

DIRECTION

Reportec

DOSSIER DI SOLUZIONI SERVIZI E TECNOLOGIE ICT

17

Direction Reportec - Volume IV n.17 febbraio - marzo 2006 bimestrale - Spedizione in A.P. - 45% - art. 2 comma 20/B legge 662/96 - Milano

Security

- **IL REPORT: ICT Security**
- **Business Continuity per il Data Center**
- **La sicurezza per il business**

Server e Storage

- **Flessibilità e affidabilità per i server aziendali**
- **Crescono i servizi WAFS**

Communication

- **L'emergenza dello standard SIP**
- **Un piccolo grande PBX per le PMI**

Software Solutions

- **L'affermazione di XML per i servizi Web**
- **Il Corporate Performance Management**

Networking

- **Il networking è sempre più veloce e intelligente**
- **I vantaggi di una rete convergente**



Indice

▷ Una sicurezza sempre più globale	3
▶ IL REPORT: ICT Security 2006	4
▶ Sempre più appliance nel futuro di Check Point	14
▶ Emerson Network Power ridefinisce la Business Continuity	16
▶ Un approccio strutturato per proteggere il business	18
▶ Sicurezza on demand per Internet Security Systems	20
▶ Le soluzioni RSA Cyota contro il phishing e le frodi online	22
▶ Symantec dichiara guerra a spyware e adware	24
▶ Il sistema informativo Dell	26
▶ EMC per la gestione proattiva dell'infrastruttura ICT	28
▶ Nuovi scenari per il Dynamic Data Center	30
▶ I server Integrity di HP sempre più "adaptive"	32
▶ I servizi WAFS per la comunicazione enterprise	34
▶ Da HP nuove soluzioni per il back up di file e data base	36
▶ Nuove tecnologie Intel per mobility e digital home	38
▶ Le soluzioni Microsoft per la gestione dello storage	40
▶ Per StorageTek un "matrimonio" orientato alle soluzioni	42
▶ Terasystem ottimizza il backup dei database Oracle	44
▶ I Managed Communications Services di Alcatel	46
▶ Nella Business Communication si diffonde lo standard SIP	48
▶ Cisco Systems unifica la comunicazione	50
▶ L'IP trasforma il modo di comunicare delle PMI	52
▷ I rischi trascurati dei documenti cartacei	53
▶ La business communication adotta XML per i servizi Web	54
▶ La SOA perno dell'innovazione del laboratorio IBM Tivoli	56
▶ Verso il Corporate Performance Management	58
▶ L'Università di Verona gestisce rete e risorse con CA	60
▶ Più vicina la rete ProCurve di prossima generazione	62
▶ I molti vantaggi di una rete convergente	64
▷ Quando la sicurezza diventa abilitante invece che un obbligo	65

Una sicurezza sempre più globale

Nel corso del 2005 si è assistito a una profonda modifica del concetto di sicurezza. Sempre più si è in presenza di una chiara percezione da parte delle aziende dell'importanza di un approccio complessivo, in cui si parte dall'oggetto che si vuole proteggere, e cioè il dato, per poi analizzare cosa possa e debba essere fatto per realizzare nel concreto questo obiettivo.

Ne è derivato un approccio sempre più pervasivo a livello di sistema ICT, dove la protezione e la sicurezza spaziano dall'assicurare l'inaccessibilità dei dati ai non autorizzati sino al garantirne la protezione, l'inalterabilità, la disponibilità nel tempo e così via.

In pratica, il concetto "sicurezza" si è esteso dalla pura protezione dagli accessi indesiderati sino a comprendere la sicurezza per quanto concerne la disponibilità del dato e alle attività e procedure che servono perchè ciò possa essere ottenuto a livello di sistema informativo e di rete.

Quello che viene legittimo chiedersi è se, una volta che a livello aziendale si decide di affrontare in modo globale il problema, intendendo con questo sia la parte attinente al sistema informativo che quanto concerne l'infrastruttura di rete estesa sino all'utenza più periferica, presso sedi fisse o di tipo mobile, vi sia da parte dei fornitori la disponibilità di soluzioni adeguate, possibilmente integrate.

La situazione appare da questo punto di vista confortante.

Da parte dei fornitori di reti trasmissive sono state rilasciate, nel corso del 2005, soluzioni che permettono di distribuire ai diversi livelli di una rete le funzioni necessarie per proteggere gli accessi, verificare gli utilizzatori, incapsulare le aree infette, in modo non solo da attuare un controllo perimetrale, ma bensì un controllo potenzialmente realizzabile in ogni elemento e livello della rete, a partire dalla congruenza del

terminale usato per accedervi sino a quanto inerente un'applicazione centrale.

A questo si abbina il fatto che una politica di protezione del dato da accessi indesiderati è integrato anche in soluzioni e architetture ILM (Information Lifecycle Management), che assicurano la disponibilità nel tempo del dato stesso. Proteggerlo, se poi il dato non è disponibile quando serve, servirebbe infatti a ben poco.

In sostanza quindi, sia a livello di fornitore che di utilizzatore, è stato metabolizzato il fatto che la sicurezza non è un concetto localizzabile, ma che deve essere preso in considerazione sin dalla fase di progettazione di un sistema Ict e relative applicazioni.

Ad esempio, quando si pensa ad una applicazione che supporti una maggior mobilità aziendale andrebbe in parallelo considerato che più si amplia la possibilità di connettività, più aumentano le possibilità di attacchi alle applicazioni ed al sistema informativo aziendale, con il rischio che un'applicazione sviluppata per aumentare la flessibilità e la produttività ottenga invece il risultato opposto.

Prima di pensare all'applicazione va quindi analizzato se la rete è predisposta per far fronte ad eventuali attacchi e cosa costa in termini economici.

In termini di rete, va poi considerato che le soluzioni convergenti dati/fonia basate su IP implicano che gli attacchi alla sicurezza della rete e un suo funzionamento degradato impattano sull'intero spettro di modalità di interazione tra dipendenti e clienti.

In sostanza, quanto più si adottano tecnologie ed applicazioni aperte, tanto più si fanno stringenti le esigenze di una sicurezza estesa in modo pervasivo all'intero sistema ICT aziendale.

Come al solito, ogni medaglia ha il suo rovescio. *



Giuseppe Saccardi

IL REPORT: ICT Security 2006

Un'analisi delle strategie, tecnologie, soluzioni, servizi, problematiche e architetture per la sicurezza in un report di oltre 600 pagine

Il mercato della sicurezza cresce spinto soprattutto dalla necessità di conformarsi alle normative vigenti. Per molte imprese questo significa dotarsi degli strumenti atti a dimostrare la compliance, prima ancora che a conseguire un'effettiva protezione. Molte altre, peraltro, hanno colto l'attimo e impostato una corretta politica d'investimenti per trasformare un obbligo in un'opportunità.

C'è da dire che è si è ormai diffusa la consapevolezza di quanto sia importante il dato e del fatto che l'informazione rappresenta un asset fondamentale per l'impresa. Ma per molte imprese, l'IT rimane un costo e l'adeguamento alle leggi consente ai responsabili dei sistemi informativi di trovare fondi. Fondi che possono essere impiegati anche per sviluppare nuovo business, abilitando, per esempio nuovi servizi alla clientela.

In ogni caso una protezione è necessaria, anche perché si sono innalzati gli obiettivi degli attacchi: agli hacker, che agiscono per spirito goliardico e sfida, si sono aggiunti i cracker, veri e propri professionisti che operano per tornaconto personale.

La Rete è spesso associata al Bronx degli anni peggiori, ma in realtà anche un alto livello di "pericolo" e l'indiscussa costante presenza di attacchi e mine vaganti non necessariamente comporta un rischio elevato per l'impresa. Il rischio, infatti, è dato dal prodotto della probabilità di subire un attacco per l'ammontare del danno che un attacco andato a buon fine potrebbe determinare. Il risultato è un valore gestibile. Troppo spesso, invece, si confonde la minaccia con il rischio e si rincorre un obiettivo di sicurezza totale che non esiste, a meno

di chiudere completamente l'impresa. Ma nel senso di fallire, perché anche senza impiegare, per assurdo, l'ICT, sussisterà comunque il pericolo che un dipendente disonesto o semplicemente disattento possa portare al di fuori dell'azienda informazioni riservate.

- Il rischio e la governance della sicurezza

Gestire il rischio significa impostare un processo ciclico che comprende appunto l'analisi del rischio, inclusa la vulnerability assessment, per poi stabilire quale sistema di sicurezza possa meglio ridurre il rischio a un livello accettabile per l'impresa. La risk analysis non a caso è una fase fondamentale della corporate governance ed è quindi evidente dove sorgono le opportunità: approcciare correttamente la sicurezza permette di impostare una gestione accurata dell'impresa, maturando benefici che possono essere trasferiti al business. È sovente il caso che un'analisi del rischio faccia emergere il reale valore di talune attività, consentendo come minimo di migliorare i processi operativi grazie a una rinnovata focalizzazione sulle strategie aziendali.

Altro punto di collegamento tra sicurezza, ICT e business è l'identity management. Passo fondamentale, soprattutto nelle medio-grandi imprese, per la gestione del personale e dei processi aziendali, la l'identity management è alla base dell'ottimizzazione dei processi organizzativi. La sua importanza, inoltre, aumenta con la diffusione del concetto di azienda estesa: un'azienda sempre più distribuita, magari anche radicata nel territorio, ma non chiusa nella propria sede bensì attiva presso clienti

e fornitori. Maggiore è l'apertura, più ampi i servizi verso la clientela e più è rilevante la capacità di gestire le identità di tutte le figure coinvolte nei processi.

Laddove l'unico rischio accettabile è quello di perdere il minor tempo possibile o nullo per mantenere attivo il servizio (si pensi alle telecomunicazioni), la soluzione si chiama business continuity e disaster recovery: cioè proteggerlo e prevenirlo il più possibile, ma mi tutelo affinché in caso d'incidente io abbia un'infrastruttura di backup e una procedura di ripristino immediato o quasi di tutto il sistema.

- **Prevenire ma pronti alla cura**

Il bisogno di prevenzione e la capacità di risposta rapida agli incidenti diventano una combinazione che porta alla gestione della sicurezza. È questo il paradigma attuale dell'ICT Security, che va quindi affrontata in maniera strategica e strutturata con un sistema olistico, assumendo un significativo orientamento al business.

Tutti i principali fornitori di soluzioni si stanno orientando in questo senso e le molte acquisizioni dell'ultimo anno dimostrano il processo di consolidamento in corso. Probabilmente continuerà ancora, ma già si delineano i protagonisti del futuro, laddove storici player del settore hanno ampliato considerevolmente la propria offerta, aggiungendo al software e talvolta soppiantandolo in buona parte appliance tese, da un lato, ad accrescere le prestazioni, dall'altro a semplificare l'amministrazione.

Quest'ultimo è un punto cruciale e su tale fronte ci sono stati significativi miglioramenti. In particolare, sono stati sviluppati nuovi motori di correlazione, che potessero mettere in relazione eventi apparentemente indipendenti, ma in realtà sintomo dello stesso male. L'accelerazione delle nuove minacce ha portato alla "0 day" threat: cioè l'attacco sferrato il giorno zero, quello in cui la vulnerabilità che l'attacco stesso sfrutta è stata annunciata. La "0 day" protection c'è già, ma significa protezione allo stato puro ed è una sfida per molti vendor, taluni dei quali ancorati a un approccio di tipo reattivo.

- **Lo stato dell'arte di architetture, soluzioni e servizi**

- **3COM**

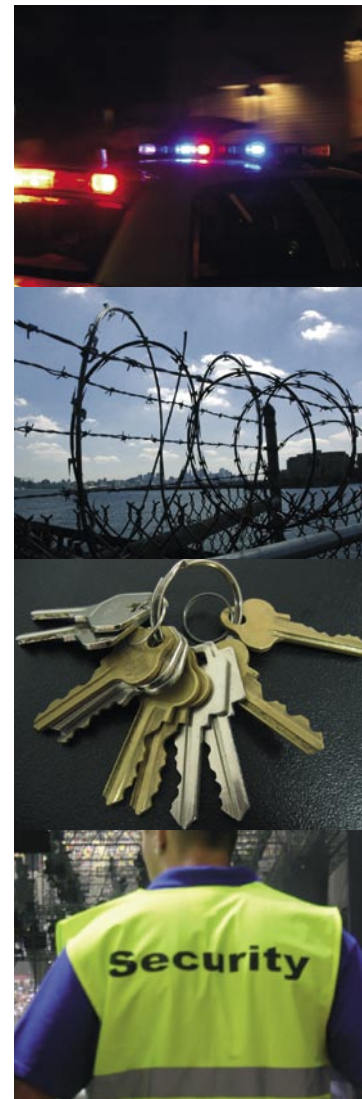
Nota specialista delle reti, 3Com ha da sempre avuto massima attenzione per la sicurezza e, negli anni, ha sviluppato soluzioni innovative, quali, per esempio, l'embedded firewall, il personal firewalling direttamente integrato sulla scheda di rete. Con l'acquisizione di TippingPoint, ormai divisione 3Com a tutti gli effetti, la società californiana è balzata sul palco dei protagonisti del settore, con un'offerta appunto basata sulle soluzioni contraddistinte dalla tecnologia TippingPoint Intrusion Prevention Systems.

Quest'ultima si fonda sulla Threat Suppression Engine (TSE), costituita da un processore di rete e da una serie di ASIC sviluppati da TippingPoint, che effettua i controlli utilizzando praticamente tutti i tipi di filtering impiegati per il rilevamento delle intrusioni, più precisamente quelli basati su: signature, vulnerabilità, anomalie dei protocolli e del traffico.

Le appliance TippingPoint non penalizzano le prestazioni, grazie ovviamente all'utilizzo di acceleratori hardware, per realizzare operazioni come IP defragmentation, riassemblaggio di flussi TCP, analisi statistiche, traffic shaping, blocco dei flussi, tracking dello stato dei flussi e analisi ad application-layer per oltre 170 protocolli di rete. Questo consente, a detta dei responsabili 3Com, di fornire protezione in tre ambiti fondamentali: application, infrastrutture e performance.

Punto di forza del TippingPoint IPS è poi il servizio Digital Vaccine. Appena viene annunciata una vulnerabilità o un virus (o se ne raccoglie traccia nelle comunità di hacker), il team di ricerca e sviluppo di TippingPoint sviluppa il "vaccino" fornisce un patching virtuale delle vulnerabilità e una protezione immediata dalle minacce di ultima generazione. Il servizio Digital Vaccine, quindi, aggiorna automaticamente gli IPS TippingPoint.

Completa l'offerta una gamma di firewall e filtri per la protezione del perimetro di rete.





• ALADDIN

Aladdin è impegnata nel fornire servizi e soluzioni di sicurezza indirizzati a proteggere le risorse digitali, realizzare applicazioni di e-business sicure e garantire la protezione dei contenuti digitali durante la loro creazione, distribuzione e utilizzo. L'offerta Aladdin è organizzata in due aree principali: le soluzioni software HASP per il Digital Rights Management (DRM) e quelle per la sicurezza delle informazioni a livello enterprise che comprendono le soluzioni di autenticazione eToken e per la sicurezza integrata dei contenuti eSafe.

HASP è una suite di soluzioni hardware e software indirizzata in particolar modo agli sviluppatori, che coniuga funzionalità per la protezione del software e della proprietà intellettuale con opzioni indirizzate al licensing e alla distribuzione sicura e controllata. La gamma comprende soluzioni adatte per singolo utente, per la protezione e il licensing del software utilizzato in ambienti di rete enterprise, per la creazione di copie di prova delle applicazioni e per la protezione dei file HTML.

eToken è la soluzione Aladdin che risponde alle esigenze di autenticazione sicura, gestione delle password e portabilità delle credenziali digitali. Si tratta di una smart card alloggiata su interfaccia USB e di dimensioni estremamente ridotte che consente, di gestire l'autenticazione memorizzando in modo sicuro sul token: password, chiavi PKI, certificati digitali e altre credenziali personali. eToken è anche integrabile con soluzioni di rilevamento di prossimità, riunendo funzionalità di accesso fisico e logico in un unico dispositivo.

Le soluzioni di Secure Content Management eSafe si avvalgono della tecnologia brevettata NitroInspection che è stata sviluppata per fornire prestazioni elevate ed effettuare un'analisi completamente "on-the fly". La protezione integrata di eSafe interviene a più livelli: anti-virus proattivo e basato su firma, exploit protection, controllo e-mail, filtri Web/URL, filtraggio delle applicazioni, gestione dello spam, blocco per gli spyware. eSafe è disponibile anche in versione appliance.

• ALCATEL

L'approccio alla sicurezza di Alcatel ha le sue basi nella considerazione che la "Sicurezza" è un concetto globale, che deve permeare un'azienda in tutte le sue componenti, siano esse applicative che di accesso o di comunicazione e essere distribuita funzionalmente a livello dell'intero sistema ICT.

Alle esigenze del mondo pubblico e privato Alcatel risponde con un approccio organico, strutturato a livelli, che adotta un'ampia gamma di tecnologie proprie o sviluppate con partner, si basa su metodi analitici e progettuali che esplorano le diverse problematiche inerenti la sicurezza, nonché sulla disponibilità di centri operativi dedicati alla gestione della sicurezza.

La strategia Alcatel per rendere completamente disponibile l'infrastruttura di rete è esemplificata dalla sua soluzione ACEIS (Alcatel Carrier Environment Internet System), che si basa su una combinazione di tecnologie hardware e software che permettono di sviluppare reti con qualità carrier grade. Un analogo approccio ha adottato per l'architettura della sua famiglia di Pbx nativi IP, che dispongono di un ampio range di criteri di sicurezza, tra i quali la ridondanza di tutte le parti critiche, sistemi operativi robusti basati su Linux, e di una dotazione di funzionalità di sicurezza sia a livello del singolo apparato che nelle configurazioni di rete. Le piattaforme per la sicurezza coprono diversi aspetti, sia nelle soluzioni per l'ambito pubblico o le grandi corporate, che per l'ambito enterprise e delle PMI.

La visione di Alcatel in termini di soluzioni può essere ricondotta a tre principali tipologie: le soluzioni per Enterprise, le soluzioni per la rete geografica e le soluzioni di Managed Security Services.

Alcatel ha poi posto alla base della sua strategia per l'Enterprise due linee principali, una consistente nel rendere sicura la IP communication, l'altra nel rendere disponibili soluzioni robuste e distribuite di sicurezza nei diversi livelli dell'infrastruttura aziendale e concretizzarsi nel suo framework CrystalSec.

• CA

CA ha sviluppato da tempo un approccio integrato alla gestione della sicurezza con un sistema olistico. La strategia improntata all'Enterprise Information Technology Management mira a unificare e semplificare la gestione dell'IT aziendale, garantendone la sicurezza. In quest'ottica, la società statunitense punta a sviluppare sistemi integrati, basati su soluzioni singolarmente d'eccellenza, perseguendo questa strategia anche attraverso acquisizioni. Nell'ambito della sicurezza queste hanno portato a consolidare un'offerta pressoché completa nelle tre aree dell'Identity e Access Management (IAM), del Threat Management e del Security Information Management, in ciascuna delle quali CA conta elementi di eccellenza.

Le aree funzionali dell'identity e access management sono coperte tutte: dall'auditing/reporting al provisioning, dalle applicazioni al Single Sign On e così via. Tale copertura, a detta di CA, è un punto di forza di eTrust IAM Suite, giunta alla release 8, che consente di seguire l'evoluzione dell'impiegato dall'assunzione alla risoluzione del rapporto di lavoro. Tutte le identità degli utenti nei diversi sistemi vengono create, modificate, sospese, revocate o eliminate in base al ruolo e alle policy applicabili all'utente nell'ambito dell'organizzazione. Analoghe funzionalità possono essere applicate alla gestione delle identità di partner, clienti e fornitori.

L'implementazione di una funzione proattiva di threat management, oltre a prevedere soluzioni per la protezione dai diversi tipi di minacce, affronta anche altre problematiche aziendali, come i contenuti non autorizzati e gli utilizzi impropri delle risorse, e aiuta a garantire la legittimità delle informazioni in entrata e in uscita dalla rete. Tra i punti di forza di CA, la soluzione integrata eTrust Information Threat Management, che comprende eTrust Antivirus e il potente eTrust Pestpatrol Antispyware.

Le capacità di visione, correlazione e gestione della sicurezza fornite da eTrust Security Command Center rappresentano il sigillo di qualità dell'offerta CA.

• CHECK POINT

Check Point, storicamente nata con il firewall e la protezione perimetrale, ha da tempo sviluppato un ampliamento della gamma, arrivando a proporre una soluzione di sicurezza end to end. Oggi, l'architettura di sicurezza di Check Point è articolata in quattro aree: Perimeter Security, Internal Security, Endpoint Security e Web Security.

Il tutto è unito dalla piattaforma NGX, che fornisce un sistema unificato per la gestione di tutte le soluzioni di sicurezza, consentendo di ottenere significativi risparmi di costo e un più alto livello di protezione.

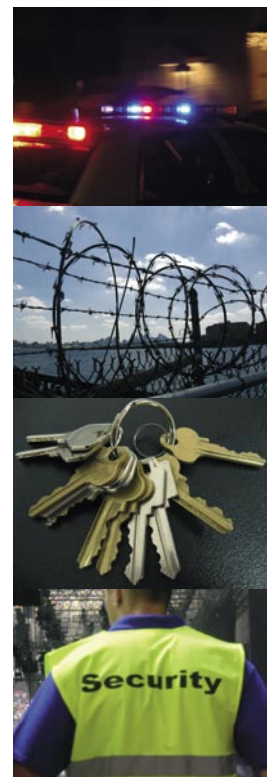
L'integrazione delle quattro diverse aree, infatti, consente alla casa di Tel Aviv di proteggere le imprese da tutti i tipi di minaccia, comprese quelle "insospettabili" determinate da comportamenti non conformi alle security policy da parte dei dipendenti. A questo si aggiunge la potenza del motore di correlazione e analisi degli eventi registrati: Check Point Eventia Analyzer.

Nell'area perimetrale, la società israeliana manifesta un'esperienza e una capacità di ricerca e sviluppo all'avanguardia, per esempio con la soluzione di Application Intelligence, che complementa le capacità di stateful inspection, inventate proprio da Check Point.

L'azione integrata delle tecniche di Internal, Web e Perimeter Security unitamente alle soluzioni client e clientless Integrity, progettate per la protezione dell'endpoint, permettono di controllare il livello di sicurezza del client prima di consentirne l'accesso. Così come è possibile mettere in quarantena e isolare un terminale che dovesse manifestare un comportamento sospetto. Potente, in questo senso, la tecnologia Malicious Code Protector, che simula l'esecuzione di un codice ritenuto potenzialmente pericoloso.

Per semplificare la gestione e aumentare la sicurezza nell'area Web, Check Point propone, infine, l'appliance Connectra.

Completano l'offerta le soluzioni per le piccole e medie imprese, denominate Safe@Office e VPN-I Edge.



• CISCO SYSTEMS

La vision Cisco Systems per il networking di nuova generazione parte da architetture orientate alle applicazioni, che andando oltre la condivisione delle risorse, consente l'integrazione di servizi applicativi e l'interazione a diversi livelli del sistema informativo. In quest'ottica, la sicurezza è uno dei servizi basilare che l'infrastruttura deve garantire.

Questo significa che Cisco ha integrato nel proprio sistema operativo Cisco IOS e in tutti i componenti di rete, soluzioni o elementi per la protezione delle informazioni e risorse e servizi a supporto della sicurezza applicativa e di tutto il sistema informativo.

La strategia è tesa a realizzare la Self Defending Network (SDN), un'infrastruttura che è in grado di riconoscere attività sospette, identificare le minacce, reagire appropriatamente, isolare le infezioni e rispondere agli attacchi in modo coordinato. Tale strategia è attuata anche con la Cisco Unified Wireless Network, che utilizza tutte le protezioni previste dagli standard, integrandole con sistemi ad hoc.

La SDN si basa su tre pilastri: le soluzioni di Secure Connectivity, che consentono di trasportare le applicazioni in maniera sicura tra i vari ambienti di rete; il Threat Defense System, che protegge contro minacce note e non note; le soluzioni per la Trust and Identity, che permettono la gestione delle identità e delle autorizzazioni per l'accesso sicuro alle risorse.

Da segnalare, il programma Network Access Control, che, tramite un client opportuno e il supporto di specifiche peculiari da parte di una serie di terze parti, consente di realizzare un sistema di controllo avanzato che impedisce l'accesso alla rete di un dispositivo non conforme alle policy di sicurezza.

Le soluzioni Cisco si articolano in una gamma vasta che comprende firewall, IPS (Intrusion Protection Systems), soluzioni di content management, di threat mitigation, di controllo degli incidenti e altre ancora, cui si aggiungono servizi online di reportistica dettagliata e altri di security intelligence, come Intellishield Alert Manager.

• DIMENSION DATA

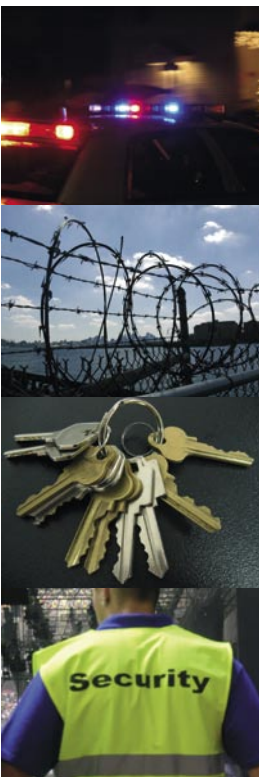
Dimension Data opera nella costruzione, implementazione e gestione operativa di network grandi e complessi. Nell'ambito specifico della sicurezza, la società propone un'ampia gamma di soluzioni e servizi per le applicazioni e le reti, affiancandosi alle aziende per sviluppare e implementare strategie di sicurezza e supportandole nell'implementazione tecnologica. La strategia seguita da Dimension Data per la protezione di un'organizzazione si fonda su tre paradigmi fondamentali di protezione, rilevamento e reazione. Questa strategia è sostenuta da una suite completa di servizi e soluzioni end-to-end per la sicurezza progettati per ridurre al minimo i tempi di inattività, consentire la massima integrità dei dati e il recupero dei sistemi, tutti i giorni dell'anno, 24 ore su 24.

Questa suite comprende:

- Valutazione dei rischi e della compliance, con analisi delle vulnerabilità, controlli sulle tecnologie, verifiche dell'architettura e dei criteri e garanzia di conformità alle normative,
- Soluzioni per la sicurezza perimetrale, che comprendono firewall e VPN, gestione contenuti
- Soluzioni per la gestione delle intrusioni: che comprendono i sistemi di protezione e individuazione delle intrusioni (IDS/IPS), gestione degli eventi attinenti alla sicurezza e gestione delle vulnerabilità
- Servizi gestiti per la sicurezza, che prevedono gestione di firewall, IDS/IPS e vulnerabilità, contenuti/filtraggio URL.

Nello svolgimento dei propri servizi la società ha sviluppato la metodologia ASI (Adaptive Secure Infrastructure) pensata per inserirsi nelle architetture e negli ambienti esistenti e integrare in essi adeguati livelli di sicurezza. Questo modello si basa su un approccio a 4 stadi, ciascuno dei quali rappresenta il fondamento del successivo: Identificazione, Classificazione, Isolamento, Controllo.

Dimension Data affianca le aziende anche nelle esigenze di protezione legate all'IP Telephony, riguardo alle minacce legate al furto del servizio, al Denial of Service e alle intercettazioni.



• D-LINK

D-Link propone una gamma articolata di soluzioni per la sicurezza di rete adatti a esigenze che variano da quelle dei piccoli gruppi di lavoro a quelle delle grandi aziende. La gamma d'offerta indirizzata in modo specifico alla sicurezza comprende, sistemi firewall, Virtual Private Network (VPN), gateway, client software e sistemi di videosorveglianza. Le soluzioni per la sicurezza D-Link si avvalgono di una pluralità di tecnologie tra cui autenticazione RADIUS, cifratura dei dati, content filtering, NAT e intrusion detection.

I firewall D-Link della serie NetDefend raggruppano, in un unico chassis, funzionalità avanzate che includono il bilanciamento dei carichi di lavoro, funzioni di fault-tolerance, la funzione Zone Defense, il filtraggio dei contenuti, l'autenticazione degli utenti, il blocco delle applicazioni Peer-to-Peer e di instant messaging, la protezione DoS e le connessioni remote sicure basate su reti VPN. Inoltre dispongono della tecnologia di protezione sviluppata da D-Link e denominata Zone Defense, che opera in modo totalmente integrato con gli switch D-Link della serie xStack, permettendo di individuare e bloccare le attività illecite all'interno della rete e di mettere automaticamente in quarantena i computer contagiati da virus, evitando la propagazione all'interno del network. La gamma comprende tre modelli di firewall siglati DFL-800, DFL-1600 e DFL-2500 dotati di porte Gigabit Ethernet configurabili dall'utente e adatti alle esigenze di piccole, medie e grandi imprese. L'Information Security Gateway NetDefend DFL-M510 rappresenta un dispositivo di sicurezza pensato per proteggere la rete dai nuovi tipi di attacchi, che permette di gestire e controllare l'utilizzo di applicazioni di Instant Messaging e P2P.

La linea di videocamere Internet D-Link rappresenta una soluzione per il monitoraggio remoto della sicurezza che riunisce funzionalità di sorveglianza audio/video, un server Web integrato e funzioni quali rilevamento di movimenti, registrazione video e notifica mediante posta elettronica.

• IBM

IBM affronta le esigenze di sicurezza con un approccio globale, mediante un'offerta che abbraccia sia l'infrastruttura, sia i processi, l'organizzazione, le soluzioni e le applicazioni. Il punto di partenza per garantire una protezione efficace è, secondo IBM, identificare quali sono gli asset realmente critici per il business considerando anche i beni immateriali e, quindi, il patrimonio intellettuale, l'immagine e i processi. Per realizzare questi obiettivi e garantire l'affidabilità, la disponibilità e la protezione delle risorse aziendali da eventuali attacchi, l'offerta della società comprende soluzioni infrastrutturali, software per la gestione dell'identità, servizi evoluti, tecnologie specifiche implementate all'interno dei propri server e anche delle stampanti.

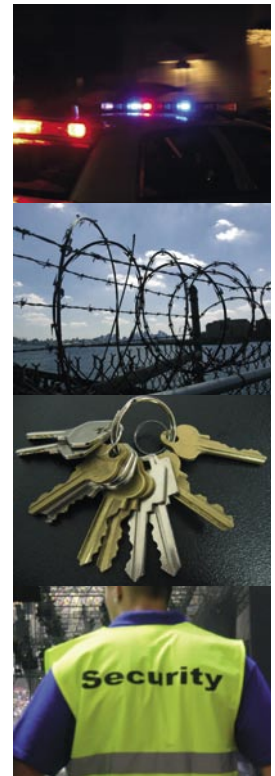
L'offerta per la sicurezza sviluppata da IBM comprende la valutazione del livello organizzativo (policy assessment), fisico (per esempio, il controllo degli accessi), logico (applicazioni) e tecnico (per esempio le reti).

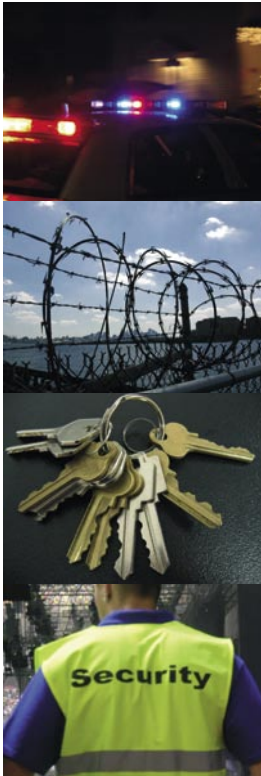
Le soluzioni Tivoli Security Management consentono di far fronte a esigenze quali la gestione degli eventi, del rischio, della compliance e molti altri.

In particolare, alle esigenze enterprise di Identity management IBM dedica Tivoli Access Manager for Enterprise Single Sign-on mentre per le realtà più piccole è disponibile Tivoli Identity Manager Express.

La sicurezza IBM si manifesta anche nelle caratteristiche e funzionalità che caratterizzano i suoi sottosistemi server e storage. Per affrontare il continuo cambiamento nelle esigenze di sicurezza delle informazioni legati all'evoluzione tecnologica, IBM pone l'accento su tre aspetti fondamentali: mitigare il rischio operativo, garantire e dimostrare la protezione del dato, mitigare il rischio dell'incertezza.

I sistemi IBM si avvalgono, perciò, di tecnologie di sicurezza integrate nei suoi sistemi operativi IBM mentre, con la famiglia di soluzioni IBM TotalStorage Resiliency mette a disposizione funzionalità orientate all'alta disponibilità, alla business continuity e al disaster recovery.





- I-NET

La strategia e le architetture per la sicurezza sviluppate e proposte da Inet partono dall'assunto di base che la sicurezza non è un concetto localizzabile ma deve comprendere sia la salvaguardia da attacchi ai dati che volto ad assicurare la loro corretta conservazione e disponibilità nel tempo.

L'approccio sviluppato per concretizzare questa vision strategica per la sicurezza si esprime nel suddividere un sistema informatico su più livelli, per ognuno dei quali ha previsto un opportuno e razionale sistema di protezione e delineato correlati piani di intervento che possono poi essere tarati sulle diverse realtà aziendali. Questi livelli sono quello perimetrale, di accesso, dei dati e operativo. Ogni livello può poi essere suddiviso in svariati sottolivelli dotati di apparati o applicazioni di sicurezza specifiche.

Peraltro, la strategia Inet è volta a permettere sia rapidi interventi di adeguamento delle caratteristiche di sicurezza di un livello che una più facile individuazione e isolamento dei potenziali problemi. In pratica, si estende ai diversi elementi che costituiscono il sistema informatico e di comunicazione aziendale sia all'interno che all'esterno, prevedendo per ogni livello una soluzione adatta e proporzionale all'importanza del livello stesso per il business dell'impresa.

Per tradurre in pratica i concetti sopra esposti, I.net ha definito un portafoglio di prodotti, servizi e soluzioni molto ampio, integrato e completato da servizi professionali nella progettazione e implementazione di sistemi Ict sicuri e di consulenza, soprattutto per quanto concerne le attività di auditing, di analisi dei rischi, di valutazione della vulnerabilità di un sistema IT e di pianificazione.

Per quanto concerne i prodotti, il focus dei suoi sviluppi comprende apparati e prodotti software che rappresentano il best of breed tecnologico, e di cui dispone a seguito di accordi con società specializzate nello sviluppo di soluzioni di sicurezza perimetrale, sicurezza interna, autenticazione, controllo e gestione.

- INTERNET SECURITY SYSTEMS

Internet Security Systems ha sviluppato il proprio approccio alla sicurezza end to end con la strategia Enterprise Security Platform (ESP), un sistema costruito dal basso, grazie all'integrazione delle tecnologie sviluppate direttamente da ISS, che, nei pochi casi di acquisizioni ha innanzitutto fuso la ricerca e sviluppo e integrato la tecnologia prima di portare prodotti sul mercato. Il tutto con un orientamento nativamente "preemptive. Cioè basato sulla capacità di prevenire i problemi e gli attacchi, anticipando lo stesso sorgere delle minacce: in pratica arrivando a garantire la "0 day" protection per la maggior parte delle vulnerabilità. Questo è possibile grazie al grande lavoro del team X-Force, che studia le vulnerabilità e sviluppa i sistemi di analisi, i quali sono basati su svariate tecnologie, comprese l'anomaly detection, l'analisi del comportamento, quella dei protocolli e così via.

L'ESP, inoltre, si adatta alle esigenze del cliente adottando un approccio di servizi on demand e facendo di ISS un partner continuamente a contatto con la propria clientela. Il tutto è completato da un avanzato e unificato sistema di gestione, che oltre a funzioni di correlazione degli eventi fornisce capacità di interazione automatiche tra i sistemi.

L'elevato valore delle soluzioni di prevenzione sarebbero nulla senza le prestazioni e per questo ISS ha sviluppato soluzioni integrate basate su appliance, che, anche grazie all'impiego di specifici ASIC consentono di ridurre al minimo l'impatto dei controlli sul traffico di rete. Questo anche per la serie Proventia M, che prevede, oltre all'IPS e al firewall, anche tutta una serie di funzionalità per la protezione da virus, worm, spyware, spamming, phishing e per il Web e content filtering. Per la sicurezza dell'endpoint, ISS ha sviluppato Proventia Desktop, una soluzione che comprende avanzate tecnologie, quali Virus Prevention System (ancora un approccio preemptive che identifica un virus anche non noto), l'antispysware proattivo e la buffer overflow exploit prevention.

• LUCENT TECHNOLOGIES

L'esperienza di Lucent Technologies nella security è nata negli storici Bell Labs, che da tempo collaborano con il Dipartimento di Stato americano per la realizzazione di sistemi e processi di sicurezza di rete in ambito Difesa e Sicurezza Nazionale. I brevetti finora depositati in tale ambito sono più di 100 e costituiscono le fondamenta dell'attuale offerta. Inoltre, nello sviluppare le reti dei principali provider mondiali, attività core business dell'azienda, Lucent pone da sempre attenzione agli aspetti di sicurezza e affidabilità. Esperienze e competenze che la società mette a disposizione di aziende e PA, anche e soprattutto tramite l'organizzazione dei servizi, Lucent Worldwide Services, che impiega 10mila esperti di reti a livello mondiale e che fornisce supporto e consulenza a clienti e partner.

La soluzione proposta da Lucent consiste in una famiglia di appliance evoluti (Lucent VPN Firewall Brick) che integrano funzionalità complete di sicurezza di rete e consentono di contenere i costi di installazione e gestione. Svolgono il compito di un Firewall, di un IPS (Intrusion Prevention System), di un Application Filter, di un VPN IPSec gateway e gestiscono in modo granulare la QoS (Quality of Service) a livello IP e di singola applicazione. Hanno inoltre funzionalità di sicurezza specifiche per il traffico Voice over IP e per le applicazioni mobile e wireless. L'offerta si completa con il software Lucent IPSec Client, che integra funzionalità di client IPSec e di personal firewall, destinato a chi accede alla rete dall'esterno, per esempio telelavoratori, agenti e consulenti.

Lucent propone anche una soluzione di autenticazione RADIUS, VitalAAA, in grado di gestire da un migliaio fino a decine di milioni di utenti. Questa grande scalabilità la rende ideale sia in ambienti enterprise, per autenticare gli utenti aziendali su rete wireless Wi-Fi o che si collegano da remoto via VPN, sia alle esigenze degli operatori di TLC, per verificare le credenziali dei propri clienti e attivare sistemi di Accounting.

• NORTEL NETWORKS

Nortel ha approciato il problema della sicurezza estendendolo ai diversi elementi di una rete. In questa sua visione l'assunto di base è che l'ampia possibilità in termini di connettività rappresenta un vero e proprio paradosso, perché da un lato, tramite Internet, permette di comunicare in modo aperto e globale, ma dall'altro, poiché internet è una infrastruttura condivisa, si apre di converso la strada della propria azienda e delle proprie applicazioni a chi fosse interessato ad accedervi in modo fraudolento.

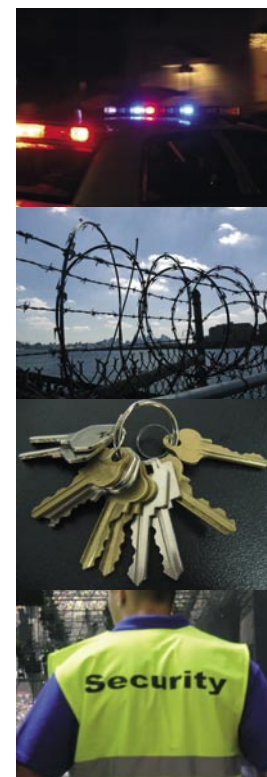
Gli stessi punti di accesso che rendono possibile il dialogo con i clienti, rappresentano punti critici per la sicurezza del business aziendale. Gli attacchi, poi, vengono sempre più portati direttamente alle applicazioni, per esempio la posta elettronica o i data base, usando poi le applicazioni stesse per moltiplicare gli effetti negativi e potenzialmente catastrofici, se non bloccati, di un'intrusione.

Nortel ritiene quindi che l'unica strategia percorribile per ottenere una rete sicura sia quella che permei tutti i livelli dell'intera rete su base end-to-end, comprendendovi quindi sia l'infrastruttura ICT nel suo complesso che gli utenti finali, indipendentemente dalle modalità di accesso, che possono essere fisse o mobili, locali o remote, tramite reti private o reti VPN pubbliche.

Questa sua vision è tradotta in un assunto chiave della sua strategia, "Security in the DNA", proprio per indicare come la sicurezza, per essere realmente efficace, debba essere attuata in modo intrinseco alla rete e agli elementi che la costituiscono.

Questa visione è a sua volta parte della visione convergente di un framework di rete riferito come "One Network. A World of Choice."

Nel corso dell'ultimo anno l'approccio alla sicurezza è stato da Nortel formalizzato in uno specifico framework riferito come "Unified Security Framework", che comprende concetti, aspetti fisici e procedurali atti a permettere, nel loro insieme, la realizzazione di una rete sicura e ad alte prestazioni.



• PROCURVE NETWORKING

ProCurve è la divisione di HP che propone soluzioni infrastrutturali per realizzare reti sicure all'insegna della visione strategica dell'architettura Adaptive EDGE. Questo approccio prevede di spostare il controllo al bordo della rete per la realizzazione di reti convergenti, mobili e fisse, caratterizzate da elevate prestazioni e massima sicurezza.

Il modello architetturale proposto da ProCurve, in cui l'intelligenza della rete viene spostata dal centro del network al suo bordo, realizza le condizioni per un approccio di Identity Driven Management (IDM). L'adozione di un modello di questo tipo sposta il focus sull'individuo, anziché sul dispositivo, permettendo agli amministratori di rete di impostare in modo dinamico i dispositivi presenti sull'infrastruttura in base all'utente, alla località, al tempo o altre variabili. L'IDM costituisce la base per la creazione di un network intelligente in grado di prevenire l'uso non autorizzato delle risorse di rete e di comportarsi diversamente in funzione degli utenti, anziché dei dispositivi di accesso.

Le soluzioni ProCurve Networking dispongono di diversi livelli di sicurezza integrati e si avvantaggiano di caratteristiche per la protezione dei dati basate su standard. Esse si inquadrano all'interno di un framework di sicurezza organizzato attorno ai tre aspetti dell'accesso al network, della gestione del network e della resilienza agli attacchi. A tal fine, le soluzioni ProCurve prevedono funzioni di controllo di accesso sulla porta secondo lo standard 802.1x, controllo MAC, supporto VLAN secondo le specifiche 802.1q e l'utilizzo delle liste di controllo degli accessi. Le funzionalità per la sicurezza gestionale presenti sugli switch ProCurve comprendono, tra l'altro, la cifratura del database relativo a user name e password, il supporto dei protocolli TACACS+ e SSL e una VLAN dedicata per il management.

Tra le tecnologie per la sicurezza va ricordato anche Virus Throttle, un software per la protezione della rete dalla diffusione di virus e worm che si basa sul rilevamento delle anomalie del traffico.

• RSA SECURITY

RSA Security è specializzata nello sviluppo di tecnologie per la sicurezza delle transazioni online e per la protezione dei sistemi informativi delle aziende da accessi non autorizzati o fraudolenti, con un'offerta che spazia dall'autenticazione e gestione dei certificati digitali e della firma elettronica, a soluzioni di sviluppo e crittografia e gestione dei privilegi di accesso alle risorse Web.

La società è particolarmente impegnata nell'identity e access management, attraverso un approccio rigorosamente conforme agli standard e, quindi, tecnologicamente neutrale rispetto all'integrazione e all'interoperabilità con diversi sistemi di identity interni ed esterni alle imprese.

Tra le principali soluzioni ricordiamo RSA ClearTrust - una soluzione di user e Web access management indirizzata a gestire gli utenti proteggendo, contemporaneamente, l'accesso alle risorse Web - e la soluzione di Enterprise Single Sign-On denominata RSA Sign-On Manager. Attraverso Federated Identity Manager (FIM) RSA fornisce, invece, una gamma di funzionalità di fascia enterprise per l'identity e l'access management che rispondono alle esigenze delle imprese di ottemperare alle normative, di automazione dei processi di business e di rafforzamento della relazione on-line con clienti e partner. FIM è basata sul modello di gestione federata promosso dall'associazione indipendente Liberty Alliance e sulle specifiche standard SAML.

RSA SecureID è la famiglia di software di autenticazione progettata da RSA che fornisce sistemi di autenticazione centralizzati a due fattori per il riconoscimento delle identità digitali. La soluzione consiste di tre componenti: un token, un server di autenticazione e un server di autorizzazione, oltre a vari agenti software.

A seguito della recente acquisizione di Cyota, RSA ha creato una nuova divisione e ha rafforzato ulteriormente la propria offerta nell'ambito dei servizi indirizzati a prevenire e combattere le frodi on line e il phishing.



• SOPHOS

Sophos, una delle aziende storiche nell'ambito dell'ICT Security, fornisce soluzioni per la protezione professionale da virus, spam, spyware e phishing indirizzate a organizzazioni di ogni dimensione, dalle grandi alle piccole imprese.

La strategia della casa inglese è fortemente orientata alle tecnologie e al servizio, mettendo al centro l'attenzione alle esigenze del cliente. Lo staff vendite, marketing e amministrativo, infatti, è impegnato a fornire all'utilizzatore competenza, assistenza in stretta collaborazione con un team qualificato di sviluppatori, programmatori e personale esperto e grazie a un call center di supporto tecnico particolarmente preparato.

La crescita continua delle minacce alla sicurezza, sia da un punto di vista quantitativo sia qualitativo, quindi in termini di una sempre maggiore complessità e rapidità di diffusione, richiede una difesa per la quale, secondo la visione di Sophos, non è sufficiente una protezione multilivello, ma occorrono soluzioni di sicurezza integrate, aggiornate in automatico e supportate adeguatamente. La casa inglese ha quindi sviluppato soluzioni enterprise che forniscono una protezione multilivello e multiplatforma, supportando tutti i principali ambienti. Particolare attenzione è stata posta nello sviluppo di strumenti che semplificano amministrazione, monitoraggio, aggiornamento e reportistica, facilitando il rispetto delle normative. A questo si aggiunge il supporto tecnico 24 ore su 24, 7 giorni su 7 e la garanzia data dalla capacità di ricerca e analisi delle minacce informatiche effettuate, anche qui continuamente, dai SophosLabs.

Alla storica tecnologia antivirus per la protezione degli endpoint, Sophos aggiunge soluzioni per la protezione del gateway e della messaggistica. In particolare, per la posta elettronica, venendo incontro alle necessità di semplificazione del management, la casa inglese ha rilasciato Email Security Appliance.

Le soluzioni per le piccole e medie imprese sono state ingegnerizzate in suite ed edizioni dedicate.

• SYMANTEC

Il concetto di sicurezza promosso da Symantec supera quello di integrazione, per indirizzarsi verso un approccio olistico in cui ogni aspetto - tecnologico, culturale, gestionale e di servizio - va considerato all'interno di una strategia specifica per la sicurezza.

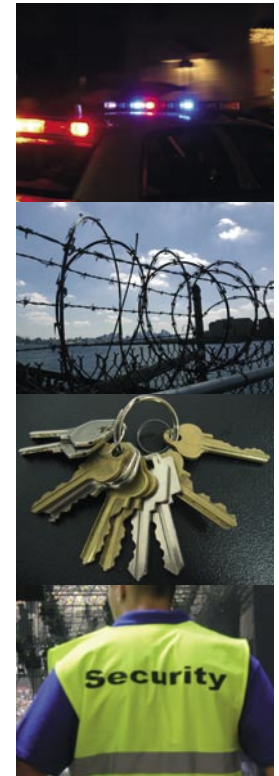
Symantec evidenzia l'importanza dell'informazione che rappresenta il vero elemento di valore per l'azienda coniugando gli aspetti di sicurezza e disponibilità mediante un portfolio estremamente ampio, grazie anche alla recente acquisizione di Veritas Software.

Le soluzioni Symantec sono state pensate e sviluppate per abilitare la realizzazione di un'infrastruttura resiliente in grado di sopportare ogni possibile inconveniente indirizzato a interrompere o rendere meno efficienti i processi e il servizio ma, nello stesso tempo, predisposta per adattarsi dinamicamente alla costante evoluzione del mercato. Un'infrastruttura di questo tipo rappresenta il presupposto per realizzare le condizioni per l'Information Integrity ovvero per garantire l'operatività, l'efficienza e la crescita dell'azienda, qualunque cosa accada.

La gamma d'offerta di Symantec comprende soluzioni di sicurezza integrata quali il software Symantec Client Security e diverse soluzioni di Gateway Security. La società propone una gamma articolata di soluzioni hardware e software per la protezione delle mail e per far fronte a fenomeni in crescita quali lo spam, le frodi on line quali il phishing e i codici maligni diffusi via e-mail. Le soluzioni indirizzate a queste esigenze includono Brightmail AntiSpam, il software Mail Security for Domino/Exchange e le Appliance Mail Security serie 8100 e 8200.

Altre soluzioni offerte comprendono Enterprise Security Manager, per la compliance, le soluzioni di early warning DeepSight, quelle contro le intrusioni (Host IDS) e per il recovery di emergenza (LiveState Recovery).

Tra i servizi offerti vanno segnalati i Managed security services che Symantec svolge attraverso i propri SOC, i Global Intelligence Services e gli Hosted mail security services..



Sempre più appliance nel futuro di Check Point

Il country manager della società israeliana delinea uno scenario del mercato italiano e illustra le strategie per conquistarlo

Per molti Check Point è quella che ha inventato il firewall. E in effetti lo è, perché ha brevettato la stateful inspection, cioè la tecnologia di filtraggio su cui si sono poi basati tutti i firewall. Ma Check Point Software Technologies è andata ben oltre, tanto che “software” nel nome ormai le va stretto. Oggi, infatti, fornisce soluzioni anche hardware, contraddistinte da una linea di appliance in crescita. Inoltre, dopo aver incrementato le funzionalità delle proprie “tradizionali” soluzioni firewall e VPN, oggi presenta una strategia di protezione end to end, realizzata anche in seguito a un’aggressiva politica di acquisizioni portata avanti negli ultimi tre anni circa. Con Andrea Rizzi, country manager di Check Point in Italia, siamo partiti da queste considerazioni per tracciare un quadro della situazione del mercato italiano e di strategie e risultati ottenuti dalla casa israeliana nel nostro Paese.

Reportec: Si potrebbe dire “Non solo firewall”, ma senza essere banali, qual è, brevemente, l’offerta di Check Point oggi e quanto gli utenti hanno percepito il nuovo corso?

Andrea Rizzi: Oggi la nostra strategia è articolata in tre aree: Perimeter Security, Internal Security, Web Security ed Endpoint Security, in un’ottica di protezione e prevenzione end to end. La piattaforma NGX risulta trasversale a tutto questo, cui fornisce una console di gestione unificata. Le soluzioni delle diverse aree, integrate tra loro, vanno dal tradizionale firewall e dalle tecnologie di VPN, alle più recenti Application Intelligence e Web Intelligence, arrivando a comprendere sistemi software e appliance. Queste ultime sono realizzate sia

in partnership con società terze sia sviluppate internamente, in particolare nella divisione SofaWare.

Ci sono diversi clienti che stanno apprezzando le caratteristiche delle nuove soluzioni, anche hardware, ma devo ammettere che, probabilmente, dobbiamo lavorare di più sul posizionamento delle stesse. All’atto pratico, sono ancora la maggior parte quelli che si stupiscono di scoprire che Check Point possiede un’ampia gamma di tecnologie ben oltre il firewall. Peraltro, per i tanti che hanno imparato a conoscere la nostra serietà e la qualità delle nostre soluzioni, si tratta di una piacevole sorpresa. Senza contare i molti clienti che ci hanno sempre sostenuto e, anzi, hanno insistito perché intraprendessimo il percorso evolutivo che, in un certo senso, il mercato impone.

R: Ma cosa cercano oggi le imprese italiane?

AR: In una parola: consolidamento. Più precisamente, le aziende italiane sono impegnate in progetti di ottimizzazione tanto delle risorse quanto dei processi organizzativi. La consolidation, in termini di hardware e software, è imposta da logiche di bilancio che mirano a ridurre i costi *opex*. Questo comporta, in taluni casi, un paradosso, poiché piuttosto che investire per rinnovare i servizi di manutenzione, si preferisce iscrivere a bilancio un *capex* e cambiare completamente tecnologia.

Non necessariamente questa situazione viene vissuta in negativo. Anzi, alcune realtà affrontano l’ottimizzazione come un investimento per ottenere maggiore flessibilità. Questo con un massiccio impiego della virtualizzazione e allora il consolidamento significa anche una

Andrea Rizzi, country manager Check Point in Italia



concentrazione di risorse fisiche all'interno dei data center, dal che discendono nuove esigenze in termini di sicurezza.

Comune a tutto ciò è il bisogno di migliorare e semplificare la gestione delle soluzioni. Si assiste, di conseguenza, a un crescente successo delle appliance o di sistemi UTM (Unified Threat Management). Se all'inizio queste soluzioni "one box" erano scelte soprattutto dalle PMI, che non avevano competenze e risorse per gestire tecnologie complesse, oggi sempre più grandi aziende stanno optando per l'inserimento di appliance nel sito remoto, con indubbi vantaggi sul fronte gestionale. Personalmente ritengo che tali benefici si possano conseguire anche con un sistema integrato svincolato dall'hardware, che, in quanto tale, non rischia di diventare obsoleto rapidamente.

R: Check Point come risponde a queste esigenze?

AR: Check Point dispone già di alcune serie di appliance e di soluzioni integrate per la gestione delle minacce, delle quali sono apprezzate appunto le caratteristiche di semplicità gestionale. Abbiamo realizzato alcuni progetti di grande interesse con Check Point VPN-I Edge, in particolare, uno di questi per un'importante comparto della Pubblica Amministrazione e un altro per una delle primarie compagnie d'assicurazioni del Paese. Molto bene stanno andando anche le appliance Safe@Office.

Un discreto successo lo abbiamo avuto poi con Connectra, la nostra appliance (oggi disponibile anche con supporto NGX) che consente di implementare un servizio di VPN SSL. È questo un caso in cui ci viene riconosciuta la competenza sulle problematiche di fondo e si acquista fiducia in questa tecnologia che consente, tra l'altro, di abilitare l'erogazione di una serie di servizi online. Si tratta comunque di una tecnologia sufficientemente nota e questo ha senz'altro favorito le vendite di Connectra. Diverso è il caso di Eventia Analyzer, appena giunto alla versione 2.0, che non deve essere confuso con un sistema di network forensic, rispetto al quale ha meno funzionalità, ma con un costo decisamente inferiore, fornisce uno

strumento potente, utile come primo indicatore per capire cosa veramente succede sulla rete. A tal proposito, è bene sottolineare che è in grado d'interfacciarsi con soluzioni multi-vendor.

R: Al nuovo corso di Check Point deve abituarsi anche il vostro canale. Cosa avete in programma?

AR: Nuovi programmi appunto. Su questo fronte compieremo grandi sforzi. A partire dalla fine del secondo trimestre ci sarà un nuovo programma che andrà gradualmente a sostituire il CSP program. Ma soprattutto chiederemo importanti investimenti, cui seguiranno ovviamente riconoscimenti e vantaggi, ma il canale ci deve seguire. I partner che non saranno in grado di prepararsi per supportare tutta la nostra gamma di soluzioni saranno lasciati indietro. Gli altri dovranno avere accesso a un laboratorio per compiere test per i loro clienti. Noi forniremo fondi e organizzeremo azioni congiunte, svilupperemo lead. Ai partner più qualificati, che vogliamo ampliare facendone crescere diversi, verranno affiancate nuove figure professionali, con maggiore esperienza di prevendita sull'utente finale. Lo scopo è quello di programmare insieme specifiche azioni su precisi prospect, per dare un forte impulso al mercato. Eventia Analyzer, per esempio, è uno dei prodotti che il canale deve conoscere meglio, per posizionarlo adeguatamente. Analogamente InterSpect e tutta la nostra offerta d'Internal Security merita più attenzione.

R: Quali aspettative state maturando con un programma così aggressivo?

AR: Riteniamo di poter crescere dal 10 al 15%, quest'anno. Nel 2005 abbiamo registrato un +9% rispetto a un 2004, che a sua volta aveva superato il 2003 del 21%. Quello che è fondamentale, però, è il trend che vede invertire il peso sul fatturato tra nuovi prodotti e manutenzioni. Nel 2004 queste erano il 52%, mentre nel 2005 la vendita di nuovi prodotti è salita al 54%. Questo significa che stiamo guadagnando market share in Italia e contiamo di continuare su questa strada.

G.D.B;

Emerson Network Power ridefinisce la Business Continuity

Cresce la potenza di calcolo nei Data Center e, con essa, il calore generato. Il cooling tradizionale è inadeguato. La risposta è la soluzione “adattiva” Liebert X-treme

In questi ultimi anni i Data Center hanno conosciuto drastiche evoluzioni che ne hanno ridisegnato le architetture. Alla base di questi sviluppi, l'esponenziale crescita delle capacità elaborative dei microprocessori caratterizzate da trend di crescita delle prestazioni rapidissimi. Questo si unisce a una tendenza sempre più marcata di concentrazione di densità di calcolo delle apparecchiature informatiche di ultima generazione come, per esempio, i blade server in configurazione rack.



Giordano Albertazzi,
amministratore delegato di
Emerson Network Power
Italia

- Crescono le prestazioni, aumenta il calore da dissipare. È evidente che una tale rivoluzione nei Data Center, apre una serie di criticità nuove. La prima e più rilevante di queste è la necessità di dissipare efficacemente il calore addizionale generato dalla concentrazione di server ad alta densità.

«I sistemi di cooling tradizionali, tipicamente delle soluzioni con mandata d'aria sottopavimento, possono raggiungere una capacità di smaltimento di circa 3 kW per metro quadrato, una potenza più che sufficiente per le apparecchiature IT di vecchia generazione. L'incremento di calore per metro quadrato generato dall'inserimento di nuovi apparati in un rack è però di un ordine di grandezza superiore, evidente che le tecnologie tradizionali non siano più sufficienti», spiega Giordano Albertazzi, Amministratore Delegato di Emerson Network Power Italia.

Si pensi infatti che se oggi i datacenter “tradizionali” hanno un carico termico di 1-2kW per metro quadrato, un rack composto da 6 blade server può arrivare a generare un carico ter-

mico di 24 kW in 0,7 metri quadrati. Dissipare tale calore, e farlo in modo efficiente diviene, dunque, un aspetto chiave per permettere la transizione tecnologia dell'infrastruttura IT e per assicurare una piena Business Critical Continuity alle organizzazioni.

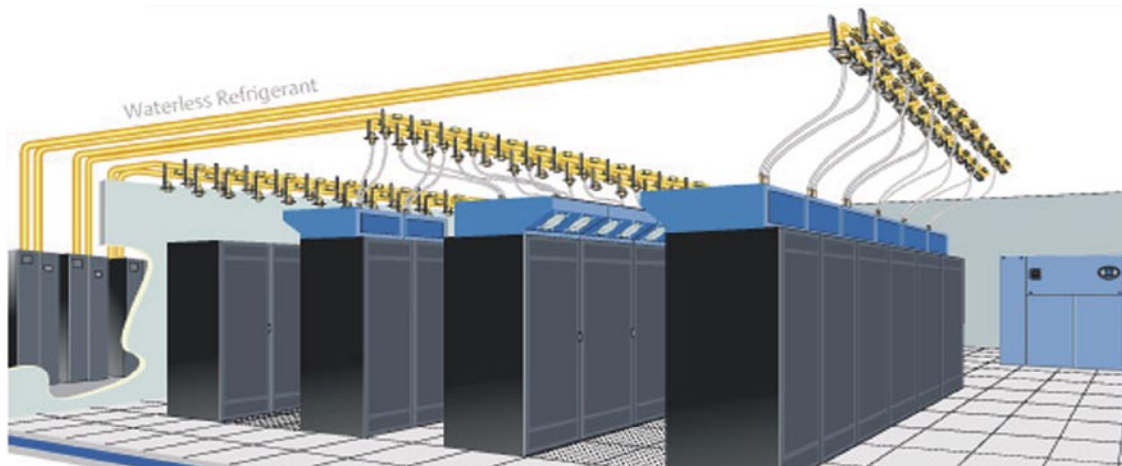
- Liebert X-treme: condizionare solo dove e quando serve. Liebert X-treme è la risposta concreta che Emerson Network Power fornisce a chi deve gestire questo esponenziale incremento di calore in un Data Center.

Questa piattaforma di soluzioni e servizi è stata realizzata basandosi sul concetto di Adaptive Cooling & Power Architecture, ovvero l'uso di un'estesa gamma di soluzioni di condizionamento e alimentazione per far fronte a tutte le esigenze di raffreddamento di una moderna infrastruttura. In questa logica, Liebert X-treme significa soluzioni per condizionamento supplementare che possono elevare la capacità di raffreddamento fino a 24 kW per rack agendo solo dove e quando serve, senza imporre una revisione complessiva degli ambienti di elaborazione, mettendo così nelle condizioni chi gestisce un Data Center di far evolvere le architetture IT senza vincoli di alcun genere.

Si pensi, per esempio, all'introduzione in una configurazione rack di server addizionali (o di soluzioni High Density) per la gestione di particolari applicazioni che, nell'area specifica, incrementano in maniera sostanziale il calore generato.

In questo caso, attraverso la soluzione Liebert XD, parte della piattaforma Liebert X-treme, si può realizzare un sistema di precision coo-

ling ad hoc, dedicato ai rack dove sono montati i server High Density (come i blade server), senza dover ridefinire il sistema di condizionamento globale dell'ambiente. Liebert XD è infatti in grado di condizio-



nare aree specifiche o interi Data Center utilizzando due modalità di distribuzione dell'aria fredda: attraverso moduli cooling posizionati direttamente sul rack oppure utilizzando moduli cooling installati a soffitto.

La soluzione adattiva Liebert XD, che gestisce il condizionamento di sistemi che erogano range di potenza da 5 a 16 kW per rack, utilizza gas refrigerante attraverso pompaggio effettuato da chiller specifici con un unità pumping. Questa soluzione ha il grande vantaggio di evitare il circolo di acqua all'interno del Data Center, incrementando sostanzialmente il livello di sicurezza degli ambienti di elaborazione che sono al riparo da eventuali danni generati da allagamenti dovuti a possibili rotture.

- Un Data Center High Density in qualunque ambiente

Oltre a fornire condizionamento supplementare, la piattaforma Liebert X-treme mette a disposizione anche una soluzione closed loop, Liebert XDFN, che isola completamente il rack con un sistema di raffreddamento dedicato e permette di gestire fino a 24kW per rack, ovvero quanto generato da un intero rack con blade server.

Liebert XDFN, infatti, è una soluzione cabinet all-in-one che ha il grande vantaggio di dissipare il calore e tutelare la continuità di funzionamento delle macchine direttamente nel rack, senza che il calore generato dalle apparecchiature IT passi all'intero ambiente. Anche questa soluzione permette inoltre di risolvere il problema del calore senza dover modificare la struttura del Data Center esistente. Que-

sto consente di ottimizzare significativamente l'utilizzo degli spazi, riducendo l'area necessaria per ospitare i sistemi di elaborazione e, quindi, incidendo in maniera sostanziale sul TCO.

Liebert XDFN, inoltre, consente di predisporre potenti Data Center anche in aree non pensate originariamente per ospitare macchine e dispositivi IT.

La possibilità di refrigerare e proteggere l'alimentazione dei server direttamente nei rack e la conseguente assenza di impatto sull'ambiente circostante (condizionamento, rumori o turbolenze) sono infatti vantaggi decisivi per realizzare Data Center High Density in qualsiasi spazio si ritenga idoneo.

Liebert XDFN, infine, prevede, oltre a un modulo di cooling ideato specificamente per i sistemi High Density, il controllo di umidità, la possibilità di ridondare il sistema cooling (N+1), il back up per la ventilazione di emergenza, l'integrazione con sistemi UPS, opzioni per il monitoraggio, la possibilità di effettuare manutenzione anche con sistema funzionante.

- Proteggere l'investimento nel tempo Software di monitoraggio, servizi di start up e un global service in grado di garantire nel tempo la disponibilità delle apparecchiature critiche, completano Liebert X-treme.

«L'ampia gamma di servizi offerti, unitamente alla nostra esperienza e alla capillare presenza sul territorio italiano - precisa Albertazzi - ci consente di meglio definire insieme ai nostri clienti la soluzione di supporto tecnico che più si adatta alle loro esigenze, al fine di garantire la continuità delle prestazioni nel tempo». G.D.B.

L'Adaptive Cooling della soluzione Liebert XD

Un approccio strutturato per proteggere il business

Rendere sicura l'azienda richiede una visione multilivello, in cui la protezione si estende dal terminale mobile remoto sino all'applicazione centrale

In un quadro in cui l'operatività aziendale dipende strettamente dalla conoscenza e dai dati, l'informazione e la sua protezione sono un bene aziendale prezioso.

La complessità della protezione cresce però con il diffondersi del concetto di convergenza. Se disporre di un'unica infrastruttura convergente multimediale integrata con l'IT dell'azienda e aperta ai clienti è un vantaggio competitivo molto forte, proprio per il fatto di essere aperta diventa critica e vitale per l'operatività aziendale.

Tutto dipende dalla continuità operativa dei processi: ne consegue che la sicurezza operativa assume lo status di esigenza primaria a cui dedicare il massimo dell'attenzione e livelli congrui di investimento, sia in risorse materiali che umane.

Il problema della sicurezza è però per certi versi aggravato proprio da uno degli aspetti più vantaggiosi per l'utilizzatore, quello della standardizzazione progressiva di applicazioni IT e Tlc, Internet in primis, ma poi i sistemi operativi, le architetture SOA, eccetera. La standardizzazione permette di razionalizzare i processi di business e le interazioni, ma lo standard ha insito un maggior rischio per quanto concerne la sicurezza, come si è verificato con Internet e gli attacchi informatici. Questi hanno potuto diffondersi con effetti anche disastrosi proprio perchè l'attacco portato al sistema informativo di un'azienda poteva essere replicato su altre aziende dotate dello stesso sistema operativo e applicazione. Gli standard, quindi, semplificano l'interoperatività, ma ne risulta una maggior vulnerabilità del sistema informativo, che si apre ad attacchi a livelli di rete e di applicazio-

ni, con la possibilità che estranei si inseriscano nei processi aziendali per carpire informazioni vitali per l'azienda e la sua competitività.

Se da una parte il mondo business è sempre più centrato su IP e su Internet per la flessibilità che ne deriva, non va trascurato che si tratta di un approccio che può essere critico per la continuità del business e la sicurezza dei dati. Se i vantaggi di un approccio aperto sono molto consistenti, gli svantaggi, per quanto concerne la sicurezza non vanno quindi dimenticati e opportunamente gestiti.

- Come affrontare il problema della sicurezza

Una cosa è certa, sempre più la sicurezza non è un concetto localizzabile e nella visione che si va affermando coinvolge tutti i livelli di un sistema ICT, a partire dal terminale periferico fisso o mobile sino alla applicazione centrale.

Inoltre, va considerato che il vulnus termini di sicurezza dei dati può provenire sia dall'interno che dall'esterno del sistema informativo aziendale, da un apparato di accesso periferico, di backbone, eccetera.

Non risulta quindi sufficiente proteggere i dati da effrazione, ma si deve garantirne la disponibilità ed accessibilità anche in condizioni fortemente critiche come quelle connesse a veri e propri disastri ambientali o ad atti terroristici. Un sistema informatico quindi, per quanto concerne la sua sicurezza, è preferibile venga suddiviso su diversi livelli di protezione concentrica, per ognuno dei quali va definito il sistema di protezione più adatto e i piani di intervento da attuare quando al suo interno si rileva un tentativo di intrusione o un attacco

in corso. Ad esempio, i livelli possono essere quello perimetrale, di accesso, dei dati ed operativo

Il vantaggio di suddividere in livelli è che un tale approccio permette poi sia l'adeguamento delle caratteristiche di un livello senza coinvolgere gli altri, sia una più facile individuazione ed incapsulamento dei problemi o la messa in quarantena degli apparati infetti.

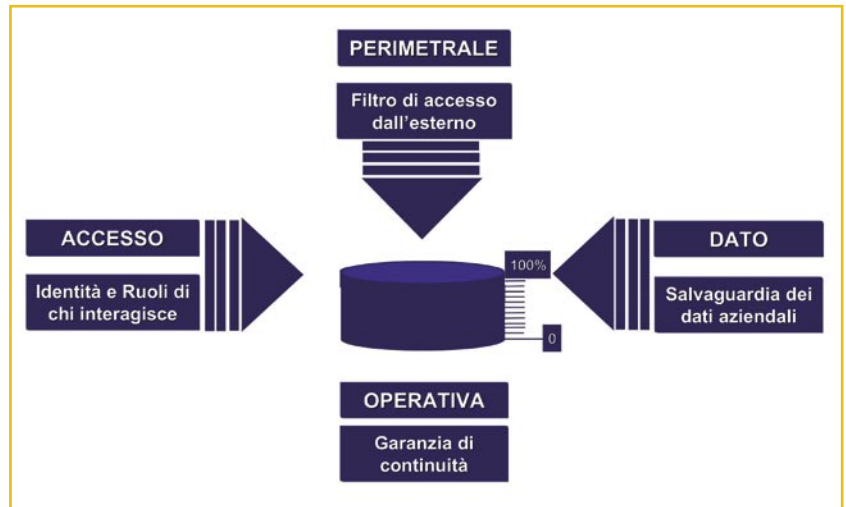
- Più connettività maggior rischio

Come assunto base, più si amplia la connettività più aumentano le possibilità che agenti esterni si inseriscano nei sistemi informativi. Gli attacchi poi non puntano al singolo utente, ma alle applicazioni, in primis la posta elettronica, per utilizzarle poi come agenti interni per moltiplicare gli effetti negativi. Un elemento critico è poi proprio quella mobilità che d'altro lato assicura una maggiore produttività individuale. Il terminale mobile può raccogliere virus quando si collega ad ambienti non protetti, che possono essere trasferiti sul sistema aziendale quando l'utente si collega al suo posto fisso aziendale.

Vanno quindi previste una serie di verifiche da effettuare sui terminali mobili quando si ricollegano al sistema ICT prima di autorizzarne l'accesso e il login alle applicazioni. Verifiche che oramai devono prevedere non solo i Pc mobili ma essere estese anche a PDA, smart phone o terminali Bluetooth, tutti oramai oggetto di attacchi da parte di virus.

Verificato che un terminale locale o remoto può connettersi alla rete aziendale il compito della sicurezza non si esaurisce, anzi, inizia la parte veramente critica relativa ai dati e applicazioni.

Concessa la connessione, il passo successivo consiste nel verificare che l'utilizzatore possa accedere alle informazioni e alle applicazioni, autorizzandolo ad usare esclusivamente le applicazioni per cui è abilitato (ad esempio scambiare mail solo con una lista di indirizzi predefiniti) al fine di contenere in aree delimitabili eventuali problemi di sicurezza. Ciò può essere ottenuto definendo per ogni utente un suo



profilo che stabilisca cosa può fare in modo da bloccarne le attività ed isolarlo dalla rete se si evidenziano accessi ad applicazioni per cui non è autorizzato.

*Possibili livelli di sicurezza
(fonte Inet)*

- Proteggere i dati

Verificato che l'accesso di un terminale al sistema ICT sia autorizzato e controllato che sullo stesso non siano presenti potenziali pericoli per il sistema e riconosciuta l'identità dell'utilizzatore del dispositivo (che può cambiare nel corso della giornata lavorativa) con la conseguente attribuzione dei privilegi e del profilo che gli è riconosciuto, si entra nella parte di attività più strettamente connesse al trattamento dei dati, ai contenuti e alle applicazioni aziendali.

È a questo terzo livello di controllo che devono essere presenti metodologie continuamente aggiornate che permettano di verificare la congruità con le applicazioni dei dati scambiati, la loro correttezza formale, la loro non pericolosità per il sistema, la garanzia della loro non modificazione rispetto all'informazione originale, la protezione da utilizzi fraudolenti, ad esempio bloccandone l'esportazione non autorizzata all'esterno dell'azienda sotto forma di allegato o corpo di una mail o tramite l'invio a spool di stampa esterni.

A questo livello vanno inoltre garantiti i diritti di proprietà dei documenti e dei contenuti nonché la loro continua disponibilità per le applicazioni che li richiedono.

G.S.

Sicurezza on demand per Internet Security Systems

Il Ceo della società statunitense illustra le strategie per lo sviluppo di un approccio orientato alla gestione end to end della security



Thomas Noonan, chairman, president e Ceo di ISS

Tra le aziende storiche della security dell'ultimo decennio, Internet Security Systems ha cambiato nel tempo l'approccio alla sicurezza, trasformandosi da azienda fornitrice di software a partner che consente di gestire il rischio aziendale e di ottenere il livello di protezione più adeguato. Thomas Noonan, Chairman, President e Ceo di ISS, ripercorre i passi fondamentali di questo processo e delinea le strategie della società.

Reportec: Internet Security Systems ha dodici anni di storia della sicurezza sulle spalle. Come è cambiata la sicurezza?

Noonan: Quando abbiamo fondato la società, nel 1994, l'ICT security andava poco oltre l'antivirus, che costituiva pressoché l'unico strumento per la protezione del computing distribuito. La sicurezza fino a quel momento era rappresentata dai sistemi chiusi e dal mainframe. Ma era già chiaro che Internet avrebbe portato a una rivoluzione. L'impulso fornito dalle nuove possibilità di contatto e condivisione delle informazioni a livello globale è tra le basi del progresso tecnologico e della sua accelerazione. Oggi più che mai i cambiamenti in infrastrutture, la mobility e i nuovi modi di utilizzare il Web creano molte opportunità di sviluppo del business. Certamente, si devono creare i presupposti per la sicurezza. È sempre stato così, ma, se guardiamo gli ultimi vent'anni dell'industria "security", il processo è rimasto invariato: ogni nuova minaccia genera una nuova tecnologia per combatterla. Questo è un modello che è destinato a esplodere. Reagire con nuovi strumenti di protezione è troppo costoso, inefficiente e non è scalabile. È ne-

cessario ribaltare il punto di vista e imparare a gestire con il rischio.

R: ISS come ha cambiato punto di vista?

N: L'eccellenza e l'avanguardia tecnologica sono da sempre gli elementi differenziatori di Internet Security Systems e i principi ispiratori di tutta la nostra strategia. ISS ha cominciato con una soluzione per l'analisi delle vulnerabilità. Da sempre, dunque, abbiamo goduto di un punto di vista privilegiato che ci ha portato a sviluppare una strategia non reattiva ma preventiva, basata non sulla scrittura di signature, ma sull'analisi delle vulnerabilità. Molte imprese del settore sono cresciute tramite acquisizioni, costruendo un portafoglio più o meno completo per combattere le varie nuove minacce, ma ottenendo un insieme di soluzioni separate ciascuna dedicata a un problema specifico. Noi abbiamo sviluppato internamente e partendo dal basso una vera e propria piattaforma per la sicurezza enterprise, perché solo un approccio olistico può contrastare le minacce ibride di prossima generazione, prevenendole.

La nostra Enterprise Security Platform risponde al bisogno di gestire il rischio, affrontando la sicurezza end to end all'interno dell'impresa e distinguendosi per tre caratteristiche. Innanzitutto, si tratta di un sistema aperto che si adatta alle realtà distribuite e mobile attuali, costruito, come accennato, dal basso e integrato. Anche quando abbiamo operato delle acquisizioni, abbiamo innanzitutto fuso la ricerca e sviluppo e integrato la tecnologia, immettendo sul mercato soluzioni che fossero allineate a tutta la nostra offerta e orientate alla prevenzione. Quest'ultima è il secondo elemento

d'eccellenza: in quanto la piattaforma ESP è "preemptive" già nel design. Anticipiamo le minacce, fornendo una protezione "0 day", cioè sin dal giorno stesso in cui viene annunciata una vulnerabilità. E anche da prima, visto che la maggior parte le scopriamo direttamente noi (il 51% secondo Frost & Sullivan – ndr). Questo è possibile grazie al grande lavoro del team X-Force, che studia le vulnerabilità e sviluppa i sistemi di analisi, i quali sono basati su svariate tecnologie, comprese l'anomaly detection, l'analisi del comportamento, quella dei protocolli e così via. Infine, l'Enterprise Security Platform si adatta alle esigenze del cliente adottando un approccio di servizi on demand e facendo di ISS un partner continuamente a contatto con la propria clientela.

R: Può chiarire meglio in cosa consistono i servizi on demand?

N: All'interno di tutti i prodotti Internet Security Systems si può utilizzare una componente di servizi: dalla gestione ad altro. Questi possono essere acquistati con la massima flessibilità. Per esempio, un servizio di monitoraggio può essere comprato a tempo: tipicamente dalle 18 della sera alle 8 del mattino, lasciando ai nostri SOC la gestione della sicurezza quando l'ufficio è chiuso, ma le attività informatiche e la rete non sono ferme (per esempio, per lo svolgimento di tutto il lavoro batch). La flessibilità è sempre stato un nostro punto di forza. Un esempio in questo senso, è Proventia G, la nostra appliance d'intrusion prevention, che può essere mantenuta off-line fino a quando il livello d'allarme segnalato da X-Force non viene innalzato. L'enorme quantità di dati raccolta da X-Force sulle reti dei nostri clienti business a livello mondiale, ci permette di avere in tempo reale il polso della situazione e di trasmettere ai nostri clienti questa esperienza.

R: Un servizio importante è quello di supporto, soprattutto nell'ambito della sicurezza. Qual è l'approccio ISS? E, più in generale, come si può aiutare l'impresa a gestire la sua sicurezza?

N: La nostra visione è sempre stata "customer

centric". Per i nostri clienti noi svolgiamo anche un ruolo di security advisor e un servizio di questo tipo è a disposizione di chiunque attraverso il nostro sito. La delicatezza del tema security, del resto, rende fondamentale la qualità del rapporto tra fornitore e cliente e non a caso abbiamo sempre investito molto per mantenerlo ad alti livelli. Continueremo a farlo: in particolare, quest'anno aumenteremo la presenza sul territorio e il numero degli operatori madrelingua nei nostri Security Operation Center. Proprio l'Italia sarà oggetto di questi investimenti, affinché ci sia sempre qualcuno che possa rispondere in italiano presso i call center. È stata aperta un'hot line che funziona senza interruzioni (24x7x365). Stiamo investendo anche nella formazione del canale, in modo da aumentare la competenza a stretto contatto con il cliente. Stiamo preparando anche nuove iniziative e comunque le imprese possono contare sui nostri servizi MSS (Managed Security Service). Oggi i servizi gestiti vanno ben oltre la gestione in outsourcing del firewall e costituiscono il complemento ideale per le soluzioni di sicurezza. Soprattutto in ambienti estesi. Si pensi alla mobilità che sposta e rende labili i confini dell'impresa. Attraverso i nostri MSS possiamo raccogliere tutta l'intelligenza distribuita dell'impresa e gestirne la sicurezza in tempo reale, grazie al Proventia Wireless Agent.

R: Per concludere, visto che ha accennato ad ampliamenti del supporto per il mercato italiano, cosa vi aspettate dal mercato italiano?

N: L'Italia e la regione mediterranea che da lei dipende rappresentano uno dei nostri migliori successi. Negli ultimi cinque anni abbiamo registrato una crescita continua con tassi del 25-30%. Riteniamo ci siano ancora grandi opportunità, che puntiamo a sfruttare innanzitutto con i prodotti che abbiamo appena lanciato e quelli che rilasceremo durante l'anno. Poi crediamo molto nel lancio del suddetto servizio di security on demand. Infine, vogliamo massimizzare l'esperienza dei clienti incrementando il servizio di supporto.

G.D.B.

Le soluzioni RSA Cyota contro il phishing e le frodi online

Grazie anche all'acquisizione di Cyota, la società americana ha potenziato l'offerta di strumenti adatti a fronteggiare le nuove minacce di Internet

È indubbio che le frodi online rappresentano un fenomeno che non è destinato a esaurirsi ed è logico che i truffatori che sfruttano Internet per condurre le loro azioni criminose tendano a individuare metodi sempre meno costosi da realizzare e più efficaci nei risultati.

Mano a mano che l'ICT evolve è dunque lecito aspettarsi che anche le tipologie di frodi si adattino e cambino di conseguenza. È quanto sta accadendo anche con il phishing, una delle minacce online apparse più recentemente ma che si è già conquistata triste popolarità a scapito delle molte vittime.

RSA Security pone molta attenzione alla lotta al phishing e alle frodi online e, nel corso dell'edizione 2006 del tradizionale appuntamento della RSA Security Conference, ha evidenziato come sia in corso un progressivo spostamento dagli attacchi di tipo più tradizionale, indirizzati in modo indistinto a una molteplicità di potenziali obiettivi, verso azioni di phishing

personalizzato. Un esempio di frode di questo tipo parte dalla sottrazione di dati personali a negozi online (nome, indirizzo e-mail, numero di carta di credito ecc.), utilizzando poi le informazioni raccolte per generare falsi e-mail di carattere finanziario corredati da dati personali e riservati dell'utente al fine di indurlo a completarli con PIN, numeri di serie o credenziali per poi rivendere tutte le informazioni a vere e proprie organizzazioni criminali.

Per fronteggiare frodi di questo e altro tipo, indirizzate agli utenti del banking online e in grado di superare i tradizionali sistemi di autenticazione basati su password statiche, RSA Security propone una gamma di soluzioni e servizi che combinano le tecnologie di autenticazione forte tradizionalmente sviluppate dalla società, con le risorse ottenute a seguito dell'acquisizione, avvenuta lo scorso dicembre, di Cyota, società a capitale privato con sede a New York, specializzata nella fornitura di soluzioni contro le frodi online.

Un esempio di dashboard disponibile online per il controllo degli attacchi di phishing



• Una rete online contro le frodi
Grazie a questa acquisizione RSA Security ha rafforzato la propria posizione nel settore dell'autenticazione sicura degli utenti per l'accesso ad applicazioni, sistemi e risorse, completando la propria offerta di strong authentication indirizzata a tutte le componenti coinvolte nell'online banking e nell'e-commerce. Cyota ha, infatti, portato in eredità a RSA non solo migliaia di clienti nelle istituzioni finanziarie, ma anche un servizio contro le frodi online e il phishing attivo 24x7x365.

Questo servizio, denominato RSA Cyota FraudAction è stato sviluppato per assistere le isti-

tuzioni finanziarie a prepararsi per un attacco prima che si portato, per rispondere quando l'attacco avviene e per affrontare in modo efficace tutte le conseguenze.

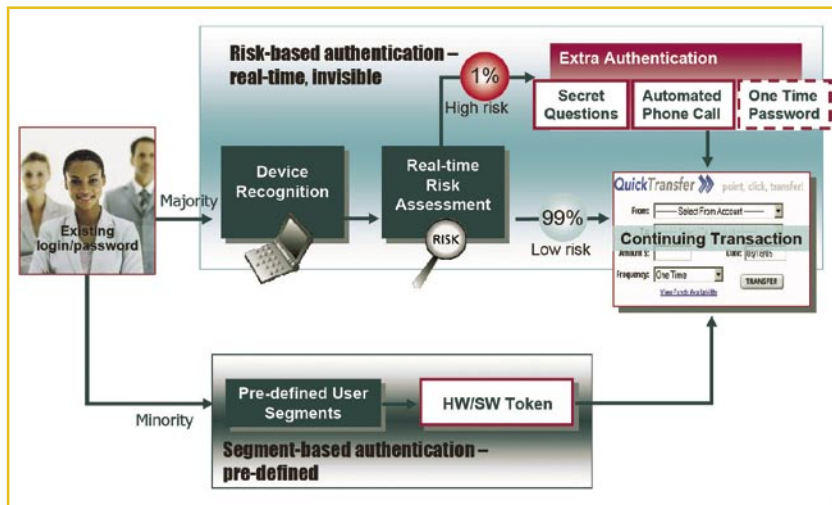
La ricetta proposta da RSA Security per combattere il phishing e i pericoli per il banking online è articolata in quattro fasi successive: segnalazione, monitoraggio, rilevamento e reporting. Queste attività comprendono, tra l'altro, la scansione di oltre 1 miliardo di e-mail ogni giorno, il monitoraggio dei Web log e degli abusi di mailbox, l'utilizzo di dashboard online. Inoltre vengono svolte attività di raccolta delle informazioni, di ricerca e comunicazione con ISP globali, l'avvio di procedure di dissuasione, la chiusura di siti fraudolenti, il blocco degli attacchi mediante collaborazioni con ISP e vendor di sicurezza e anche analisi "forensic" per acquisire informazioni sempre più dettagliate.

- Autenticazione dinamica

L'acquisizione di Cyota ha anche dato origine a una nuova divisione di RSA denominata RSA Cyota Consumer Solutions, indirizzata a fornire soluzioni di autenticazione, servizi anti-phishing e di monitoraggio in tempo reale delle transazioni e a controllare eventuali frodi per l'online banking e l'e-commerce. A tal fine RSA Security ha rilasciato una nuova soluzione denominata RSA Adaptive Authentication, che introduce il concetto di autenticazione basata su regole e differenziata in base al rischio associato alla specifica attività o, semplicemente, alla preferenza degli utenti.

Questa soluzione consente, per esempio, di affiancare funzioni di autenticazione "leggera" (idonee per la maggior parte degli utenti) con quelle di autenticazione "forte" basata sull'impiego di password monouso, per i pochi utenti con specifiche esigenze di sicurezza elevata.

RSA Adaptive Authentication interpreta l'esigenza delle banche di fornire ai propri clienti la possibilità di scegliere tra una molteplicità di tipologie di autenticazione. La soluzione genera automaticamente report relativi ai profili di rischio e permette di individuare gli utenti che potrebbero richiedere una forma più robusta



di autenticazione sulla base dei loro comportamenti e abitudini in rete. Questa soluzione permette quindi, alle istituzioni finanziarie, di passare da una tipologia di autenticazione all'altra semplicemente modificando la segmentazione degli utenti attraverso l'uso degli strumenti integrati di profilazione.

RSA Adaptive Authentication può essere implementata all'interno dell'infrastruttura informatica di chi eroga i servizi di autenticazione oppure fornita come servizio gestito che si appoggia sulla rete Go ID di RSA Security, consentendo agli utenti di utilizzare le stesse credenziali digitali per più account online, evitando il fastidio di doversi dotare di più token e senza la necessità di preventivi accordi tra i provider, come richiederebbe un modello basato su identità federate.

Il motore di analisi dei rischi della soluzione RSA Adaptive Authentication è dotato di un meccanismo di autoapprendimento basato su analisi in tempo reale dei dati, riconoscimento del dispositivo, profilazione dell'utente ed è in grado di richiedere automaticamente un ulteriore livello di autenticazione per talune transazioni se giudicate a rischio. Il motore prevede l'inserimento automatizzato e istantaneamente aggiornato delle informazioni relative ai nuovi attacchi alla sicurezza derivanti dalla RSA Cyota eFraudNetwork, al fine di garantire che le decisioni sui livelli di autenticazione da erogare siano in linea con la situazione reale delle minacce..

R.F.

RSA Adaptive Authentication consente di differenziare la tipologia di autenticazione in base ai profili di rischio

Symantec dichiara guerra a spyware e adware

La società guidata da John Thompson fornisce soluzioni per combattere il fenomeno, basate su un approccio strutturato e su tecnologie di rilevamento e filtering

La costante evoluzione dello scenario delle minacce informatiche sta attraversando una fase in cui agli attacchi legati a ragioni goliardiche o visioni pseudo-politiche, si stanno sostituendo quelli mirati e organizzati, basati su precise motivazioni di profitto. Uno dei rischi maggiori e in più rapida diffusione è legato al furto dell'identità e delle informazioni personale, finalizzato a perpetrare frodi, che ha portato all'attenzione il fenomeno dello spyware.

Gli spyware sono programmi standalone in grado di monitorare in modo nascosto l'attività di un computer - per esempio tramite il controllo della pressione dei tasti durante il login, la cattura di traffico e-mail o di quello di instant messaging - e di indirizzare le informazioni raccolte a un altro sistema. Gli spyware sono in grado di acquisire informazioni sensibili prima che vengano crittografate e, pertanto, sono potenzialmente in grado di superare molte contromisure di sicurezza quali firewall o VPN.

Sia le piccole sia le grandi aziende subiscono gli effetti dello spyware su base quotidiana, in termini di aumento di chiamate all'help desk e maggiore impiego del personale di supporto per riportare le macchine degli utenti allo stato originale di configurazione.

META Group stima che le attività di "ripulitura" dei client infetti da spyware occupi circa il 20% degli sforzi dell'help desk IT, mentre una ricerca condotta nel 2005 da Forrester Research tra i decision maker del mondo IT ha evidenziato che il 40% degli intervistati non aveva idea del numero di sistemi infettati da spyware all'interno della loro organizzazione,

mentre chi era in grado di rispondere dava indicazioni di una percentuale di circa il 20% dei sistemi.

Gli spyware sono difficili da definire, individuare e rimuovere poiché il confine tra lecito e illecito è ancora molto labile. In alcuni casi si tratta, infatti, di programmi legittimi indirizzati, per esempio, a monitorare l'utilizzo di Internet fatto dai dipendenti durante l'orario di lavoro; un altro esempio tipico di spyware sono i cosiddetti "cookie", che in molti casi sono utilizzati in modo lecito per migliorare le prestazioni di risposta di un sito durante la sua consultazione.

- **L'approccio Symantec per combattere lo spyware**

Per queste ragioni le tecnologie di sicurezza indirizzate a risolvere il problema dello spyware stanno guadagnando successo e diffusione all'interno del mercato della sicurezza IT. Si tratta di una lotta spesso accomunata a quella contro gli adware, programmi simili per natura agli spyware che determinano la visualizzazione di contenuti pubblicitari sul monitor di un utente senza un suo consenso o la sua consapevolezza e che, in alcuni casi, sono in grado di raccogliere e inviare a un computer remoto informazioni personali legate all'utilizzo del browser Internet o alle abitudini di navigazione sul Web.

Combattere lo spyware e l'adware è, come si è detto, un compito impegnativo, che richiede competenza elevata e strumenti adatti.

Symantec ha dedicato consistenti risorse in termini di R&D per la messa a punto di soluzioni indirizzate a combattere questo tipo di

minacce. Il risultato di questi sforzi è rappresentato da un approccio metodologico strutturato, che viene condotto attraverso una serie di servizi, tecnologie e prodotti per le aziende, tra cui Symantec Client Security 3.0, Symantec Antivirus Corporate ed Enterprise Edition e Symantec Network Security Serie 7100, e per il consumer e i professionisti con Norton Internet Security 2006.

L'approccio Symantec alla lotta allo spyware parte da un meccanismo di classificazione e assessment del rischio per la sicurezza legato ad applicazioni sospette, che fornisce agli utenti gli strumenti per prendere decisioni più consapevoli su cosa mantenere e che cosa rimuovere dal loro computer.

Mediante un sistema di calcolo del rischio, l'effetto generale delle applicazioni viene classificato in quattro categorie differenti: impatto sulle prestazioni, impatto sulla privacy, facilità di rimozione e capacità di celarsi; all'interno di ogni categoria, all'applicazione è poi associato un livello di rischio, definito come basso, medio o alto, accompagnato da una serie di raccomandazioni su come procedere.

- Una gamma di soluzioni diversificate in base alle esigenze Symantec offre una suite di soluzioni di sicurezza per affrontare i problemi generati da spyware e da adware indesiderati. Ognuno dei prodotti e servizi proposti da Symantec utilizza il sistema di classificazione di rischio descritto, ma si differenzia nel modo con cui questa classificazione viene utilizzata per proteggere gli utenti.

Tutti i prodotti Symantec di questo tipo forniscono la scansione in tempo reale, dispongono di funzioni di rilevazione e rimozione automatica e di tool integrati per porre rimedio agli effetti dello spyware, senza richiedere alcun intervento amministrativo.

Il punto di partenza con cui Symantec affronta la sfida di spyware e software potenzialmente indesiderabile è di riconoscere che gli utenti hanno preferenze e tolleranze differenti per il rischio. Tipicamente, le aziende scelgo-

no di rimuovere i programmi che non sono stati installati dal personale IT. In funzione di ciò il software Symantec Client Security 3.0, per fronteggiare i programmi potenzialmente rischiosi per la sicurezza, adotta come metodologia di default, la messa in "quarantena" che neutralizza il programma, ma permette, se richiesto, di ripristinarlo sulla macchina.

Questo comportamento può essere modificato dall'amministratore e reso più o meno aggressivo: per esempio con la possibilità di rimuovere automaticamente spyware/adware o, semplicemente, di limitarsi a segnalarne la presenza.

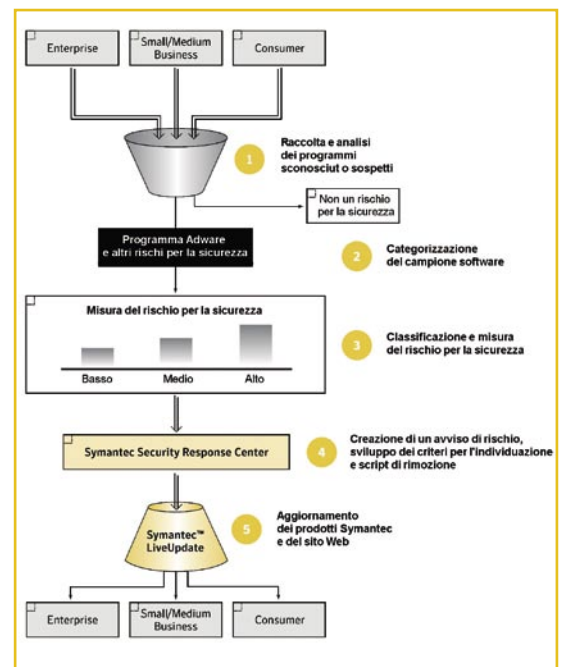
Inoltre, una particolare applicazione permessa all'interno dell'organizzazione, può essere esclusa facilmente dalla rilevazione da parte del software.

Per soddisfare le esigenze specifiche dell'impresa, Symantec ha anche sviluppato le appliance di intrusion prevention Network Security Serie 7100, su cui è possibile impostare opportune policy per rilevare e bloccare sia l'installazione di spyware e adware in base al tipo di applicazione o

alla categoria, sia la comunicazione che questi programmi attivano tra l'host che li ospita e server esterni di raccolta, evitando così che le informazioni confidenziali siano trasmesse al di fuori dell'ambiente aziendale e permettendo ai dipartimenti IT di identificare e ripulire più rapidamente i sistemi infettati.

Al settore consumer e dei professionisti è, invece, indirizzato il software Norton Internet Security 2006, che utilizza il sistema di classificazione del rischio di Symantec per il controllo di programmi potenzialmente nocivi quali spyware e adware.

L'approccio Symantec per la classificazione del rischio rappresenta il presupposto per la lotta a spyware e adware



R.F.

Il sistema informativo Dell

Le piattaforme Dell sono adottate ampiamente nel suo ambito aziendale e rappresentano uno degli strumenti chiave per dimostrare la validità delle soluzioni.

Non esiste virtualmente una società che operi nell'ICT, dal semplice produttore di hardware sino allo sviluppatore di complesse applicazioni di Business Intelligence o di Customer Relationship Management, che non affermi come alla base dei propri positivi risultati di mercato vi sia l'adozione diretta nel proprio ambito aziendale proprio delle soluzioni che propone poi ai clienti. Se si analizzano più in profondità queste affermazioni, pur del tutto veritiere, quello che emerge è che ciò ricalca, in reale efficacia e trasportabilità del modello di business, la dimensione e la tipologia dell'offerta e sovente il tutto si riduce all'utilizzo o di alcuni apparati Ict o di limitati moduli software.

La realtà Ict di un'azienda anche medio-piccola è però molto complessa e cresce con le dimensioni del suo business, del numero di fornitori e dei clienti, della sua distribuzione territoriale nonché delle esigenze in termini di logistica, di processamento degli ordini, di gestione dei magazzini, del volume della produzione, eccetera.

In pratica, sono poche le società del settore IT che possono affermare di basare una parte significativa del proprio sistema informativo e dei processi aziendali su proprie soluzioni e di aver messo a punto su queste delle applicazioni e un modello di business che ne dimostrano la reale ed efficace congruità con le esigenze espresse dai propri clienti. E soprattutto modelli che siamo applicabili anche in altri contesti.

- Un IT Dell basato su Dell

Uno degli esempi concreti è rappresentato da Dell, che, in accordo a quanto emerge dai dati e dall'analisi delle piattaforme che ha adottato, proprio su soluzioni che per il 95% sono



le proprie basi un business annuo di oltre 50 miliardi di dollari, comprendendo in queste piattaforme sia quelle server che storage e le relative capacità elaborative.

L'aspetto che evidenzia Dell è che, pur operando in un settore specifico e che per certi aspetti costituisce una società unica in quanto a modello di business adottato, deve però affrontare le problematiche e le medesime sfide che si trovano ad affrontare i suoi clienti, soprattutto per quanto concerne l'utilizzo di piattaforme e applicazioni IT o infrastrutture di rete per sviluppare il proprio business, e questo mentre nel frattempo si attua una politica di consolidamento e di razionalizzazione dei processi applicativi.

In effetti, proprio perchè la maggior parte del suo business è basato sul modello diretto e prevede un elevato grado di utilizzo dell'e-Business, Dell ha dovuto necessariamente sviluppare un sistema di supply chain e di logistica estremamente efficace, che si è tradotto in una permanenza a magazzino dei prodotti che è di pochi giorni lavorativi, un'attuazione più che concreta e su larga scala del concetto di produzione e delivery just in time. Tradotto in numeri, ad esempio, ogni giorno Dell spe-

disce e gestisce con la sua supply chain oltre 150.000 sistemi.

- Standard e consolidamento
gli elementi base

Ma su cosa si basa un modello efficace come quello sviluppato da Dell e che la società ritiene può essere replicato dai suoi clienti adottando le sue soluzioni? Su alcuni fattori chiave dell'attuale sviluppo tecnologico, architetturale e di processo relativo al mondo IT e alle strategie di mercato delle aziende: una estensiva adozione degli standard di mercato, un processo di consolidamento che ha permesso di ottimizzare i costi ma contemporaneamente di razionalizzare i processi produttivi e l'adozione di strumenti software ottimizzati. Dell ritiene che proprio la larga adozione di piattaforme basate su standard di mercato sia la chiave dei risultati ottenuti al suo interno per quanto concerne la riduzione dei costi operativi.

Il passaggio ad una visione basata su standard, peraltro con una migrazione tecnologica realizzata in pochi anni, ha permesso alla società di focalizzare meglio la propria forza lavoro, che invece di continuare a spendere il proprio tempo per mantenere in vita sistemi legacy particolarmente complessi e costosi, ha potuto focalizzarsi nello sviluppo e nel delivery di nuove soluzioni, sia per uso interno che a disposizione dei propri partner nella filiera produttiva e distributiva, come la FedEx, l'UPS o la DHL.

In base ad un'analisi interna, ha valutato Dell, la sola sostituzione di sistemi e piattaforme proprietarie con sistemi standard e aperti ha permesso all'organizzazione IT di focalizzarsi sui nuovi progetti con una capacità realizzativa quintuplicata rispetto alla precedente e questo in presenza di una diminuzione anno su anno dei costi operativi, se valutati in termini percentuali rispetto al fatturato.

Va anche osservato che questa diminuzione si è basata, puntualizza Dell, su un transfer price delle proprie tecnologie al proprio ambiente IT che è lo stesso che viene praticato ai suoi clienti e quindi i miglioramenti di efficacia ot-

tenuti rappresentano un dato reale a cui fare riferimento.

L'altro elemento chiave dell'evoluzione di Dell è stato il processo di consolidamento dell'infrastruttura di rete e di storage, che ritiene sia uno dei principali motivi dei risultati positivi ottenuti.

Il consolidamento del sistema informativo ha infatti permesso alla società di ridurre la complessità dell'IT e l'ha portata a disporre di un ambiente tecnologico in cui non solo è più semplice attuare politiche di scale out tarandole sulle esigenze reali di business ma è anche notevolmente più semplice da mantenere.

Il processo di consolidamento, va osservato, è stato molto spinto, perchè in pochi anni ha portato da una situazione in cui erano presenti più di 20 Data Center e centinaia di server farm ad una situazione attuale con due Data Center e alcune dozzine di server farm, con una razionalizzazione che ha portato anche il beneficio aggiuntivo di poter effettuare il restore in meno di 4 ore delle oltre ottanta applicazioni business critical. G.S.

I numeri chiave dell'ICT di Dell

Il fatto che le piattaforme ICT di Dell costituiscano un ambiente di test molto severo per le sue soluzioni lo si verifica nel concreto quando si considerano i numeri in gioco.

In pratica, mediante le piattaforme installate e la strategia di pianificazione e gestione che ha sviluppato, nell'anno fiscale 2006 il settore IT ha completato più di 1000 progetti, con oltre il 65% delle risorse IT dedicate allo sviluppo di applicazioni.

Il settore IT ha poi anche la responsabilità di gestire un sistema molto esteso di oltre 800 access point wireless, che supportano complessivamente circa 15000 notebook.

Ancora più elevati sono i numeri connessi alla sua rete di comunicazione mondiale su cui si appoggiano le infrastrutture IT e le relative applicazioni.

Si tratta complessivamente di migliaia di sistemi e di server che sono utilizzati per l'accesso alle applicazioni aziendali business critical.

Ad esempio, l'applicazione Dell.Com supporta sino a 65000 richieste al minuto in 81 paesi e in 24 lingue diverse. L'applicazione di gestione degli ordini, che utilizza server Dell su cui gira Oracle 10g RAC in una configurazione a grid computing, può invece supportare sino a 12000 sessioni concorrenti.

A livello globale si tratta di 80000 sistemi client distribuiti nelle sue sedi mondiali, 5000 server, 1,75 petabyte di storage, oltre 100 siti WAN e 31000 utilizzatori di servizi VoIP.

EMC per la gestione proattiva dell'infrastruttura ICT

Con l'acquisizione di Smarts, l'azienda espande la piattaforma software per la gestione e completa la migrazione da storage company a infrastructure company

L'acquisizione di Smarts, una società specializzata nello sviluppo di applicazioni per la gestione di soluzioni di rete e di intere infrastrutture Ict, sta cambiando profondamente il profilo della società di storage.

Con questa ulteriore espansione delle proprie competenze e la sua integrazione nella propria gamma di offerta software e di management, EMC completa un percorso che in pochissimi anni l'ha trasformata da società che forniva prevalentemente hardware per lo storage in una Information company prima ed ora in una vera e propria "infrastructure company".

- Verso un management globale

Con l'acquisizione effettuata, infatti, le soluzioni di management del suo ricco portafoglio di software, che oramai rappresenta una parte estremamente significativa del suo fatturato, si espandono sino a comprendere le componenti che costituiscono l'Ict nel suo complesso.

In particolare, le funzioni di modeling e di gestione dell'infrastruttura dell'azienda, dallo storage ai server e alle componenti di rete, sia per quanto concerne l'ambito geografico che locale.

Peraltro, va considerato che le funzionalità che ha reso disponibili sono a largo spettro, ha osservato Renato Simone, marketing manager di EMC Italia, e interessano sia la rilevazione di malfunzionamenti che del degrado funzionale dell'infrastruttura.

Inoltre, sono abbinate a funzionalità che permettono di capire qual'è l'impatto sulle diverse applicazioni aziendali e sull'operatività degli utenti derivanti dal verificarsi di un guasto in

uno qualsiasi degli apparati Ict, sia di EMC che di terze parti. Queste funzionalità sono particolarmente utili quanto più estesa è la rete perchè permettono di coinvolgere adeguatamente e in modo ottimale le risorse tecniche disponibili e in modo proporzionale alla gravità del guasto nonchè dell'impatto che può avere sui processi di business.

Con le applicazioni Smart al personale tecnico viene poi proposto in modo automatico dalle applicazioni software tutta una serie di tipologie di intervento e di proposte sul come procedere per la rimozione dei problemi riscontrati. L'approccio, che si evidenzia come fortemente propositivo, da una parte velocizza gli interventi tecnici di soluzione dei problemi e dall'altra permette anche a personale non estremamente specializzato di intervenire, ad esempio se il malfunzionamento si è verificato in un'area periferica della rete, una filiale, una sede secondaria, eccetera.

Ampio il range delle aziende a cui la soluzione Smarts è indirizzata, ma tipicamente di fascia medio/alta o nella gamma della grande corporate. Ad esempio, una delle ultime ad adottare la soluzione di EMC è stata British Telecom per il controllo della sua infrastruttura Ict.

Nel complesso, Smarts è una famiglia di applicazioni che permettono di realizzare funzioni molteplici nell'ambito di una rete Ict, orientate ad ottimizzare la gestione sia della sua topologia che delle singole componenti e, in particolare, a permettere interventi di tipo preventivo mettendo a disposizione una visione non solo dei guasti ma, soprattutto, degli impatti negativi sul funzionamento delle applicazioni business critical e degli utilizzatori.

- **Un inventario con Smarts Discovery Manager**

È una funzione che permette di realizzare la ricerca automatica, la modifica e la gestione dell'inventario. In particolare, permette di individuare le reti IP esistenti in azienda, i diversi componenti e le relazioni esistenti. La funzione di inventario consente di visualizzare in modo rapido e semplice la topologia precisa dell'ambiente di rete gestito individuando dinamicamente i componenti variabili dell'infrastruttura in modo automatico e in tempo reale, inclusi tutti gli elementi fisici e logici dei livelli 2 e 3. In pratica, è possibile ottenere le informazioni necessarie per controllare le risorse tecnologiche, assicurare la disponibilità delle reti business-critical e supportare gli obiettivi di gestione. La topologia dettagliata dell'ambiente di rete può essere visualizzata attraverso l'interfaccia utente EMC Smarts. L'utente ha poi la possibilità, impostando i parametri di ricerca, di generare report d'inventario esportando i dati individuati verso qualsiasi strumento di reporting standard.

Tra i benefici ottenibili che si evidenziano come particolarmente significativi vanno annoverati:

- La riduzione del TCO tramite la gestione delle risorse per l'intero ciclo di vita.
- La razionalizzazione derivante dall'individuazione e l'utilizzo di risorse in precedenza utilizzate in modo poco efficiente.
- L'acquisizione di informazioni dettagliate sui dispositivi e sulle connessioni.

- **Smarts IP Performance Manager**

È una applicazione che permette di identificare le principali cause di problemi e il loro impatto su una rete IP aziendale tramite il monitoraggio di tutte le risorse host e server presenti in rete e di cui individua i problemi che possono causare un degrado delle prestazioni.

L'obiettivo primario della applicazione, ha illustrato EMC, è quella di fornire avvisi preliminari dei potenziali problemi inerenti l'ambiente gestito in modo da garantire i tempi di risposta necessari per risolvere i problemi alle prestazioni di rete prima che determinino

conseguenze tali da pregiudicare la fornitura del servizio. Dal punto di vista funzionale IP Performance Manager esegue il monitoraggio dei dispositivi di rete, incluse le risorse host e server, e utilizza la tecnologia EMC Smarts CCT (Codebook Correlation Technology) per individuare le eccezioni prima che si verifichino guasti ai dispositivi. Tra le funzioni realizzate vi sono:

- Esecuzione di analisi in tempo reale relative all'origine e all'impatto dei problemi.
- Monitoraggio delle risorse di disco, file system, processore e memoria.
- Rilevamento dei problemi prima che pregiudichino le prestazioni.
- Applicazione di soglie e regole di polling personalizzate o predefinite.

- **Smarts IP availability Manager**

È una funzione che effettua l'analisi automatizzata delle principali cause di problemi e del loro impatto sulle reti IP e ne semplifica la risoluzione riducendo, mediante appositi filtri, virtualmente migliaia di eventi ad un numero limitato di problemi.

In pratica, EMC Smarts IP Availability Manager non solo automatizza l'analisi in tempo reale dell'origine dei problemi di disponibilità della rete IP ma fornisce anche un'analisi estesa dell'impatto sulle applicazioni.

Svariati i benefici che permette di ottenere.

Tra questi, l'individuazione dei problemi che influiscono sui servizi, l'ottimizzazione della disponibilità e delle prestazioni dei servizi business-critical e l'utilizzo dell'automazione intelligente integrata al fine di semplificare l'implementazione delle soluzioni.

A questo si aggiunge anche un insieme di aspetti relativi alla disponibilità dell'infrastruttura a costi ridotti derivanti dall'isolamento automatico di problemi critici e del loro impatto sugli elementi dell'infrastruttura IP, l'aggiornamento automatico del modello e dell'analisi intelligente in base ai cambiamenti dell'ambiente IT. di cui è possibile disporre e l'eliminazione dell'esigenze di una ridefinizione continua delle regole di manutenzione del sistema. G.S.

Nuovi scenari per il Dynamic Data Center

La tecnologia di virtualizzazione di Fujitsu Siemens Computers si è concretizzata in soluzioni che ottimizzano gli ambienti IT e la gestione delle applicazioni

Le nuove soluzioni che si stanno diffondendo nel mondo IT, dalle tecnologie blade alle architetture orientate ai servizi, sono sempre più percepite come strumenti che permettono di razionalizzare l'ambiente informativo aziendale e permettere la realizzazione di una infrastruttura IT più agile, più efficiente, più flessibile e, in definitiva, più affidabile in modo intrinseco, e questo senza dover sopportare costi non in linea rispetto ai budget a disposizione.

In tutto questo, ritiene Mario Guarnone, responsabile marketing operations di Fujitsu Siemens Computers, un ruolo fondamentale lo ricopre l'evoluzione del data center dalla sua struttura convenzionale verso il concetto di Dynamic Data Center. Per poter comprendere pienamente la situazione che si vuole raggiungere, è necessario prima analizzare il presente.

Oggi le strutture IT sono molto complesse, caratterizzate da una sostanziale staticità tra l'istanza applicativa e l'infrastruttura sottostante. Ciò implica una inevitabile lentezza nell'evoluzione di un sistema informativo. Il problema principale però è quello della scarsa efficienza in termini di rapporto tra gli investi-

menti in tecnologia e quello che rappresenta il ritorno in termini di grado di utilizzo di una infrastruttura. Ad esempio, nei primi anni 2000 uno studio Gartner riportava come la percentuale di utilizzo di una piat-

taforme mainframe fosse intorno al 60/70 %, quella di sistemi Unix al 50/60% mentre per sistemi industry standard quali i server Intel scendesse intorno al 20%.

Lo scenario attuale non è molto cambiato e le piattaforme standard continuano ad avere un grado di utilizzo relativamente basso rispetto alle potenzialità che le caratterizzano. Ciò deriva dal fatto che l'accoppiamento tra applicazioni e risorse è sostanzialmente di tipo statico, con un server che viene assegnato ad una specifica istanza applicativa.

- Dallo statico al dinamico ed al virtuale

Il concetto di virtualizzazione e di dinamico modifica profondamente questo scenario e permette di incrementare notevolmente il grado di utilizzo delle risorse, disaccoppiando quella che è la piattaforma elaborativa da quella applicativa e traendo un consistente beneficio sia dalle architetture multiprocessore che dalle nuove piattaforme blade.

Il Dynamic Data Center è alla base della strategia di Fujitsu Siemens Computers per quanto concerne l'approccio alla virtualizzazione e si riferisce all'insieme di tecnologie e applicazioni di management che permettono di ottimizzare le risorse all'interno di un Data Center.

«Sostanzialmente permette di passare da un'architettura statica ad una in cui tutte le risorse, storage, server, back up, sono gestite in pool tramite una regia che permette di associare le istanze applicative alle risorse, quando un processo richiede l'esecuzione di questa istanza. Al termine dell'elaborazione la risorsa viene rilasciata e può esser utilizzata da un al-



*Mario Guarnone,
responsabile marketing
operations di Fujitsu
Siemens Computers*

tro processo», ha illustrato Guarnone.

Da questo punto di vista un Dynamic Data Center (DDC) si presenta come un ambiente omogeneo in cui tutti i sistemi vengono conditi dalle applicazioni e le risorse sono allocate alle istanze applicative in base a livelli di servizio SLA che sono definiti o con i diversi ambiti aziendali (produzione, amministrazione, vendite, eccetera) o con i propri clienti.

Il risultato che deriva dalla trasformazione di un Data Center in un DDC è quindi una maggiore agilità dei processi, con caratteristiche di business continuity elevate per quanto concerne il funzionamento delle applicazioni, che possono essere riassegnate automaticamente ad una diversa unità elaborativa in caso di guasto di quella su cui stanno girando.

«Riteniamo che quello di DDC, proprio perchè il suo elemento essenziale è la virtualizzazione e la separazione logica tra piattaforma e applicazione, sia un concetto che permette di far evolvere l'architettura IT di un'azienda verso un approccio di Service Oriented Architecture, e in quanto tale rappresenta la nostra proposta per una architettura SOA», ha affermato Guarnone.

Uno degli aspetti salienti del DDC e della virtualizzazione delle risorse è, in definitiva, che permette ad un'infrastruttura di rispondere molto più rapidamente alle esigenze di cambiamento di una azienda. Con una struttura dinamica è molto più semplice aggiungere il supporto di una applicazione o estendere l'infrastruttura ad un numero maggiore di utenti. In quanto tale un DDC rappresenta una effettiva marcia in più per una struttura informatica aziendale.

Se i vantaggi derivanti da un DDC sono chiari non va trascurato il fatto che la virtualizzazione è un concetto relativamente nuovo e applicarlo ad una infrastruttura vuol dire intervenire contemporaneamente sulla capacità di calcolo, di storage, di back up, di rete, e così via e quindi il problema deve essere affrontato nel suo complesso, senza trascurare il fatto che le applicazioni hanno caratteristiche ed esigenze diverse.

La virtualizzazione in pratica

Una prima soluzione virtuale resa disponibile è stata FlexFrame, sviluppata insieme con SAP. "FlexFrame for mySAP" è un sistema dinamico che permette di assegnare servizi SAP residenti in remoto a qualunque server appartenente a un gruppo di risorse SAP.

In caso di necessità è possibile sia installare un nuovo server per supportare un particolare servizio SAP soggetto a forte domanda da parte dei clienti, sia riassegnare tale servizio a un server più potente. La commutazione a un server più capace viene effettuata dinamicamente nell'arco di qualche minuto, normalmente, dai 15 ai 20 minuti per ulteriori Web server, cinque minuti per allineare le applicazioni SAP, e dai 15 ai 20 minuti per allineare le risorse database.

Una seconda applicazione del concetto di virtualizzazione è FlexFrame for Oracle, che adotta i medesimi principi della precedente. Si tratta però di una infrastruttura end-to-end per Oracle Grid Computing, ed è progettata per automatizzare tutti i compiti di una griglia di calcolo e ricavare una visione univoca dell'intero ambiente server. L'approccio a grid adottato permette di eliminare il rallentamento o il crash delle applicazioni aziendali. FlexFrame for Oracle riunisce all'interno di un'unica soluzione componenti server, storage e software preconfigurati e certificati insieme con tecnologie di automazione, virtualizzazione e deployment e i relativi servizi. Come soluzione si indirizza all'intero mercato delle applicazioni basate su J2EE, gira su blade server e storage standard. Costituisce una piattaforma aperta sulla quale è possibile virtualizzare la struttura dati del software e far girare servizi applicativi e database su qualunque server della griglia di calcolo in qualunque momento.

Un terzo esempio di virtualizzazione è costituito dalla soluzione CentricStor per l'ambito storage. CentricStor, la virtual tape appliance di Fujitsu Siemens Computers, è una soluzione storage aperta che virtualizza le attività su nastro in ambienti mainframe e open system basati su Unix e Windows. In pratica, permette di disporre di un numero pressoché illimitato di risorse virtuali, interfacce di sistema standardizzate ad alta disponibilità e all'interno di una SAN permette di fornire a ciascun sistema collegato numerose risorse altamente efficienti e continuamente disponibili per le varie esigenze di backup e archiviazione su nastro virtuale.

Per risolvere questo problema Fujitsu Siemens Computers ha messo a punto un processo denominato TRIOLE che consente di implementare rapidamente la virtualizzazione delle risorse minimizzando i rischi insiti nella migrazione.

In pratica, TRIOLE si basa su soluzioni che comprendono server, storage, software di virtualizzazione e automazione che sono pre integrati e pre testati in pacchetti specifici per aree applicative.

Tra quelle già rese disponibili dalla società vi sono, ad esempio, soluzioni IT dinamiche per Web, SAP, Oracle e il back up. G.S.

I server Integrity di HP sempre più “adaptive”

Un nuovo chipset, più affidabilità, funzionalità aggiuntive e una gestione semplificata forniscono un'ulteriore spinta al successo delle macchine basate su Itanium

Le imprese sono fortemente concentrate nell'ottimizzazione delle risorse, con progetti di consolidamento, ma anche di aumento della flessibilità per continuare a supportare il business con la rapidità necessaria, senza dover rivoluzionare il sistema informativo. In un momento come questo, gli utilizzatori guardano certamente a Total Cost of Ownership e Return On Investment, ma sono soprattutto alla ricerca di soluzioni per i loro problemi. Per rispondere a queste esigenze, HP ha introdotto diverse novità hardware e software per la propria gamma di server HP Integrity, rendendone più flessibile la capacità, più semplice la gestione e più sicura la disponibilità.

«HP ha portato avanti la roadmap annunciata insieme all'adozione della piattaforma Itanium, cancellando rapidamente lo scetticismo iniziale», dichiara Simone Bruni, product marketing manager HP Business Critical Systems, precisando inoltre: «Con un ecosistema di oltre 7400 applicazioni, i server Integrity rispondono ormai alle esigenze di ambienti mission critical anche tra i più esigenti. Il successo che stiamo riscontrando anche in Italia ci dà la spinta per continuare a sviluppare e migliorare le soluzioni. L'obiettivo, però, non è la rincorsa alle prestazioni o al “record” tecnologico. Fedele alla filosofia dell'Adaptive Enterprise, HP vuole portare valori reali alle aziende. Le nuove caratteristiche raccolgono e concretizzano i desiderata

dei nostri clienti, con i quali siamo sempre in stretto contatto».

- Una maggiore flessibilità

La virtualizzazione è alla base del concetto di flessibilità. «Finora, però, l'esperienza ha mostrato che un progetto di virtualizzazione può richiedere molto tempo, anche a causa del tanto lavoro di adattamento applicativo che deve essere svolto», ammette Cipriano Manca, altro product marketing manager HP BCS. Questi spiega: «Oggi, è possibile dimezzare i tempi d'implementazione dell'HP Virtual Server Environment, grazie a configurazioni testate precedentemente in fabbrica con applicativi BEA, Oracle, SAP e IBM WebSphere. Per esempio, un progetto con BEA WebLogic che, per la sua realizzazione, richiederebbe tipicamente da 4 a 8 mesi, oggi può essere portato a termine in 2-4 mesi».

Sempre al fine di migliorare la flessibilità, HP ha sviluppato la funzione Global Instant Capacity per HP-UX II. Di fatto, alla precedente Instant Capacity, che consentiva di attivare all'occorrenza le risorse dormienti di un server, viene conferita una potenza “globale”, cioè la possibilità di considerare server distribuiti come fossero un unico insieme e, quindi, di ottenere un'unica capacità elaborativa che attraversa i data center.

- Il nuovo chipset sx2000

Le prestazioni non sono tutto, ma comunque aiutano. Aldilà dei



Simone Bruni, product marketing manager HP Business Critical Systems

“numeri” della piattaforma standard, a fare la differenza sono le caratteristiche del chipset, in particolare il nuovo sx2000 che equipaggia le macchine, a partire dai modelli rx8640, rx7640 e Superdome. Un chipset dall’architettura innovativa che migliora del 30% circa le performance «misurate in contesti reali (su processi d’I/O particolarmente stressanti e su carichi di lavoro misti) e rese possibili da una riduzione delle latenze, grazie a un rinnovato design, e da un aumento della banda, dovuto a un nuovo bus più ampio» chiarisce Manca, che aggiunge: «Questo con il processore Itanium 2, ma l’sx2000 supporta non solo le attuali generazioni di Itanium, ma anche, oltre alla prossima d’imminente rilascio nota come Montecito, le successive rappresentando un investimento due. È quindi destinato a durare nel tempo».



- Più sicurezza e disponibilità

Anche in termini di sicurezza e disponibilità, il nuovo chipset presenta notevoli miglioramenti, tanto da avvicinarlo all’affidabilità di un mainframe: doppio chip di scorta per maggiori disponibilità di memoria, tripla ridondanza delle fabric per una più grande ampiezza di banda, sistema di clock replicato e regolatori di voltaggio per eliminare i single point of failure.

Ma HP è andata oltre “generiche” caratteristiche che irrobustiscono le soluzioni Integrity, puntando ancora a fornire funzionalità in contesti concreti. In particolare, per progetti di disaster recovery, la casa di Palo Alto ha messo a disposizione dei clienti di HP-UX 11i l’esclusivo supporto per il ripristino intercontinentale di ambienti Oracle 10g e il supporto di connessioni SONET (Synchronous Optical Network).

Nuove HP Serviceguard Extensions per SAP, inoltre, aumentano la semplicità di configura-

zione di soluzioni d’alta disponibilità in ambienti HP-UX 11i e Linux. Mentre, la disponibilità sotto Windows può essere migliorata con HP Competent Cluster Service, «con vantaggi immediati soprattutto per i progetti di consolidation», come sottolinea Manca. Sempre sotto Windows viene favorita la definizione di una soluzione completa di disaster recovery in ambiente SAP, grazie al software ad alta disponibilità HP Cluster Extension.

Per chi ha comunque bisogno dei “muscoli”,

HP Integrity Superdome

il nuovo modello fault tolerant, Integrity Non-Stop NSI4000, che abbassa il livello d’ingresso in questa fascia di sistemi. La quale, che si posiziona al top della gamma in termini di affidabilità, è attualmente basata su processori Itanium, a ulteriore dimostrazione dell’importanza conferita da HP a questa architettura a 64 bit.

- Gestione dei data center più semplice

Le novità in HP-UX 11i si concludono con un importante miglioramento nella gestione e nel raggiungimento dell’efficienza operativa in un data center. Utili soprattutto all’amministratore dello stesso, le utility HP-UX 11i Distributed Systems Administration Utilities permettono a un unico amministratore, con notevole semplicità, di sincronizzare file e configurazioni per un massimo di 500 istanze di HP-UX 11i.

Più estesa l’usufruità degli sviluppi apportati a HP Systems Insight Manager, la piattaforma di gestione unificata per tutti i server HP, che è ora in grado di individuare automaticamente le applicazioni in un Virtual Server Environment (VSE) HP. «In questo modo – spiega Manca –, per un data manager risulta notevolmente semplificata la gestione delle risorse. G.D.B.

I servizi WAFS per la comunicazione enterprise

I Wide Area File Services rispondono alle esigenze delle aziende con molte filiali, migliorando l'affidabilità delle risorse di rete, il back up e lo storage

L'esigenza di comunicazione all'interno delle grandi aziende con più filiali rende insufficienti le tradizionali prestazioni delle WAN, mettendo a nudo quelle criticità della comunicazione interaziendale a cui una nuova gamma di servizi è in grado di porre rimedio.

Nelle grandi aziende con più filiali, solitamente i dati sono situati fuori dai data center centralizzati, memorizzati sui portatili dei dipendenti o su server remoti in altre sedi. Nella maggior parte dei casi questi dati sono sincronizzati periodicamente col data center centrale attraverso delle procedure di backup su WAN che fanno uso di nastri magnetici soggetti a usura e a richieste di banda geografica molto elevate. Con queste premesse, il mercato globale dei servizi dei file su aree geografiche (WAFS, Wide Area File Services) si presenta indubbiamente molto appetibile: questi servizi vengono incontro ai bisogni delle aziende con filiali dislocate geograficamente per migliorare l'affidabilità delle risorse di rete degli uffici distaccati e le loro prestazioni, così come facilitano il backup, lo storage e la condivisione dei file in tempo reale a livello aziendale.

Ogni grande azienda organizzata in filiali decentralizzate ha bisogno che i suoi dipendenti possano interagire comunicando fra di loro dovunque essi siano; nel tempo queste esigenze hanno determinato un aumento dei costi di gestione e infrastrutturali dei reparti IT. Il mercato dei WAFS si è sviluppato rapidamente a causa di questi costi, ma anche per la sempre più accentuata tendenza alla delocalizzazione dei vari reparti e, in generale, per espandere gli affari in tutti i mercati del mondo.

I prodotti WAFS permettono agli utenti degli uffici, ovunque essi siano, di accedere e condividere file con le prestazioni di accesso e di trasferimento dati tipiche di una LAN, sull'infrastruttura di una WAN. Le reti WAN, a differenza delle LAN, non sono indicate per la gestione dei file a causa dei loro alti tempi di latenza e per il throughput spesso molto limitato. Nonostante queste limitazioni, le aziende con più filiali che sfruttano le tecnologie WAFS riescono a consolidare lo storage su data center centralizzati, eliminando così la necessità di effettuare e mantenere i backup dei dati che prima si trovavano nelle filiali remote. Dato che buona parte dei dati effettivamente risiede al di fuori dei data center, la tecnologia WAFS assicura prestazioni di accesso molto elevate mentre le aziende hanno la garanzia che questi dati sono al sicuro e protetti; il tutto a costi minori.

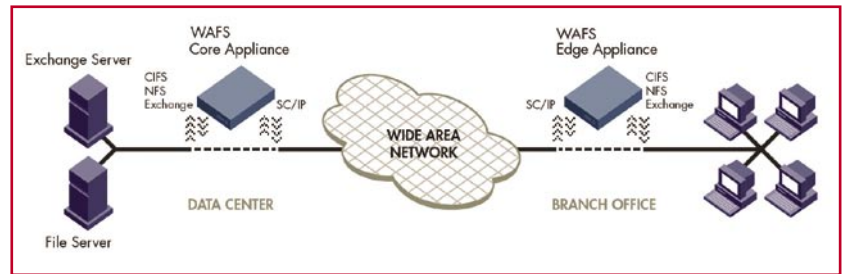
- **L'uso dei WAFS nell'e-mail**

Una situazione in cui l'uso di servizi WAFS può fare la differenza in termini di costi e di prestazioni è la gestione della posta. Negli anni l'utilizzo di strumenti di collaborazione basati su e-mail è cresciuto molto, soprattutto all'interno delle grandi aziende, dove una corretta gestione dell'informazione permette di incrementare notevolmente la produttività. L'utilizzo di questi strumenti in ambiente distribuito rappresenta una grossa sfida in termini di performance, di utilizzo delle risorse di rete e della gestione. Vi sono, infatti, diversi fattori che impattano sulle performance in ambito WAN come la ridondanza dei dati trasmessi. Se la stessa mail viene spedita a 10 dipenden-

ti, genera un traffico dieci volte superiore alla dimensione del messaggio stesso. Nonostante alcuni client di posta si comportino meglio di altri nella gestione della memoria e nell'utilizzo della rete, di norma c'è uno spreco generalizzato di risorse di rete, anche per il traffico aggiuntivo dovuto all'aggiornamento della casella "posta spedita" e per la sincronizzazione delle cartelle alla chiusura del client. Alcuni client di posta, inoltre, trasferiscono i dati solo attraverso buffer di pochi Kbyte: se il messaggio contiene un allegato, la trasmissione avviene dividendo la mail in blocchi, ognuno dei quali richiede la segnalazione di "corretta ricezione" prima che possa essere inviato il successivo, aumentando ulteriormente il traffico sulla rete. Se si considera un'azienda con qualche centinaio di dipendenti con un centinaio di messaggi di posta ognuno, si intuisce facilmente quanto i requisiti di banda diventino grandi per garantire delle prestazioni adeguate.

Per far fronte a questi problemi le aziende hanno adottato diverse strategie: l'upgrade verso sistemi di posta con una gestione più oculata delle risorse di rete, l'ottimizzazione della WAN o l'installazione di sistemi di posta distribuiti. Tuttavia ciascuno di questi approcci introduce nuove problematiche da gestire, dall'aumento dei costi alla riduzione delle prestazioni, passando per problemi legati alla sicurezza. Utilizzare server di posta distribuiti (uno per ogni filiale dell'azienda) risolve i problemi delle prestazioni ma aumenta i costi di gestione (hardware, storage, eventuali licenze software e risorse IT) dato che generalmente i server di posta sono piuttosto difficili da configurare, ottimizzare e amministrare, e le politiche aziendali di tutte le aziende di certe dimensioni prevedono il backup di tutte le mail. L'ottimizzazione della WAN viene effettuata attraverso l'intercettazione e la successiva compressione del traffico di posta al fine di ridurre la quantità di dati trasferiti: l'indubbio vantaggio legato al minor traffico viene però mitigato dalla possibile incompatibilità con protocolli di sicurezza quali RPC (Remote Procedure Call) su HTTPS. L'aggiornamento a

nuove versioni dei server di posta non sempre migliora il traffico generato dai sistemi di posta in quanto le nuove release possono privilegiare l'aspetto prestazionale rispetto a quello del risparmio di risorse.



• Le appliance per il WAFS

Per evitare questi compromessi fra prestazioni e costi, il mercato offre oggi soluzioni dedicate all'implementazione dei servizi WAFS in forma di appliance: uno dei miglioramenti principali consiste nell'eliminazione della spedizione degli allegati ridondanti nei messaggi di posta verso le filiali distaccate. Attraverso l'integrazione con i server di posta è possibile, inoltre, ridurre i tempi di latenza e accelerare i tempi di trasmissione degli allegati sulla WAN: gli allegati vengono effettivamente trasmessi solo una volta e replicati localmente, mentre una gestione differenziale delle revisioni degli allegati permette di trasmettere solo le modifiche a un allegato invece di doversi fare carico della ritrasmissione di tutto il documento. Grazie a questi miglioramenti è possibile risparmiare banda, effettuare un consolidamento dei server di posta e ridurre significativamente i tempi di attesa degli utenti per la posta.

Il funzionamento di questo tipo di appliance è basato sull'interazione fra un componente client integrato nel client di posta e un componente server che risiede direttamente sull'appliance che può essere installata nel data center. Quando un utente di una filiale spedisce un messaggio di posta con allegati, è il client WAFS che stabilisce una connessione con il server sull'appliance per effettuare una trasmissione più efficiente, grazie alla compressione dei dati o alla spedizione delle sole differenze rispetto ad allegati già inviati. R.F.

Un esempio di implementazione di appliance per i servizi WAFS (fonte: Brocade)

Da HP nuove soluzioni per il back up di file e data base

I prodotti si inseriscono negli sviluppi della società per estendere un approccio ILM alle PMI e alla gestione ottimizzata e automatica di file e data base

Nell'ambito dei processi di razionalizzazione aziendale si assiste al progressivo diffondersi di applicazioni software per la virtualizzazione delle risorse e, in particolare, di quelle di storage. Ciò è dovuta da una parte al fatto che l'utilizzatore è sempre più conscio che la virtualizzazione è un elemento fondamentale nell'ambito di una corretta politica di Information Lifecycle Management e dall'altra che le soluzioni proposte sul mercato sono sempre più semplici da usare. La "semplicità", è un fattore ritenuto di primaria importanza soprattutto nell'ambito delle PMI, dove non sempre si dispone in azienda di uno skill specializzato e la semplicità è uno dei parametri di scelta primari nell'individuare la tecnologia di storage da adottare in alternativa al back up realizzato in modo manuale.

Va poi osservato che anche a livello di PMI si è oramai consci che non basta acquisire un hardware sofisticato e performante, ma che una adeguata politica di ILM risulta efficace solo se ad esso si abbinano applicazioni di virtualizzazione automatiche e semplici da gestire. È per rispondere concretamente a questa esigenza che il software di virtualizzazione dello storage sta assumendo nella proposta di HP un ruolo sempre più importante e centrale e di recente si è arricchito di una nuova gamma di prodotti.

- Gestione integrata e semplice con HP Storage Essentials

HP Storage Essentials è un software di management che, nella strategia HP, ha la caratteristica essenziale di rispondere alle esigenze di utilizzatori che possono trarre un notevole

beneficio da una soluzione che gestisce in modo integrato ambienti server e storage. Elemento saliente della soluzione è che il responsabile dei server e dello storage aziendale viene a disporre di un unico strumento che gli permette una gestione completa dell'infrastruttura IT, con la visibilità contemporanea dello stato dei server e dello storage.

«È un approccio che gli utilizzatori ritengono molto interessante perché permette di ridurre gli investimenti in risorse umane specializzate e razionalizza la gestione, con una visione esaustiva dell'ambiente IT che è caratteristica della proposta di HP», ha dichiarato Paolo Votta, product marketing manager di HP.

Il crescente interesse da parte del mercato per la soluzione deriva anche dal fatto che si basa su un software di gestione che HP include gratuitamente nelle sue piattaforme. Con questo approccio, particolarmente aperto e caratteristico della strategia HP, un utilizzatore dispone già di base di una efficace soluzione di gestione e può adottare HP Storage Essentials in un momento successivo quando vuole ottenere i benefici che derivano da una gestione integrata di server e storage. In pratica, Storage Essentials gli permette di eliminare software diversi e disomogenei, che richiedono risorse specializzate e sono difficili da integrare e mantenere.

- RIM per ottimizzare i data base
Mettere in pratica una strategia ILM non vuol dire provvedere in modo più o meno automatico alla migrazione dei dati aziendali da un supporto fisico a un altro meno costoso. Richiede che contestualmente si realizzi questa

migrazione in base alla loro importanza per le applicazioni e alla frequenza con cui vengono acceduti.

Questo modo di procedere è del tutto necessario nell'ambito di applicazioni concernenti in particolare i data base, perchè la crescita eccessiva del volume dei dati memorizzati si tramuta in tempi di ricerca delle informazioni sempre più lunghi.

Ottimizzare le informazioni memorizzate in un data base, dal punto di vista dell'applicazione, vuol dire quindi mantenere il più contenuto possibile il volume di dati, limitandolo a quelli più frequentemente acceduti e di maggior importanza. L'ottimizzazione dei data base è però spesso realizzata con interventi manuali, volti a rimuovere dal data base parte dei dati e a procedere ad un tuning delle applicazioni. Si tratta però di interventi costosi che rimuovono il problema solo temporaneamente, causano il fermo macchina e richiedono tipicamente personale specializzato.

Proprio per eliminare questi problemi HP ha sviluppato una soluzione chiamata RIM (Reference Information Manager for Databases) che provvede a migrare in modo automatico i dati meno usati su un supporto diverso.

Il beneficio immediato che apporta è quello di rendere più veloce l'applicazione, ridurre i tempi di risposta e risparmiare i costi di interventi manuali. Inoltre, la gestione automatica dei dati memorizzati sull'archivio principale mantiene sempre il volume dei dati stessi a quello effettivamente necessario e quindi permette di effettuare più rapidamente sia le periodiche operazioni di back up che quelle di restore.

- Protezione dei dati con HP StorageWorks DPSS

HP StorageWorks Data Protection Storage Server (DPSS) è una soluzione che permette di effettuare il back up su disco in modo veloce e semplice, ha illustrato Roberto Patano, business manager per lo storage di HP.

Consiste in un server con installato Windows Storage Server 2003 e il software di back up

Data Protection Manager 2006. In pratica, l'utilizzatore riceve un box preconfigurato come hardware e software, con incluso la licenza per la gestione di tre server e deve solamente installarlo in rete. Le successive operazioni sono realizzate automaticamente dal software della soluzione, con un approccio propositivo che non richiede personale specializzato. L'applicazione effettua in modo automatico il discovery dei server presenti in rete e poi chiede all'utilizzatore quali funzioni realizzare, quali policy adottare e per quali server si desidera effettuare il back up.

L'approccio, fortemente propositivo, è volto a far fronte alle esigenze specifiche di ambienti quali quelli di una PMI.

La soluzione, ha affermato Patano, è stata pensata per utilizzatori che devono realizzare frequenti back up, anche su base oraria, ed essendo basata su Windows ha il vantaggio di interfacciarsi direttamente con Windows Shadows Copy per quanto concerne la funzione di snapshot copy. In pratica, si viene a disporre di una soluzione di "near continuity data protection" in grado di assicurare una continuità operativa prossima al 100%.

Si tratta di una soluzione specifica per il back up su disco e il salvataggio di file, ma è prevista una futura integrazione per il back up di data base, soprattutto in ambiente Microsoft.

Quattro le versioni della soluzione disponibili, rispettivamente con capacità di back up di 1, 3, 6 e 9 Terabyte, con tre licenze per server già incluse. Nel caso si desideri inserire nel back up ulteriori server è necessario acquisire la sola licenza aggiuntiva senza installare ulteriore software.

Nella famiglia delle soluzioni dei software di backup, HP Data Protector Express è ideale per ambienti sino a dieci server, pur essendo un prodotto entry ha però le funzionalità dei software di classe enterprise. È infatti un prodotto strutturato a livelli che permette di realizzare il back up su disco, su cassetta, su supporto magneto-ottico o su libreria virtuale e che supporta ambienti Windows, Linux e Netware.

G.S.

Roberto Patano, business manager per lo storage di HP



Paolo Votta, product marketing manager per lo storage di HP

Nuove tecnologie Intel per mobility e digital home

Con mobile Intel Centrino Duo e Viiv, la società apre la strada a soluzioni multicore a basso consumo che rappresentano un balzo in avanti per multimedialità e mobility

L'annuncio della disponibilità delle piattaforme tecnologiche Intel Centrino Duo e Intel Viiv è destinato a cambiare profondamente il modo di vivere l'intrattenimento in casa e in movimento e a favorire una sempre maggiore convergenza fra dispositivi di elaborazione e comunicazione. Peraltro, va osservato che il rafforzamento di una strategia volta a permettere a Intel di mantenere la posizione di avanguardia nello sviluppo di tecnologie e architetture di elaborazione si abbina anche a una nuova "brand identity", adottata per rimarcare la svolta significativa che questi annunci rappresentano per la società californiana.

La nuova brand identity sancisce, infatti, l'evoluzione di Intel verso la produzione di soluzioni in grado di guidare le tendenze del mercato. Un'evoluzione iniziata all'inizio del 2005 con la presentazione di una nuova organizzazione interna volta a favorire lo sviluppo di piattaforme tecnologiche complete, con una focalizzazione su quattro mercati chiave: mobility, digital home, enterprise e sanità.

La nuova "brand identity" di Intel comprende nuovi logo per la tecnologia Intel Viiv e la tecnologia mobile Intel Centrino Duo, e logo ridisegnati per i singoli processori, chipset, schede madri e altre tecnologie di Intel.

Nel logo di ciascun prodotto è presente il nuovo logo Intel, che include una tagline "Intel. Leap Ahead" - cioè "fa un balzo in avanti" - che rappresenta la missione di Intel di identificare e guidare i "passi avanti" nella tecnologia,

nell'education, nella responsabilità sociale, nei processi produttivi e in altri ambiti.

Ma un balzo in avanti, nella vision di Intel, in termini di qualità di vita, di lavoro, di divertimento per chi sceglie la sua tecnologia.

- Un balzo centrato su Intel Centrino Duo e Intel Viiv

Due le nuove tecnologie della strategia di Intel: la Intel Viiv, destinata a una nuova generazione di Pc per l'entertainment domestico; e la mobile Intel Centrino Duo, per i pc portatili.

La tecnologia Intel Viiv permette al pc di entrare nel soggiorno di casa, diventandone il cuore o hub e condividendo informazioni e contenuti digitali con gli altri dispositivi già presenti: TV, DVD record, impianto Hi-fi, ecc...

Con Intel Viiv, in pratica, diventa più facile gestire e controllare i contenuti digitali attraverso l'uso di un telecomando, proprio come il televisore di casa.

Le piattaforme tecnologiche Intel Viiv comprendono una gamma di processori dual core, tra cui il Pentium D, Pentium Extreme Edition e Intel Core Duo, le famiglie di chipset Intel 945, 955 o 975 Express, e la connessione di rete Intel PRO/1000 PM o Intel PRO/100 VE/VM.

La tecnologia mobile Intel Centrino Duo invece migliora ulteriormente le funzionalità che rendono le applicazioni di ufficio veramente mobili (banda disponibile permettendo) e migliorano la capacità di risposta e l'efficienza dei mobile workers.

Uno degli obiettivi che Intel si è posta con lo sviluppo della tecnologia mobile Intel Centrino Duo è di permettere alle aziende di migliorare



Dario Bucci, amministratore delegato di Intel Corporation Italia

la capacità di risposta e produttività grazie a migliori prestazioni multitasking, funzionalità di collaborazione, comprese quelle basate su voce e video su IP, e una durata prolungata della batteria.

La piattaforma supporta, inoltre, sia le tecnologie Intel Active Management che Intel Virtualization, sviluppate proprio per permettere di disporre di un miglior livello di gestibilità e sicurezza.

La piattaforma mobile Centrino Duo è costituita dal processore Intel Core Duo con elaborazione dual-core e dalla famiglia di chipset Intel 945 Express.

La piattaforma comprende, inoltre, la connessione di rete Intel PRO/Wireless 3945ABG, la connessione di rete Intel di ultima generazione, che migliora le prestazioni WLAN delle reti a standard Wi-Fi, e supporta funzionalità avanzate che aumentano la capacità di connessione e risposta.

Sotto il profilo prestazionale, i processori Intel Core Duo T2300, T2400, T2500 e T2600 hanno una velocità compresa tra 2.8 GHz e 3.4 GHz.

«Intel è focalizzata sulla creazione di piattaforme di elaborazione innovative che apriranno una nuova era nel modo di lavorare e vivere - ha affermato Dario Bucci, amministratore delegato di Intel Corporation Italia.

Le piattaforme tecnologiche Intel Viiv e Intel mobile Centrino Duo rappresentano un nuovo "balzo in avanti" nel modo in cui da oggi le persone possono lavorare e divertirsi, e il nostro impegno su più settori contribuisce a garantire la disponibilità di contenuti, software e dispositivi che consentono di sfruttare al meglio i vantaggi di una nuova generazione di impieghi ed esperienze».

- **Comincia l'era dell'elaborazione multi-core**

Il cuore delle piattaforme Intel Centrino Duo e Intel Viiv è costituito dai suoi nuovi processori dual-core ovvero con due cervelli di elaborazione su un unico processore, che adottano la tecnologia a 65 nm.

Un esempio è il processore Intel Core™ Duo che presenta il vantaggio di combinare livelli prestazionali nettamente superiori al single core con una efficienza energetica altrettanto elevata, e che quindi permette di realizzare pc e notebook sia innovativi come design che caratterizzati da una durata maggiore delle batterie.

Oltre alle tecnologie Intel Centrino Duo e Intel Viiv, Intel ha poi presentato il processore Pentium D basati su tecnologia a 65 nm, un nuovo processore dual-core per pc desktop disponibile su molti modelli della tecnologia Intel Viiv e che è in grado di fornire prestazioni potenziate per applicazioni multi-tasking, multi-user e di intrattenimento, soprattutto dove è necessario scaricare brani musicali, foto, l'editing video e la codifica audio. G.S.

Intel Centrino Duo Un futuro di portatili ultrasottili a basso consumo

La tecnologia mobile Intel Centrino Duo rappresenta l'ultima generazione della piattaforma Intel per la mobility, pensata per favorire lo sviluppo di notebook più sottili e leggeri in grado di fornire prestazioni superiori alle attuali, grazie ai processori dual-core e alla durata maggiore della batteria.

Va osservato che i miglioramenti sono significativi, come ha illustrato Intel, per tutti e quattro i vettori della mobilità, con prestazioni più elevate, funzionalità wireless evolute, una durata migliorata della batteria e formati più piccoli.

Peraltro, le nuove tecnologie aprono la strada alla realizzazione di strumenti particolarmente adatti per ambienti business.

Infatti, abbinano alla capacità di elaborazione dual-core funzioni evolute per la gestione e la sicurezza, due cose sempre più richieste in applicazioni mobili, e comprendono opzioni estese di connettività che consentono una maggiore flessibilità nella collaborazione.

Ad esempio, tramite notebook basati sulla tecnologia mobile Intel Centrino Duo un responsabile IT è in grado di:

- gestire l'ambiente IT con patch che distribuite in background.
- disporre di throughput elevato e selezione intelligente degli access point.
- gestire più reti WLAN con un'interfaccia utente semplificata.
- controllare i costi con il programma Intel Stable Image Platform.

Intel ritiene, inoltre, che un altro degli elementi che favorirà l'adozione della sua nuova tecnologia sarà la possibilità per i mobile worker di eseguire simultaneamente diverse applicazioni, mentre in background verranno eseguiti i programmi di sicurezza e di protezione antivirus.

Inoltre, riveste particolare interesse per collaborare con colleghi e fornitori tramite e-mail, condivisione di applicazioni, messaggistica immediata e telefonia su pc tramite Internet.

Le soluzioni Microsoft per la gestione dello storage

I nuovi strumenti integrati all'interno di Windows Server R2 consentono di definire quote, organizzare la capacità e predisporre il provisioning in ambienti SAN

L'esplosione nella richiesta di capacità e requisiti dello storage indotta dalle crescenti richieste di dati da parte di sistemi di e-commerce, delle applicazioni mission-critical e dei database ha determinato un deciso incremento di complessità nella gestione delle risorse di storage.

Molte aziende hanno implementato soluzioni di storage networking con l'obiettivo di superare le inefficienze dei modelli DAS (Direct Attached Storage) ma hanno poi dovuto confrontarsi con i requisiti di complessità di questo tipo di soluzioni e con temi quali la mancata adozione di uno standard per la gestione, a fronte di requisiti comuni di una visione unica e centralizzata dello storage e dell'esigenza di semplificazione delle operazioni di pianificazione, provisioning e manutenzione.

Microsoft individua cinque aspetti fondamentali che devono essere affrontati da ogni soluzione di gestione dello storage per soddisfare le richieste del business e degli amministratori Windows: scalabilità, fault tolerance, protezione di dati, gestibilità, convenienza.

Per far fronte a questi requisiti Microsoft ha esteso le funzionalità storage mediante l'integrazione di due nuovi tool denominati File

Server Resource Manager e Storage Manager for SANs all'interno degli ambienti operativi Microsoft orientate alla gestione dello storage.

- Un'evoluzione che segue lo sviluppo delle SAN

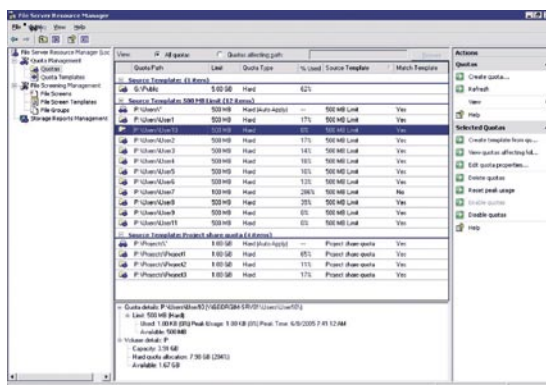
Microsoft ha introdotto funzioni a supporto della gestione dello storage fin dal rilascio di Windows NT 4.0 che incorporava la tecnologia abilitante per la connettività SAN. Alla progressiva diffusione ed evoluzione delle SAN Microsoft ha accompagnato un corrispondente sviluppo delle funzioni dedicate allo storage all'interno della piattaforma Windows.

Con Windows 2000 Server è stata aumentata la scalabilità con il supporto per 32 processori e le funzioni di failover clustering a otto nodi per far fronte alle crescenti esigenze di storage delle grandi imprese.

Windows Server 2003 è stato, quindi, sviluppato pensando in modo specifico alle esigenze dello storage in rete, prevedendo una serie di nuovi servizi che includono:

- Volume Shadow Copy Service (VSS), che abilita il backup di volumi, cartelle o file in modalità snapshot;
- Virtual Disk Service (VDS), che consente alle applicazioni software di configurare e gestire sistemi storage all'interno di una SAN indipendentemente dallo specifico tipo di implementazione
- Funzionalità avanzate di gestione disco quali la possibilità di ingrandire i volumi (utilizzando Virtual Disk Service)
- Supporto per il boot da remoto, un sistema

File Server Resource Manager è integrato all'interno di Windows Server 2005 R2



di montaggio dei volumi flessibili e un modello di driver per supportare scenari di deployment delle SAN

- Supporto MPIO (Multiple I/O Path) per le soluzioni di alta disponibilità e di load balancing.

In aggiunta al supporto per le SAN basate su Fibre Channel, Microsoft ha incluso in Windows Server 2003 il supporto per iSCSI per abilitare la connettività SAN su infrastrutture Ethernet.

All'interno del Service Pack 1 di Windows Server 2003 è stato esteso il supporto per volumi di grandi dimensioni in modo da includere i dischi GPT (GUID Partition Table) su tutte le piattaforme server Windows, è stato implementato il supporto per LUN (Logical storage UNit) più grandi di 2 TB mentre la dimensione massima del file system NTFS è stata portata fino a 256 TB. A queste funzioni si affiancano altri tool per migliorare la scalabilità, l'affidabilità e la segnalazione di errori o malfunzionamenti.

- **File Server Resource Manager e Storage Manager for SANs**

Nella R2 di Windows Server 2003 sono state introdotte due nuove funzionalità indirizzate in modo specifico alla gestione dello storage. File Server Resource Manager è una suite di tool indirizzata a far fronte a tre delle principali esigenze di storage management ovvero la gestione della capacità, delle policy e delle quote.

In particolare File Server Resource Manager permette di assegnare due tipi di quote:

- una quota a livello hardware che impedisce agli utenti di salvare file dopo che è stato raggiunto il limite di spazio assegnato;
- una quota software che non condiziona il limite, ma genera opportune notifiche configurabili.

Le funzioni di gestione della capacità presenti nella R2 del sistema operativo Microsoft permettono di superare le limitazioni delle quote NTFS disponibili a partire da Windows 2000 che potevano essere applicate unicamente su

base per utente o per volume. Le quote possono, ora, essere assegnate a una directory specifica e a un ramo di directory, applicando la quota a tutti i file interni a quell'entità storage, indipendentemente dal proprietario del file.

Inoltre, File Server Resource Manager permette di creare modelli o template per impostare set standard di limiti di quota e di soglie di notifica. Le esigenze di gestione delle policy sono affrontate in File Server Resource Manager prevedendo l'uso di "file screen" applicabili sia a un albero di cartelle sia a volumi con in più la possibilità di disporre di sofisticati report sullo storage. Le regole di screening sono basate su gruppi di file consentendo di impostare differenti policy per differenti set di file. È supportato lo screening sia di tipo passivo (gli eventi sono semplicemente registrati) sia attivo (impedisce il salvataggio di tipologie di nomi di file).

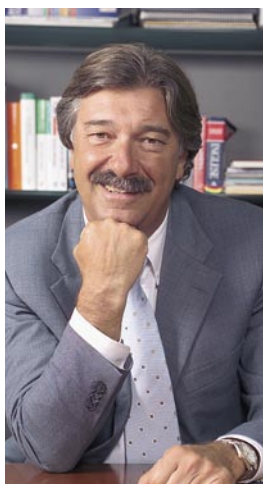
Storage Manager for SANs è uno snap-in della Microsoft Management Console che mette a disposizione degli amministratori Windows uno strumento semplice per cominciare a condividere e gestire lo storage tra i server presenti nella propria organizzazione, senza dover sostenere spese onerose per tecnologie aggiuntive.

Questo strumento software sfrutta la tecnologia Microsoft Virtual Disk Service (VDS) e fornisce funzionalità di discovery e provisioning dello storage per le SAN di dimensione più piccola. Garantisce il provisioning su dispositivi storage sia Fibre Channel sia iSCSI e consente l'assegnazione di connessioni logiche ai dispositivi storage indipendentemente dalla tecnologia sottostante.

Sui dispositivi sui cui è installato un provider hardware VDS 1.1 è possibile effettuare diversi task di setup: per i dispositivi Fibre Channel SMSs individua i server e configura le loro porte HBA (Host Bus Adapter) mentre per gli apparati storage basati su iSCSI individua i server e configura i loro initiator, crea sullo storage uno o più target iSCSI abilitando i portali corrispondenti e svolge anche le funzioni di configurazione della sicurezza. R.F.

Per StorageTek un “matrimonio” orientato alle soluzioni

L'acquisizione della società da parte di Sun Microsystems riunisce storage, server e applicazioni in un portfolio di portata ampia, che estende le opportunità di business



Dario Pardi, VP Sales & Marketing EMEA Southern Region e amministratore delegato di StorageTek Italia

Il primo giugno 2005 l'annuncio dell'acquisizione di StorageTek da parte di Sun Microsystems ha raggiunto il mercato, promettendo interessanti opportunità nel settore dello storage. A partire dal primo settembre 2005 StorageTek Corporation ha, dunque, lasciato il posto alla nuova divisione DMG (Data Management Group) di Sun Microsystems che, a livello mondiale, ha mantenuto il marchio StorageTek. A livello europeo l'integrazione è tuttora in corso, seguendo differenti tempistiche e l'Italia sarà proprio uno degli ultimi paesi a completare la fusione. Nel nostro Paese, infatti, fino al primo luglio del 2006 esisteranno ancora due distinte entità legali.

Per fare il punto sull'evoluzione delle soluzioni di storage e sul posizionamento sul mercato italiano del rinnovato player risultante dall'integrazione tra le due società, Reportec ha incontrato Dario Pardi, VP Sales & Mktg EMEA, Southern Region e AD di StorageTek Italia.

Reportec: A che punto è l'integrazione tra Sun e StorageTek e come si caratterizza la nuova divisione?

Pardi: Sta procedendo tutto molto bene, probabilmente grazie anche alla limitata sovrapposizione dell'offerta. Si tratta di un'integrazione a livello di soluzioni, che avviene sulla base delle esigenze dei clienti. Il tema dello storage è differente da quello delle applicazioni o degli ambienti di sviluppo. Questo ha determinato la creazione della divisione DMG che coniuga l'approccio di StorageTek e di Sun in un'offerta che integra le architetture SAN, NAS, la parte applicativa e quella di sicurezza. Siamo, attualmente, il quarto fornitore di storage in termini

assoluti, ma il portfolio che consegue da questa acquisizione non ha eguali sul mercato.

R: Come opera la divisione DMG?

P: La divisione è formata da specialisti dei servizi consulenziali, responsabili commerciali e di prevendita, responsabili marketing di prodotto che si avvarranno delle capacità distributive dell'organizzazione di vendita di Sun. Nei casi di progetti dedicati allo storage ci sarà un rapporto diretto e immediato, mentre nelle trattative dove lo storage è inserito all'interno di progetti di più ampia dimensione, la struttura DMG opererà a supporto. Il brand StorageTek garantirà un approccio verso lo storage a sostegno di un data center centralizzato e preposto a erogare servizi, in perfetta sintonia con la strategia globale di Sun.

R: Quali sono stati i risvolti di tipo strategico?

P: La strategia storage resta confermata e anche le roadmap di sviluppo; l'unica razionalizzazione riguarda la linea dischi, soprattutto in relazione all'offerta di storage primario. Resta un commitment molto forte verso il mondo enterprise e dei mainframe e, a conferma di ciò, abbiamo appena rilasciato il T10000 che è il prodotto che si colloca nell'ambito delle soluzioni tape drive indirizzate al segmento enterprise (con 120 MBps di throughput nativo e 500 GB di capacità nativa, N.d.R.) e prosegue la direzione verso maggiori capacità e prestazioni. Anche nell'ambito dei servizi stiamo ampliando la nostra offerta per migliorare ulteriormente la qualità del supporto.

R: Con l'arrivo della divisione DMG si aprono an-

che nuove possibilità verso il mercato delle aziende di livello medio?

P: Sono convinto di sì. La media impresa cerca soluzioni piuttosto che semplice hardware. È un tipo di mercato che, in precedenza, StorageTek, essendo focalizzata sullo storage, difficilmente poteva approcciare, nonostante la nostra offerta preveda anche librerie di fascia bassa. Queste, infatti, non potevano risolvere un'esigenza di soluzione completa, ma venivano piuttosto integrate dal canale come attached storage. Insieme a Sun, oggi, possiamo invece vendere soluzioni complete che comprendono anche la parte server e le applicazioni di Identity Management.

R: La vostra offerta come si colloca nell'ambito di una logica di ILM?

P: Stiamo assistendo a un maggiore riavvicinamento tra IT e business, che si concretizza attraverso soluzioni indirizzate ai processi e interpretate in un'ottica di ILM. Noi siamo l'unica azienda in grado di gestire il dato dalla nascita alla sua morte. Le soluzioni di backup su tape, che rappresentano il settore tradizionale di StorageTek, si integrano perfettamente con l'approccio ILM di cui costituiscono una parte rilevante. A StorageTek mancava l'integrazione con il mondo delle soluzioni a disco di tipo primario, che sono proprio uno dei punti di forza di Sun. Il mercato dello storage, inoltre, si sta indirizzando verso il software di gestione, con soluzioni di virtualizzazione e analisi e in cui noi possiamo proporre prodotti quali Global Storage Manager (il software di storage resource management derivante dall'acquisizione da parte di StorageTek, nel 2004, di Storability NdR.); il contributo del settore di Ricerca e Sviluppo di Sun darà un impulso notevole a questa parte dell'offerta.

R: Qual è la ricettività del mercato verso l'ILM?

P: La ricettività del mercato è in fase crescente. C'è un comparto di aziende che cerca di recuperare gap tecnologico rispetto alla competition ed è interessato alle esigenze più immediate: per esempio alcune aziende di financial

service che sono condizionate dalle direttive di Basilea II per il disaster recovery. Ma ci sono anche aziende che capiscono che gestire il dato è un'attività mission critical perché parte integrante del loro business. Da un punto di vista strategico, queste realtà si rendono conto dell'investimento che questo richiede e rivolgono, perciò, grande attenzione agli aspetti legati all'economicità nella gestione del dato. Questo ha determinato una maggiore apertura verso il concetto di ILM.

R: Quali sono i settori che più di altri sono sensibili a queste esigenze?

P: Il settore delle telecomunicazioni, i financial services, una buona parte delle grandi aziende e anche gli enti pubblici. La PA italiana sta rivolgendo molta attenzione alle nuove tecnologie, implementando il corretto approccio di selezionare quelle soluzioni indirizzate a offrire servizi migliorativi, anziché un'adozione passiva di strumenti tecnologici. In ambiti quali il Ministero degli Interni, la Polizia e in altri progetti che stiamo seguendo abbiamo potuto riscontrare la presenza di comparti tecnologicamente attenti e con competenze molto accentuate, orientati alla soluzione dei problemi. Le banche italiane sono partite un po' tardi rispetto ad altri Gruppi europei, ma stanno ora cercando soluzioni più sofisticate e recuperando un po' di gap tecnologico.

R: Si ripropone il legame tra storage e sicurezza?

P: Si tratta di due elementi indissolubili, così come storage e business. C'è un'evoluzione dello storage come risorsa strategica, così come 5 anni fa è successo per il networking, 10 anni fa per le telecomunicazioni ISDN e 20 anni fa per il pc.

R: Quali sono gli attuali trend di crescita di StorageTek in Italia?

P: Nel 2005 in Italia, escludendo il trimestre tra luglio e settembre che è stato condizionato dall'acquisizione, StorageTek ha avuto una crescita intorno al 12-13%. I dati del primo trimestre del 2006 confermano questo trend.R.F.

Terasystem ottimizza il backup dei database Oracle

La soluzione Terasystem Oracle RMAN automatizza la definizione degli script per le operazioni di salvataggio e ripristino con un approccio grafico

La presenza di svariati ambienti Oracle distribuiti a livello aziendale, ognuno con le sue specificità in termini temporali o di frequenza per quanto concerne le attività di backup e di restore, è una realtà che caratterizza un numero crescente di aziende, di fascia sia enterprise sia media.

La preparazione degli script che descrivono come queste attività devono essere svolte è un compito che spetta all'amministratore di sistema e che, dunque, diventa sempre più oneroso.

Questo sia per la modalità stessa della preparazione basata su script, che richiedono una conoscenza specializzata e approfondita, sia per l'ampio numero di parametri connessi agli ambienti che devono essere considerati in fase di scrittura.

Inoltre, va considerato che più estesa è l'azienda, maggiore risulta il pericolo che alcune componenti o funzionalità possano essere trascurate nella preparazione degli script, con il rischio di non includervi elementi essenziali per il funzionamento di alcuni dei business aziendali che necessitano di Oracle.

- Automatizzare gli script per semplificare la gestione

La soluzione Terasystem Oracle RMAN (TOR) risponde alle esigenze degli amministratori di sistema e li assiste con un approccio pratico e razionale nell'approntamento degli script per le attività di backup e di restore in ambienti Oracle.

L'aspetto saliente della soluzione è che sostituisce, all'approccio classico di preparazione, un approccio grafico, intuitivo, semplice, basa-

to su finestre che propongono i range di valori e di parametri da scegliere per le attività di backup e di restore.

Una volta compilati i campi previsti (con l'applicazione che verifica automaticamente la congruità dei dati inseriti con le caratteristiche del sistema, riducendo così la possibilità di errori e permettendo di affidare tale attività anche a personale meno specializzato) è TOR che automaticamente trasforma tutti i valori definiti nell'interfaccia a maschere video nello script che poi serve, in ultima fase, per istruire il sistema su come deve essere effettuato il backup dei data base.

Non solo, un ulteriore valore aggiunto è rappresentato dal fatto che l'applicazione TOR di Terasystem effettua in modo automatico anche il discovery degli ambienti informatici e delle istanze Oracle presenti nel sistema informativo aziendale, evitando quindi che alcuni aspetti possano essere trascurati nella preparazione degli script.

- Una soluzione aperta e multiplatforma

Un altro elemento significativo offerto da TOR è la sua indipendenza dal software di backup. TOR è uno strumento software che è nativamente indipendente dal software di backup adottato perchè lavora a livello RMAN di Oracle e quindi, anche se l'ambiente data base deve essere necessariamente Oracle, per quanto concerne le applicazioni di backup e di restore dello storage può essere adottato per ambienti basati sia su software Veritas sia EMC Legato Networker. TOR non è poi una soluzione vincolata a una particolare piattaforma

ma è aperta alle diverse piattaforme di sistema operativo che supportano Oracle, come tutte quelle Microsoft Windows.

Il suo funzionamento e utilizzo è semplice. Una volta che tramite TOR lo script per il backup/restore di Oracle è stato preparato in modo automatico a partire dai dati inseriti in modo guidato a video, Terasystem lo integra all'interno delle sue piattaforme, così da istruire i server di rete con le informazioni inerenti allo svolgimento automatico delle attività pianificate: a che ora deve partire il backup, le componenti interessate e così via.

Numerose le funzioni automatiche che semplificano la gestione.

Per esempio:

- permette di definire facilmente e centralmente le policy per il backup e il restore;
- effettua automaticamente il discovery delle istanze;
- permette di predisporre semplicemente gli script sia per il backup che il restore;
- riduce i tempi di preparazione degli script e ne verifica la congruenza con l'ambiente Oracle;
- è utilizzabile in tutti gli ambienti operativi su cui gira Oracle.

• L'intelligenza di TOR

Il discovery delle istanze è una delle attività salienti di TOR. Lo strumento è in grado di individuare la presenza delle istanze in rete di Oracle tramite una funzione che le individua e le cataloga. Anche questa funzione si basa su una semplice interfaccia grafica che permette di definire il range di indirizzi IP di rete da verificare.

Al termine della scansione i risultati sono evidenziati a video in una tabella grafica su cui sono riportati due diversi elenchi, quello che contiene le istanze attive e quelle spente, per cui non è stata rilevata nessuna istanza.

E poi possibile decidere quale delle istanze evidenziate devono essere incluse nella preparazione automatica degli script per le funzioni di backup e di restore.

Come accennato, obiettivo principale della

soluzione sviluppata da Terasystem è quello di facilitare la preparazione degli script. Selezionata l'istanza Oracle, lo strumento propone a video al system administrator un insieme di scelte, inerenti alle funzioni previste dal catalogo Oracle, che lo guidano nella preparazione delle modalità di backup/restore. Completato l'inserimento delle informazioni preliminari il wizard grafico richiede la definizione della tipologia di script da compilare proponendo tre diverse modalità: Database online, Archive log, Recover senza control file.

Una volta che il system administrator ha selezionato la modalità prescelta, viene proposta, sempre tramite interfaccia grafica, la possibilità di determinare:

- il livello di backup, se full o incrementale;
- il numero di sessioni da utilizzare per il backup/restore;
- la possibilità di escludere dalle operazioni di backup le tabelle off-line o read-only;
- l'inserimento i parametri software Legato Networker o Veritas da utilizzare nell'allocatione dei canali;
- specificare la nomenclatura del backup set.

Terminata la selezione dei parametri proposti da inserire nello script RMAN, il wizard grafico termina e TOR genera automaticamente lo script pronto per l'uso e da importare sulla macchina oggetto dell'attività di backup e restore.

GDB

Il backup in ambienti Oracle

La diffusione dei sistemi di backup centralizzato e il costante aumento dei livelli di servizio richiesti, comporta una crescita esponenziale dei database applicativi e congiuntamente una continua riduzione della finestra temporale da dedicare alle attività di backup/restore.

A fronte di queste esigenze sono state definite specifiche strategie di integrazione dei database all'interno di politiche di backup a caldo.

Ogni singolo database integra uno specifico modulo di backup/restore che necessita uno script per assicurare la messa in sicurezza del DB senza dover fermare le istanze (quindi a caldo).

In ambienti Oracle, per esempio, tale modulo è definito RMAN (Recovery Manager) e l'integrazione del DB nell'ambiente di backup richiede una corretta configurazione tra questo e il software di backup terze parti. Tale attività viene assolta tramite un apposito script che deve essere compilato dall'amministratore del DB o da un consulente Oracle esperto di RMAN.

I Managed Communications Services di Alcatel

La società ha sviluppato servizi che permettono di fornire al mondo enterprise soluzioni che riducono fortemente capex e opex delle infrastrutture ICT

Una delle componenti più significative della proposta tecnologica di Alcatel è costituita dalla sua piattaforma di servizi gestiti, raccolti nell'offerta di Managed Communication Services (MCS). Questi peraltro si abbinano alla sua proposta a 360 gradi di soluzioni voce/dati e di infrastrutture per reti private e pubbliche praticamente in tutti gli ambiti di rete, dalle Wan alle Man, dal rame alla fibra ottica, dalle reti Sdh a quelle Ip e MPLS. Mentre quest'ultime piattaforme si rivolgono sostanzialmente alla realizzazione in house di infrastrutture sia per l'ambito pubblico che privato, gli MCS hanno come target primario quello dei service provider, a cui permettono di erogare rapidamente nuovi servizi al mondo enterprise e delle Pmi, mettendo in condizione un'azienda di ottenere consistenti benefici perchè può fortemente contenere il Capex e annullare quasi del tutto l'Opex connesso alla gestione di una propria infrastruttura ICT.

La modularità della soluzione e il fatto di basarsi su applicazioni software fa sì che gli MCS possano trovare utilizzo anche in ambiti Corporate, laddove è utile disporre di servizi da erogare alle divisioni o società del gruppo, con un approccio da centro servizi e con il billing per i diversi centri di costo realizzato in base all'uso che viene fatto dell'infrastruttura Ict.

Con questa proposizione Alcatel fornisce una soluzione completa per tutte le applicazioni di IP Communication, integrando soluzioni ed apparati di fascia enterprise con soluzioni e piattaforme tipiche per operatori, in modo da garantire la fruibilità di servizi IP carrier grade anche alle imprese, ed in particolare alle PMI, che altrimenti non potrebbero permettersi gli

investimenti per accedere alle tecnologie di nuova generazione.

- Un focus su 4 categorie di MCS Alcatel è focalizzata su quattro diverse categorie di Managed Communication Services. Managed Network Services (MNS), pongono l'enfasi sui Converged Virtual Private Networking Services (VPNS), supportano reti virtuali private di tipo IP (IP VPN), servizi Lan virtuali private (VPLS) e servizi di linee affittate virtuali (VLL).

Managed Business Communication Services (MBCS), sono un insieme di servizi che permettono di erogare funzioni di IP-Pbx di tipo avanzato, comprese opzioni per la gestione degli utenti mobili, sia via rete che con soluzioni di tipo "on premises". Ad esempio, MBCS mette in grado di utilizzare telefoni portatili per accedere ad applicazioni aziendali (anche con i IP-Pbx esistenti) o di supportare telefoni dual-mode che commutano automaticamente tra reti WiFi e reti cellulari pubbliche in funzione del tipo di copertura. Attraverso queste soluzioni è di fatto possibile la migrazione graduale dalla tecnologia TDM a quella IP e la convergenza tra il mondo fisso e quello mobile.

Managed Employee Interaction Services (MEIS) sono delle soluzioni che permettono di erogare agli utenti servizi di Unified Communication che permettono di accedere alle proprie risorse aziendali (telefoni, email, directory) da qualsiasi terminale e servizi di Collaborative Working integrate con Audio e Video Conferenza, e al contempo far sì che il telefono di utente possa essere visto come una extension del Pbx Legacy o come un telefono mobile

standard nell'ambito della rete a commutazione di circuito.

Managed Customer Interaction Services (MCIS) sono un insieme di servizi che mettono a disposizione sofisticate funzioni di Contact Center multicanale, incluso tra questi il dialogo interattivo e il routing delle chiamate basato su elaborate funzioni di inoltro, anche in questo caso sia via rete che con soluzioni di tipo "on premises". Le soluzioni sono sia stand alone (per grandi progetti) sia agenti software da installare su IP-Pbx per piccole realtà.

La proposta di MCS si è espansa con una nuova gamma di soluzioni destinate ai carrier e ai service provider. Le novità includono la soluzione Alcatel 8628 Multimedia Instant Conferencing (MMIC) per servizi gestiti di interazione intra-aziendale e la suite Alcatel Corporate Mobility Manager (CMM) che includono Virtual PBX e Intelligent Mobile Redirect per le comunicazioni convergenti fisso-mobile.

- **Alcatel 8628 MMIC per la comunicazione intra-aziendale**

Parte della suite di Alcatel per i servizi gestiti di comunicazione intra-aziendale, l'Alcatel 8628 MMIC fornisce servizi di audio, dati e video conferenza, oltre a funzionalità di instant messaging e di condivisione di documenti.

In pratica, con Alcatel 8628 MMIC, i dipendenti possono comunicare istantaneamente con i loro contatti, condividere documenti e applicazioni da qualunque postazione abilitata e interagire con i colleghi in tempo reale.

L'8628 MMIC è una soluzione carrier-grade e basata su web, e quindi accessibile anche da differenti Intranet. Adotta un'architettura thin client che limita i requisiti e le funzionalità software richieste al terminale dell'utente, un approccio che presenta il vantaggio di consentire ad un'azienda una elevata libertà nella scelta e nell'impiego di terminali, garantendo una maggiore flessibilità e mobilità.

Il beneficio non si ha solo per gli utilizzatori perchè la soluzione Alcatel permette di ridurre anche il TCO degli operatori, grazie al sostanziale contenimento dei costi di sviluppo

dei nuovi servizi e di manutenzione. Inoltre, permette di risolvere anche il problema della complessità delle reti di comunicazione perchè l'utente non deve più configurare porte specifiche nei firewall di rete. Come soluzione, l'Alcatel 8628 MMIC è stato già adottato da una decina di operatori nel mondo, ed è basato sull'applicazione aziendale Alcatel My Teamwork. La funzione di Videocollaboration viene implementata in accordo con le soluzioni di IP VideoConference di Polycom, società tra i leader mondiali del settore).

- **Il Corporate Mobility Manager**

Attraverso la propria applicazione di Corporate Mobility Manager, Alcatel fornisce una soluzione integrata di VPN voce e dati per servizi fissi e mobile, una soluzione di Virtual PBX che permette agli utenti di cellulari di accedere alla maggior parte dei servizi del PBX (direttore-segretaria, directory, ecc.) direttamente dal proprio telefono cellulare ed infine una soluzione specifica per le imprese, integrata con i PBX aziendali per permettere le comunicazioni integrate anche in ambiente WLAN. In particolare attraverso IMR un dipendente provvisto di cellulare o PDA dual mode (WiFi-GPRS) può iniziare una comunicazione sotto una copertura (es. GSM) e continuarla con hand-over automatico nel momento in cui si trova sotto l'altra (es. WiFi). G.S.

KPN ha scelto Alcatel per servizi di telefonia pay-per-user per le PMI dei Paesi Bassi

KPN ha scelto la soluzione Alcatel Managed Communications Service per erogare servizi di telefonia avanzata alle aziende sul modello pay-per-user.

Destinata ad aziende dai 20 ai 250 dipendenti, l'offerta di servizi IP-PBX gestiti KPN Zakelijke TelefoonCentrales propone una tariffa di 9,95 euro al mese per utente. La soluzione, che consente alle aziende di incrementare o diminuire mensilmente il numero di utenti e servizi, permette ai clienti di pagare esclusivamente quanto effettivamente utilizzato. Poiché la proprietà e il funzionamento delle apparecchiature IP-PBX sono a carico di KPN, i clienti possono contenere al massimo gli investimenti di capitale iniziali necessari per approntare e attivare il sistema. I servizi si basano sulla piattaforma OmniPCX Office, e forniscono innovative funzioni di telefonia, tra cui funzioni di telefonia IP standard ed avanzate, messaggistica vocale e mobilità.

Nella Business Communication si diffonde lo standard SIP

IP assurge sempre più a standard universale per la comunicazione e ad esso si abbina la diffusione e la progressiva adozione dello standard SIP

L'ultimo anno ha visto continuare la diffusione di IP come elemento portante nello sviluppo delle soluzioni di fonia. A questo si è accompagnato un pari fenomeno di diffusione di standard di mercato e, in particolare, di Linux come sistema operativo e di SIP come protocollo per realizzare le sessioni di comunicazione tra utenti finali.

Entrambi i fenomeni si inquadrano nella evoluzione più ampia verso reti convergenti fonia dati e una pari convergenza tra applicazioni informatiche e di telecomunicazione.

Uno degli aspetti che maggiormente caratterizza le reti convergenti multifunzione è proprio il fatto che adottano progressivamente modalità di colloquio tra i terminali di utente, di tipo standard, atte a favorire la comunicazione tra dispositivi disparati ed intelligenti. In pratica, questi standard prevedono lo spostamento dell'intelligenza dalla rete e dai suoi apparati verso i terminali di utente, sia che si tratti del telefono, fisso o mobile, sia di un pc portatile su cui giri un'applicazione SoftPhone.

- Nuovi apparati per nuove funzioni
Nell'ambito di reti a commutazione di pacchetto, realizzate in base al modello IP, va osservato che le sessioni di comunicazione costitui-

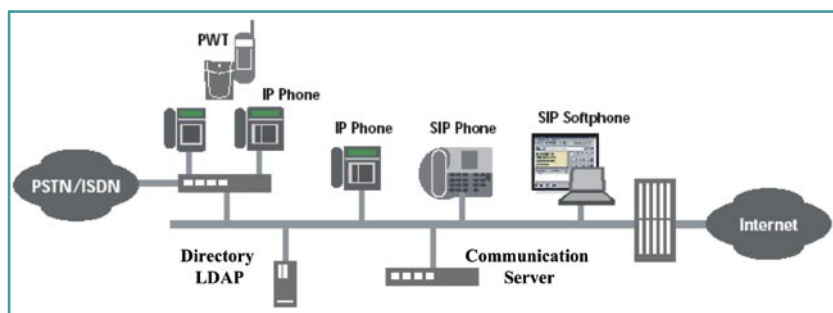
scono delle ulteriori applicazioni di rete e, in quanto tali, richiedono da parte della rete un insieme di servizi che ne supportino adeguatamente il transito, rispettandone le caratteristiche di base. Queste esigenze hanno condotto allo sviluppo di funzionalità specifiche riferibili come classi funzionali, che sono implementate su apparati specializzati, ad esempio il Communication Processor.

Una di queste comprende le funzioni di Call Processing e di segnalazione, in pratica la funzione di gateway per lo scambio della segnalazione al fine di rendere possibile stabilire la chiamata attraverso la rete a commutazione di pacchetto/IP. In questa classe, ad esempio, è compreso quanto necessario per il trasferimento di segnalazioni telefoniche di tipo convenzionale.

Una seconda classe comprende funzioni di Packet Processing e ha il compito di elaborare i pacchetti di segnalazione e di trasporto della voce, aggiungendovi le intestazioni necessarie per il trasporto in rete prima di passarli alla rete, che non necessariamente deve essere di tipo IP. Rientra nell'ambito di questa classe anche la trasformazione dei criteri di segnalazione telefonica nella codifica di pacchetto, definita dal protocollo di rete. La classe di Call e Packet Processing può poi comprendere altre funzioni specifiche per l'elaborazione della voce o per la gestione.

La funzione di Voice Processing predispone i campioni di voce per la trasmissione sulla rete dati con modalità di campionamento che dipendono dallo standard adottato. È una funzione molto critica, che richiede una forte capacità elaborativa e in genere realizzata me-

Esempio di sistema di fonia basato su IP



dianete circuiti integrati DSP dedicati.

Di particolare importanza è la funzione di Call Processing, alla base del funzionamento di una rete convergente per la componente di fonìa, anche se esiste il problema della presenza di diversi standard di segnalazione che devono essere supportati a livello di rete.

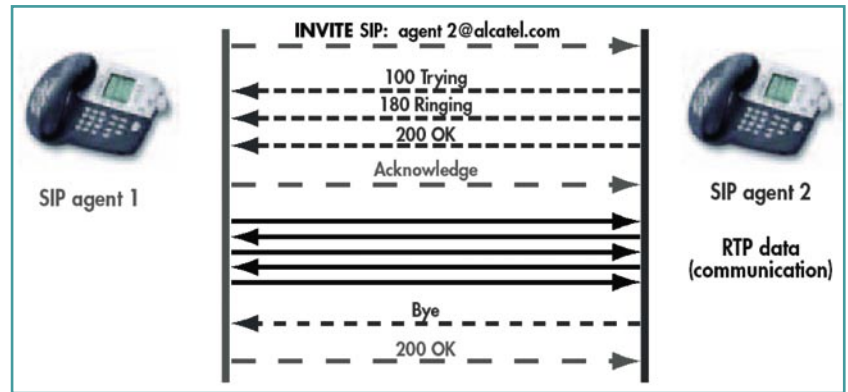
- L'affermarsi di SIP

Lo standard SIP (Session Initiation Protocol) sta progressivamente sostituendo il più datato H.323. Sviluppato in ambito Internet e IP, è stato definito dall'IETF con l'RFC 2543 del marzo 1999. Ha un'architettura completamente diversa da quella che caratterizza lo standard H.323, perché non prevede una gerarchia di apparati di rete e si basa sostanzialmente sul concetto tipico di applicazioni IP client/server. Mentre con l'H.323 la capacità elaborativa, gli standard e la realizzazione dei servizi è concentrata principalmente negli apparati della rete con il SIP le funzionalità necessarie alla realizzazione delle funzioni di comunicazione sono concentrate nei terminali di utente. Nell'ambito di applicazioni multimediali e, in particolare, di telefonia su IP, all'interno di un terminale vengono così a coesistere entrambe le funzioni di un'architettura client/server.

Quando il terminale effettua la chiamata funziona come client mentre quando la riceve opera come server. Un terminale SIP deve quindi essere sempre on line e mantenere attivi quei processi che gli permettono di rilevare una chiamata in arrivo.

SIP opera a livello applicazione e ha il compito di permettere lo stabilire e terminare chiamate o sessioni multimediali e di invitare altri membri a partecipare a una sessione già attiva. Pur essendo stato pensato per operare in modo ottimale in ambiente IP, di cui adotta il formalismo, può operare anche su reti che adottano protocolli diversi dall'IP, quali il Frame Relay o l'ATM, e quindi supporta anche reti in fase di migrazione.

La visione IETF che pone Internet e il client/server al centro dell'ICT, si rispecchia anche nella struttura sintattica del protocollo di se-



Esempio di attivazione di una sessione e modalità di dialogo (fonte Alcatel)

gnalazione, che ripercorre la strada già adottata per il Web, basata su una messaggistica di tipo testo, con una sintassi conforme a quanto si ha per l'HTTP.

Peraltro, un tale orientamento facilita l'integrazione con l'ambiente Internet, perché non solo per il linguaggio, ma anche per gli indirizzi utilizzati nell'ambito dello standard SIP si segue una struttura analoga a quelli di posta elettronica.

- Come si stabilisce la sessione

SIP prevede che una sessione tra due utenti sia realizzata mediante un insieme di servizi che permette di determinare la localizzazione dell'utente di destinazione, la capacità dell'utente stesso in termini dei parametri da usare durante la sessione, la disponibilità dell'utente di comunicare, il setup effettivo della chiamata, stabilendone i relativi parametri, e, infine, la gestione della chiamata stessa. Come è possibile osservare, tra le funzionalità elencate non rientra quella di allocare risorse di rete, ma esclusivamente l'individuazione dei parametri che le due parti in sessione devono utilizzare una volta entrate nella fase effettiva di conversazione.

SIP dispone anche di servizi di sicurezza che prevedono l'autenticazione dell'utente, meccanismi per la protezione da attacchi del tipo denial-of-service. Inoltre, essendo i messaggi di tipo testuale, vi è la possibilità di cifrare il corpo del messaggio.

Tutte caratteristiche, quelle descritte, che ne giustificano ampiamente la progressiva diffusione.

G.S.

Cisco Systems unifica la comunicazione

Al via la strategia Unified Communications, che punta a integrare le molteplici soluzioni oggi usate in azienda per aumentare la produttività

Nelle aziende oggi si assiste al proliferare delle soluzioni di comunicazione. Per raggiungere un collega, abbiamo a disposizione, secondo una recente ricerca di Sage Research, una media di sei strumenti a testa, scegliendo fra una telefonata, sul fisso o sul cellulare, un sms, un'e-mail, un messaggio in segreteria telefonica (anche qui sul fisso o sul mobile), una chat e via dicendo. Il risultato è che una persona può ricevere più volte la stessa informazione e che questo eccesso di comunicazioni non correttamente indirizzate porta a ritardi nei processi decisionali.

A questo, si aggiunge il fatto che la mobilità è in continuo aumento, con il 27% delle persone che si sposta dall'ufficio almeno una volta al mese. Ciò porta con sé l'esigenza di essere reperiti nel modo più opportuno, anche perché il fatto che non si riesca a raggiungere una persona causa, in definitiva, il rallentamento del progetto su cui si sta lavorando.

«È positivo che siano nati nuovi strumenti di comunicazione - afferma Danilo Ciscato, Direttore Business Development & Marketing di Cisco Systems Italy -. Ma la mancanza di integrazione fra questi strumenti porta, paradossalmente, a un calo di produttività».

Secondo Cisco, queste esigenze spingono a fare un ulteriore passo in avanti nell'evoluzione delle soluzioni di telefonia IP, un settore in cui l'azienda ha fatto il proprio ingresso nel 1997. Da allora, passo dopo passo, Cisco ha conquistato

una posizione di primo piano, posizionandosi, secondo Synergy, al primo posto, in termini di fatturato, alla fine del 2005. I clienti in questo ambito sono 38mila, mentre i telefoni IP consegnati hanno raggiunto quota 7,5 milioni.

È venuto, dunque, il momento di unificare le comunicazioni: d'ora in avanti, tutte le soluzioni di IP Communications di Cisco aggiungeranno la parola "Unified" al proprio nome.

• Focus sulle applicazioni

Negli anni passati, la strategia dell'azienda si è concentrata dapprima sulla convergenza voce e dati a livello di media, con l'obiettivo primario di ridurre i costi delle comunicazioni grazie all'unificazione dei flussi, e, in una seconda fase, sulla convergenza dei servizi, con le tecniche di virtualizzazione.

Il varo di Unified Communications, sposta il focus sulle applicazioni, con l'obiettivo di creare un sistema in cui sono "annegati" tutti gli strumenti attualmente in uso mentre l'utente può accedervi con un'unica interfaccia, in base alle sue preferenze.

«I pilastri del sistema Unified Communications sono tre - illustra Gianluca Ferrè, Business Development Manager Unified Communications -. In primo luogo l'efficacia, che deriva dall'integrazione, in secondo luogo la collaborazione, ovvero permettere alle persone di lavorare anche in mobilità, e in terzo luogo l'apertura agli standard, per poter integrare dispositivi e applicazioni di fornitori diversi».

Unified Communication riguarda il sistema di IP communication nella sua totalità: i terminali e il sistema di call processing, ovvero le piattaforme utilizzate dagli utenti, le infrastrutture e

*Danilo Ciscato,
Direttore Business
Development e
Marketing di
Cisco Systems
Italy*



le applicazioni. L'offerta di prodotti è ampia e articolata e consente di rispondere alle richieste delle organizzazioni più piccole, a partire da 8 utenti, fino alle grandi multinazionali. Per i clienti che dispongono di versioni precedenti delle soluzioni Cisco, inoltre, è possibile effettuare l'upgrade con programmi flessibili, in base alle esigenze.

Anche lo schema di pricing è stato rivisto, con un orientamento che tiene conto del numero di utenti che effettivamente utilizzano il sistema.

- Unified CallManager V.5.0 e Presence Server

Un'importante novità riguarda il software di call processing CallManager, il cuore della soluzione Cisco, che nella nuova versione 5.0 supporta il protocollo SIP in maniera nativa, a dimostrazione della volontà di utilizzare standard aperti per poter utilizzare applicazioni e terminali anche di terze parti. «Già nel 2000 – specifica Ferrè – avevamo introdotto le prime funzionalità SIP. Ma solo ora l'abbiamo integrato in modo nativo perché ritenevamo che, in precedenza, il protocollo non avesse raggiunto un livello di maturità tale da supportare tutte le funzioni che i clienti ci chiedevano».

CallManager è anche disponibile nella versione Express, adatta alle PMI, e ora anche come appliance, basato sul sistema operativo Linux.

Un altro nuovo elemento dell'offerta è Unified Presence Server 1.0, che utilizza SIMPLE (SIP for Instant Messaging and Presence Leveraging Extension) per fornire al sistema informazioni su quello che l'utente sta facendo, in termini di strumenti di comunicazione: se è al telefono, se è impegnato in una riunione, se è assente. Inoltre, consente di sapere a quale tipo di servizio un certo utente è abilitato: se può ricevere una videochiamata, se dispone di Instant Messaging, se può fare Web Collaboration.

- Unified Personal Communicator

Lo strumento che, nella pratica, consente di trovare il contatto giusto, al momento giusto, con lo strumento giusto è Unified Personal Communicator, un software per pc che crea

una finestra intuitiva che permette all'utente di "concentrare" tutti gli strumenti. «Vedo chi mi ha cercato - spiega Ferrè - e in che modo, posso fare il click-to-talk, ascoltare la casella vocale, cercare un contatto e capire con quale strumento quella persona è raggiungibile».

Se durante una conversazione due utenti vogliono condividere un file, basta prenderlo dal desktop del pc e trascinarlo dentro la finestra. Ancora, se arriva una chiamata e l'utente non può rispondere, può inviare un messaggio predefinito di testo al chiamante (tipo: ti chiamo fra 5 minuti) e, se non si tratta di un utente aziendale che dispone di questo sistema, il messaggio viene letto dal sistema con il text-to-speech.

- Unified Mobility Manager

Per estendere i vantaggi della soluzione anche agli utenti in mobilità, sono possibili due vie alternative. La prima è quella in cui gli utenti mantengono due terminali, un telefono fisso e un cellulare, con la possibilità deviare le chiamate dal fisso al mobile se l'utente non è in ufficio e con un seamless handover da un terminale all'altro. Basta schiacciare un bottone per passare la chiamata dal mobile al fisso. Il prodotto che consente questo è Unified Mobility Manager, un'altra novità che si aggiunge all'offerta.

La seconda via è quella del terminale unico dual mode Wi-Fi/GSM. Per ottenere questa soluzione, Cisco ha stretto un accordo con Nokia per sviluppare un software che permetterà di trasformare i cellulari della serie E della casa finlandese in client telefonici del CallManager.

Sempre in tema di dispositivi di altri vendor, Cisco ha certificato la compatibilità del diffusissimo Blackberry di Rim con il proprio sistema.

M.G.



Videata di Cisco Unified Personal Communicator

L'IP trasforma il modo di comunicare delle PMI

Una nuova generazione di centralini per l'IP Telephony rende accessibili applicazioni di telefonia prima appannaggio solo di grandi organizzazioni

Le nuove soluzioni per l'Information e Communication Technology si stanno proponendo come uno strumento particolarmente efficace per le aziende appartenenti al segmento dello small and medium business (SMB), sia per migliorare e sviluppare i servizi che forniscono ai propri clienti che per meglio interagire nella propria filiera produttiva con le aziende da cui dipende la fornitura dei componenti base e la proposta al mercato dei prodotti finiti.

Uno degli strumenti alla base di questa evoluzione è la nuova generazione di PBX, o meglio, di IP PBX, che permettono di proiettare nel contesto Internet un'azienda sino a poco prima abituata a comunicare esclusivamente in fonia.

Le resistenze che si sono dovute superare affinché anche nello SMB si affermasse il concetto di fonia su IP non sono state poche. In primis, l'iniziale alto costo delle soluzioni e il timore di non saper gestire un apparato che comunque presentava una complessità superiore al PBX TDM installato.

Questa visione negativa si è ora molto attenuata, se non del tutto cancellata. Ciò perché da una parte oramai gli operatori offrono la voce su IP nei loro portafogli di servizi, e quindi vi è la sicurezza della qualità e della bontà della soluzione, poi perché i costi si sono di molto ridotti. Non ultimo, perché al costo o poco più di un PBX ora una società dello SMB può dotarsi non solo di uno strumento per la gestione di fonia su IP, di interconnessione a Internet e così via, ma anche di una soluzione su cui può far risiedere contemporaneamente applicazioni che prima richiedevano apparati

o server dedicati, per esempio la funzione di contact center multimediale o di mail server, ovviamente oltre a funzioni consolidate quali quelle di gestione fax, voice mail, messaggistica unificata o IVR.

Va osservato che i produttori stanno rispondendo meglio anche alle specificità delle aziende SMB, che si differenziano come esigenze sia da quelle piccolissime che da quelle della fascia enterprise.

Le prime, infatti, utilizzano frequentemente soluzioni presenti e disponibili per il mercato residenziale, mentre le seconde dispongono di competenze tecniche e di supporto interne che possono anche realizzare soluzioni integrate a partire da piattaforme proposte da diversi fornitori, scegliendo il meglio sul mercato per quanto concerne, per esempio, la soluzione di messaggistica, di contact center o di fonia su IP.

Se invece ci si sposta sul piano delle SMB, quello che emerge come esigenza di soluzione da acquisire o di servizio di outsourcing erogato da un service provider sono aspetti quali:

- la necessità di disporre di una soluzione semplice da mantenere e da gestire, che concorra nell'espandere il proprio business e i servizi erogati alla clientela;
- soluzioni a costi compatibili con i livelli di investimento praticabili e facilmente inseribili nel contesto operativo aziendale;
- un adeguato supporto nell'installazione e nella qualità della soluzione installata.

Queste esigenze hanno portato alla disponibilità di una generazione di soluzioni preconfigurate e facilmente customizzabili in base alle specifiche esigenze. G.S.

I rischi trascurati dei documenti cartacei

Lo sviluppo tecnologico sta continuando ad alimentare il processo di digitalizzazione, e facendo crescere esponenzialmente la quantità di dati da dover gestire. Il percorso verso la sostituzione del documento cartaceo con il suo corrispettivo virtuale è, però, da considerarsi tutt'altro che compiuto. Le normative sulla conservazione sostitutiva emanate all'inizio del 2004 hanno risposto all'esigenza, molto sentita, di un'equivalenza legale tra la gestione dei documenti cartacei e quella dei documenti dematerializzati, aprendo ampie prospettive di riduzione nei costi di gestione e nell'ottimizzazione dei processi di archiviazione e recupero dei documenti fiscali relativi al ciclo attivo e passivo, dei registri contabili e altro ancora.

I documenti a validità fiscale sono, forse, gli ultimi arrivati nel gruppo delle informazioni riservate e business critical che circolano sulla rete aziendale. La crescente attenzione per garantire la sicurezza delle informazioni digitali, affidata agli IT manager o ai security manager, rischia però, paradossalmente, di spostare troppo l'attenzione sulle informazioni dematerializzate, dimenticandosi del fatto che sono ancora moltissime le informazioni business critical che circolano ogni giorno, all'interno delle aziende, su supporto cartaceo.

Una ricerca sulla sicurezza del documento condotta a livello europeo da Ipsos Global nel novembre 2005 su oltre 1.000 dipendenti aziendali, ha evidenziato che la carente sicurezza dei documenti cartacei rappresenta una consistente minaccia per il business aziendale. Emerge che il 19% degli intervistati lascia documenti contenenti informazioni confidenziali aperti sulla propria scrivania e che l'11% non distrugge i documenti riservati lasciandoli "sedimentare" sulla scrivania.

Il documento cartaceo, inoltre, è paradossalmente più semplice da esaminare o replicare (fotografandolo o fotocopiandolo) senza la-

sciare traccia mentre, in un ambiente informatico gestito opportunamente, l'accesso e la replicazione dei file è controllata da policy ed è tracciabile dall'amministratore.

Sono scarse o mancano del tutto una serie di policy adeguate indirizzate alla protezione dei documenti cartacei che contengono informazioni riservate. Come al solito, si tratta di un processo che richiede lo sviluppo di cultura interna all'azienda indirizzata alla sicurezza, con la definizione di regole di comportamento adeguate a gestire il flusso documentale e una maggiore consapevolezza del ruolo e del contributo dei dipendenti rispetto alla tutela delle informazioni critiche della propria azienda.

Un altro elemento di rischio riguarda la stampa, magari su stampanti di rete distanti dalla postazione di invio, di documenti e file contenenti informazioni critiche.

Le stampe, in genere, elidono i controlli tradizionalmente implementati per la documentazione cartacea ufficiale, proprio perché la protezione delle informazioni che contengono è stata pensata rispetto all'accesso non autorizzato o alla copia tramite la rete dei file corrispondenti.

In Italia, sempre secondo la ricerca Ipsos Global, il 69% dei documenti dimenticati dagli impiegati sulle stampanti contiene informazioni aziendali riservate o confidenziali e, di conseguenza, è emerso che il 18% dei dipendenti ha potuto accedere a documenti riservati che chiunque altro avrebbe potuto leggere o portare via. In particolare, il 41% ha ammesso di averli lasciati sul vassoio della stampante senza preoccuparsi di proteggerli, il 5% di averli letti, il 3% li ha conservati e il 2% li ha addirittura gettati nella spazzatura.

Tutto ciò nonostante il fatto che, tuttora, un quarto degli impiegati italiani consideri i documenti cartacei più importanti e autorevoli rispetto agli omologhi in formato elettronico. ❖



Riccardo Florio

La business communication adotta XML per i servizi Web

Come prima l'IP, il linguaggio XML è diventato un requisito base nella realizzazione di soluzioni di comunicazione unificate

La definizione delle specifiche per i servizi Web ha i suoi prodromi nella fine degli Anni Novanta come prima risposta concreta al diffondersi di esigenze di semplificazione, maggiore rapidità ed ottimizzazione dei costi per l'integrazione tra le applicazioni.

Il successivo boom e la diffusione universale del modello di comunicazione basato su Internet ha fatto crescere ulteriormente l'esigenza di sviluppare sistemi informativi aziendali in grado di erogare applicazioni aperte e integrabili sia su scala interna e sistemi proprietari che su scala globale nel panorama dell'World Wide Web. In un periodo tutto sommato breve, ne è derivato che i principali operatori industriali nei settori connessi, ognuno con le sue specifiche caratterizzazioni e la propria vision per quanto concerneva l'integrazione delle applicazioni, hanno progressivamente optato per adottare XML come il linguaggio universale utilizzato per codificare lo scambio sia di informazioni che di servizi Web. Il lavoro congiunto ha portato in breve tempo ad elaborare una specifica comune per la definizione dei meccanismi atti ad assicurare l'interoperabilità tra applicazioni IT in ambiti di reti aperte pubbliche o private.

L'importanza di una tale scelta strategica emerge immediatamente se si considera che lo standard dei servizi Web fornisce un semplice linguaggio XML basato su testo per accedere in modalità trasparente potenzialmente a qualsiasi tipo di sistema e in grado di elaborare il flusso delle informazioni originate da applicazioni che sono scritte in linguaggi quali Java o C++, con l'interazione dell'utente basata ge-

neralmente su browser HTML. In pratica, XML e i servizi Web finiscono con il rappresentare un vero e proprio collante atto ad assicurare l'integrazione di applicazioni interattive che possono essere allocate su reti di tipo eterogeneo in un sistema di comunicazioni unificato e distribuito.

- I vantaggi nello sviluppo delle applicazioni

L'ampia accettazione di XML e dei servizi Web deriva direttamente dalla possibilità per il mercato di generare soluzioni economiche e, soprattutto, interoperabili, espandibili in fase successiva al loro rilascio in parallelo al diffondersi di nuovi servizi di information technology o di telecomunicazione. Peraltro, va considerato che le nuove strutture di comunicazione comprendono ora e si riferiscono non solo al mondo IP o alle applicazioni Internet ma comprendono anche i servizi interni ad una azienda, che è proprio l'ambito in cui un middleware o interfacce proprietarie portano inevitabilmente a reti infrastrutturali generalmente più costose e complesse da gestire e mantenere.

Un secondo fattore di interesse è poi la possibilità di disporre di uno standard universalmente condiviso nello sviluppo di soluzioni a valore aggiunto che proprio per questo risultano nativamente di tipo aperto, sono caratterizzate da un grado di flessibilità elevato e permettono di pianificare evoluzioni future con meno vincoli e timori. Le tecnologie XML si stanno rivelando, in sostanza, un'alternativa semplice, stabile ed economica a interfacce applicative quali TAPI, JTAPI o altre modalità

proprietarie orientate a coprire le esigenze del mondo delle telecomunicazioni.

- **Un impatto non solo tecnologico**

Quello che è facilmente prevedibile, peraltro, è che in prospettiva l'impatto derivante dalla diffusione dei servizi Web nell'ambito delle comunicazioni aziendali non risulterà solamente di carattere tecnologico, ma finirà con il cambiare profondamente il rapporto esistente tra i fornitori di prodotti e servizi e i loro clienti. Se ci si limita a considerare cosa avviene a livello di fornitori di soluzioni Tlc, è possibile notare come questi sempre più frequentemente abbiano rapporti anche con aziende attive nel settore dell'integrazione in ambito IT e non solo con i partner tradizionali, un ulteriore segno dell'evolvere della convergenza voce-dati verso la convergenza Tlc-IT.

Il vantaggio nell'adottare modalità di sviluppo standard aumenta poi l'interazione con il cliente e facilita lo sviluppo di soluzioni in linea con le sue esigenze applicative e temporali. Non a caso le società che sviluppano applicazioni basate su linguaggi che sono compatibili con lo standard XML, ad esempio Java o strutture di applicazioni .NET, collaborano in modo più intenso con gli utenti finali proprio al fine di sviluppare soluzioni ottimizzate per i processi di business aziendali. In sostanza, fornitori e clienti stanno adeguando il tradizionale rapporto verticale con un modello di tipo orizzontale e collaborativo in modo da sfruttare al massimo le possibilità rese disponibili da XML nel trasformare in sistemi aperti le soluzioni di comunicazione aziendale, sia verso l'esterno che l'ambiente IT.

- **Un valore aggiunto per le applicazioni**

Se ci si focalizza sul settore delle telecomunicazioni, una delle aree in cui l'impatto degli standard sta dispiegando tutti i suoi benefici è quella inerente all'uso sempre più diffuso di XML e servizi Web al fine di integrare e far convergere in tempo reale i processi aziendali con i servizi di comunicazione sia in voce/dati

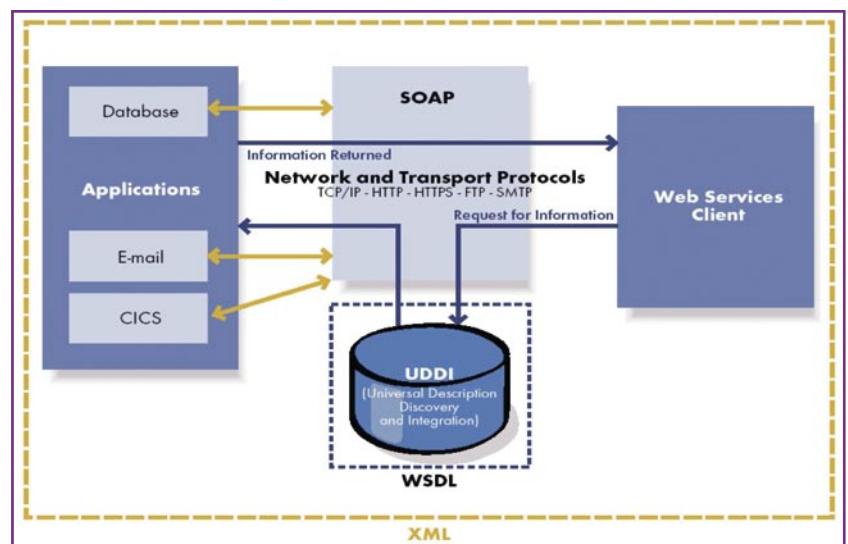
che di messaggistica unificata o di contatto multimediale. Alcune abitudini poi sono già consolidate. Ad esempio, le interazioni spontanee o la gestione di eccezioni rispetto al flusso di lavoro e decisionale normale sono eventi con cadenza quotidiana in tutte le aziende, eventi che necessitano di un contatto e una collaborazione su base di continuità tra le persone e gli enti preposti. Per quanto concerne gli eventi imprevisi, ad esempio, strumenti quali il telefono, la videoconferenza, la messaggistica immediata, applicativi di gestione della presenza, la localizzazione del personale sono ormai opzioni indispensabili.

È proprio in questo che i servizi Web evidenziano il loro potenziale, perché semplificano l'integrazione di queste attività e facilitano la risoluzione dei problemi in tempo reale o integrano le attività di comunicazione con i sistemi informativi.

In pratica, in modo del tutto simile a quanto si è verificato alla fine degli anni 90 per la voce su IP, i servizi Web e le tecnologie XML sono oggi caratterizzati da una fase innovativa e si trovano nella parte iniziale del loro ciclo di sviluppo. Tuttavia, con il progressivo espandersi, le tecnologie basate su XML stanno già ponendo le basi per una migliore ed estesa collaborazione all'interno dell'ambito aziendale, aggiungendo maggior valore ai processi di business soprattutto per quanto concerne i servizi erogati agli utenti.

G.S.

Ambito di applicazione di XML in applicazioni di contatto di nuova generazione (fonte Alcatel)



La SOA perno dell'innovazione del laboratorio IBM Tivoli

La struttura romana si pone all'avanguardia nello sviluppo di soluzioni software per una gestione dinamica del flusso di lavoro basata sul servizio

La IBM Software Group rappresenta una realtà molto ampia e variegata del panorama dell'ICT. Attualmente, la struttura è organizzata in una serie di brand attraverso i quali IBM mette a disposizione i tasselli per la costruzione di infrastrutture on-demand: WebSphere riunisce la parte dedicata ai processi transazionali e di messaging, la parte di "collaboration" ricade in Lotus, mentre quella di management e gestione dell'infrastruttura a livello applicativo è affrontata all'interno del brand Tivoli. Infine vi sono le soluzioni IBM DB2 per la gestione delle informazioni e quelle di sviluppo software della gamma Rational. Ognuno di questi brand ha una struttura trasversale a IBM e dispone di proprie risorse in termini di Ricerca e Sviluppo, di una struttura dedicata all'interazione diretta con i clienti e si avvale di una serie di laboratori. Tra questi vi è il laboratorio Tivoli di Roma, che rappresenta un centro di eccellenza tecnologica per il nostro Paese e opera sotto la direzione di Giovanni Lanfranchi.



*Giovanni Lanfranchi,
responsabile del laboratorio
Tivoli di Roma*

Reportec: Quante persone operano all'interno del Laboratorio Tivoli?

Lanfranchi: La struttura ospita oltre 500 addetti, di età media intorno ai 33 anni, con un'elevata specializzazione e livello di istruzione e provenienti per la maggior parte dalle università italiane di Roma, Napoli e Catania.

R: Quali sono le attività prevalenti del Laboratorio?

L: Il laboratorio di sviluppo software di Roma è nato per essere dedicato alle soluzioni Tivoli ma, nel tempo, si è indirizzato alle soluzioni tecnologiche innovative del software IBM e

attualmente rappresenta l'unico laboratorio europeo IBM dedicato alla ricerca e sviluppo software. Il fatto di lavorare molto su progetti con il mondo universitario, sia nazionale sia internazionale, riteniamo sia uno degli elementi che ci permette di acquisire e mantenere una posizione di leadership a livello mondiale sul fronte della ricerca tecnologica che, per un laboratorio come il nostro, rappresenta un elemento essenziale di successo.

R: Quali sono gli indicatori per valutare il successo di un laboratorio come quello di Roma?

L: Negli ultimi due anni il laboratorio Tivoli ha quasi quadruplicato il numero di brevetti sottoposti, superando le 250 sottomissioni per anno. Un altro indice di successo è dato dal fatto che il rapporto tra i brevetti sottoposti e quelli che vengono riconosciuti come una vera invenzione e depositati, supera il livello medio per questo tipo di attività che è del 20%. Va anche evidenziato che i brevetti sottoposti dal laboratorio di Roma si devono a una base molto allargata di ricercatori e non a pochi "superinventori" e questo è un segnale di vitalità e di una distribuzione capillare di competenze.

R: Può fare un esempio di qualcuna delle attività attualmente in corso?

L: Una delle missioni che stiamo affrontando in questo momento riguarda il workflow scheduling. Attualmente, le soluzioni software indirizzate all'organizzazione del flusso di lavoro adottano un approccio statico rispetto al set di risorse informatiche coinvolte: per esempio si prevede l'esecuzione di un job con modalità prefissate, in una specifica data, verso una risorsa o un'applicazione predefinita. Stiamo sviluppando uno "scheduler" di tipo più evo-

luto in grado di definire il workflow in modo dinamico sulla base di regole, così da poter individuare e scegliere la macchina e le modalità su cui eseguire il job in base alla sua disponibilità, al carico di lavoro che sta svolgendo e così via.

R: Qual è il vostro approccio rispetto ai Web service?

L: Tutte le soluzioni che stiamo sviluppando saranno abilitate ai Web service con un set di interfacce aperte a disposizione di ISV, partner e così via. Ma non solo. All'interno del laboratorio di Roma e, più in generale a livello strategico come IBM Software Group, siamo in una fase di definizione di tutti i nostri asset software come servizi all'interno di una Service Oriented Architecture (SOA). Riprendendo l'esempio del dynamic workflow scheduler di cui abbiamo parlato prima, ciò significa che definiremo i blocchi che compongono questo software come servizi che si affacciano sull'Enterprise Service Bus di una SOA. La parte di esecuzione del software potrà, perciò, essere invocata come servizio da un'applicazione che si affaccia sulla SOA in maniera completamente trasparente, senza doversi preoccupare di come il servizio è stato costruito.

R: Quanto tempo ci vorrà prima che queste soluzioni passino da prospettiva a realtà disponibile per le aziende?

L: Non si tratta solo di tecnologia, ma anche di adozione, del modo con cui sono definiti i processi di business e anche dell'audit. Non si può parlare perciò di una data di adozione, ma piuttosto di un processo evolutivo. Per quanto riguarda il service e workflow management, a partire dall'anno scorso abbiamo condotto "customer validation" a Roma su oltre 50 clienti mondiali e interagito con loro per affinare tecnologie e obiettivi. Metteremo a disposizione soluzioni che vanno in questa direzione e in grado di fornire valore per i nostri clienti già nel 2006.

R: Quali sono gli aspetti più importanti su cui porre l'attenzione nella gestione?

L: È fondamentale focalizzarsi sul processo IT e noi abbiamo evidenziato tre aspetti chiave

associati a esso: release, availability e lifecycle management. Vogliamo fornire al mercato "process manager" per ognuno di questi processi, con l'obiettivo di migliorare l'efficienza del business.

R: Cosa vi differenzia dalla competition?

L: I nostri competitor sono ancora focalizzati sul tool, che resta sicuramente un elemento importante e su cui anche noi lavoriamo. Tuttavia noi siamo indirizzati verso lo step successivo del service management. Per questo è importante focalizzarsi sul lifecycle, partendo dalla modellazione del servizio e definendo i Service Level Agreement (SLA) che lo caratterizzano in base a opportuni indici chiave del processo e a criteri di management. A questo punto deve essere la "service infrastructure" che prende in carico il SLA e permette di monitorarlo e di intraprendere, in modo automatico o almeno semiautomatico, azioni correttive o di recovery.

Nel caso del workflow, per esempio, questo significa che se il broker non trova una risorsa in grado di garantire il SLA previsto, sia possibile lanciare automaticamente un'attività di provisioning cambiando la topologia IT in modo tale che sia soddisfatto il SLA. Questo richiede una capacità di integrare a livello di service management in cui il focus non è sulla gestione di un'entità ma sul management del servizio.

IBM ha la capacità di fare questo

R.F.

*Il laboratorio romano di
IBM Software Group*



Verso il Corporate Performance Management

Dalla convergenza della Business Intelligence e dell'ERP deriva il CPM, un approccio che aumenta la visibilità delle performance del business aziendale.

Se gli acronimi nel settore informatico sono già tanti, i manager IT si devono preparare a sentire parlare sempre di più di uno nuovo: CPM, ovvero Corporate Performance Management.

Sull'argomento è intervenuto di recente anche Gartner, che ha definito un suo quadrante proprio per le società che sono già attive in questo settore di mercato che si annuncia come un segmento molto interessante per i fornitori perchè risponde alla crescente esigenza da parte del management aziendale di strumenti che permettano di disporre in modo rapido e sofisticato di dati di analisi delle prestazioni aziendali in rapporto agli obiettivi prefissati e a eventuali variabili.

Ma quali sono gli elementi che stanno portando sempre più un approccio basato su strumenti di Corporate Performance Management al centro degli interessi di chi in azienda è coinvolto nelle definizioni di budget e nel controllo che quanto poi previsto si verifichi?

Sostanzialmente due. Il primo è la richiesta crescente di compliance a precisi requisiti definiti su scala aziendale e internazionale. Il secondo elemento è invece l'esigenza di disporre di informazioni precise atte a capire e pilotare le performance complessive, in modo da intervenire con le opportune correzioni il prima possibile.

- Un'ampia copertura funzionale per un management efficace

Come in tutte le fasi evolutive in cui più strumenti convergono in uno unificato, non sempre risulta facile per gli utilizzatori aziendali e chi ne deve decidere l'acquisto capire appieno

il grado di estensione e copertura come applicazioni e i reali benefici di una soluzione CPM. In generale infatti, una soluzione di Corporate Performance Management indirizza, oltre che i processi che servono per gestire le performance, come ad esempio quelli necessari per definire le strategie, le analisi previsionali o quelle di budget, anche un insieme di metodologie che possono agire come driver di alcuni dei processi aziendali stessi. Si estende inoltre sino ad includere opportune metriche che permettono di valutare il grado delle performance in atto in rapporto agli obiettivi strategici ed operativi che si erano prefissati. Ad esempio, osserva Gartner, alcune applicazioni CPM permettono di visualizzare i risultati di processi di pianificazione evidenziando anche il valore in termini economici e correlando le performance con gli obiettivi.

Se i benefici per le aziende sono concreti e ne giustificano ampiamente il crescente interesse, l'interesse per questa nuova area di mercato da parte dei fornitori di soluzioni deriva da aspetti molto più concreti. Infatti, di fronte ad una dimensione del mercato che nel 2003 ammontava a 520 milioni di dollari, le stime di Gartner per il 2009 ne fanno un mercato di oltre 900 milioni di dollari. Una crescita media anno su anno intorno al 10% che, in presenza della sostanziale stasi di altri segmenti di mercato inerenti i prodotti per la gestione aziendale, giustifica ampiamente la costante crescita di vendor che entrano in questo segmento, soprattutto le società già attive nell'ERP e nella Business Intelligence, con una crescita delle aziende interessate al settore che è avvenuta sia in termini numerici che dimensionali. Il

2005 ha visto, in tal senso, l'acquisizione o il merge di numerose società interessate ad allargare la copertura proprio dell'offerta di soluzioni di CPM.

- **Quali sono gli elementi principali del CPM**

Con il crescere del numero delle società presenti nell'arena del software di Corporate Performance Management cresce quasi in pari misura il numero di interpretazioni che viene dato e delle funzioni che sono ritenute necessarie perchè un prodotto possa essere definito tale.

In generale però, e prendendo ancora Gartner come riferimento, è possibile definire un insieme ridotto di aree funzionali che devono essere coperte.

- **Applicazioni per il Budgeting, il Planning e il Forecasting**

È un insieme di applicazioni volte a supportare il management nell'attuazione delle attività inerenti gli aspetti strettamente connesse al budget, alla pianificazione e alle previsioni. In quanto tale vanno oltre una mera visione a breve termine degli aspetti finanziari delle attività di budget e permettono una pianificazione sul lungo termine nonchè la gestione di piani strategici di alto livello. Oltre a questo, queste applicazioni dovrebbero comprendere anche la possibilità di definire appositi workflow inerenti la creazione, la gestione e l'approvazione di piani di budget e disporre di servizi che permettano di simulare in modo dinamico condizioni e scenari particolari in cui un'azienda si potrebbe trovare ad operare e vedere quale ne è l'effetto in termini di efficienza e di risultati aziendali.

Completa il quadro di questo insieme funzionale il supporto di un modello di planning esteso all'intera azienda che permetta di stabilire uno stretto legame tra i piani operativi e i budget finanziari e la possibilità di scambiare dati con applicazioni specifiche, ad esempio quelle connesse alla pianificazione di attività di supply chain.

- **Applicazioni di Profitability Modeling**

È un insieme che comprende applicazioni ABC (Activity Based Costing) utilizzabili per determinare e allocare i costi con una granularità spinta nonchè applicazioni ABM (Activity Based Management), e cioè un insieme di funzioni che mettono in grado l'utilizzatore di valutare l'effetto che hanno dal punto di vista della profittabilità strategie diverse di allocazione delle risorse e dei costi aziendali.

- **Applicazioni per il Financial Consolidation**

Si tratta di applicazioni che mettono in grado un'organizzazione di riassumere e consolidare i dati finanziari in base alle diverse modalità di accounting previste dai diversi stati o regolamenti di settore. Nell'insieme costituiscono una componente fondamentale di una applicazione CPM perchè permettono di disporre di una funzione di auditing dei dati finanziari aziendali, rendendone possibile lo scambio omogeneo con altre applicazioni CPM, con l'obiettivo finale di analizzare lo scostamento dei risultati in corso da quelli inizialmente definiti come obiettivo.

- **Applicazioni di Financial Reporting**
Sono delle applicazioni che complementano necessariamente le applicazioni CPM mettendo a disposizione degli strumenti per attività di reporting finanziario in modo formattato o secondo principi di accounting che devono aderire a regole precise, ad esempio quelle GAAP o a standard internazionale per quanto riguarda il reporting finanziario. Ulteriori strumenti permettono poi di supportare la rappresentazione dell'andamento del budget ed il suo scostamento dai dati previsti.

G.S.

Un mondo di acronimi

ABC:	Activity Based Costing
ABM:	Activity Based Management
BI:	Business Intelligence
CPM:	Corporate Performance Management
SEM:	Strategic Enterprise Management
SPM:	Strategic Performance Management
EPB:	Enterprise Planning and Budgeting
EPM:	Enterprise Performance Management
ERP:	Enterprise resource planning
GAAP:	Generally Accepted Accounting Principles

L'Università di Verona gestisce rete e risorse con CA

Il prestigioso ateneo unifica e rende sicure le infrastrutture distribuite, attuando un monitoraggio centralizzato costante



L'Università degli Studi di Verona, uno dei più importanti centri di studio nel comprensorio Nord Est e punto di riferimento a livello nazionale, ha da sempre come obiettivo quello di operare una costante trasformazione culturale, promuovendo al proprio interno sia il miglioramento della qualità del lavoro sia, conseguentemente, il potenziamento dei servizi forniti alla propria utenza. Con quattro poli nella città di Verona, uno scientifico, uno umanistico-economico, uno giurisprudenziale e l'ultimo dedicato alle scienze motorie, e con altre 12 sedi distaccate sul territorio delle tre regioni del Nord Est, attualmente l'università raccoglie la costante frequenza di oltre 20.000 studenti, iscritti a 8 facoltà e numerosi corsi di laurea. La struttura di supporto, comprendendo docenti e personale amministrativo presente nella sede centrale e nei distaccamenti periferici, coinvolge

circa 1.500 addetti. Di questi, 22 costituiscono lo staff IT, il cui obiettivo principale consiste nella consulenza finalizzata al supporto delle facoltà e dipartimenti, che a tal scopo dispongono di, seppur pochi, tecnici aggiuntivi.

- Un'infrastruttura distribuita da gestire completamente

Dopo una fase iniziale di decentramento delle strutture informatiche, volendo perseguire una strategia innovativa d'integrazione, è stato realizzato un progetto per uniformare alcune prestazioni del sistema informativo distribuito.

L'ambiente operativo che si è venuto a creare è molto eterogeneo e attualmente si basa su circa 50 server, nella maggior parte dei casi funzionanti in ambiente Windows NT, 2000 e 2003, ma con alcune realtà operative sotto sistemi operativi Linux, FreeBSD oppure Unix Solaris. I servizi offerti dal sistema informativo vengono distribuiti a circa 3.000 stazioni di lavoro, comprendendo sia quelle dei laboratori di ricerca, dove prevalentemente l'ambiente operativo è basato su Linux, sia quelle presenti nelle differenti unità amministrative sparse su tutto il territorio servito, che normalmente utilizzano l'ambiente Windows in differenti versioni.

«Già da tempo esistono rapporti consolidati con CA, - afferma Giovanni Michele Bianco, Responsabile dei Servizi Informativi dell'Università di Verona - dato che eravamo utenti nell'area storage di prodotti come ARCserve e in quella della sicurezza dell'antivirus Inoculate, ora eTrust Antivirus. Tuttavia, queste soluzioni erano limitate a necessità specifiche,

mentre il problema che stavamo affrontando era più generale».

- La gestione centralizzata di un ambiente eterogeneo

L'idea, infatti, era quella di adottare un prodotto che avesse già integrate tutte le componenti di base per la gestione di ambienti hardware disomogenei e per il monitoraggio di una rete complessa come quella dell'ateneo veronese.

«Abbiamo subito riconosciuto in Unicenter tutte le caratteristiche che ritenevamo indispensabili, – prosegue Bianco – però abbiamo preferito procedere per gradi, data la complessità dell'ambiente e la molteplicità dell'utenza da integrare. Il principale obiettivo era quello di un costante monitoraggio di base, relativamente alla corretta funzionalità sia dei numerosi sistemi sia della rete, con velocità mista da 34 a 155 Mbps. A questo si aggiungevano le necessità di un controllo sistematico delle licenze impiegate, di un sistema di sicurezza antivirus, particolarmente mirato sui servizi di posta elettronica, e di un'applicazione centralizzata per la gestione dei backup».

Per questi motivi, nella prima fase di sperimentazione, l'uso di Unicenter Network and System Management è stato limitato alle funzioni basilari, implementate solo su 400 stazioni nell'area amministrativa che costituivano l'utenza campione individuata. Progressivamente la soluzione si va estendendo a tutta l'utenza. Impiegando il modulo Unicenter Remote Control, il team di Bianco è stato subito in grado di risolvere direttamente dalla sede centrale i problemi che vengono rilevati dagli utenti. Possono essere inoltre gestiti in modo centralizzato gli allarmi identificati da Unicenter in ambiente Windows, Unix e Linux. Grazie alla rappresentazione molto realistica, tutte le segnalazioni generate dalle anomalie operative dei vari elementi che costituiscono l'infrastruttura sono riprodotte sulle mappe grafiche, per fornire informazioni visive dirette relativamente allo stato delle risorse controllate e alla loro capacità operativa.

«Una delle caratteristiche più innovative, che

abbiamo rilevato nella soluzione offerta da CA – osserva il manager veronese –, è quella di rappresentare la topologia della rete, le strutture dei sistemi e la composizione delle stazioni di lavoro installate in periferia, in formato grafico 3D. Questo è un modo veramente immediato di trasmettere le informazioni, che si traduce nella facilità di navigazione e di interpretazione degli allarmi, anche da parte di personale interno non esperto». Le esigenze erano molteplici e dovevano tenere conto anche degli sviluppi successivi, per quanto riguardava l'estensione del servizio a tutto l'insieme degli utenti dell'università, partendo dall'area amministrativa centrale per giungere poi anche all'utenza dislocata nelle numerose sedi periferiche. Una necessità specifica, inoltre, è quella dell'integrazione con l'Azienda Ospedaliera di Verona, dove risiedono molti utenti universitari, sia docenti, che sono al contempo medici e che insegnano presso le strutture dell'ateneo, sia tecnici amministrativi universitari che lavorano anch'essi al di fuori dello spazio fisico dell'ateneo. «È essenziale per noi poter gestire tali utenti come se fossero all'interno di una nostra sottorete e, utilizzando una VPN (Virtual Private Network) riteniamo che Unicenter Remote Control risolve egregiamente questa problematica», spiega Bianco.

Utilizzando il modulo Unicenter Asset Management, inoltre, il gruppo di supporto interno è in grado di tenere sotto controllo l'inventario sia dell'hardware sia del software presente nell'ambito delle diverse strutture universitarie. È inoltre possibile tenere traccia di tutte le variazioni di configurazione che vengono apportate ai sistemi e alla rete stessa. Sempre grazie alle soluzioni offerte da CA, l'istituto è ora in grado di esercitare un maggiore controllo sul corretto uso delle licenze software per un elevato numero di prodotti, impiegati anche nelle aree della ricerca. Inoltre, grazie alla componente Unicenter Software Delivery, è possibile provvedere automaticamente all'aggiornamento tempestivo di tutte le postazioni di lavoro con le versioni aggiornate del prodotto antivirus. G.D.B.

Più vicina la rete ProCurve di prossima generazione

La divisione di HP rilascia un nuovo ASIC ad alta integrazione e nuovi switch a chassis e stackable caratterizzati da prestazioni wirespeed e Gigabit PoE integrato

La rete sta, progressivamente, diventando più intelligente.

Ad alimentare questa tendenza concorrono una serie di elementi quali la richiesta di maggiore sicurezza, l'esigenza di abilitare una forza lavoro mobile, di ridurre i costi operativi e di preparare il network per le applicazioni future a elevate richieste favorendo, nel contempo, maggiore flessibilità e scalabilità.

ProCurve networking, la divisione di HP dedicata alle soluzioni infrastrutturali di rete, ha da tempo dedicato i propri sforzi al conseguimento di questi obiettivi avviando un percorso evolutivo all'insegna di una strategia che promuove un'architettura denominata Adaptive EDGE, indirizzata a spostare l'intelligenza alla periferia mantenendo il controllo al centro della rete.

La rete sta attraversando un'evoluzione analoga a quella che ha caratterizzato gli ambienti di elaborazione.

Il passaggio da mainframe centralizzati a modelli client/server per approdare a un computing distribuito con la diffusione dei pc si sta riproponendo, secondo ProCurve, nell'evoluzione da un network tradizionale privo di intelligenza, a uno di tipo ibrido in cui vengono incorporate componenti essenziali di intelligenza, per approdare, infine, al network di prossima generazione caratterizzato da un'intelligenza ottimizzata.

ProCurve ritiene che il network di prossima generazione sposterà l'intelligenza sempre più verso il punto in cui avviene il primo incontro tra il network e l'uten-

te ovvero il bordo della rete. Questa visione strategica compie ora un ulteriore passo in avanti con lo sviluppo, da parte di ProCurve, di un nuovo ASIC e il rilascio degli switch periferici intelligenti a chassis Serie 5400 e stackable Serie 3500.

• Il ProVision ASIC

I sistemi switch recentemente rilasciati da ProCurve si caratterizzano per prestazioni, funzionalità e caratteristiche di alimentazione. Parte di questi risultati sono ottenuti grazie allo sviluppo della quarta generazione del ProVision ASIC, sviluppato interamente all'interno dei Laboratori ProCurve.

HP vanta una lunga storia rispetto allo sviluppo interno di processori ASIC che inizia oltre 10 anni fa con l'HP AdvanceStack Switch 2000.

Lo sviluppo del ProVision ASIC segue la visione strategica di ProCurve indirizzata a portare capacità high-end sugli switch a un costo contenuto e persegue diversi obiettivi:

Innanzitutto quello di fornire un equilibrio ingegneristico tra funzionalità, prestazioni e prezzo. L'intelligenza "wire speed" inserita all'interno del ProVision ASIC abilita poi una serie di funzionalità all'interno dei nuovi switch 5400 e 3500 in grado di ampliare l'esperienza dell'Adaptive EDGE Architecture e di portare sofisticate funzioni di controllo al bordo della rete.

Tra le principali caratteristiche di questo ASIC vanno evidenziate funzioni di resilienza intrinseche, la presenza di un motore interno per il rafforzamento delle policy e un'architettura altamente integrata che riduce il numero di componenti richiesti all'interno dello switch,

Gli switch ProCurve Serie 5400 e 3500



migliorando l'affidabilità e, potenzialmente, riducendo il Total Cost of Ownership.

Il ProVision ASIC dispone, inoltre, di un processore di rete programmabile che consentirà di inserire in futuro nuove funzionalità all'interno dell'ASIC, che non potevano essere previste al momento del suo sviluppo.

L'integrazione non si ferma all'ASIC perché, per esempio, anche il sottosistema PoE è stato integrato all'interno del blocco connettore RJ45, facilitando un'implementazione più compatta e riducendo il numero complessivo di componenti e determinando moduli più piccoli e meno costosi.

L'ASIC ProVision sarà progressivamente utilizzato su un ampio numero di prodotti ProCurve, favorendo la costruzione di una gamma di soluzioni altamente scalabile.

- Gli switch ProCurve Serie 5400 e Serie 3500

Lo switch Serie 5400 è un'apparato a chassis che coniuga un'elevata densità di porte Gigabit (confrontabile con quella dei sistemi stackable) con altre funzioni tipiche di un sistema chassis quali un backplane ad alta velocità, flessibilità nel tipo di media e nelle opzioni di alimentazione, disponibilità di un unico punto di gestione. Il modello siglato 5406 dispone di 6 slot mentre il 5412 supporta 12 slot e può essere utilizzato per mantenere un'elevata densità di porte oppure per mettere a disposizione slot per l'aggiunta successiva di moduli add-in, senza limitare in modo non necessario le connessioni di rete disponibili per il client.

Il ProCurve 5400 è in grado di alloggiare fino a 288 porte all'interno di uno chassis di dimensioni 7U (5412) e fino a 144 in uno da 4U (5406). Questo switch prevede funzionalità complete di routing layer 3 e include la tecnologia software per la protezione contro le minacce online Virus Throttling, che interviene proattivamente in base all'identificazione di anomalie.

Il 5400 dispone anche di un modulo di gestione rimovibile che favorisce il rimpiazzo in caso di failure e che consente di effettuare l'upgra-

de successivo della memoria e della CPU.

Per il ProCurve 5400 sono disponibili due moduli di alimentazione da 875 o 1500 Watt: 600 W sono richiesti per alimentare lo chassis 5406 e 1200 W per il 5412. I restanti Watt sono disponibili per il PoE di access point, telecamere di sicurezza ecc.

La potenza è disponibile attraverso tutti gli slot dello chassis ed è additiva all'aumentare degli alimentatori.

Per il 5400 sono disponibili un modulo PoE a 2 porte 10/100/1000 e un modulo a 20+4 porte adatto nelle situazioni in cui sono richieste connessioni in fibra, come "downlink" verso altri switch distanti o connessioni switch-to-switch.

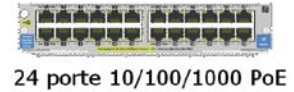
A metà del 2006 sarà disponibile anche il modulo mGBIC a 24 porte da usare come aggregatore negli ambienti distribuiti e il modulo 10G CX-4 utilizzabile come sistema di interconnessione 10 GbE a basso costo tra due switch o per il downlink ad alta velocità verso uno switch ProCurve 3400 o 3500 o qualsiasi commutatore che supporti connessioni CX4.

Gli switch Serie 3500 sono dispositivi stackable di dimensione 1U, disponibili in versione a 24 e 48 porte Gigabit Ethernet PoE e dotati di quattro porte di uplink Gigabit.

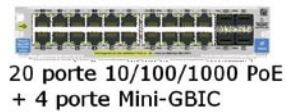
Hanno funzioni e prestazioni identiche a quelle degli switch 5400 e possono essere utilizzati come un'estensione dell'intera famiglia. Per esempio si potrebbe utilizzare uno switch ProCurve 3500 a 24 porte nelle aree in cui è necessario solo questo numero di porte ma che devono disporre delle stesse funzionalità e prestazioni degli altri switch presenti in rete, contribuendo a favorire la scalabilità generale. Le porte per la console e le porte USB sono collocate frontalmente sul modello a 24 porte e posteriormente su quello a 48 porte.

L'alimentatore integrato fornisce 275 W per il PoE; per disporre di maggiore potenza è possibile aggiungere un alimentatore esterno.

Il 3500 dispone di uno slot in cui è possibile alloggiare un modulo da 10 GbE con 2 porte X2 e 2 porte CX-4 che si mantengono tutte attive contemporaneamente. R.F.



24 porte 10/100/1000 PoE



20 porte 10/100/1000 PoE + 4 porte Mini-GBIC



4 porte 10GbE X



Alimentatore 875 W e 1500 W



24 porte Mini-GBIC



4 porte 10GbE CX4

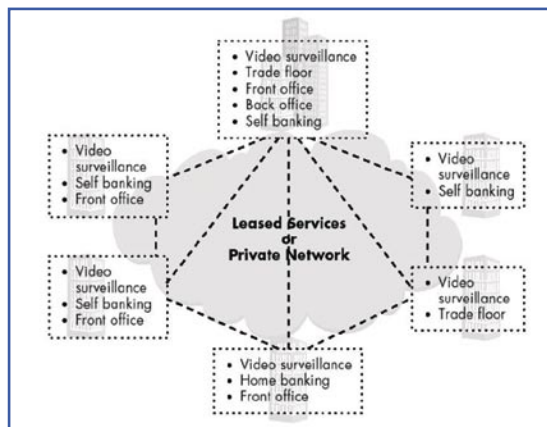
I moduli disponibili per lo switch ProCurve Serie 5400

I molti vantaggi di una rete convergente

Le nuove tecnologie di rete offrono concreti benefici, ma il loro utilizzo va calato nel contesto aziendale con attenzione e in funzione della criticità delle applicazioni

Una rete convergente offre numerosi vantaggi ad un ambiente business. Combinando diverse reti separate in un'unica infrastruttura omogenea come apparati, topologia e applicazioni di gestione, si possono non solo far viaggiare sulle stesse dorsali geografiche o locali voce, dati o video, ma anche erogare servizi multimediali convergenti, il che non vuol dire trasmettere voce o dati, ma sessioni in cui la voce, i dati e le immagini costituiscono un modo integrato di comunicare. Questa evoluzione è particolarmente utile per razionalizzare il modo di lavorare soprattutto per aziende distribuite, che possono avviare servizi di cooperative working tra le sedi, o per i carrier, che possono erogare alle aziende servizi in outsourcing di nuova generazione. Gestire una sola rete, soprattutto quando su di essa si appoggiano anche applicazioni business critical, ad esempio i backbone che connettono data center centrali primari e secondari, permette poi di identificare più rapidamente eventuali problemi e attuare politiche previsionali di adeguamento infrastrutturale e di pianificazione delle espansioni necessarie sia

Tipologie di traffico interessanti l'ambito aziendale (fonte Alcatel)



come apparati che come linee e disponibilità di banda. Questo è il lato positivo della medaglia. L'altro è rappresentato da esigenze più stringenti in termini qualitativi, di continuità operativa, di capacità di allocare on demand la banda necessaria alle

diverse sessioni o di gestire classi di priorità in funzione dell'importanza che una specifica attività ha per il core business di un'azienda. Ovviamente le esigenze e le funzionalità che caratterizzano una rete convergente possono essere molto diverse da settore a settore. Per un service provider che eroga servizi di back up l'aspetto saliente è posto sulla affidabilità estrema delle linee ottiche che collegano le sue sedi con le sedi dei clienti. Per un istituto finanziario la velocità è meno stringente mentre lo è maggiormente la robustezza e la sicurezza delle VPN che sulla rete possono essere ricavate e dedicate alla gestione dei vari flussi e tipologie di traffico, ad esempio quello dei POS per i pagamenti con le carte di credito. Elementi fondamentali sono la disponibilità di svariate classi di servizio in cui possa essere suddiviso il traffico, di ritagliare reti virtuali assegnabili ad un dipartimento o ad una applicazione, di disporre di strumenti per reinstradare automaticamente il traffico e, non ultimo, di gestire e trasportare in rete protocolli diversi. Una rete convergente non è infatti sinonimo di univocità di protocolli. Anche se prosegue impetuosa l'evoluzione verso IP, per un periodo non prevedibile coesisteranno ancora applicazioni che utilizzano protocolli dedicati, sia perchè IP non è sempre l'ottimo, sia perchè sostituire dispositivi non IP può rivelarsi non fattibile sotto il piano economico.

In questo caso la soluzione può essere rappresentata da una rete MPLS in grado di convogliare in modo trasparente i diversi protocolli. Soluzione, peraltro, che è stata adottata dai principali fornitori di tecnologie di rete e praticamente da tutti i principali operatori. G.S.

Quando la sicurezza diventa abilitante invece che un obbligo

Il mercato della sicurezza sta crescendo. Bene. Ma sta crescendo male. Una delle principali spinte all'adozione di soluzioni di sicurezza è la cosiddetta necessità di compliance: in altre parole, l'obbligo a ottemperare ai requisiti previsti dalle leggi. Un dato testimoniato dalle principali società di ricerca di mercato e confermato dai molti vendor del settore che pubblicamente ringraziano le normative, a partire dalla privacy, per l'impulso dato al mercato. Ma un numero sempre maggiore di tali vendor si sta accorgendo del rovescio della medaglia: cioè della "povertà" degli investimenti prodotti dalla compliance. Di fronte a un obbligo, infatti, si reagisce tipicamente con fastidio ed eliminare quest'ultimo diventa l'obiettivo principale. Quello che tipicamente ne consegue è che si cerca di spendere il meno possibile per adempiere agli obblighi di legge, perdendo di vista le opportunità che in questa situazione si possono cogliere.

Ci sono poi anche lati nascosti della medaglia: perché spesso la compliance è un'ottima, a volta unica, scusa per recuperare un po' di fondi. Il risultato è che ufficialmente, grazie alle leggi, si è aumentato il livello di sicurezza in azienda, riducendo il rischio, ma all'atto pratico, spesso, s'implementano tecnologie solo basilari e neanche correttamente. Il problema è che non basta possedere la tecnologia, bisogna saperla usare, altrimenti il rischio aumenta invece di diminuire con il disastroso effetto di lasciare un falso senso di sicurezza.

Fortunatamente, esistono molti casi di lungimiranza, anche in Italia. È il classico "trasformare una debolezza in un punto di forza". Per ottemperare alla legge è necessario implementare una serie di strumenti organizzativi e tecnologici, ma, se invece di "rafforzare" qualcosa, s'investe intelligentemente studiando le opportunità che tali strumenti comportano, si ottiene un ritorno dagli investimenti e, magari,

anche la possibilità di aumentare il business aziendale.

Lo hanno fatto molte banche, che hanno creato i sistemi Internet retail, aumentando la raccolta del risparmio e le possibilità di contatto con i clienti. Quest'ultimo aspetto non va trascurato: c'è modo e modo di operare. Consigliare l'anziano di attivare l'home banking per non affaticarsi in coda allo sportello, non è detto che sia un servizio anche socialmente utile, se non gli si fornisce un supporto formativo adeguato, lasciandolo facile preda del phishing. Anche qui, una politica di protezione contro questa minaccia, considerato che alla fine di truffa si tratta e la banca ne è quindi responsabile, è un obbligo o un'opportunità? Lo ha fatto chi ha dovuto affrontare l'unificazione dei sistemi informativi a seguito di operazioni di fusione. Lo hanno fatto diverse grandi imprese, per esempio aumentando la produttività della forza vendita, rendendola mobile.

Lo sta facendo, senza cercare esempi limite, chi vuole accrescere il time to market di applicazioni e servizi alla propria utenza finale. L'azienda anche manifatturiera, ma che ha una componente importante di business sui servizi (si pensi all'assistenza sugli elettrodomestici, sull'impiantistica varia e così via), può utilizzare nuove tecnologie e varie forme di contatto con la clientela a patto di garantire la riservatezza delle comunicazioni. Tutto quanto consente di accelerare i processi di supporto si traduce non solo in aumento di produttività, ma in incremento di business, potendosi formulare contratti più ricchi.

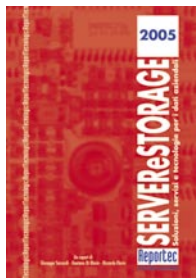
Soluzioni di supply chain, CRM, mobility, enterprise application integration, senza trascurare l'e-commerce e per arrivare ai Web Service e così via, tutte hanno bisogno di sicurezza.

Creare un sistema di sicurezza potente ed efficiente può abilitare il business e, già che c'è, fornisce la conformità alle normative. *



Gaetano Di Blasio

I report tecnologici



I Report Tecnologici costituiscono un'opera di analisi e approfondimento dello stato dell'arte di architetture, soluzioni e servizi nell'ambito dell'Information e Communication Technology.

Ogni report è un utile strumento di consultazione e un sussidiario che fornisce ai responsabili dei sistemi informativi aziendali e ai professional del settore un chiaro quadro dello scenario evolutivo delle tecnologie e delle soluzioni presenti sul mercato italiano. Ciascun Report è composto da una prima parte, che costituisce una cospicua trattazione degli aspetti tecnologici, e da una seconda parte, in cui vengono accuratamente descritte l'offerta e la strategia dei principali player del mercato.

Uno dei temi più attuali del momento è quello Motore e sede dei dati aziendali, server e storage sono gli elementi centrali di un sistema informativo che si articola in infrastrutture sempre più complesse che rispondono alle crescenti esigenze di elaborazione e all'esplosione dei dati, ma che devono risultare semplici per l'utente finale. Le nuove architetture evolvono in questa direzione, favorendo il consolidamento dei sistemi.

Un report di circa 600 pagine analizza tutti gli aspetti del settore, esaminando, oltre alle tecnologie, le soluzioni e l'offerta di servizi in Italia.

Capitolo 1

Dall'e-business all'azienda virtuale

Capitolo 2

L'evoluzione delle piattaforme server

Capitolo 3

Le architetture di elaborazione

Capitolo 4

La specializzazione delle appliance server

Capitolo 5

Le risorse per la memorizzazione dei dati

Capitolo 6

L'evoluzione verso lo storage in rete

Capitolo 7

Business Continuity e disaster recovery

Capitolo 8

Virtualizzazione e gestione dello storage

Capitolo 9

Information Lifecycle Management e Content Management

Capitolo 10

Lo storage a disposizione della PMI

PARTE SECONDA

Tecnologie e strategie dei fornitori di soluzioni e servizi

Acer • Brocade • Cisco Systems • Computer Associates • Dell • EMC2 • Fujitsu Siemens Computer • Hitachi Data Systems • HP Soluzioni Server • HP Divisione Storage • IBM Soluzioni Server • IBM Soluzioni Storage • Mc Data • Microsoft • Storagetek • Terasystem • Veritas Software

I sistemi e le tecnologie di rete per realizzare le architetture che rappresentano il cuore del sistema informativo aziendale hanno subito una profonda evoluzione negli ultimi anni. La convergenza tra reti dati e reti voce e tra fisso e mobile ha al tempo stesso semplificato e complicato la gestione di un'infrastruttura vitale, accrescendo il ricorso all'outsourcing. Un report di circa 500 pagine analizza tutti gli aspetti del networking, soffermandosi sulle architetture, le piattaforme e, non ultima, l'offerta di servizi in Italia.

Capitolo 1

Lo scenario del Business Networking

Capitolo 2

Architetture e servizi delle reti di comunicazione

Capitolo 3

LAN, il sistema nervoso dell'azienda

Capitolo 4

Le reti locali wireless

Capitolo 5

Le reti metropolitane

Capitolo 6

Le reti per la fonia mobile

Capitolo 7

Virtual Private Network

Capitolo 8

Il network management

Capitolo 9

Un network protetto

Capitolo 10

Servizi e outsourcing

PARTE SECONDA

Tecnologie e strategie dei fornitori di soluzioni e servizi

3Com • Alcatel • Brocade - CIE Telematica
RAD Data Communications • Cisco Systems
• Computer Associates • Easynet • Marconi
• Microsoft • Procurve Networking • U.S. Robotics



Tutto l'hardware del mondo sarebbe inutile senza le soluzioni che su di esso si basano. La piattaforma software e l'infrastruttura applicativa rappresentano il vero cuore del sistema informativo e il punto di contatto tra questo e chi lo utilizza in azienda, dal semplice impiegato all'amministratore delegato. Un report di 400 pagine analizza gli elementi delle soluzioni software, soffermandosi sulle architetture, le piattaforme e, non ultima, l'offerta di servizi in Italia.

- Capitolo 1
Applicazioni per l'azienda: il quadro comune
- Capitolo 2
Database e datawarehouse
- Capitolo 3
L'Enterprise Resource Planning
- Capitolo 4
Business Intelligence e Business Process Management
- Capitolo 5
IT Governance
- Capitolo 6
La gestione integrata dell'IT
- Capitolo 7
Supply Chain Management
- Capitolo 8
Il Customer Relationship Management
- Capitolo 9
Gli strumenti per l'integrazione delle applicazioni
- Capitolo 10
Web Services
- Capitolo 11
Service Oriented Architecture ed Enterprise Service Bus
- Capitolo 12
Il document management
- Capitolo 13
Gli ambienti di sviluppo
- Capitolo 14
Il middleware

PARTE SECONDA

Tecnologie e strategie dei fornitori di soluzioni

Adobe Systems • Computer Associates • Hewlett Packard • IBM Software Group • Microsoft • Océ • Software AG • Sun Microsystems



I sistemi e le tecnologie di rete per realizzare le architetture che rappresentano il cuore del sistema informativo aziendale hanno subito una profonda evoluzione negli ultimi anni. La convergenza tra reti dati e reti voce e tra fisso e mobile ha al tempo stesso semplificato e complicato la gestione di un'infrastruttura vitale, accrescendo il ricorso all'outsourcing. Un report di oltre 500 pagine analizza tutti gli aspetti del networking, soffermandosi sulle architetture, le piattaforme e, non ultima, l'offerta di servizi in Italia.

- Capitolo 1
Lo scenario evolutivo della Business Communication
- Capitolo 2
Architetture e standard per i nuovi PABX
- Capitolo 3
I nuovi sistemi di comunicazione per le PMI e l'ambito enterprise
- Capitolo 4
L'integrazione tra computer e telefono
- Capitolo 5
Gli IP-PABX: caratteristiche e funzionalità dei PABX di nuova generazione
- Capitolo 6
I voice portal
- Capitolo 7
Call Center e gli scenari per l'azienda
- Capitolo 8
Messaging integrato e unified communication
- Capitolo 9
La sicurezza nei sistemi di comunicazione aziendale
- Capitolo 10
Le architetture delle reti carrier per la Business Communication
- Capitolo 11
La videocomunicazione

PARTE SECONDA

Tecnologie e strategie dei fornitori di soluzioni e servizi

3Com • Alcatel • Avaya • Cisco Systems • Easynet • Ericsson • IBM Software Group • Microsoft • Nortel Networks • Promelit • Selta • Siemens

I Report Tecnologici sono disponibili in volumi stampati in formato A4 con copertina rigida, al costo di 215 euro a copia (più IVA). Per ordinarli o per ulteriori informazioni: 0234592314.

Servizi per gli abbonati

I REPORT

Business Networking

IT Security

Server e Storage

Business Communication

Business Software Solutions.

I rapporti annuali di Reportec possono essere acquistati in formato A4 rilegato in hard cover con sovracopertina al prezzo di 215 euro più IVA cadauno.

FORMULA ABBONAMENTO

Abbonandosi al dossier bimestrale Direction, si ha diritto a ricevere sei numeri di aggiornamento e approfondimento completi delle versioni su CD ROM dei report annuali e una copia stampata e rilegata di uno dei report pubblicati.

Il prezzo dell'abbonamento a Direction è pari a euro 100 più IVA e comprende le spese di spedizione del report stampato.

L'abbonato ha diritto ad acquistare copie stampate dei report al prezzo unitario riservato di 100 euro più IVA (comprese spese di spedizione).

Per sottoscrivere l'abbonamento inviare un'e-mail a servizi@reportec.it
oppure un fax al numero 0234532848

