White Paper

Gestire i rischi della sicurezza informatica

Sumner Blount, CA Solutions
Febbraio 2006

Sommario

Executive Summary

Diversi fattori legati all'andamento del mercato e del comparto hanno reso la gestione dei rischi in azienda un problema sempre più critico per singoli dirigenti e interi consigli di amministrazione. Non ultimo fra questi, la crescente minuziosità con cui vengono messe sotto esame tutte le attività aziendali attraverso normative di legge e di settore. Inoltre, l'aumentata visibilità e i catastrofici effetti finanziari causati da alcuni recenti casi di violazione della *security* hanno trasformato la gestione dei rischi di vario tipo in un argomento di scottante attualità per qualsiasi impresa.

L'elemento forse più importante di qualunque programma per la gestione dei rischi aziendali (Enterprise Risk Management o ERM) è costituito della sicurezza informatica, i cui elementi principali sono la protezione di asset critici e la disponibilità ininterrotta dei servizi IT. Se i rischi connessi a questi due aspetti vengono adeguatamente attenuati, anche i pericoli cui è esposta l'azienda nel suo complesso risulteranno notevolmente inferiori. Inoltre, riducendo i rischi informatici tramite l'adozione di efficaci misure di controllo interno si semplifica considerevolmente la conformità normativa.

Questo documento prende in esame gli elementi essenziali di un programma aziendale di *risk management* e tratta le diverse metodologie possibili in base al tipo di rischio e al livello di tolleranza ritenuto accettabile. Esso illustra altresì le componenti fondamentali della gestione della sicurezza informatica ed esplora alcune soluzioni tecnologiche utilizzabili per ridurre in modo significativo il rischio di possibili violazioni.

La crescente importanza della gestione dei rischi

Tradizionalmente, la maggioranza delle imprese ha sempre gestito i rischi in modo quantomeno informale e generalmente localizzato, attraverso "silos" in cui ciascuna divisione o *business unit* tentava di ridurre la rischiosità complessiva delle proprie attività – per lo più senza alcun coordinamento con altre funzioni aziendali. Ancor peggio, la gestione dei rischi è stata spesso trattata come problema marginale anziché come disciplina formale da integrare in qualsiasi procedura operativa e decisionale.

In tempi recenti, gli effetti negativi di questo approccio sono divenuti dolorosamente evidenti. La crescente presa di coscienza della necessità di discipline formali per la gestione dei rischi è stata stimolata da diversi fattori, fra cui:

- **Complessità e interdipendenza dei rischi aziendali.** Oggi il mondo del lavoro è incredibilmente più complesso rispetto al passato. La disponibilità di dati e applicazioni *on-line*, l'allargamento dei rapporti a partner e fornitori e la velocità dei mutamenti economici comportano la necessità, per le imprese, di prendere in considerazione un numero molto maggiore di rischi. Inoltre tali rischi sono raramente indipendenti fra loro; spesso si intersecano gli uni agli altri secondo modalità complesse e di difficile gestione. Un problema in un'area dell'attività commerciale può avere ricadute drammatiche su altre aree.

- **Aumento delle normative di legge.** La *compliance* normativa è diventata un argomento all'ordine del giorno negli ultimi anni, in gran parte sulla scia dei recenti scandali aziendali. Oggi le imprese devono far fronte a una serie di richieste, complesse e spesso poco chiare, contenute in normative di legge e di settore. E la responsabilità è diventata personale: i CEO rispondono in prima persona della *compliance* aziendale, e ciò crea un forte incentivo al rispetto delle leggi sia nello spirito che nella lettera.

- **Crescente globalizzazione.** La crescente espansione geografica di molte aziende e la complessità dei regolamenti interni da rispettare implicano la necessità di una gestione dei rischi su base planetaria. Azioni semplici come fornire informazioni sui clienti a una filiale estera possono oggi comportare notevoli rischi legali. Inoltre, la spinta alla penetrazione dell'attività commerciale in nuove aree con una contemporanea riduzione dei costi crea rischi e pressioni da gestire con cautela.

- **Maggiore visibilità di perdite catastrofiche.** I notiziari sono pieni di cronache di aziende che hanno subito catastrofiche perdite finanziarie e di immagine, molte delle quali culminate nella bancarotta. Società come Barings PLC, Worldcom, Enron e altre sono esempi di fallimento a tutti i livelli nella gestione e nel controllo dei rischi. Ovviamente nessuna azienda desidera andare ad aggiungersi a questo triste elenco, perciò cresce l'adozione di tecniche e misure di controllo nuove e più severe per gestire i rischi aziendali.

I fattori sopra elencati sono alcune delle principali ragioni che spingono le imprese a implementare programmi e iniziative formali di *risk management*. La gestione dei rischi è diventata un ulteriore imperativo commerciale, insieme ad altri più noti quali il ROI e la riduzione dei costi.

Cosa si intende per ERM (Enterprise Risk Management)

Tutti sappiamo a livello intuitivo cosa sia un rischio e conosciamo alcune delle aree in cui può manifestarsi. Tuttavia l'ERM è molto più che la semplice gestione di singoli rischi indipendenti fra loro. Il Gartner Group definisce il rischio come "una possibilità di perdita o di esposizione a una perdita". Ne consegue che l'ERM è una gestione sistematica e formale dei rischi che punta non solo a ridurre le perdite, ma anche a sfruttare le opportunità. Scopo del *risk management* è proteggere l'azienda e la sua capacità di portare avanti la propria missione strategica.

Obiettivo dell'ERM non è la costituzione di una burocrazia centralizzata per la gestione dei rischi, ma piuttosto la creazione di una metodologia efficace e sostenibile in grado di gestire qualsiasi forma di rischio in ogni parte dell'azienda. Ciò

è possibile solo se il *risk management* è un processo che permea tutti i processi decisionali aziendali, a qualsiasi livello. In termini di corporate governance, efficienza ed efficacia, un buon programma di gestione dei rischi può comportare vantaggi notevoli, alcuni dei quali saranno discussi in un paragrafo successivo.

Sebbene il valore di programmi di questo tipo sia ampiamente riconosciuto, la loro adozione rimane alquanto limitata. Il settimanale *Compliance Week* riferisce che, secondo un sondaggio svolto fra dirigenti d'azienda, il 91% delle imprese "è ben disposto" verso il valore dell'ERM, ma solo l'11% ha attuato un programma ERM a tutto tondo, perciò lo sviluppo potenziale di questa metodologia è ancora molto elevato.

Il successo limitato dell'ERM non sorprende se si considerano le problematiche connesse alla sua implementazione. La gestione di rischi complessi e a volte sconosciuti in diverse *busines unit*, ad esempio, presenta seri problemi organizzativi, e anche la complessità e la natura spesso conflittuale dei mandati internazionali rende assai difficoltosa la gestione dei rischi normativi. Infine, la scarsa conoscenza delle *best practice* di settore e la mancanza di esperienza nella loro applicazione lasciano le imprese prive di direttive da seguire. Perciò, pur comprendendo la necessità di un programma ERM formalizzato, molte aziende non sanno bene come procedere o quali tecnologie adottare a supporto di tale processo.

Classificazione dei rischi

Quali tipi di rischi gestisce l'ERM? Come suggerisce il nome, dovrebbe gestire *qualsiasi* rischio in grado di influire in modo non trascurabile sull'azienda. La classificazione generale dei rischi che la maggior parte delle imprese deve affrontare comprende:

- **Rischi naturali** (incendi, inondazioni, furti, ecc.)
- **Rischi finanziari** (prezzi, credito, inflazione, ecc.)
- **Rischi strategici** (concorrenza, innovazione tecnologica, modifiche alle norme di legge, danni all'immagine di un marchio, ecc.)
- **Rischi operativi** (funzionamento dell'IT, operatività commerciale, minacce alla sicurezza, ecc.)

Il monitoraggio e la gestione di tutti questi tipi di rischi sono cruciali per un'azienda, e in casi estremi ciascuno di essi potrebbe avere conseguenze catastrofiche. La tipologia spesso più facile da prevedere e controllare è quella dei rischi operativi che riguardano la normale attività dell'azienda e sui quali è più semplice intervenire attraverso un miglioramento e un rafforzamento dei controlli interni.

I rischi operativi possono essere *interni* o esterni. Fra i rischi operativi interni si annoverano:

- **Persone.** Perdita di personale, carenza di *know-how*, attriti, ecc.
- **Processi.** Controlli di processo inadeguati, fusioni, ecc.
- **Tecnologia.** Sicurezza e affidabilità inadeguate dei sistemi, obsolescenza, ecc.

Le categorie dei rischi operativi *esterni* sono simili, e comprendono:

- **Processi.** Rischi legali, rischi legati a partner e fornitori, ecc.
- **Tecnologia.** Sicurezza fisica, sicurezza dei siti di archiviazione dei dati, ecc.

In un paragrafo successivo vedremo come gran parte dei rischi operativi di un'azienda possa essere mitigata con soluzioni tecnologiche accuratamente selezionate.

Il rischio non deve sempre essere evitato ad ogni costo. Al contrario, un'impresa può crescere solo accettando livelli di rischio cosiddetti "prudenziali". Alcuni rischi possono e devono essere considerati come parte della normale attività operativa. Esistono quattro approcci generici alla gestione di qualsiasi tipologia di rischio:

- **Evitare.** Modificare l'attività in modo che un particolare rischio venga eliminato.
- **Trasferire.** Passare per intero o in parte il rischio ad altri (compagnie di assicurazione, partner, ecc.).
- **Mitigare.** Creare un numero di controlli e parametri di verifica sufficienti a ridurre il rischio e la gravità della perdita.
- **Accettare.** Assumersi il rischio e i costi ad esso associati.

L'approccio più adatto dipende molto dal tipo di rischio e dalla gravità delle conseguenze. Il grafico che segue illustra alcuni principi generici relativi alla gestione di diverse tipologie di rischi aziendali.

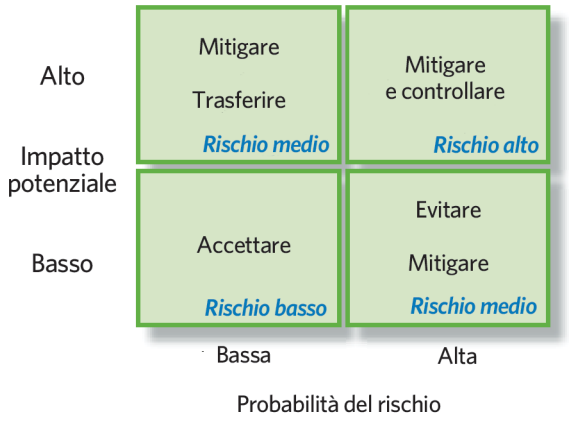

Figura 1. Matrice di gestione dei rischi.

Per sua stessa natura, questo grafico rappresenta un tentativo di riunire un gran numero di rischi in quattro semplici riquadri. Come tale, esso costituisce solo un ambito concettuale e non rispecchia per intero la complessità di molti rischi operativi odierni.

Esaminiamo brevemente ciascun approccio. Evitare i rischi è difficile, e a volte limita notevolmente le scelte aziendali. Ciò significa che l'eliminazione di un rischio potrebbe avere sulla crescita dell'azienda ripercussioni ancora più negative del rischio stesso. Il trasferimento dei rischi può comportare alcuni vantaggi finanziari, ma spesso questi non sono tali da soddisfare le esigenze del business aziendale. Ad esempio, anche se un impianto produttivo è coperto da una polizza assicurativa, l'impatto negativo prodotto dalla sua uscita di servizio potrebbe essere comunque catastrofico.

Come si vede, la mitigazione è spesso l'approccio più comune. Essa comporta la creazione di **meccanismi di controllo** atti a ridurre possibili perdite, nonché **capacità di monitoraggio** in grado di garantire che l'analisi dei rischi correnti sia sempre corretta. La quantità e il livello dei meccanismi di controllo in uso dipendono largamente dalla gravità del rischio per l'azienda nel suo complesso: alcuni rischi richiedono un monitoraggio e un'analisi costanti e fortemente proattivi, altri un livello di attività lievemente inferiore.

La mitigazione è anche l'approccio più indicato per una soluzione tecnologica che contribuisca all'implementazione dei meccanismi di controllo. Un paragrafo successivo di questo documento esaminerà alcuni metodi atti a garantire una piattaforma di mitigazione efficace.

Una piattaforma per la gestione dei rischi

Obiettivo di qualunque programma ERM dovrebbe essere la creazione di un ambiente e di un'infrastruttura che permeino l'attività e le politiche decisionali dell'intera azienda. Generalmente un programma di questo tipo conterrà alcuni elementi di base che devono essere integrati fra loro e comunicati con la massima capillarità per garantirne il successo. Il grafico che segue illustra tale modello. Esaminiamone le fasi una ad una per capire come influiscano sul programma ERM nel suo complesso.

Figura 2. Piattaforma di gestione dei rischi.

Strategia aziendale di gestione dei rischi

Questa fase, di cui è responsabile la leadership manageriale, serve a tradurre la tolleranza del rischio ritenuta accettabile in *policy* specifiche che il resto dell'azienda dovrà seguire. Ciò comporta generalmente la definizione di categorie di rischio, la determinazione dei possibili livelli di rischiosità e la creazione di linee guida relative ai rischi che l'azienda nel suo insieme è disposta a tollerare. Successivamente dovranno essere stabiliti i livelli di rischio accettabili per ogni *business unit*, da comunicare poi in modo capillare nell'ambito della stessa. A *business unit* diverse potrebbero essere assegnati diversi gradi di tolleranza in base agli elementi specifici dell'ambiente commerciale e finanziario in cui operano. Sta quindi a ciascuna *business unit* rendere operative tali direttive nelle varie situazioni specifiche che si trova ad affrontare.

Pianificazione e analisi dei rischi

Una volta create dal team esecutivo, le direttive passano alle unità operative, dove fungono da linee-guida per la pianificazione e le decisioni legate all'attività quotidiana.

Successivamente le *business unit* sviluppano un'analisi dettagliata dei rischi cui sono esposte e una classificazione degli stessi in base al loro potenziale impatto sull'attività commerciale. Tale classificazione consente di collocare ciascun rischio in uno dei quattro quadranti della matrice sopra descritta.

Quando sono stati analizzati e classificati tutti i rischi, è necessario mettere a punto un piano di risposta che spieghi come verrà gestito ciascuno di essi. In alcuni casi il rischio sarà considerato semplicemente come un "costo dell'attività

commerciale" e verrà accettato, senza alcun piano per la sua eliminazione. Nella maggior parte degli altri casi dovrà invece essere sviluppato un piano di mitigazione che illustri come creare meccanismi di controllo e capacità di monitoraggio in grado di abbattere notevolmente ciascun rischio e le relative conseguenze.

È opportuno eseguire un'analisi costi/benefici su ciascuno dei rischi mitigati. In alcuni casi, infatti, il costo della mitigazione risulterà superiore alle conseguenze negative del rischio stesso e quindi potrà essere più indicato un approccio alternativo quale il trasferimento o l'accettazione del rischio. Nella maggior parte dei casi, tuttavia, un piano specifico può comportare notevoli vantaggi dal punto di vista della possibilità di controllare i diversi esiti.

Gestione e monitoraggio dei rischi

La fase successiva consiste nel creare e installare meccanismi pratici di controllo dei rischi e nel monitorarne successo ed efficacia. Per "meccanismi di controllo" si intende tutto ciò che può diminuire la probabilità che un rischio si verifichi, o le eventuali ripercussioni: può trattarsi di soluzioni tecnologiche, di migliorie procedurali o, più probabilmente, di entrambe.

Dell'intero processo ERM, questa è l'area su cui la tecnologia può avere l'impatto più profondo. Nel caso della sicurezza informatica, ad esempio, il rischio di determinate minacce o esiti può essere largamente controllato attraverso l'adozione di tecnologie e soluzioni di comprovata efficacia. Questo tipo di approccio può inoltre creare una piattaforma sostenibile in grado di contribuire al contenimento dei rischi in via continuativa che quindi, non solo aumenta la sicurezza, ma spesso riduce anche i costi complessivi legati alla sua gestione.

Ad esempio, la maggioranza delle aziende è soggetta al rischio che persone non autorizzate possano accedere a dati, applicazioni o sistemi protetti. Tale rischio non può essere incluso nella categoria "Accettabile" e deve venire ridotto il più possibile tramite l'utilizzo, ad esempio, di una efficace soluzione di *access management.*

Allo stesso modo, uno dei rischi fondamentali per molte imprese riguarda il cosiddetto eccesso di autorità che consente a determinate persone di avere più diritti di quelli che sarebbero necessari allo svolgimento degli incarichi loro affidati. Un esempio assai comune è la concessione a molti dipendenti dell'accesso a interi sistemi in qualità di super-utenti, anche se per le loro mansioni basterebbe in realtà una qualifica inferiore. La situazione peggiora quando un dipendente ha facoltà non solo di avviare, ma anche di approvare determinate transazioni commerciali. In casi come questo la probabilità che si verifichi una frode è significativa, e va ridotta a tutti i costi.

Si noti che questi ***meccanismi di controllo interni*** sono identici a quelli richiesti per la conformità normativa. Qualunque sia la norma in oggetto, una serie di efficaci controlli di sicurezza interni costituisce l'essenza dei suoi requisiti. Creare tali controlli non solo contribuisce alla gestione e alla riduzione dei rischi, ma allo stesso tempo semplifica notevolmente l'ottemperanza alle normative di legge e di settore.

Elemento essenziale in questa fase è un **monitoraggio** costante dell'efficacia di ciascun meccanismo di controllo. Ciò comporta non solo sorveglianza e reporting sui meccanismi esistenti, ma una continua rivalutazione dei rischi e dei relativi piani di mitigazione in base ai mutamenti dello scenario operativo. La comparsa di nuovi rischi, come pure l'importanza crescente/decrescente di quelli già noti, richiedono modifiche al piano di gestione e ai meccanismi di controllo utilizzati per mitigarli.

Cosa comporta il monitoraggio? Nel caso della sicurezza informatica può comportare reporting di eventi specifici, filtraggio e correlazione automatici degli eventi al fine di identificare possibili problemi, validazione dei privilegi di accesso di tutti gli utenti per verificare che non siano superiori al necessario, ricerca ed eliminazione di eventuali eccessi di autorità, e così via.

Il monitoraggio non può limitarsi all'analisi di eventi specifici (ad esempio tentativi multipli di autenticazione falliti), ma deve estendersi anche agli eventuali trend, dato che a volte i problemi di security possono essere identificati solo osservando l'evoluzione degli eventi nel tempo. Sebbene richieda spesso una qualche forma di intervento umano, questo tipo di monitoraggio può essere in gran parte automatizzato utilizzando un'efficace soluzione di *security event management.*

Ottimizzazione dei meccanismi di controllo

I meccanismi di controllo interni e la loro efficacia devono essere analizzati su base continuativa. Sono molti, infatti, gli elementi che possono modificare la strategia di gestione dei rischi in atto: comparsa di nuovi rischi, variazioni di priorità dei rischi esistenti, fallimento delle tecniche di mitigazione, e così via. Inoltre, l'andamento dell'attività operativa può facilmente comportare mutamenti nella tolleranza ai rischi: quando le cose vanno bene, anche un livello di rischio maggiore può diventare accettabile.

L'ottimizzazione dei meccanismi di controllo richiede semplicemente che l'attività di monitoraggio di cui sopra venga utilizzata per modificare in modo dinamico i meccanismi impiegati nella gestione di ciascun rischio. Si tratta di un processo senza fine, in quanto i rischi sono sempre in una certa misura dinamici: non si arriverà mai alla perfezione, si riuscirà solo a migliorare.

Compliance reporting

L'ultima fase riguarda in genere la creazione di report e informazioni da utilizzare per eventuali revisioni della *compliance* normativa. I documenti prodotti non saranno solo quelli specifici da sottoporre ai revisori ufficiali, ma anche report per uso interno che contribuiscano a determinare il livello di conformità raggiunto.

Si noti che questa fase, pur non facendo parte dell'ERM in senso stretto, rappresenta una conseguenza naturale dello sforzo e dei risultati prodotti nell'ambito complessivo della procedura. Proprio questo rende l'ERM così importante per un'efficace *compliance* normativa: esso sviluppa una piattaforma in grado di affrontare rischi di qualsiasi tipo in ogni parte dell'azienda, e consente la creazione di meccanismi di controllo interni che non solo pongono rimedio a tali rischi, ma producono anche *report* e informazioni a riprova dell'avvenuto raggiungimento degli obiettivi di *compliance.*

Principi di un'efficace gestione dei rischi

Nonostante un maggiore interesse apparente verso il *risk management*, la situazione pratica si rivela tuttora scarsamente efficace. Ciò dipende dal fatto che in molte aziende la gestione dei rischi viene attuata in modo indipendente da ciascuna *business unit*, secondo priorità ed esigenze commerciali in gran parte stabilite a livello locale. Spesso non esistono una supervisione o una visibilità a livello centrale di questi sforzi, e il risultato è una scarsa uniformità tra le varie divisioni aziendali. La mancanza di una piattaforma di *risk management* comune e omogenea cui ogni *business unit* debba conformarsi genera una serie di approcci differenziati e isolati.

Quali sono gli attributi di un efficace programma di *risk management*? L'elenco che segue riporta alcune delle sue principali caratteristiche.

- **Una piattaforma ERM estesa all'intera azienda.** La gestione dei rischi deve essere attuata in modo uniforme, sulla base di priorità e *policy* valide per tutta l'impresa. Il metodo più efficace è rappresentato dall'adozione di una piattaforma comune da parte di tutte le *business unit* affinché i rischi possano non solo essere comunicati attraverso un modello unico, ma anche gestiti con tecniche omogenee. Una piattaforma generalmente accettata e utilizzabile a questo scopo è la COSO[1] ERM.

- **Gestione e misurazione costanti.** Il successo (o insuccesso) di un programma ERM dev'essere costantemente monitorato, con misurazioni specifiche del livello di funzionamento. Tali informazioni devono quindi essere consolidate a livello centrale per consentire un adeguamento dei parametri che controllano l'attività di *risk management.*

- **Coinvolgimento di tutti i dipendenti.** La comunicazione delle strategie e degli obiettivi di gestione dei rischi deve avvenire capillarmente in ogni parte dell'impresa. Per avere successo, un programma ERM deve coinvolgere la totalità dei dipendenti a tutti i livelli.

- **Controllo e visibilità del programma ERM a livello centrale.** Le *business unit* hanno la responsabilità di implementare una gestione dei rischi adeguata e conforme alle direttive centrali. Per garantirne l'attuazione è necessario un qualche tipo di autorità centrale che supervisioni le iniziative di *risk management* dell'intera azienda.

L'elemento **più importante** di qualsiasi programma di *risk management* è la **riduzione dei rischi a un livello accettabile.** Un'infrastruttura del tutto priva di rischi è, all'atto pratico, inattuabile. Persino la riduzione dei rischi a un livello estremamente basso può vincolare eccessivamente la crescita del business. Il livello di rischio che un'impresa è disposta ad accettare dipende da molti fattori, fra cui il potenziale impatto di un evento, il grado di tolleranza aziendale complessivo, le conseguenze per la crescita del business e lo scenario competitivo, per citarne solo alcuni.

Il paragrafo che segue illustra le aree critiche della sicurezza informatica e spiega come gestirne efficacemente i rischi.

Gestione dei rischi informatici

Qualsiasi programma completo di *risk management* dovrà necessariamente comprendere e gestire una vasta gamma di rischi aziendali, ma la sicurezza informatica rappresenta una delle sue aree più importanti. Rischi quali attacchi di *hacker*, malware e accessi non autorizzati a risorse e sistemi protetti richiedono efficaci piani di mitigazione per poter essere mantenuti a livelli accettabili.

Quando si prendono in esame i rischi alla sicurezza informatica che un'azienda deve fronteggiare, tre sono le aree principali da considerare:

Protezione degli asset. Come garantire che le preziose risorse aziendali siano sicure e protette, accessibili solo a persone debitamente autorizzate ed esclusivamente per gli scopi consentiti?

Continuità del servizio. Come garantire che i servizi forniti a dipendenti, partner e clienti siano sempre disponibili secondo necessità, senza alcuna perdita di qualità o deterioramento del livello di servizio?

Compliance. Come dimostrare agli *auditor* informatici interni o esterni che tutte le norme sono state effettivamente rispettate?

Dovrebbe risultare subito ovvio che queste aree sono strettamente correlate fra loro. La mancanza di un'efficace strategia per combattere i rischi che minacciano gli *asset* critici, ad esempio, comporta il rischio di una compromissione della continuità del servizio. E l'assenza di un programma in grado di gestire i rischi in queste due aree ridurrà la capacità dell'azienda di garantire la *compliance* normativa.

Esamineremo ora ciascuno di questi elementi che sono fondamentali per la creazione di strategie in grado di gestire tutti i rischi informatici nel loro complesso.

[1] Committee of Sponsoring Organizations (COSO) della Commissione Treadway.

Tutela degli asset

Una delle principali responsabilità dello staff informatico è la protezione delle risorse digitali confidenziali e riservate dell'azienda. Qualsiasi rischio di accesso o utilizzo non autorizzato di dati sensibili è per definizione inaccettabile. Di conseguenza, è assolutamente essenziale un'efficace infrastruttura che controlli l'accesso a tutte le risorse aziendali.

Diamo uno sguardo alle tipologie di *asset* e di risorse che necessitano di protezione. Alcune forse non risulteranno ovvie sin dall'inizio, ma i rischi che ne possono derivare in assenza di misure efficaci sono significativi.

Accesso alle applicazioni

L'accesso alle applicazioni aziendali è una delle aree più critiche, e richiede un'efficace infrastruttura di gestione. Il progressivo espandersi delle catene produttive e distributive delle imprese provoca una crescita costante del numero di clienti e partner commerciali che accedono alle applicazioni *on-line*, e di conseguenza la necessità di robuste misure di *access management*.

Internamente, le informazioni riservate e sensibili devono essere protette tramite una rigida regolamentazione degli accessi. Il personale informatico deve essere in grado di creare *policy* centralizzate che stabiliscano esattamente quali utenti possono accedere a ciascuna applicazione, le condizioni che consentono loro l'accesso e le operazioni che sono autorizzati ad eseguire.

Durante la valutazione delle soluzioni di *access management*, il personale informatico dovrà tenere presenti i seguenti requisiti per poter garantire il soddisfacimento delle esigenze presenti e future:

- Supporto di una vasta gamma di efficaci metodi di autenticazione
- *Policy* di *access management* basate su ruoli e su regole
- Supporto di *policy* di accesso dinamiche, basate sui contenuti di informazioni esterne (eventualmente anche in tempo reale)
- Possibilità di federazione delle identità in varie organizzazioni esterne
- Integrazione delle funzioni di autenticazione e autorizzazione con applicazioni *enterprise* pacchettizzate
- Supporto dell'integrazione diretta con applicazioni personalizzate
- *Policy* di *access management* uniformi su piattaforme e organizzazioni diverse
- Contenimento e delega dei diritti di super-utente di sistema
- Protezione delle funzioni di *auditing* e dell'integrità dei log
- *Reporting* e *auditing* robusti di tutti gli eventi di accesso

Web Services

Non solo l'accesso alle applicazioni Web, ma anche i Web service "sensibili" devono essere efficacemente protetti. Chiunque richieda un Web service dev'essere autenticato e autorizzato in modo molto simile agli utenti in carne ed ossa che tentino di accedere a un'applicazione *on-line*. Anche se tale processo viene svolto tramite l'uso di documenti XML, una protezione efficace è importante anche per i Web service, o forse persino di più.

File critici di sistema e database

Ogni team informatico tiene sotto controllo non solo le applicazioni aziendali sensibili, ma anche i sistemi e i file critici che risiedono al loro interno. Fra gli esempi di risorse da proteggere si annoverano repository Windows, file di sistema UNIX, elenchi di password e database aziendali di ogni genere. Per garantire che solo il personale debitamente autorizzato possa accedere a queste risorse è necessaria un'efficace infrastruttura di *access management* che dovrà consentire la creazione di *policy* centralizzate con cui vengano definiti gli utenti autorizzati ad accedere a ciascuna risorsa critica in base all'identità, al ruolo, alla divisione di appartenenza, e così via. Per garantire l'efficacia di questa operazione, è assolutamente indispensabile che il modello di *policy* sia flessibile.

Controllo dei servizi critici di sistema

Sebbene questa possa non essere considerata una "risorsa", la capacità di sospendere determinati servizi critici di sistema dev'essere tenuta rigorosamente sotto controllo. In particolare, l'interruzione accidentale o non autorizzata di tali processi (ad esempio la creazione dell'*audit log*) deve essere inclusa in qualsiasi programma completo per la gestione dei rischi informatici. Un'efficace piattaforma di *risk management* provvede ad assegnare in modo granulare i diritti di interruzione dei servizi di questo tipo.

Diritti di accesso in modalità di super-utente

In ogni ambiente IT, a un certo numero di amministratori vengono assegnati diritti di accesso illimitati in modalità super-utente (definita Root in UNIX e *Amministratore* in Windows). È raro, tuttavia, che ogni super-utente abbia realmente necessità di tutti i diritti di accesso che tale qualifica concede. Ciò si traduce in un problema di responsabilità e in un'esposizione dei sistemi, cioè nel rischio che vengano eseguite operazioni dalle conseguenze nefaste che non possono essere fatte risalire all'esecutore né annullate con facilità.

Un modo per ridurre tale rischio è costituito dall'adozione di una soluzione che provveda ad assegnare granularmente i diritti di super-utente in modo tale ciascun amministratore possa eseguire solo determinate operazioni su determinati sistemi. È altresì necessaria una identificazione individuale degli utenti per evitare le difficoltà che si creano quando tutti gli amministratori utilizzano lo stesso nome.

Infine dev'essere rigorosamente controllato l'accesso ai *log* di sistema. Se un singolo amministratore può non solo eseguire un'operazione sospetta, ma anche modificare i relativi file di registro, il rischio che una transazione fraudolenta non venga scoperta diventa reale. Di conseguenza, è importante poter disporre di un metodo centralizzato per la limitazione degli accessi (in modalità di sola lettura o di lettura/scrittura) a tutti i *log* di sistema. Allo stesso modo, la possibilità di interrompere il *logging* degli eventi deve essere concessa solo agli amministratori più fidati. Dato che la security nativa dei sistemi operativi spesso non offre il livello di granularità richiesto da questo tipo di protezione, si dovrà prendere in considerazione una soluzione di *access control* specializzata.

User Account

Un'ultima area di rischio riguarda l'utilizzo improprio di *user account* debitamente costituiti. Due sono gli aspetti che destano preoccupazione a questo proposito. Il primo si riferisce all'eventualità che un dipendente lasci l'azienda e che i suoi *account* e diritti di accesso non vengano tempestivamente disattivati. Quando ciò accade, il rischio di un utilizzo improprio di quegli *account* è elevato, soprattutto se il dipendente è stato sollevato dall'incarico contro la sua volontà.

Una seconda area di rischio riguarda l'esistenza di *user account* che rimangono inutilizzati per parecchio tempo. Ciò può avvenire per diverse ragioni, ma il caso più comune è quello di un utente che cambia ruolo in azienda senza che gli *account* relativi alle sue mansioni precedenti vengano eliminati. Di conseguenza, alcuni dipendenti possono essere proprietari di svariati *account*, alcuni dei quali non più validi. Questi *account* "orfani" creano un rischio di utilizzo improprio che deve essere tenuto sotto controllo. Un'efficace soluzione di *access management* contiene funzioni che analizzano l'intero ambiente alla ricerca di account non utilizzati di recente (dove la definizione di "recente" viene fornita a livello locale) e li chiudono.

Risorse residenti su mainframe

Durante la pianificazione di una strategia di *risk management* si dimentica spesso l'esistenza dei mainframe: un errore che può rivelarsi assai dispendioso. È importante che lo stesso livello di controllo degli accessi utilizzato per tutti i sistemi distribuiti sia disponibile anche per i mainframe che operano nel medesimo ambiente. Le soluzioni di questo tipo devono supportare *policy* basate su ruoli che identifichino gli utenti autorizzati ad accedere a risorse e applicazioni protette residenti su mainframe, nonché le condizioni in cui l'accesso verrà consentito.

Continuità del servizio

Per la maggioranza delle imprese, la disponibilità costante dei servizi *on-line* è letteralmente una questione di vita o di morte. Le società finanziarie perdono in media svariati milioni di dollari per ogni ora del giorno in cui i loro servizi non risultano accessibili. Lo stesso vale per le applicazioni e i servizi interni utilizzati dai dipendenti: se per qualsiasi motivo un dipendente non riesce a collegarsi, le perdite di produttività e di supporto ai processi di business possono essere disastrose. In breve, la disponibilità ininterrotta dei servizi IT è un imperativo commerciale e uno degli aspetti fondamentali della gestione dei rischi informatici.

Uno degli ostacoli principali alla continuità del servizio è rappresentato dalle minacce ai computer. Oggi gli utenti subiscono attacchi da parte di virus, *hacker* e applicazioni fraudolente spesso installate senza autorizzazione a loro insaputa. Collettivamente note come "malware," queste applicazioni possono eseguire una serie di attività che vanno da semplici azioni di disturbo a operazioni potenzialmente devastanti, come ad esempio la riconfigurazione di sistemi operativi e browser, il monitoraggio della posta elettronica, la registrazione e trasmissione di sequenze di tasti (password comprese), e l'accesso a dati riservati. L'elemento centrale di qualsiasi programma per la gestione dei rischi informatici deve quindi essere costituito da meccanismi di controllo efficaci in grado di contrastare virus e tentativi di intrusione di ogni genere.

Fra gli altri problemi ricordiamo il software fraudolento a carattere non virale (ad esempio, spyware e adware). Sebbene in genere meno distruttivi di alcuni virus, questi programmi possono ridurre notevolmente la produttività non solo del proprietario della macchina infetta, ma anche degli amministratori della security o del personale dell'Help Desk.

Un'altra importante area della sicurezza informatica è la gestione delle vulnerabilità di sistema. Di norma, quando viene pubblicatamente annunciata una vulnerabilità insieme alla relativa patch, la comunità degli *hacker* trova quasi immediatamente un modo per "sfruttarla". La tempestiva installazione dei *fix* su ciascuna macchina della rete è un'operazione essenziale, ma spesso assai difficile. In molti casi, per lo staff informatico non è neppure facile scoprire quali *patch* siano già state applicate a un determinato sistema, per non parlare dell'installazione in tempi rapidi dei nuovi *fix* su un gran numero di macchine. Queste vulnerabilità rappresentano un rischio assai significativo per la continuità dei servizi IT, e rendono quindi essenziale l'utilizzo di un metodo centralizzato e automatizzato per la registrazione, la gestione e l'installazione delle *patch*.

Conformità

L'ultimo elemento della gestione dei rischi informatici riguarda l'ottemperanza a varie normative di legge e di settore. La *compliance* è diventata un imperativo commerciale e una colonna portante delle strategie aziendali di *risk management*. I suoi requisiti toccano problematiche quali visibilità, sicurezza, disponibilità, *privacy* e trasparenza. Se un'impresa non affronta adeguatamente questi problemi rischia sanzioni pesanti, accompagnate da un calo di fiducia degli investitori e da una riduzione di valore dei suoi marchi.

Si noti che, in un certo senso, la *compliance* è semplicemente **uno dei risultati** di un buon programma di *risk management* attuato nelle altre due aree. In altre parole, l'esistenza di un programma efficace che mitighi i rischi alla protezione degli asset e alla continuità del servizio crea sostanzialmente le condizioni necessarie per il rispetto delle norme di sicurezza previste dalla maggior parte dei nuovi regolamenti.

La *compliance* normativa sta obbligando molte aziende a rivalutare (e in molti casi a migliorare notevolmente) *policy* e procedure di sicurezza interne. Sebbene le norme di queste leggi (ad esempio la Sarbanes-Oxley, la HIPAA e la Gramm-Leach-Bliley) differiscano spesso fra loro, l'unico elemento comune è rappresentato dalla necessità di *efficaci controlli interni.* Se un'azienda riesce a dimostrare di possederli, può essere pressoché certa di riuscire a ottemperare alle norme di sicurezza di qualsiasi legge.

Vediamo cos'è un meccanismo di controllo interno e perché è così importante per creare procedure di gestione dei rischi robuste ed efficaci.

Un meccanismo di controllo interno è una serie di processi in grado di garantire il buon esito di una pratica o di una transazione di business. Nel caso della sicurezza, spesso garantisce che solo il personale debitamente autorizzato abbia accesso a informazioni, applicazioni e risorse riservate.

La maggioranza delle aziende dispone di meccanismi di controllo interni di vario tipo che vengono utilizzati nel tentativo di creare un ambiente sicuro. Sfortunatamente questi controlli sono in genere manuali, costituiti da documenti e iter approvativi, e lasciano spazio a numerose possibilità di errore. Il segreto di una *compliance* sostenibile sta nell'*automazione dei controlli di sicurezza interni*. Oltre ad essere l'unico modo per rendere gestibili i costi della *compliance*, ciò può anche consentire notevoli aumenti di efficienza (cioè riduzioni di costo) nella gestione della sicurezza e dell'Help Desk. (Nota: Per maggiori informazioni sul miglioramento dell'efficienza nell'area della *security management* si rimanda al white paper "Ridurre i costi di gestione della sicurezza informatica", disponibile sul sito ca.com).

L'area in cui l'automazione dei controlli di sicurezza assume la massima importanza è la gestione degli utenti e dei loro accessi alle risorse aziendali protette – ovvero la gestione delle identità degli utenti e dei diritti di accesso loro concessi.

L'automazione dei meccanismi per il controllo dell'identità e dei diritti di accesso presenta tre aspetti importanti che, sebbene non unici, costituiscono l'essenza di qualsiasi programma di questo tipo:

1. *Policy* centralizzate che controllino automaticamente qualunque accesso a risorse protette di ogni genere all'interno dell'impresa. Questo è il nucleo centrale di qualsiasi efficace sistema di controllo della privacy, per cui rappresenta un elemento essenziale per ottemperare alle norme di molte nuove leggi.
2. Allocazione (e de-allocazione) automatica degli *account* e dell'accesso alle risorse secondo *policy* definite a livello centrale, generalmente basate sul ruolo o sulla posizione di ciascun utente in seno all'impresa.
3. Automazione delle attività di raccolta, filtraggio, visualizzazione e analisi di tutti gli eventi ambientali riguardanti la sicurezza. In questo modo l'*auditing* della security diventa non solo possibile, ma anche scalabile.

Quando vengono implementate capillarmente all'interno dell'azienda, queste funzioni possono migliorare enormemente la *compliance* e renderla sostenibile attraverso l'automazione di tutti i controlli di sicurezza interni.

(Nota: Per maggiori informazioni sulla creazione di un efficace ambiente di gestione della compliance normativa si rimanda al white paper "The Role of Security Management in Regulatory Compliance", disponibile sul sito ca.com).

Soluzioni per la gestione della sicurezza informatica

Nei paragrafi precedenti di questo documento sono state illustrate alcune aree fondamentali della sicurezza informatica, prendendo in esame soluzioni tecnologiche in grado di contribuire alla riduzione e al controllo dei relativi rischi. I due settori più importanti a questo riguardo sono la gestione delle identità e degli accessi, oltre alla gestione integrata delle minacce.

Gestione delle identità e degli accessi

In quasi tutte le aziende le identità e i privilegi di accesso degli utenti sono un elemento essenziale della strategia di e-business. Dietro quelle identità stanno infatti i dipendenti, i fornitori, i partner, i clienti e tutti coloro che portano avanti i diversi aspetti dell'attività operativa. La gestione delle identità è costituita da una serie di processi e sistemi che puntano a stabilire chi possa accedere a determinate applicazioni, database e piattaforme, e in quali condizioni debba essere consentito tale accesso. Le domande fondamentali cui deve rispondere la componente "identità e accessi" di un programma di *security management* sono:

- Chi ha accesso a cosa?
- Cosa è stato fatto?
- Quando è stato fatto?
- Come è possibile dimostrarlo?

Rispondendo a queste domande, le imprese possono ridurre in modo efficace i rischi alla sicurezza informatica, tutelare risorse vitali, semplificare le operazioni di business e ottenere la conformità normativa. Il grafico che segue illustra le principali componenti di una piattaforma efficace per la gestione di identità e accessi, e mostra come esse interagiscano per ridurre il complesso dei rischi alla sicurezza.

Le principali funzioni da integrare per ottenere un'efficace gestione di identità e accessi sono:

- **Amministrazione delle identità.** Consente la creazione e l'amministrazione di identità e di informazioni sul profilo degli utenti.
- **Provisioning.** Assegna a ciascun utente gli *account* e i diritti di accesso alle risorse aziendali adeguati al suo ruolo, eliminandoli poi al momento opportuno (ad esempio quando l'utente lascia l'azienda).
- **Gestione degli accessi.** Contribuisce a garantire l'integrità delle informazioni e delle applicazioni aziendali attraverso la prevenzione degli accessi non autorizzati. Un efficace servizio di *access management* deve proteggere l'accesso non solo alle applicazioni Web, ma anche ad applicazioni enterprise, sistemi, servizi critici di sistema, file e repository sensibili.
- **Monitoraggio/Auditing.** Facilita la registrazione e il *reporting* degli accessi, per ridurre il rischio di una mancata identificazione dei problemi di sicurezza, garantire la *compliance* normativa e, se necessario, consentire l'esecuzione di analisi a *posteriori* per fini legali.

Durante la valutazione di soluzioni di *identity management* si dovrà verificare che queste componenti siano strettamente integrate e creino una piattaforma unificata a livello funzionale. Diverse sono le ragioni che rendono necessaria una piattaforma integrata. Innanzitutto, alcuni concetti fondamentali (ad esempio, i ruoli degli utenti, l'appartenenza o meno a gruppi e le *policy* di accesso) sono comuni a tutte le componenti e trovano applicazione ovunque. Infatti, se ciascuna componente definisse un "ruolo" in modo diverso, sarebbe praticamente impossibile monitorare i diritti di accesso di quel ruolo all'interno degli elementi che costituiscono la piattaforma di *compliance*. Allo stesso modo, è essenziale che la componente di *auditing* e monitoraggio possa consentire la visualizzazione dell'intera infrastruttura, indipendentemente dal luogo in cui ha origine un evento. Senza questo livello di integrazione nel monitoraggio non sarebbe possibile avere una visione unificata di tutto l'ambiente. Infine, una piattaforma integrata semplifica enormemente la gestione e aumenta la sicurezza. Le componenti non integrate sono infatti intrinsecamente più complesse, e di conseguenza più difficili da gestire e maggiormente soggette a produrre "falle" nella security.

Gestione integrata delle minacce

Sul mercato esistono letteralmente centinaia di prodotti che affermano di poter eliminare dall'ambiente aziendale vari tipi di malware e spyware. Alcuni sono migliori degli altri; tuttavia, l'adozione di soluzioni punto-a-punto nelle diverse aree di un programma di *threat management* può essere problematica. Le soluzioni possono infatti essere in conflitto fra loro, e in genere richiedono una duplicazione degli sforzi per poter essere tutte gestite efficacemente. Hanno procedure di installazione e interfacce amministrative indipendenti, meccanismi e tempi di aggiornamento diversi, e tutto ciò può aumentare i costi complessivi di gestione dell'ambiente IT. Ma, cosa ancora più importante, prodotti fra loro indipendenti non offrono il livello di integrazione e omogeneità funzionale necessario per combattere gli attacchi di malware oggi più diffusi, in continua evoluzione e sempre più sofisticati.

La gestione della security non si occupa solo delle comuni minacce rappresentate dal malware, ma anche di vulnerabilità di sistema note (già pubblicate) o potenziali. Spesso l'*exploit* di una vulnerabilità annunciata pubblicamente è disponibile già pochi giorni, o a volte addirittura poche ore dopo l'annuncio. La gestione e l'installazione dei *fix* su un gran numero di macchine rappresentano un problema complesso, e un ritardo può avere conseguenze disastrose. Ecco perché è importante disporre di un meccanismo automatizzato e uniforme di gestione delle *patch* in tutto l'ambiente. Tale meccanismo comprende tecniche di determinazione delle priorità, gestione del processo di installazione e verifica dello stato delle *patch* su tutti i sistemi critici.

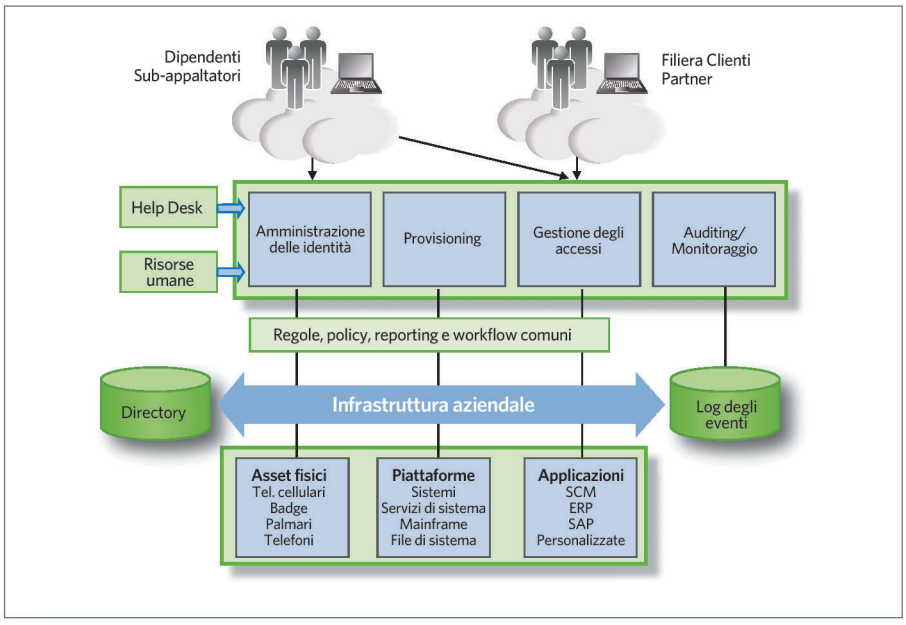

Figura 3. Una piattaforma IAM

Durante la valutazione di soluzioni per la gestione delle minacce si tenga presente che le seguenti funzioni svolgono un ruolo importante nel ridurre i rischi alla sicurezza informatica:

- Integrazione di antivirus, anti-spyware e meccanismi di *intrusion* detection in un'unica soluzione omogenea
- Gestione e visualizzazione centralizzate dello stato di virus e spyware in tutto l'ambiente
- Ampiezza della gamma di malware gestibile (virus, spyware, spamming, adware, cavalli di Troia, furti di sequenze di tasti, minacce P2P, *hacker* e attacchi distribuiti di tipo "denial-of-service")
- Funzioni di allerta (allarmi) e *logging* flessibili che consentano a utenti e amministratori di identificare i problemi in tempo reale. I meccanismi di allerta devono poter essere configurati in base alle esigenze di ciascun ambiente informatico locale.
- *Policy* di configurazione dinamiche che consentano ai meccanismi protettivi di rispondere in tempi rapidi alle variazioni di profilo delle minacce
- Funzioni di quarantena che permettano di isolare raidamente gli attacchi al fine di proteggere risorse di valore.

Riepilogo

Un efficace programma di *risk management* rappresenta un elemento essenziale di qualsiasi strategia ERM ben congegnata. Per sua stessa natura, la sicurezza informatica comporta una serie di rischi che devono essere affrontati in modo olistico e completo al fine di garantire la protezione degli *asset* critici dell'azienda e la disponibilità ininterrotta dei servizi di business. Infine, una buona gestione dei rischi informatici può costituire la base di un programma di *compliance* normativa efficiente ed efficace.

La tabella che segue riassume alcuni dei principali elementi di ciascuna area del *risk management* che devono essere presi in considerazione durante lo sviluppo di un programma completo per la gestione dei rischi informatici.

L'approccio più efficace alla protezione degli asset aziendali è costituito da una piattaforma integrata di *identity and access management*. Attraverso questo tipo di soluzione è possibile controllare, mediante efficaci *policy* di sicurezza, l'utilizzo di tutte le risorse critiche e registrare/monitorare tutti i tentativi di accesso.

Il metodo migliore per garantire la continuità del servizio è invece una soluzione completa e integrata di *threat management*. Al contrario, l'impiego di soluzioni punto-a-punto di *vendor* diversi spesso si rivela un modo poco efficace per combattere questi rischi.

COSA PROTEGGERE	
PROTEZIONE DEGLI ASSET	Applicazioni Web Web services Applicazioni enterprise Accesso ai sistemi operativi File critici di sistema e database Controllo dei servizi di sistema Diritti di accesso in modalità super-utente Audit log di sistema User account "orfani" Risorse su mainframe
DA COSA PROTEGGERSI	
CONTINUITA' DEL SERVIZIO	Virus Spamming Tentativi di intrusione Spyware Attacchi di tipo "denial of service" Furto di sequenze di tasti Altro malware Vulnerabilità di sistema
RISULTATO	
COMPLIANCE NORMATIVA	Efficaci controlli interni Compliance dimostrabile

Infine, un efficace deployment di soluzioni di questo tipo può semplificare enormemente il processo, spesso difficile, di conformità con le normative di legge e di settore. La presenza di meccanismi di controllo interni migliori e automatizzati può non solo avere un'influenza significativa sull'efficienza e sui costi del personale informatico, ma anche incrementare la *performance* dell'azienda nel suo complesso.

Le soluzioni CA per la gestione della sicurezza

CA, leader in questo settore, offre una serie integrata di soluzioni di *security management* che comprendono *identity & access management* (per gestire efficacemente utenti e accessi) e *threat management* (per combattere la complessità delle minacce odierne). Le sue soluzioni consentono di gestire efficacemente la sicurezza informatica attraverso una piattaforma completa ed integrata che aiuta a determinare e a controllare chi abbia accesso alle risorse aziendali critiche, a stabilire cosa stia accadendo nell'ambiente e a garantire che le decisioni giuste vengano prese al momento giusto, rendendo così molto più semplice ed economica anche la conformità normativa.

La piattaforma CA per la gestione della sicurezza comprende una serie di prodotti che, insieme, formano una *suite* integrata all'avanguardia nel settore.

Identity and access management

Gestione delle identità e *provisioning*

CA® Identity Manager. CA Identity Manager fornisce una piattaforma di gestione integrata che automatizza la creazione, la modifica e la sospensione delle identità degli utenti e il loro accesso alle risorse aziendali, aumentando il livello di sicurezza e *compliance* e riducendo contemporaneamente i costi amministrativi e migliorando il contesto di utilizzo per gli utenti stessi. Inoltre, Identity Manager fornisce servizi di *auditing* utilizzabili da parte di revisori sia interni che esterni per stabilire se le pratiche aziendali di concessione dei diritti siano tenute sotto controllo e garantiscano a tutti gli effetti la riservatezza dei dati. Identity Manager è più che un semplice sistema di *provisioning*: prendendo atto della progressiva scomparsa dei tradizionali confini dell'impresa, offre una soluzione unificata che consente la gestione di gruppi di utenti sempre più vasti e diversificati (dipendenti e utenti esterni tradizionali come clienti e business partner).

Gestione degli accessi

***e*Trust® SiteMinder®.** Le avanzate funzioni di security basate su *policy*, la capacità gestionale, la comprovata affidabilità e la scalabilità di *e*Trust SiteMinder supportano il rapido sviluppo, *deployment* e gestione di sofisticati sistemi software di *web security*, consentendo la capillare distribuzione di informazioni e applicazioni essenziali a dipendenti, partner, clienti e altri utenti dell'azienda.

***e*Trust® TransactionMinder®.** Simile nell'architettura ad *e*Trust SiteMinder, *e*Trust TransactionMinder consente una gestione sicura, centralizzata e basata su *policy* di autenticazioni e autorizzazioni per l'utilizzo dei Web service. Integrandosi con le piattaforme di Web service standard, fornisce un controllo granulare degli accessi ai documenti XML richiesti nelle diverse fasi di una transazione commerciale.

***e*Trust® Access Control.** Implementa una *policy* di accesso uniformemente efficace su piattaforme e sistemi operativi distribuiti. Questa soluzione determina, sulla base di *policy*, chi possa accedere a determinati sistemi, file e applicazioni, per quali scopi e in quali momenti, consentendo inoltre la gestione dei privilegi di super-utente a garanzia di una maggiore sicurezza amministrativa.

***e*Trust® CA-ACF2 e *e*Trust® CA-TopSecret Security.** *e*Trust CA-ACF2 Security ed *e*Trust CA-Top Secret Security consentono una condivisione controllata dei mainframe e dei relativi dati, prevenendo nel contempo la distruzione, la modifica, la divulgazione e/o l'utilizzo improprio (accidentali o deliberati) delle risorse informatiche. Consentono di controllare chi utilizza le risorse e forniscono le informazioni necessarie per un efficace monitoraggio delle *policy* di sicurezza. I tentativi di accesso non autorizzato vengono automaticamente respinti e registrati. È inoltre possibile registrare anche qualsiasi utilizzo non consentito di risorse sensibili, ai fini di un riesame successivo.

Gestione delle informazioni sulla security

***e*Trust® Security Command Center.** è uno strumento essenziale per gestire in modo proattivo le complessità dell'ambiente aziendale di security. La sua tecnologia consente agli amministratori di visualizzare in tempo quasi-reale possibili minacce ai sistemi finanziari o di altro tipo, di identificare vulnerabilità presenti nei sistemi finanziari e di fornire al responsabile della security o della *compliance* una visione integrata degli asset informatici (ad esempio contabilità o paghe e contributi).

***e*Trust® Audit.** *e*Trust Audit raccoglie le informazioni di auditing sui sistemi e sulla sicurezza da ogni parte dell'impresa e le memorizza in un database centrale, semplificandone l'accessibilità e l'utilizzo a scopo di reporting e consolidando dati provenienti da server UNIX e Windows NT, nonché da altri prodotti CA. Gli amministratori dispongono così di informazioni di monitoraggio, allerta e *reporting* riferite all'attività degli utenti su tutte le piattaforme.

***e*Trust® Vulnerability Manager.** *e*Trust Vulnerability Manager offre servizi e tecnologie avanzate che riuniscono valutazione delle vulnerabilità, applicazione delle *patch* ed eliminazione dei problemi di configurazione in un'unica soluzione facilmente installabile, dotata di un'interfaccia utente di tipo Web.

Threat management

CA Integrated Threat Management. La *suite* Integrated Threat Management r8 unisce i prodotti all'avanguardia *e*Trust PestPatrol® Anti-Spyware ed *e*Trust Antivirus in un'unica consolle di gestione, aumentandone l'efficienza attraverso un *agent*, una struttura di *logging* e una serie di tool di aggiornamento comuni. La *suite* notifica, individua, analizza e risolve un'intera gamma di minacce, attacchi e codici fraudolenti (virus, worm, spyware, furti di sequenze di tasti e cavalli di Troia) per ridurre al minimo rischi, interruzioni di servizio e perdite di produttività. Uno dei vantaggi fondamentali è la sua architettura flessibile, modulare, aperta ed estensibile che consente agli utenti di scegliere fra più prodotti di sicurezza CA in base alle esigenze aziendali.

eTrust® Antivirus. *e*Trust Antivirus è una soluzione completa di difesa dai virus che contribuisce a proteggere tutti i punti dell'ambiente aziendale, dal perimetro ai palmari. Aiuta a gestire la minaccia rappresentata dai virus attraverso un'unica soluzione completa che elimina le infezioni, semplifica e automatizza l'amministrazione e il processo di aggiornamento.

eTrust® PestPatrol Anti-Spyware. Le soluzioni *e*Trust PestPatrol Anti-Spyware forniscono un'efficace protezione da spyware, adware e altre minacce non virali. Gli attacchi di questo tipo, in rapida crescita, provocano un brusco rallentamento di PC e reti, aumentano le chiamate all'help desk e introducono nuovi e pericolosi rischi per la sicurezza e la privacy, rendendo vulnerabili le informazioni riservate. *e*Trust PestPatrol Anti-Spyware offre una protezione totale all'azienda, individuando ed eliminando lo spyware in tempo reale, semplificando la gestione e fornendo aggiornamenti sulle ultime minacce emerse per consentire una navigazione in Internet senza problemi. CA consente di scegliere il livello di protezione più adatto a ogni azienda: un singolo PC, una piccola attività commerciale o un'intera rete.

eTrust® Secure Content Manager. *e*Trust Secure Content Manager è una soluzione integrata di sicurezza dei contenuti basata su *policy*. Protegge le aziende da minacce quali spamming, virus, perdita di informazioni riservate e utilizzo improprio di Internet. Garantisce la continuità dell'attività operativa, mitiga i rischi, simplifica la gestione, riduce tempi e costi di amministrazione, migliora la produttività dei dipendenti, contribuisce alla conformità normativa e ottimizza l'uso delle risorse IT.

Quality System
Quality Endorsed Company
ISO 9001 Lic. 2443

MP295210206
BPP183131 ITARSMRC-WP.05.06