

- Le grandi aziende considerano la sicurezza l'elemento più critico nel decidere se investire o meno nel cloud, pur riconoscendone la validità.
- I fornitori di cloud pubbliche o private devono garantire la sicurezza delle loro soluzioni e best practice.
- I provider di soluzioni cloud devono poter verificare l'effettiva funzionalità ed efficacia dei propri meccanismi di sicurezza.

Il servizio IBM di cloud security assessment risponde a queste esigenze, supporta i clienti nell'affrontare la sfida associata al dover garantire la

sicurezza di un ambiente cloud, e mette a disposizione best practice che permettono ai professionisti IBM di identificare rapidamente lacune nella sicurezza e delineare rapidamente un elenco di raccomandazioni per porvi rimedio e migliorare la sicurezza dell'architettura. Inoltre, fornisce un supporto duraturo e continuo per effettuare periodici assessment. Il servizio di Cloud Security Assessment si basa su una serie di elementi che affrontano un ampio insieme di aspetti:

- Fasi di un progetto cloud coperte: sono coperte le fasi di progetto, implementazione e operation.
- Verifica di eventuali gap nella sicurezza: prevede la revisione dei programmi di sicurezza, l'analisi delle modalità di protezione dei dati, la revisione dell'architettura di sicurezza nel suo complesso.
- Test tecnico in condizioni stazionarie: consiste in un approfondito test dell'infrastruttura e delle applicazioni.
- Raccomandazioni: sono fornite al fine di migliorare la posizione aziendale per quanto concerne la sicurezza globale di un ambiente cloud.

### 7.5.2 Il servizio di Cloud Security Strategy Roadmap

Evolvere da una infrastruttura IT convenzionale a una basata su cloud, sia che si tratti di un public cloud realizzato da un provider di servizi che di un private cloud tramite il quale erogare servizi all'interno del proprio ambito aziendale, richiede una accurata pianificazione. Inoltre, è necessario definire una precisa roadmap per quanto concerne gli step per la sicurezza che devono essere implementati prima e durante lo sviluppo dell'ambiente cloud in modo da mitigare i rischi e garantire il desiderato livello di sicurezza. Per supportare i clienti in questo non semplice compito, IBM ha messo a punto un servizio che supporta nel definire la strategia e la roadmap per la sicurezza di un ambiente cloud. Il servizio permette di supplire a:

- La mancanza di esperienza aziendale nell'affrontare i problemi di sicurezza e di privacy in ambienti cloud siano essi pubblici che privati.
- L'incapacità nel godere completamente dei benefici del cloud a causa della mancanza di una robusta e affidabile strategia per la sicurezza.
- Mancanza di chiarezza nel definire le diverse responsabilità per quanto concerne la sicurezza del cloud.

Il servizio per la definizione di una roadmap per la sicurezza di ambienti cloud permette di disporre una serie di benefici. Tra questi: l'accesso all'esperienza e ai professional Ibm per quanto concerne le sfide poste dalla privacy e dalla sicurezza di infrastrutture cloud; un sofisticato aiuto nell'identificare

rapidamente le implicazioni per la sicurezza dei diversi scenari cloud che si possono delineare; la possibilità di disporre di una roadmap di alto livello utile nell'implementare la sicurezza desiderata e ridurre il rischio.
Il servizio prevede una prima fase costituita da sessioni di lavoro on-site abbinate alla raccolta off-site di informazioni utili nel definire la roadmap per la sicurezza e la realizzazione dei report. A questa prima fase segue la seconda fase che prevede la definizione della roadmap per la cloud security e che copre i seguenti aspetti:

- Esigenze legali, regolamentatorie e di sicurezza.
- Analisi dei carichi di lavoro del cloud e definizione delle strategie più appropriate per mitigare i rischi.
- Definizione delle modalità e degli strumenti da utilizzare per la valutazione del fornitore di servizi cloud.

Testi a cura di Reportec srl, Milano

Finito di stampare nel mese di Agosto 2010

IBM Italia S.p.A.
Circonvallazione Idroscalo
20090 Segrate (Milano)
www.ibm.com