

DIRECTION Reportec 53

DOSSIER DI SOLUZIONI SERVIZI E TECNOLOGIE ICT



Storage

Lo storage di Ibm diventa più efficiente

Data Center

I servizi di Fujitsu ottimizzano il data center

Communication

Samsung «racconta» l'eccellenza di Campari

Survey Reportec

L'estratto del Survey Servizi e tecnologie per l'ICT Security nelle aziende italiane



IL REPORT

ICT Security e Business continuity

Protezione degli asset aziendali e garanzia della continuità operativa

CON LA PARTECIPAZIONE DI



Indice

▷ Sempre più spazio al video nella comunicazione business	3
▶ Il REPORT ICT Security e Business Continuity 2012	4
▶ Sicurezza integrata in 3D per Check Point	9
▶ Fortinet e il «Power to Control»	10
▶ L'approccio unificato di HP alla «enterprise security»	11
▶ La sicurezza intelligente di Ibm	12
▶ La protezione data centrica di Trend Micro	13
 Servizi e tecnologie per l'ICT Security nelle aziende italiane. Stato attuale e scenari di diffusione futura	14
▷ Tremate: arrivano i Millennials	17
▶ I servizi di Fujitsu ottimizzano il data center	18
▶ Lo storage IBM diventa più efficiente	20
▶ I vantaggi del virtual workerplace	22
▶ Una sinergia che migliora le applicazioni in rete	24
▶ Samsung racconta l'eccellenza di Campari	26
▶ POP Channel rende la comunicazione nei punti vendita dinamica e misurabile	28
▶ Il backup Symantec fa un passo in avanti	28
▶ Dimension Data con decisione nel cloud	29
▶ Una nuova generazione di processori Intel	29
▷ Con i maker nasce la generazione del «fare»	30

COGLI L'OPPORTUNITÀ DI RICEVERE COMODAMENTE NELLA TUA CASELLA DI POSTA DIRECTION E SOLUTIONS SE SCEGLI DI RICEVERE LA TUA RIVISTA VIA E-MAIL SCRIVI SUBITO A servizi@reportec.it

Mai più copie "rubate" dal collega, ma possibilità di rapida condivisione dei nostri esclusivi contenuti. Sfrutta il formato elettronico per una più veloce consultazione e creati il tuo archivio personale. Rispetta l'ambiente e aiutaci a usare meno carta



Giuseppe Saccardi

Sempre più spazio al video nella comunicazione business

Tra i trend che maggiormente interessano l'ICT e che sono visti come uno dei mezzi più immediati per ottimizzare i processi aziendali, l'interazione dei dipendenti e contemporaneamente ridurre i costi, la mobility continua a ricoprire una posizione predominante. Ma la mobilità è una condizione, un modo di lavorare che non può prescindere dalla disponibilità di strumenti adatti, che facciano sì che un dipendente mobile possa interagire con colleghi, clienti o fornitori con modalità quanto più simili possibili a una relazione "de visu".

È questo il campo dell'unified communication e collaboration e, al suo interno, dei servizi di videocomunicazione. Videocomunicare presenta il beneficio di abbattere le barriere psicologiche che sono insite nel parlare senza vedersi e permette di stabilire un legame più diretto e produttivo con l'interlocutore. In tal senso si giustifica la forte crescita dell'interesse per la videocomunicazione, interesse che si riferisce sia alla semplice aggiunta del video alla conversazione telefonica tra chiamato e chiamante, facilitata dalla disponibilità di schermi del dispositivo mobile di ampie dimensioni, che ai sistemi di videoconferenze basati su pc o, all'estremo, su sale appositamente attrezzate dove è possibile interagire con più destinatari remoti come se fossero presenti allo stesso tavolo e lavorare congiuntamente su lavagne elettroniche o su documenti che vengono condivisi.

Se la videocomunicazione sta crescendo nell'interesse i fattori in gioco sono perlomeno tre. Di questi, uno è l'abilitatore tecnologico, l'altro è sostanzialmente economico, il terzo è la predisposizione dell'utente.

Per video comunicare con efficacia la cosa che serve soprattutto è la banda, disponibile in modo diffuso e a prezzi accettabili, altrimenti il rapporto costo/benefici risulta fortemente negativo e l'interesse per la videocomunicazione come strumento di efficientamento decade rapidamente quando si devono saldare le prime bollette. È questo il motivo per cui i tentativi di diffondere la videocomunicazione che sono stati fatti

a partire dagli anni 90 utilizzando reti Isdn sono sostanzialmente falliti. Costosi e complicati da usare e limitati all'ambito di rete fissa. Ora la banda disponibile esiste a prezzi tutto sommato abbordabili, così come a costi aperti a tutti gli utenti aziendali sono anche i dispositivi necessari per farlo all'interno di una soluzione di unified communication.

Il secondo fattore, quello economico, è invece più inerente ai costi complessivi connessi agli spostamenti delle persone in azienda per effettuare riunioni in sedi diverse o per interagire a livello di gruppi di lavoro.

È in questo campo che la videocomunicazione si presenta come lo strumento più adatto per ridurre gli elevati costi di trasferta e per ottimizzare l'efficienza, che poi è un ulteriore modo per recuperare costi.

Ora predisporre una sala attrezzata a videoconferenza o utilizzarne un'offerta sotto forma di servizio è sostanzialmente alla portata di tutte le medie aziende e, se servono soluzioni non eccessivamente sofisticate, anche delle piccole aziende.

Un ultimo fattore va poi considerato: la predisposizione all'utilizzo. Nel ricorrere al video esiste, inutile negarlo, una certa riottosità, perché viene a mancare quella sensazione di libertà che si ha con le sole conversazioni audio. Anche in questo però un aiuto viene dalla tecnologia, che ha messo in mano agli utenti di un domani prossimo, strumenti gratuiti come Skype o YouTube che hanno creato una generazione di persone abituate ad avere a che fare quotidianamente con la videocomunicazione e quindi la vedranno come uno strumento aziendale del tutto naturale. Anzi, il non averla potrebbe diventare causa di disaffezione e portare a un modo di lavorare insoddisfacente e meno produttivo. ■

All'interno del CD allegato a questo numero di Direction vengono approfonditi i temi che definiscono la sicurezza informatica, affiancati dall'analisi esaustiva delle soluzioni e strategie dei principali vendor

IL REPORT ICT Security e Business Continuity 2012

Protezione degli asset aziendali e continuità operativa in un'ottica di gestione del rischio e conformità normativa



Lo scenario ICT sta rapidamente cambiando sotto la spinta di una serie di fattori tecnologici e di mercato che modificano le tipologie di dati, di dispositivi responsabili per la loro creazione, le modalità di utilizzo dell'ICT e i modelli tecnologici di distribuzione e implementazione delle risorse e i modelli di business.

Crescono le logiche di IT basato su servizio, mentre l'automazione e la mobilità favoriscono la creazione di dataset di grandi dimensioni, eterogenei e tendenzialmente destrutturati (i cosiddetti "Big Data"), che trovano nei modelli di cloud computing la naturale risposta alla loro gestione.

Crescono i rischi legati all'aumento dei dispositivi mobili e al modo di utilizzarli, le minacce diventano mirate e persistenti, i dati aziendali trovano collocazione su server distribuiti a livello globale mentre la virtualizzazione, a ogni livello, richiede nuovi approcci.

Uno scenario caratterizzato da forte dinamicità che offre grandi opportunità alle aziende vendor di ICT, ma anche alle organizzazioni che sapranno costruire su questi nuovi tasselli elementi di vantaggio competitivo.

La sicurezza nel cloud

In generale le modalità di fruizione dell'ICT come servizio si stanno diffondendo rapidamente: spesso accade che gli stessi dipendenti attivino servizi online, scavalcando l'IT aziendale. Soprattutto nelle grandi organizzazioni, infatti, la lentezza dei processi porta a cercare scorciatoie. Uno degli ambiti emergenti in cui la sicurezza gioca un ruolo fondamentale abilitante è il cloud computing. La "nuvola", che si manifesta in diverse modalità (private, public e mixed), promette risparmi notevoli in infrastrutture e, di fatto, molte imprese stanno già utilizzando servizi che sfruttano risorse virtuali trasparenti per l'azienda stessa: per esempio la posta elettronica o il Web server in hosting presso un provider. Il cloud modifica il concetto di perimetro aziendale all'interno del quale risiedono i dati business e quindi porta a rivedere le metodologie con cui affrontarne la protezione. Inoltre, uno dei nodi centrali che limitano l'uso del modello tecnologico del cloud computing è la perdita della possibilità di controllo diretto della gestione del patrimonio informativo aziendale e di dati sensibili personali.

In questi casi la dislocazione delle diverse infrastrutture che ospitano i dati dell'azienda potrebbe rappresentare un ostacolo alla possibilità di conoscere esattamente dove questi sono ubicati.



Per ora non sono stati definiti dal punto di vista normativo requisiti specifici, ma il Garante della Privacy si è "limitato" a fornire alcune indicazioni per un utilizzo consapevole del cloud quali, per esempio, di verificare l'affidabilità e la competenze del fornitore, controllare l'allocazione fisica dei dati o stabilire in fase contrattuale i Service Level Agreement a cui riferirsi.

La sicurezza negli ambienti virtualizzati

La diffusione di ambienti IT virtuali in ambito enterprise ha portato l'attenzione verso le problematiche di sicurezza legate all'uso di queste soluzioni che, per la loro particolarità di trasformare ciò che è fisico in virtuale, presentano alcune specifiche criticità.

Nel passaggio a un ambiente virtualizzato si devono considerare alcuni aspetti critici che potrebbero minacciare la sicurezza. In un ambiente virtualizzato, infatti, le tre componenti infrastrutturali di base, cioè il networking, lo storage e i server, dovranno presentare il minor numero possibile di point of failure ed essere adeguatamente dimensionate e configurate per garantire la massima affidabilità.

Quando si affronta l'architettura storage è opportuno predisporla in modo da consentire la "live migration" di una Virtual Machine (VM) o di un'applicazione tra diverse macchine fisiche senza disconnettere il client o l'applicazione. Lo storage deve essere accessibile da tutti i server fisici garantendo la massima affidabilità e, per questo, sono consigliabili connessioni ridondate a ognuno di essi.

A livello server va prevista invece l'adozione di processori che supportano nativamente la virtualizzazione completa e una configurazione pensata in funzione dei sistemi virtualizzati che saranno eseguiti.

La sicurezza dei sistemi virtualizzati deve essere realizzata focalizzando l'attenzione su accorgimenti specifici rivolti a individuare possibili minacce alla sicurezza. Per proteggere gli ambienti virtuali è fonda-

mentale affrontare anche la questione dell'Integrità delle VM, che si traduce in un aspetto legato alla sicurezza dell'host che ospita le immagini dei dischi di tutte le macchine virtuali a esso collegate.

Protezione dei dispositivi mobili e consumerizzazione

Un altro trend che sta rivoluzionando il mondo della sicurezza ICT è legato al progressivo utilizzo di dispositivi mobili personali per svolgere attività lavorative. Inoltre l'evoluzione dei dispositivi mobili, che sono diventati apparecchi di facile utilizzo, sufficiente potenza elaborativa e grande capacità comunicativa e collaborativa, aumenta notevolmente il numero di applicazioni che è possibile gestire in mobilità e i rischi associati.

Tutto ciò delinea un fenomeno a cui si è dato il nome di consumerizzazione e che spesso viene ricondotto all'immane sigla made in USA: Bring Your Own Device (BYOD).

Si tratta di una "tentazione" a cui cedono molte aziende perché risparmiano sugli acquisti ed ottengono una maggiore soddisfazione dell'utente (libero di usare lo strumento che gli è più congeniale) che si traduce con una maggiore efficienza lavorativa. Non mancano anche at-





teggiami reticenti, ma in molti casi una forte spinta viene proprio dal top manager, magari il titolare o il figlio dello stesso, che pretende l'integrazione del proprio smartphone o tablet di ultimo grido: una situazione che lascia poco margine di azione al dipartimento informatico che si deve adeguare, trovandosi a volte a dover fronteggiare il problema di un amministratore delegato

che vuole utilizzare il tablet e che non comprende il rischio di far finire i dati di bilancio in mano alla concorrenza.

In sintesi si può dire che non è pensabile opporsi a un processo di questo tipo, che pure pone delicate questioni relativamente alla sicurezza e alla possibilità di controllo su un apparecchio privato, che richiede quindi di essere affrontato in modo strategico e coordinato con una gestione integrata all'interno della visione complessiva di sicurezza aziendale.

Attacchi mirati e persistenti

Tutti i rapporti divulgati dalle principali società impegnate nella sicurezza concordano su un dato: aumentano il numero degli attacchi "mirati", cioè condotti con un preciso fine, e di quelli "silenti", cioè orientati a un obiettivo evitando di "far rumore".

In altre parole, l'hacker ha smesso i panni goliardici per trasformarsi in un esperto criminale, che studia le sue vittime e colpisce a sorpresa. Ci sono casi molto "personali", talvolta casi di spionaggio industriale, ma più spesso l'attacco è "semplicemente" finalizzato a carpire identità elettroniche con le quali commettere frodi. La maggior parte degli attacchi che vanno a buon fine si basa sullo studio delle potenziali vittime,

al fine di indurle a cliccare un link contenuto in un messaggio e-mail. Tramite tale link viene scaricato il codice maligno (detto malware) che si annida sul computer, ricerca determinati tipi di dati e li invia al suo creatore. Lo fa sfruttando i tempi morti, disturbando la normale operatività il meno possibile.

Un'altra sigla che si è affacciata nel mondo della sicurezza è APT, che identifica quelle minacce note per saper abilmente eludere i sistemi di sicurezza convenzionali che operano a livello perimetrale e sui contenuti.

Il termine APT viene solitamente riferito a pattern di attacchi sofisticati perpetrati in modo continuativo per lunghi tempi indirizzati a governi, aziende e attività di carattere politico. Gli attacchi APT includono minacce quali spionaggio perpetrato tramite Internet oppure la diffusione di media "infetti", attività indirizzate a compromettere la supply chain o di social engineering.

La convergenza tra sicurezza fisica e sicurezza logica

Per molto tempo la sicurezza ICT è rimasta separata dalla sicurezza fisica, intesa come impianti antincendio, sistemi antifurto, barriere all'ingresso.

Di fatto si tratta di due mondi sempre meno disgiunti e crescono gli ambiti tecnologici in cui questa convergenza si realizza, per esempio, quello del controllo degli accessi o delle presenze in azienda, oggi sempre più attuato con badge elettronici direttamente connessi con i sistemi ERP aziendali, oppure mediante lettura di dati biometrici digitalizzati. Un altro ambito di convergenza è quello dei nuovi edifici, cablati e permeati di sensori, che diventano così sempre più "intelligenti" e in grado di esercitare in modo autonomo controlli di sicurezza efficaci e di effettuare correlazioni tra gli eventi che attivano automatismi. In questo contesto (ma non solo in questo) va registrato un costante sviluppo: è quello della videosorveglianza cosiddetta di quarta generazione basata su un'architettura



di rete IP, in cui la rete stessa costituisce la matrice video per il trasporto delle immagini.

È indubbio che realizzare architetture di videosorveglianza all'avanguardia permette di ottenere maggiore affidabilità, un livello più elevato di disponibilità del sistema e, al contempo, più versatilità e interoperabilità tra tecnologie e soluzioni proprietarie che sino a ieri non potevano colloquiare tra di loro.

La possibilità di far confluire le funzioni di switching video all'interno di un ambiente IP preesistente, permette poi di ridurre la complessità dell'infrastruttura e, di conseguenza, i costi di installazione di un sistema di videosorveglianza, seppur mantenendo l'investimento progressivo e le competenze umane a esso associate.

La protezione dell'infrastruttura di rete

L'avvento di nuovi modelli di business che aprono le aziende verso clienti, partner e fornitori, ha reso progressivamente più complicato riuscire a definire in modo netto il perimetro della rete aziendale.

Il network richiede l'implementazione di tecnologie che lo rendano intrinsecamente sicuro. Inoltre va garantita la protezione dai rischi alimentati dal mobile computing, dato che sono aumentati notevolmente il numero di utenti remoti, le piattaforme e metodologie di accesso, il numero e la varietà dei terminali per la connettività alla rete, i cosiddetti endpoint, rappresentati da laptop, desktop, PDA, smart phone e così via. La presenza di endpoint insicuri costituisce un grosso elemento di vulnerabilità tanto che, in molti casi, gli utenti con accesso autorizzato pongono più rischi di chi deve compromettere un firewall per entrare in rete.

Le nuove evoluzioni nei modelli di protezione devono quindi considerare in modo diverso la rete.

Questo non significa che le soluzioni di protezione di tipo più tradizionale siano sorpassate o vadano abbandonate. Piuttosto vanno rafforzate e i nuovi obiettivi sono quelli di arrivare

a una loro integrazione con i nuovi strumenti di sicurezza favorendo una gestione unificata e semplificata.

Garantire la continuità del business

Il problema della sicurezza di funzionamento, ovvero la continuità operativa e la disponibilità dei dati, ha assunto per un'azienda una valenza primaria. Correlato alla sopravvivenza e alla continuità delle operazioni vi è quindi il problema di come far fronte a disastri che minino in parte o in toto la disponibilità dei dati aziendali e la continuità di un'elaborazione degli stessi.

Pertanto, eventi qualificabili come vere e proprie catastrofi sono usualmente l'eccezione mentre, generalmente, i motivi di un fermo di sistemi e applicazioni si presentano sotto forma di guasti hardware, di malfunzionamenti applicativi o di errori operativi da parte degli addetti che causano il crash dei sistemi e la conseguente indisponibilità delle informazioni.

L'esperienza sul campo indica in circa un ottanta per cento i fermi macchina provocati da malfunzionamenti dell'hardware o da interruzioni operative dovute a errori umani, anche se non ne deriva che il relativo impatto sull'azienda sia meno devastante. Poiché questi eventi non possono essere del tutto evitati, la capacità di un'azienda di contenere queste minacce dipende essenzialmente dal suo stato di preparazione, in quanto buona parte dei potenziali malfunzionamenti derivanti da un evento catastrofico possono essere evitati con un'adeguata pianificazione, implementazione e sperimentazione di un adeguato piano di emergenza e con la scelta di tecnologie e progettazioni adeguate.



Dalla protezione del business alla gestione e controllo del rischio

La costante dinamicità che caratterizza il concetto di protezione lo rende sempre più correlato al tema della gestione del rischio in senso ampio del termine ovvero legato al business complessivo dell'azienda. Ne segue che anche le pratiche per l'Information Security devono rientrare tra le decisioni per la governance

aziendale, guardando alla sicurezza come a un elemento abilitante per il business e uno strumento per imporre policy comportamentali che consentano di affinare la governance dell'impresa.

Pensare alla governance è quindi la strategia che può dare i maggiori benefici, aiutando le imprese a governare la sicurezza in sintonia con il resto dell'azienda per uno scopo comune: la gestione e il controllo del rischio. Questo non vuol dire avere imprese poco dinamiche e senza spirito d'innovazione.

Tutt'altro, significa che anche nel gettarsi in nuove avventure lo si farà con i piedi per terra, salvaguardando i beni principali dell'azienda e, quindi, la loro sopravvivenza in ogni situazione. Ogni azienda deve quindi valutare le proprie esigenze in termini di sicurezza, identificando le aree di interesse e gli ambiti nei quali sarà necessario adottare gli opportuni strumenti. È fondamentale studiare le infrastrutture utilizzate, le applicazioni e i processi aziendali, al fine di comprendere quali investimenti conviene effettuare. Il risultato è un trade-off tra l'investimento richiesto e il livello di protezione che si vuole o può ottenere.

L'approccio gestionale alla sicurezza dei dati

Il riconosciuto valore dell'informazione per un'azienda, accompagnato dalla crescita indiscriminata del numero delle stesse, ha portato all'attenzione verso la definizione di regole di tipo standard per l'organizzazione della sicurezza.

Un sistema di gestione per la sicurezza delle informazioni (SGSI) prevede che l'azienda implementi una politica di sicurezza allo scopo di gestire le aree a rischio. Alla base di un SGSI c'è la definizione di una gamma di policy per la sicurezza delle informazioni, che preveda l'assegnazione specifica di responsabilità e l'implementazione di metodologie che considerino la gestione della business continuity, il report degli incidenti e una serie di controlli periodici per assicurare il raggiungimento degli obiettivi previsti nell'ambito della security. Tutto ciò all'interno di un processo di educazione, sensibilizzazione e training verso le tematiche della sicurezza. Il passo successivo è quello di adottare un sistema per verificare il proprio SGSI, attraverso una certificazione, in conformità ad alcuni standard specifici. La tipologia di azienda maggiormente interessata a questo tipo di certificazione è quella che deve proporre all'esterno un'immagine di sicurezza e comprende, per esempio, aziende operanti in ambito finanziario, delle telecomunicazioni, dell'erogazione di servizi IT o la PA.

I vantaggi nel disporre di una certificazione del sistema con cui viene gestita la sicurezza delle informazioni risiedono nella possibilità, da parte dell'azienda, di dimostrare in modo tangibile a partner e clienti la propria attenzione nella garanzia della sicurezza delle informazioni, promuovendo la credibilità dell'azienda, contribuendo alla creazione di una "cultura della sicurezza" all'interno della propria organizzazione e garantendo che i dati vengano archiviati e conservati all'interno di un sistema di gestione aziendale. L'adozione di procedure standardizzate e certificate consente di individuare le aree di maggiore criticità attraverso un'analisi dei rischi e di fornire un orientamento preciso ai processi di implementazione della politica di sicurezza stabilita. ■



Con l'architettura Software Blade funzionalità su misura per ogni esigenza di protezione e controllo, partendo da policy, utenti ed enforcement. APT, Botnet, mobile, tra le ultime novità

Non è più il tempo dei sistemi per la sicurezza "assemblati" in casa con la logica del best of breed. Lo sostengono in Check Point Software Technologies, che pure sull'eccellenza delle proprie soluzioni di firewalling ha posto le basi per il successo in questo mercato. Oggi, però, la società israeliana ha maturato una visione integrata basata sul concetto della "3D Security", che deve essere considerato un processo aziendale di business come altri. Un processo che parte dalla definizione dei propri obiettivi di sicurezza e, quindi, delle policy. A questa prima dimensione si aggiunge poi l'elemento "people": Quelle persone che devono essere coinvolte nel processo della sicurezza, mentre in passato le direttive e le tecnologie venivano calate dall'alto e non spiegate, con il rischio concreto che il comportamento dell'utilizzatore ne inficiasse l'efficacia.

Per ultima la terza dimensione: la tecnologia, che consente l'enforcement delle policy e il coinvolgimento delle persone. «La tecnologia è davvero l'elemento meno importante del processo», sostiene Rodolfo Falcone, country manager di Check Point in Italia, perché, spiega: «Solo quando si hanno chiare le policy e quindi le aree critiche per l'azienda, è possibile stabilire quali tecnologie sono realmente utili. Non è il caso di acquistare dispositivi UTM (Universal Threat Management) che fanno tutto, quando sono necessarie solo alcune funzionalità. Nei nostri colloqui con i clienti abbiamo verificato come, grazie a questo approccio, potessero risparmiare e ottenere il livello di sicurezza adeguato alle loro esigenze».

L'architettura in una release

Indirizzando dunque un sistema integrato per la sicurezza, Check Point ha sviluppato un'architettura unica, concretizzata nella release R75, che permette d'implementare l'approccio della 3D Security

Sicurezza integrata in 3D per Check Point

sulla base della software blade architecture, già introdotta da un paio d'anni circa. Quest'ultima consta di un gateway (un dispositivo multifunzionale, più che un firewall) e di una serie di applicazioni che abilitano le diverse funzionalità di protezione e un utilizzo sicuro delle risorse IT e di quelle Internet.

Le appliance sono state rinnovate, aumentando prestazioni e flessibilità di scelta, anche grazie a un sistema di metrica delle capacità deonominato SecurityPower. Le "blade" disponibili sono: Firewall; IPSEC VPN; Mobile Access; Identity Awareness; Application Control; IPS; DLP; Web Security; URL Filtering; Antivirus & Anti-Malware; Anti-Spam & Email Security; Advanced Networking; Acceleration & Clustering; Voice over IP (VoIP); Security Gateway Virtual Edition e, ultima solo in ordine di arrivo con la release R75.40, la AntiBot software Blade, per la protezione contro le botnet. Da sottolineare, inoltre, lo sforzo di Check Point per la "cultura" della sicurezza, rappresentato sia da un'attività di formazione presso gli utenti finali, sia dagli automatismi impliciti nelle soluzioni. Questi ultimi, in particolare, sono "accompagnati" dalla funzione User Check, già introdotta da qualche tempo con la prima versione del DLP, per un enforcement "informato". Tutte le attività sono registrate e il sistema avverte l'utente degli eventuali comportamenti non consentiti o non consigliati: è possibile bloccarli o permettere una sorta di "autocertificazione", con regole definibili in maniera granulare. In questo modo, si limita il rischio di "errori" dovuti all'ingenuità dell'utente. ■



Controllare la sicurezza per migliorare la gestione, la protezione, l'efficienza delle persone in uno scenario sempre più complesso, puntando sul management integrato e sulle prestazioni

Fortinet e il «Power to Control»

L'evoluzione delle minacce richiede strumenti sempre più potenti e avanzati, ma, parafrasando una famosa pubblicità: la potenza è nulla senza il controllo. Fortinet, che sin dalla fondazione nel 2000 ha dato vita al concetto di Unified Threat Management, ha basato il proprio successo sulla realizzazione di ASIC (Application Specific Integrated Circuit) con cui ha realizzato i primi sistemi basati su coprocessori di rete in grado di indirizzare contemporaneamente più minacce.

Oggi le soluzioni Fortinet forniscono una protezione accurata contro tutti i più importanti attacchi perpetrati attraverso strumenti sempre più integrati e sofisticati, all'interno di scenari caratterizzati da una crescente complessità. Le Advanced Persistent Threat, in particolare, rappresentano una minaccia in continua espansione, la cui espressione più diffusa è quella delle botnet. Fortinet ha esteso le proprie soluzioni per identificare questo tipo di minacce, comprese quelle sviluppate per realizzare botnet che comprendono dispositivi wireless, come smartphone e tablet.

La mobility è un altro dei temi emergenti cui la società statunitense si è dedicata, anche per rispondere alle problematiche legate al cosiddetto fenomeno BYOD (Bring Your Own Device). Quest'ultimo è "figlio" della consumerization, cioè della spinta innovativa in ambito consumer che sta superando quella interna alle aziende. Ciò porta molti dipendenti, a cominciare dai top manager, a chiedere

di poter utilizzare per lavoro il proprio dispositivo, tipicamente mobile, più potente e avanzato di quello messo a disposizione dall'impresa, con tutti i problemi che ciò comporta in termini di gestibilità e sicurezza.

Monitoraggio e controllo

Gli obiettivi delle soluzioni per la sicurezza di Fortinet sono essenzialmente: monitorare l'accesso alla rete e ai dati e rendere la trasmissione dati lungo la rete sicura. Il tutto, appunto, in uno scenario complesso, in cui i dispositivi, gli strumenti di produttività e i media utilizzati sono sempre più diversificati, comprendendo un massiccio utilizzo del Web.

Per questo è necessario poter controllare i dispositivi, le reti, consolidando, come sottolineano i responsabili della società statunitense, le attività operative, la gestione e la stessa architettura del sistema per la sicurezza. Una semplificazione che è implicita nel Dna di Fortinet e basata sul concetto stesso di UTM. La crescita delle minacce viene bilanciata dall'aumento costante delle prestazioni degli ASIC, mentre la gestibilità viene migliorata grazie alla visibilità e alla capacità di controllo sugli utenti e sulle applicazioni, definendo per ciascuno gli opportuni privilegi di accesso alle risorse.

Le soluzioni Fortinet sono quindi in grado di identificare le minacce, grazie alla capacità d'ispezione profonda e accurata di ogni pacchetto, senza penalizzazione delle prestazioni, come evidenziano presso la società, sottolineando come il controllo sia possibile non solo a livello di gateway, ma end to end, grazie a una stretta integrazione delle soluzioni Fortinet con i dispositivi di rete. Il tutto anche in ambienti virtualizzati, per i quali sono state sviluppate specifiche soluzioni software. ■



L'ampliamento nel portafoglio del vendor di soluzioni e servizi che riunisce le famiglie TippingPoint, ArcSight e Fortify, realizza una protezione end-to-end

La crescente diffusione di mobilità, cloud computing e social media sta ampliando i rischi a cui si trova esposto il patrimonio informativo aziendale e, per far fronte in modo efficace a queste sfide, le aziende puntano sempre più verso una gestione della sicurezza e del rischio integrate.

La risposta di HP a queste esigenze si concretizza nel framework di protezione ESP (Enterprise Security Products), che fornisce funzionalità per la gestione intelligente della sicurezza delle informazioni e che è stato recentemente ampliato per garantire un livello di protezione end-to-end.

All'interno del framework HP Enterprise Security Products si collocano le soluzioni per l'intrusion prevention (IPS) HP TippingPoint a cui si sono recentemente aggiunte quelle derivanti dall'acquisizione di ArcSight e di Fortify, in un contesto di integrazione che coinvolge servizi, applicazioni e prodotti.

La piattaforma IPS HP TippingPoint è un elemento centrale per la sicurezza dell'infrastruttura di rete e del data center poiché permette di filtrare il traffico in ingresso e in uscita sulla rete aziendale, bloccare i contenuti maligni, identificare comportamenti pericolosi o tentate violazioni di policy. Questa soluzione è composta da tre tasselli: le piattaforme hardware specializzate per la prevenzione delle intrusioni (IPS); le soluzioni appliance e virtual machine HP TippingPoint Security Management System (SMS) che forniscono funzioni di gestione della sicurezza di livello enterprise a tutti i prodotti di sicurezza HP TippingPoint; l'organizzazione di ricerca per la sicurezza DVlabs che fornisce le informazioni intelligenti di sicurezza che alimentano le piattaforme IPS, come il fondamentale Digital Vaccine e il servizio integrativo di reputazione dinamica della rete pubblica RepDV. Le soluzioni IPS HP TippingPoint individuano le vulnerabilità presenti sulla rete e intervengono applicando delle "patch" virtuali

L'approccio unificato di HP alla «enterprise security»

che ne impediscono lo sfruttamento. La piattaforma HP ArcSight Enterprise Threat and Risk Management (ETRM) è una suite integrata di prodotti di security information e di event management (SIEM) per la raccolta, l'analisi e la correlazione delle informazioni di sicurezza e degli eventi di rischio, la protezione delle applicazioni e la difesa della rete. Questa gamma di soluzioni software permette di correlare log, ruoli dell'utente e flussi di rete per individuare eventi legati alla sicurezza in base ai quali definire priorità e predisporre risposte efficaci e preventive a breccie, attacchi, ma anche a minacce provenienti dall'interno del perimetro aziendale.

Il terzo tassello della soluzione HP per la sicurezza enterprise unificata è la Suite HP Fortify Software Security Center. Si tratta di una soluzione per automatizzare e gestire la sicurezza applicativa, in grado di testare la sicurezza delle applicazioni e di identificare le vulnerabilità, che può essere utilizzata sia in modalità on-premises sia on-demand. ■



Un approccio integrato supportato da un'architettura consolidata e una strategia lineare che porta a sfruttare la competenza nelle applicazioni analitiche per Governance, Risk Management e Compliance

SECURITY

La sicurezza intelligente di Ibm

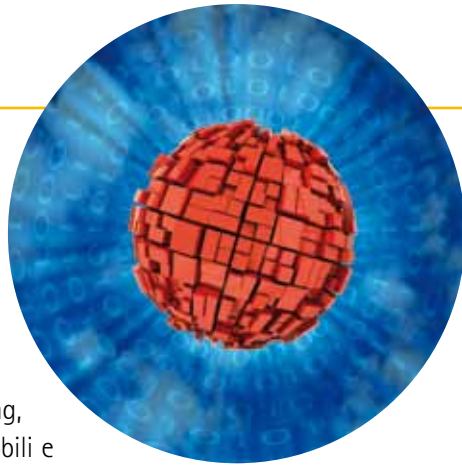
Non c'è sicurezza senza capacità di gestione e controllo. Fedele a questa impostazione, Ibm da circa dieci anni ha impostato una strategia di crescita in questo settore attraverso ricerca e sviluppo e acquisizioni, proponendo, con la propria business unit Ibm Security Systems, un approccio integrato, che parte dalla governance, la gestione del rischio e la compliance.

Fondandosi sulla visione dello "Smarter Planet", in cui tutto e tutti sono interconnessi e dove crescono ogni giorno i mezzi tecnologici a disposizione, Ibm ha sviluppato una strategia per un "pianeta più sicuro". Per questo la società statunitense ha sviluppato tecnologie che proteggono non solo l'IT aziendale, ma che contribuiscono a realizzare infrastrutture, informatiche e non, sicure e "resilienti", considerando quindi anche la continuità dei processi e delle operazioni di business. Una visione che è evoluta con il concetto di security intelligence, che sfrutta le competenze maturate da Ibm nell'ambito degli Analytics, ma che, soprattutto, significa utilizzare strumenti integrati su un framework comune e sfruttare un insieme di dati unificati per affrontare i problemi sull'intero spettro della sicurezza. In pratica, secondo quanto spiegato da Ibm, la security intelligence è la capacità di incorporare diverse tecnologie di sicurezza e di rete in un sistema integrato, anziché in prodotti che operano in maniera indipendente. Il vantaggio è l'efficienza operativa: un migliore uso delle risorse umane, del tempo e dell'infrastruttura. Infatti, secondo la visione Ibm, sempre più la responsabilità della sicurezza viene affidata

ai team di gestione della rete e a questo consolidamento di responsabilità a livello operativo deve corrispondere un consolidamento a livello di intelligence. Questo significa pensare in termini di supporto di più compiti in un'unica piattaforma e di sviluppo interfunzionale di competenze in tutta l'organizzazione per poi implementare l'accesso sulla base dei ruoli. La security intelligence inoltre apporta valore ad altre aree dell'IT, quali la localizzazione di problemi del sistema, problemi di rete, supporto utente e analisi dell'autorizzazione. In funzione di questo Ibm continua ad ampliare il proprio Security Framework, che su quattro direttrici (persone, dati, applicazioni, infrastruttura) integra un portafoglio completo di servizi, soluzioni, architetture e prodotti specifici e integrati. Il framework per la sicurezza recepisce quanto previsto da standard internazionali, esperienze progettuali di Ibm e best practice di settore, fornendo una visione di business e identificando le aree coinvolte nei processi di Security Governance, Risk Management e Compliance. Attraverso i professional service, i managed service e le proprie soluzioni hardware e software, trasversali alle suddette aree, Ibm, a detta dei suoi responsabili, copre tutte le esigenze di sicurezza di business.

Collaterale all'aspetto della sicurezza vi è quello della business continuity, che Ibm, da tempo, declina come "business resiliency". Più precisamente, nell'ambito della divisione Business Continuity and Resiliency Services, Ibm propone una metodologia di Enterprise Risk Management, che, partendo dal business (e coinvolgendone tutte le linee) arriva ai problemi tecnologici, proponendo la realizzazione di un'infrastruttura "resiliente", cioè capace di adattarsi rapidamente alle situazioni sia di rischio sia di opportunità e di garantire la continuità delle operazioni, coerentemente con le esigenze delle linee di business. ■

Il vendor propone un framework unificato adatto a rispondere alle nuove esigenze di protezione degli ambienti mobili, virtualizzati e cloud



La protezione data centrica di Trend Micro

Trend Micro promuove la visione di un nuovo modello di sicurezza "più intelligente" (o Smarter) ispirato da un cambiamento nello scenario tecnologico segnato dalla consumerizzazione, dall'adozione del cloud computing, dalla diffusione dei dispositivi mobili e dalla proliferazione degli attacchi mirati.

Soprattutto la crescita nell'uso dei dispositivi mobili personali e le implementazioni cloud, che rendono i dati accessibili sempre e ovunque, portano a rivedere la sicurezza tradizionale basata sull'assunzione di un perimetro di rete aziendale definito e delimitato al cui interno risiedono i dati critici, in favore di un nuovo modello che sposta l'attenzione sui dati e prevede una protezione che li segue nei loro spostamenti attraverso ambienti fisici, virtuali e in-the-cloud.

Il modello di sicurezza proposto da Trend Micro prevede un framework unificato per la gestione e protezione di dati, infrastrutture, dispositivi mobili e applicazioni e integra:

- una protezione «smarter» dalle minacce e dagli attacchi mirati, che porta la tecnologia globale e cloud-based di Trend Micro per la rilevazione delle minacce e la correlazione delle informazioni di sicurezza all'interno dell'ambiente locale dell'utente;
- una protezione «smarter» dei dati attraverso l'intera organizzazione per garantirne la riservatezza e la protezione in ambienti fisici, virtuali e in-the-cloud.

Alla base di un approccio verso la sicurezza come servizio Trend Micro pone la Smart Protection Network, un'infrastruttura di protezione dei contenuti progettata per tutelare gli utenti dalle minacce a fronte di un impatto ridotto su reti e sistemi. Abbinando tecnologie "in-the-cloud" a client leggeri, diventa possibile accedere alle più recenti

misure di protezione ovunque e in qualsiasi modo ci si connetta: da casa, dalla rete aziendale o anche in viaggio.

Per rispondere alle sfide della Data Protection Trend Micro ha predisposto un ampio portafoglio di prodotti che punta a garantire la totale sicurezza dei dati ovunque questi risiedano. Le soluzioni software di Trend Micro sono in grado anche di rispondere alle nuove esigenze di sicurezza che caratterizzano il progressivo percorso verso la virtualizzazione, con soluzioni quali Trend Micro Deep Security 8 sviluppata in stretta collaborazione con VMware e dotata di funzioni antimalware agentless oppure come Trend Micro OfficeScan per la sicurezza degli endpoint negli ambienti virtualizzati. Con Trend Micro SecureCloud il vendor fornisce sicurezza "dal cloud" con l'infrastruttura Trend Micro Smart Protection Network e sicurezza "per il cloud" con server e tecnologie crittografiche. A supporto delle esigenze di protezione alimentate dalla consumerizzazione IT Trend Micro mette a disposizione Trend Micro Mobile Security, una soluzione di sicurezza rivolta alle aziende enterprise e di media dimensione per la protezione di un'ampia gamma di dispositivi mobili quali: iPhone, iPad, sistemi in ambiente Android e BlackBerry OS e Apple. Il vendor affianca le proprie soluzioni software con una gamma di servizi SaaS (Software as a Service), mediante i quali le aziende, invece di acquistare software e installarlo, possono usufruire della flessibilità di affittarlo su base mensile o annuale. ■

ESTRATTO:

Servizi e tecnologie per l'ICT Security nelle aziende italiane

Stato attuale e scenari di diffusione futura

Metodologia

Il Survey si basa sulle indicazioni fornite da un numero significativo di aziende italiane, sia di fascia media sia alta, a cui sono state poste una serie di domande volte a determinare il livello di conoscenza e di adozione delle tecnologie di protezione, degli strumenti di gestione della sicurezza e dei servizi che, nell'insieme, concorrono a definire lo scenario dell'ICT Security in Italia.

È stato realizzato sia attraverso una serie di interviste dirette sia con la compilazione di approfonditi questionari seguendo un approccio di tipo qualitativo. Le risposte ottenute hanno messo a disposizione degli analisti di Reportec il substrato in base al quale delineare uno scenario di adozione ed evoluzione, integrato poi da considerazioni derivate dall'analisi preventiva e approfondita delle tecnologie in oggetto.

Il risultato è il presente Survey, che completa in modo critico il cerchio analista-utente-vendor. Pur inevitabilmente soggettivi, i risultati sono esposti in modo del tutto indipendente a tenere in considerazione aspetti che esulano dalla semplice interpretazione dei dati effettuata all'interno di analisi di tipo quantitativo.

Le domande sono state predisposte al fine di ottenere indicazioni relative al livello di diffusione dei servizi e delle tecnologie per la protezione aziendale. Un ulteriore obiettivo, non meno importante, è stato quello di individuare le priorità che hanno guidato gli investimenti passati e che guideranno quelli futuri da parte delle aziende. Una volta definito lo "stato di fatto" che caratterizza le aziende italiane, si è esaminato quali sono i progetti e le previsioni di adozione su un arco temporale di 18 mesi (fino alla metà del 2013), abbracciando un'ampia casistica tra chi ha deciso di trovare una soluzione a un'esigenza e situazioni in cui il processo di valutazione è stato già superato, per approdare a quello di pianificazione dell'implementazione dei nuovi strumenti tecnologici e dei servizi. Si è inoltre posto in evidenza il livello di utilizzo e le aspettative associate a specifiche tecnologie, al fine di verificare l'effettiva evoluzione e la corrispondenza con il trend previsto.

Il campione

Il campione degli intervistati è formato dai direttori e responsabili dei sistemi informativi/CIO/CTO. Si tratta di figure aziendali con compiti analoghi e decisionali la cui differenziazione è spesso legata principalmente alla dimensione aziendale. Per la realizzazione del Survey sono stati intervistati 69 responsabili, di cui il 50% con un numero di dipendenti fino a 100 addetti, il 14,7 % costituito da aziende con un numero di addetti compreso tra 101 e 500 e il restante 35,3% da aziende con un

Il Survey nella sua versione completa (acquistabile da Reportec) include anche le previsioni di adozione delle tecnologie e dei servizi di ICT Security fino alla prima metà del 2013. Per informazioni inviare un'e-mail all'indirizzo: info@reportec.it

numero di dipendenti maggiore di 500 (di cui la maggior parte ha oltre 1000 dipendenti). I settori di attività che caratterizzano le aziende prese in considerazione sono stati raggruppati in cinque segmenti:

- Industria
- Finanziario
- Pubblica Amministrazione
- Servizi
- Commercio e Distribuzione

Priorità degli investimenti in sicurezza

Per fornire una valutazione del modo con cui si è orientata nel 2011 e si indirizzerà nei prossimi 18 mesi la spesa in sicurezza ICT è stato chiesto ai partecipanti del Survey di indicare una graduatoria nelle priorità di investimento, in relazione a tre temi:

- la compliance (rispettare gli obblighi imposti dalla legge),
- la protezione (garantire la business continuity e la confidenzialità e integrità dei dati),
- abilitare nuovi servizi (per migliorare processi e aprire nuove opportunità di business).

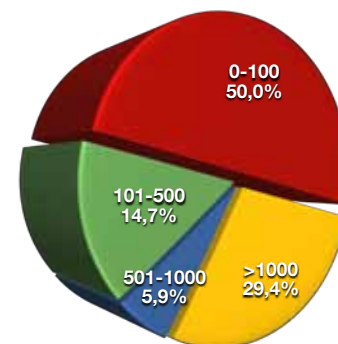
È emerso che nel 2011 il principale driver per gli investimenti di sicurezza è stato quello della protezione dei dati seguito dal tema, anch'esso molto forte, del conseguimento della conformità alle normative. Circa il 60% delle aziende ha dichiarato, invece, che durante lo scorso anno non sono stati intrapresi investimenti (o perlomeno questi non hanno avuto una valenza centrale) in sicurezza indirizzati verso l'abilitazione di nuovi servizi - per esempio indirizzati al controllo degli accessi, alla gestione della riservatezza o dell'identità - in un'ottica indirizzata a individuare all'interno delle tecnologie di protezione nuove opportunità per ridurre i costi, migliorare la qualità del servizio e, in definitiva, conquistare nuove leve di vantaggio competitivo.

Le indicazioni per il futuro mantengono centrale tra le priorità il tema della protezione dei dati, mentre sembra affievolirsi quello della compliance per lasciare spazio proprio all'adozione di nuovi servizi.

Si tratta di un trend che può essere compreso se si considerano le nuove evoluzioni dell'ICT all'insegna dei modelli orientati al cloud computing e all'IT as a Service che, oltretutto, risultano centrali all'interno di un campione costituito per quasi la metà da aziende che operano proprio nell'ambito dei servizi.

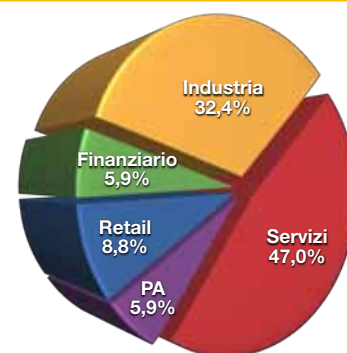
Numero di dipendenti

Distribuzione percentuale per numero di addetti delle aziende coinvolte nel Survey



Settore di appartenenza

Distribuzione percentuale per settore di appartenenza delle aziende coinvolte nel Survey



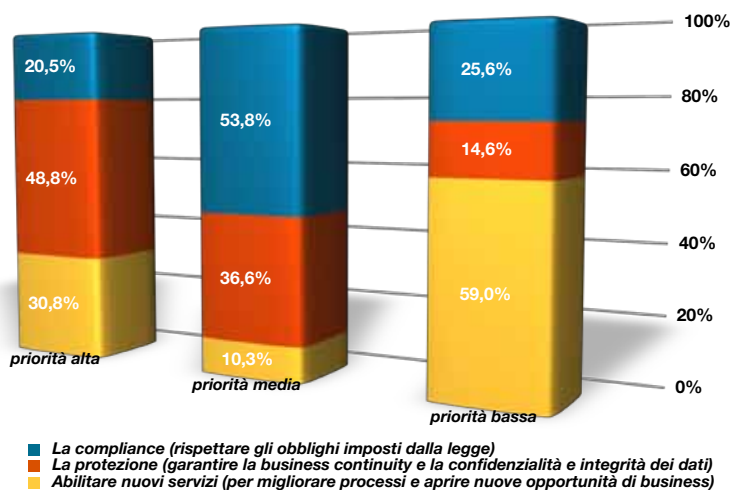
Il livello di adozione delle tecnologie di protezione

Il Survey ha analizzato anche il livello di penetrazione delle differenti tecnologie di protezione e le previsioni di adozione fino al 2013 (queste ultime sono presenti nella versione integrale del Survey).

Osservando la situazione "congelata" al 2011 appare al 100% la penetrazione delle tecnologie "classiche" di antivirus, firewall e antispyware.

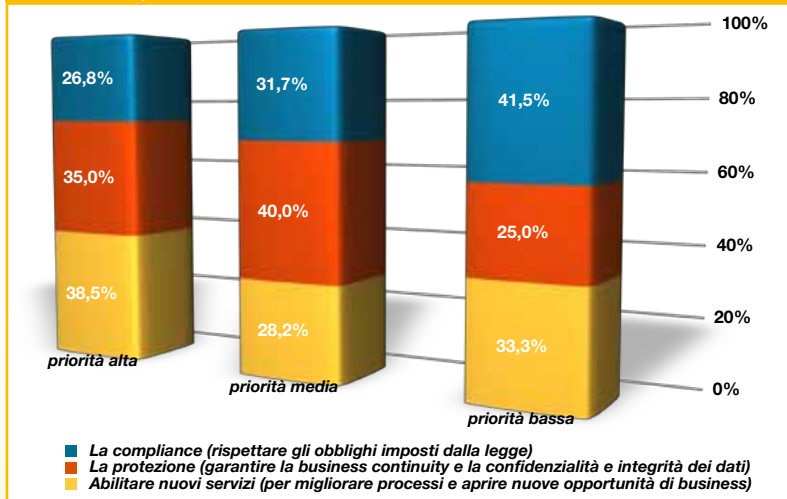
Poco sotto il 60% si ferma invece l'adozione di soluzioni di Intrusion Prevention/Protection, che pure

Priorità che hanno guidato gli investimenti in sicurezza nel 2011



dovrebbero caratterizzare ogni tipologia di business, in modo trasversale per settore e dimensione aziendale. Questa tipologia di tecnologie risultano presenti all'interno delle aziende più grandi mentre sembrano quasi assenti tra le aziende più piccole, nonostante ormai esistano soluzioni a bassissimo costo, spesso addirittura integrate all'interno delle versioni più complete di quelli che potremmo chiamare per semplicità i "pacchetti "antivirus". Questo dato lascia intuire come il mancato utilizzo sia da ricondurre più alla mancanza di consapevolezza che di riduzione dell'investimento ovvero alla mancanza di competenze interne capaci di comprendere e gestire rischi di questa natura.

Priorità che guideranno gli investimenti in sicurezza fino alla prima metà del 2013

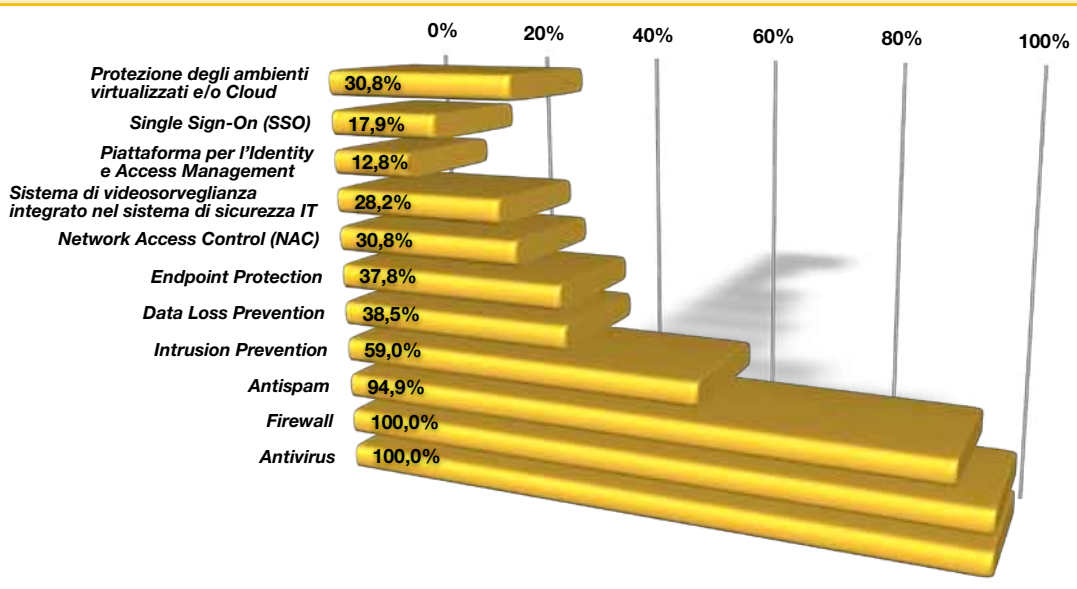


Meno del 40% del campione intervistato dichiara di adottare una soluzione specifica per prevenire la perdita dei dati. A questo dato sconcertante si aggiunge quello del basso livello di adozione di soluzioni di protezione degli endpoint. Un tema, quest'ultimo, su cui sarà necessario intervenire in modo importante e rapidamente, in vista dei processi di consumerizzazione e della crescente diffusione dei dispositivi mobili.

Un dato interessante riguarda quello relativo alla protezione degli ambienti virtualizzati e cloud, per i quali poco meno di un'azienda su tre dichiara di avere già adottato alcune soluzioni di protezione. Si tratta di un dato che in realtà nasconde un livello di ritardo maggiore rispetto al puro numero percentuale e che va ricondotto a una certa mancanza di precisione nella definizione della questione e nella terminologia associata al cloud. In diversi casi, a fronte di una richiesta di dettagliare in modo più preciso la tipologia di soluzioni è emerso che la protezione a cui si faceva riferimento era legata a soluzioni per il ripristino di server virtuali nella loro configurazione operativa e non invece dedicate alla salvaguardia delle informazioni da perdite o da diffusione non autorizzata all'interno di ambienti virtualizzati e in-the-cloud.

Un dato interessante riguarda quello relativo alla protezione degli ambienti virtualizzati e cloud, per i quali poco meno di un'azienda su tre dichiara di avere già adottato alcune soluzioni di protezione. Si tratta di un dato che in realtà nasconde un livello di ritardo maggiore rispetto al puro numero percentuale e che va ricondotto a una certa mancanza di precisione nella definizione della questione e nella terminologia associata al cloud. In diversi casi, a fronte di una richiesta di dettagliare in modo più preciso la tipologia di soluzioni è emerso che la protezione a cui si faceva riferimento era legata a soluzioni per il ripristino di server virtuali nella loro configurazione operativa e non invece dedicate alla salvaguardia delle informazioni da perdite o da diffusione non autorizzata all'interno di ambienti virtualizzati e in-the-cloud.

Livello di adozione attuale di tecnologie di protezione





Gaetano Di Blasio

Tremate: arrivano i Millennials

Negli Stati Uniti si dibatte sull'impatto che i Millennials stanno avendo sul mondo del lavoro. Millennials è il termine in voga per quella che era già stata chiamata Generazione Y e che, in sintesi, identifica i giovani tra i 18 e i 30 anni. Purtroppo in Italia, questi ultimi hanno qualche difficoltà in più ad affacciarsi sul mondo del lavoro rispetto ai loro coetanei d'Oltreoceano. A volte, però, giocano un ruolo indiretto, "mostrando" ai loro genitori i vantaggi dell'innovazione tecnologica in ambito consumer, rispetto ai sistemi aziendali ormai piuttosto "ingessati". In buona sostanza, dispositivi come gli smartphone e i tablet e, soprattutto, tutti i servizi a essi connessi, tipicamente residenti su cloud, permettono un agile utilizzo della tecnologia e un notevole incremento della produttività.

Il risultato è che si è abituati a trovare online tutti i contatti e gli strumenti che servono per organizzare la propria vita sociale. È normale ritenere di poter fare lo stesso sul mondo del lavoro.

Avviene, per esempio, nelle microimprese, dove l'imprenditore agisce senza dover passare attraverso gerarchie aziendali per "improvvisare" processi di business più snelli. Lo dimostra un'indagine condotta per conto di Epson da Coleman & Parkes, attraverso 1250 interviste ad altrettante micro imprese (250 per ciascuna dei 5 paesi coinvolti: Italia, Francia, Spagna, Germania e Inghilterra).

In particolare, emerge il forte uso del Web: l'89% delle piccole imprese italiane intervistate riferisce di comprare attraverso Internet e ben il 94% utilizza questo strumento per vendere i prodotti/servizi, ma solo il 35% effettua business tramite e-commerce, anche se è prevista una crescita del 44% nei prossimi due anni. Sul fronte della dotazione tecnologica sono proprio gli strumenti wireless d'ultima generazione a prevalere: nel 48% delle microimprese italiane sono impiegati il tablet (contro una media del 43% negli altri paesi) e lo smartphone (51% vs 28%). A parte l'invidia dettata da ragioni anagrafiche, dai Millen-

nials c'è in realtà apparentemente poco da temere, visto i benefici in termini di produttività che possono derivare dalla trasposizione delle abitudini consumer in ambito lavorativo. Se non fosse per due problemi: governance e sicurezza. Innanzitutto, la creatività sui processi è senz'altro un'opportunità da cogliere, ma deve essere occasione per una revisione dell'organizzazione e dei processi stessi, altrimenti si rischia il caos negli ordini, nella produzione, nell'amministrazione e via dicendo. Nuovi modelli flessibili sono possibili, ma vanno comunque codificati. Una piena libertà del "fai da te" procura inevitabilmente una situazione ingovernabile, che può forse funzionare solo nella piccola impresa non strutturata.

Il problema maggiore è però rappresentato dalla sicurezza dei dati: l'amministratore delegato che vuole utilizzare il tablet e che non comprende il rischio di far finire i dati di bilancio in mano alla concorrenza. I dispositivi mobili sono generalmente poco sicuri, qualcuno più qualcuno meno, ma è il comportamento degli individui a costituire il pericolo maggiore: ormai gli attacchi sono mirati e utilizzano tecniche miste, partendo, in molti casi, dal social engineering. Il giovane millennial potrà anche essere consapevole di non dover divulgare informazioni aziendali, ma è in grado di capire che pubblicare su facebook tutta la sua vita privata, come è abituato a fare, rappresenta un rischio per l'impresa stessa? Proprio attraverso queste informazioni, infatti, gli hacker riescono a costruire attacchi phishing per rubare identità elettroniche e con esse penetrare nelle reti aziendali.

La consumerization e il BYOD sono fenomeni incontrollabili: è impossibile opporvisi. È possibile che ci sarà un'ondata di ritorno, ma nel frattempo si dovrà correre ai ripari, sia attraverso l'adozione di sistemi di protezione (a cominciare dalla crittografia estesa a tutti i dati aziendali), sia promuovendo la formazione alla sicurezza all'interno delle proprie organizzazioni. ■

L'adozione di tecnologie di analisi fluidodinamica permette a Fujitsu di ottimizzare i costi energetici di un data center, con consistenti risparmi nel budget IT

DATA CENTER

I servizi di Fujitsu ottimizzano il data center

Ottimizzare il data center è il desiderio di molti CIO, soprattutto da quando il costo dell'energia rientra nei budget dell'IT e non più nelle spese generali. Ridurre i consumi energetici è così un modo immediato per recuperare budget da dedicare a nuovi progetti. Per capire cosa può essere fatto in proposito e dove e come è possibile intervenire abbiamo chiesto il parere di Denis Nalon, Portfolio & Business Programs manager di Fujitsu.



Denis Nalon, Portfolio & Business Programs manager di Fujitsu

Direction: Cosa si può fare di concreto e con ritorni rapidi, per ottimizzare un data center?

Denis Nalon: Innanzitutto puntare sugli elementi salienti senza disperdersi. Ad esempio, noi stiamo portando avanti un programma che si chiama "Reshaping the Data Center" che prende atto delle maggiori esigenze espresse dai CIO e cioè: come ridurre i costi, come incrementare la qualità dei servizi e come rendere più dinamico e reattivo l'IT. Per rispondere a queste esigenze interveniamo soprattutto nell'ambito del data center, che rappresenta il punto di partenza più logico. In questa fase evolutiva si tratta di infrastrutture interessate da trend quali la virtualizzazione o il consolidamento, ma che per come sono stati costruiti non sempre riescono a rispondere alle attuali esigenze di dinamicità e di ottimizzazione. Con questo programma interveniamo su

diversi piani di ottimizzazione, analizziamo i diversi elementi che compongono un data center, il loro profilo energetico, il loro consumo puntuale o su intervalli di tempo, le problematiche di condizionamento in relazione alla posizione fisica che un dispositivo occupa in un rack o in relazione agli altri rack e ai dispositivi a cui è interconnesso. Alla fine proponiamo una soluzione di ottimizzazione che permette di ridurre i consumi e aumentare l'efficienza complessiva. In pratica creare un data center più green.

D: È solo un problema di consumi o anche di altro?

DN: Quella del data center è una realtà in cui l'evoluzione tecnologica in atto origina molti aspetti critici. Di fatto ogni suo rack ha un consumo energetico e l'energia è una delle sfide principali nel data center perché con l'aumento della densità di lame e processori richiede sempre più energia per metro quadro di superficie e spesso capita che non ne arrivi a sufficienza per alimentarli. In pratica, si creano effetti secondari critici dal punto di vista impiantistico, con data center mezzi vuoti, corridoi caldi disottimizzati, con il consumo di un rack che aumenta in modo sensibile, a volte del tutto insostenibile. E nei prossimi anni, con un hardware che sarà in grado di erogare sempre più capacità di calcolo o di storage, aumenterà costantemente la densità e il relativo consumo. È quindi indispensabile intervenire in modo proattivo su alimentazione

e condizionamento, oltre che sulla capacità di elaborare le applicazioni business, come ad esempio SAP.

D: Che interventi proponete con il programma di Reshaping per ottenere un data center più green?

DN: Sostanzialmente interveniamo su 4 fronti a livello di: singolo dispositivo, rack, sala e servizi. In particolare, la componente "servizi" è molto importante e in proposito abbiamo attivato servizi di Facility Readiness Assessment che utilizzano del software per l'analisi e la rilevazione della fluidodinamica di un DC che ci permette di capire quale è la sua configurazione partendo dalla situazione e dai vincoli impiantistici e di installato esistenti. Ad esempio rilevare se si è in presenza di rack parzialmente occupati, o con utilizzo elevato oppure scarsamente sfruttati. Va poi considerato che non sempre c'è accordo tra i costruttori nel definire le modalità ingegneristiche del raffreddamento, sul come posizionare il corridoio caldo e su come fluisce l'aria, e questo ovviamente si ripercuote negativamente sull'efficienza energetica globale, oltre che causare un possibile surriscaldamento degli apparati. I nostri servizi e lo studio ambientale in base ai principi di fluido dinamica ci permettono di intervenire in modo preciso e identificare le misure che possono essere adottate per incrementare l'efficienza dei flussi di raffreddamento e di alimentazione, ad esempio riallocando diversamente i diversi dispositivi o intervenendo sulle modalità del loro utilizzo da parte delle applicazioni, distribuendo meglio il carico di lavoro, i consumi energetici e le esigenze di raffreddamento. E alla fine, in linea con le richieste europee, forniamo anche servizi di certificazione su diversi livelli sull'efficienza energetica raggiunta, dalla semplice certificazione a quella Premium.

D: Tornando al tema della densità, è un problema davvero così rilevante?

DN: Sì. È un fenomeno che ha un impatto consistente sul data center. Il problema deriva dal fatto che i diversi produttori lavorano molto bene sul loro dispositivo, magari garantendo il funzionamento anche a temperature di qualche grado più elevato, cosa che di per sé è molto interessante perché permette di risparmiare sul raffreddamento, ma non sempre

questo va d'accordo con l'efficienza del data center nel suo complesso, perché quando il dispositivo viene inserito nel rack nella maggior parte delle volte non si viene a trovare nelle condizioni ideali pensate dal costruttore o dal facility manager. Servono quindi servizi che risolvano i problemi che ne possono derivare ed è quello che facciamo. Analizziamo la situazione, la modelliamo, facciamo delle simulazioni su cosa vuol dire aumentare la capacità dei server, dello storage, o consolidarla, oppure quale può essere l'impatto di nuove applicazioni sui consumi energetici. E possiamo anche analizzare quanto consuma il singolo dispositivo o applicazione o rack e decidere se non convenga spostare una macchina da un rack all'altro per aumentare l'efficienza termica.

D: Come è possibile ottimizzare dal punto di vista energetico un dispositivo?

DN: Innanzitutto senza spingere oltremisura certi parametri di funzionamento che possono portare al risultato opposto al voluto. Ad esempio è inutile cercare di portare all'eccesso la velocità dei dischi se poi li si utilizza in modo disottimizzato o fermandoli del tutto quando non sono utilizzati. Va considerato che più alta è la velocità di rotazione maggiore è il consumo, ma che se si fermano e si fanno ripartire di frequente per ridurlo si ha una forte usura delle parti meccaniche e a una significativa diminuzione dell'MTBF. Nei nostri sistemi Storage Eternus abbiamo così adottato dischi con tecnologie che permettono di rallentare la velocità senza però fermarli del tutto, in modo che sia ridotto al minimo contemporaneamente sia lo stress meccanico che il consumo. Inoltre, sui nostri Server le ventole sono 20-30% più grandi dell'usuale, cosa che ci permette di raffreddare con maggiore efficacia consumando anche in questo minor potenza. Un altro tipo di intervento è di tipo architettonico, per esempio la modalità costruttiva del nostro CX 1000 e del più recente CX 400, una famiglia di dispositivi per cui il raffreddamento avviene con l'estrazione dell'aria calda dall'alto e che ha i cavi di connessione posti frontalmente. Il risultato è di forte impatto in un data center, perché permette di eliminare un corridoio caldo e quindi, oltre che ottimizzare il raffreddamento, anche di dimezzare gli spazi necessari.

G.S.

Grazie a tecnologie avanzate, integrate sui propri sistemi o disponibili in modalità standalone, il vendor delinea un percorso strutturato per affrontare in modo efficace la gestione di volumi di dati in costante crescita

STORAGE

*Giovanni Calvio,
manager of
storage platform
di Ibm Italia*

Lo storage IBM diventa più efficiente

Il 2011 si è chiuso all'insegna della crescita per lo storage su disco di IBM. Dati rilasciati recentemente da IDC Italia confermano per il vendor il primato nel 2011 sul mercato degli external disk storage (in termini di revenue), nel settore dei dischi high end e, per la prima volta, anche il primo posto nel quarto trimestre 2011 nel mercato midrange disk.

«La crescita nel volume dei dati ha un forte impatto sulle applicazioni di business - ha spiegato Giovanni Calvio, manager of storage platform di IBM Italia - che portano a dover ridurre le finestre di backup, ad accelerare il ripristino dei dati e rendono difficile garantire tempi di risposta accettabili. Tutto ciò crea un gap tra il livello di servizio offerto e quello richiesto dal business. IBM si propone di cambiare la curva dei costi grazie a un approccio di tipo olistico e promuovendo investimenti mirati all'efficienza e alla sostenibilità nel tempo. In questo contesto si inseriscono le nostre soluzioni di business optimization».

L'efficientamento proposto da IBM interviene sulla riduzione di capacità fisica richiesta, sul migliore utilizzo delle risorse e sulla riduzione degli oneri gestionali. In particolare, le soluzioni e tecnologie con cui IBM supporta il conseguimento di questi obiettivi intervengono su quattro fronti. Il primo è di fornire funzioni che ottimizzano in modo automatico le prestazioni dell'ambiente collocando i dati al posto giusto attraverso una gestione dinamica e distribuita dello storage multilivello. A corredo di questa esigenza IBM ha introdotto nei propri sistemi storage la tecno-

logia Easy Tier, che provvede in modo automatico, sulla base della frequenza di accesso, a spostare i blocchi di dati attraverso i diversi livelli storage disponibili: SSD, dischi ad alte prestazioni, dischi ad alta capacità o tape. Complementare alla precedente vi è l'esigenza di gestire le informazioni in base a specifiche policy aziendali, a cui IBM indirizza la tecnologia IBM Active Cloud Engine che permette di sovrintendere la gestione dei dati sia a livello locale sia a livello globale in modalità cloud.

Un secondo fronte di intervento riguarda la possibilità di trattare solo i dati che servono, utilizzando tecnologie che ne riducono il volume. A supporto di queste esigenze IBM fornisce soluzioni di thin provisioning, di deduplica e una tecnologia di compressione/decompressione in tempo reale dello storage primario, capace di intervenire solo sugli specifici blocchi di memoria richiesti. Il terzo fronte di intervento indirizza la questione di mettere a disposizione dei dati un maggiore spazio grazie all'utilizzo di meccanismi di virtualizzazione sempre più sofisticati. SAN Volume Controller è la soluzione di riferimento di IBM per realizzare una virtualizzazione indipendente dalla tipologia di sistemi storage utilizzati. Il quarto e ultimo livello riguarda una gestione autonoma e sempre più automatizzata dell'infrastruttura storage sfruttando le caratteristiche di Virtual Storage Center, l'interfaccia comune ai sistemi storage IBM.

R.F.

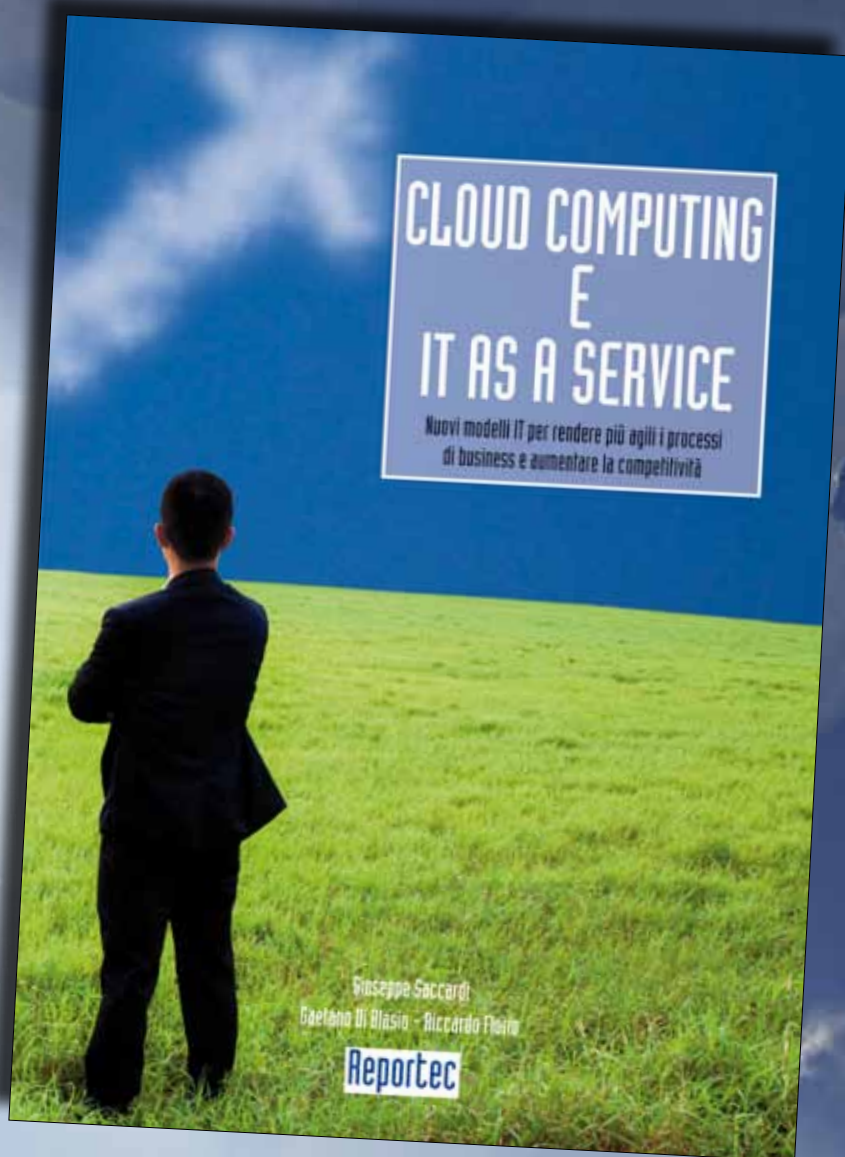


È disponibile il libro sul **CLOUD COMPUTING**

Realizzato da Reportec, in oltre 350 pagine analizza i prodromi del Cloud Computing, le modalità di fruizione e i benefici che derivano dall'adozione di questa innovativa possibilità di utilizzo del più avanzato IT senza dover immobilizzare ingenti capitali.

Completa il volume l'analisi delle soluzioni sviluppate per il Cloud Computing da parte di un ampio numero di primarie aziende del settore attive nel campo delle infrastrutture, delle applicazioni e dei servizi.

Il volume è uno strumento unico in Italia per affrontare le tematiche del Cloud Computing e approfondire gli aspetti, bilanciando i concetti e la teoria con quanto di concreto attualmente esistente. Conoscere è infatti la condizione sine qua non perché un manager possa decidere. Questo obiettivo è perseguito mediante un esame analitico degli aspetti più importanti, gli economics e le modalità di realizzazione e di adozione di un'infrastruttura Cloud Computing.



È anche disponibile il libro
UN'IMPRESA SEMPRE PIÙ MOBILE

Il libro è acquistabile al prezzo di 50 euro (più IVA) richiedendolo a
info@reportec.it - tel 02 36580441 - fax 02 36580444

Lo sviluppo delle tecnologie di comunicazione e dei sistemi informativi aziendali consente di dematerializzare il posto di lavoro con benefici sia per l'azienda sia per il dipendente

MOBILITY

I vantaggi del virtual workplace

Lavorare da casa, senza doversi recare ogni giorno sul posto di lavoro e bilanciando impegni di vita privata con i meeting aziendali è un sogno per molte persone. Se i lavoratori oggi chiedono maggiore flessibilità ai propri datori di lavoro su orari e presenza in ufficio non significa che vogliono lavorare di meno. Semplicemente sono consapevoli che le tecnologie a loro disposizione consentono una maggiore mobilità e flessibilità nelle attività quotidiane. Questa consapevolezza non deve spaventare i manager aziendali perché, in realtà, secondo le stime di istituti di ricerca del settore, il lavoro svolto fuori ufficio rappresenta un vantaggio sia per chi lavora sia per l'azienda. Difatti lavorare lontano dalla propria scrivania, da remoto, in quello che viene definito il "virtual workplace", porterebbe alle aziende una serie di benefici, poiché incrementerebbe la produttività, minimizzando i costi e aumentando i profitti, e in più farebbe bene anche all'ambiente.

Il compito di fornire le tecnologie abilitanti per un'ambiente di lavoro virtuale va all'IT che, però, da solo non è sufficiente perché per portare benefici al business la dematerializzazione del lavoro deve necessariamente cambiare anche la struttura, i processi e la natura stessa delle organizzazioni.

Benefici del virtuali workplace

Il virtual workplace non può essere localizzato all'interno di uno spazio definito, come l'edificio

un'azienda, ma nemmeno in qualsiasi altro spazio fisico. Si può dire piuttosto che esistono diversi luoghi collegati tra loro attraverso le persone che, da remoto, fanno parte di un team di lavoro. In questo modo le aziende possono diminuire gli uffici, mantenendoli soltanto per i dipendenti che li necessitano, e avere dei notevoli risparmi sui costi di mantenimento della struttura fisica. In più evitando di spostarsi ogni giorno da casa all'ufficio, il virtual worker contribuisce anche a diminuire l'emissione di diossido di carbonio che danneggia l'ambiente.

Secondo dati diffusi da istituti di ricerca, risulta anche che nella maggior parte dei casi il lavoratore virtuale sia più produttivo rispetto a quello che si trova in ufficio.

La condivisione come risorsa aziendale

Il mondo in cui viviamo è sempre più in movimento, interconnesso e interattivo grazie agli sviluppi della tecnologia che ha cambiato le abitudini di vita e di lavoro delle persone. Le aziende hanno capito il potenziale degli strumenti di unified communication e collaboration per rendere immediate e veloci le comunicazioni a vantaggio della produttività, oltre che per risparmiare sui costi di viaggi e trasferte per meeting fuori sede o all'estero. La necessità di creare team di persone che collaborano, sia all'interno dello stesso edificio sia da sedi lontane, ha portato all'inte-

grazie nei sistemi di comunicazione aziendali di strumenti quali l'Instant messaging, la presence, la videocomunicazione, ma anche di blog, wiki e social network. Grazie a queste tecnologie si può concretizzare la condivisione di informazioni all'interno delle aziende, che è diventata una risorsa fondamentale per il business.

Dall'Intranet al virtual workplace

La condivisione di informazioni in ambito aziendale è iniziata con la nascita delle Intranet che non hanno inizialmente goduto di molta attenzione da parte delle risorse umane e dei top manager. Solo successivamente, con l'evoluzione dei sistemi informativi verso l'interoperabilità e l'integrazione, l'emergere degli standard XML, dei Web Services e delle SOA c'è stato un cambiamento che ha portato verso la convergenza di mondi prima separati, quali ad esempio le Intranet, ERP e sistemi CRM, in una maggiore ottica di comunicazione e condivisione di informazioni all'interno dell'intera organizzazione.

Oggi, il grado di convergenza raggiunto dai sistemi informativi offre l'ambiente e il supporto ideale per realizzare il virtual workplace, anche se le tecnologie da sole non sono sufficienti perché i cambiamenti che si devono affrontare per ottenere dei benefici dalla dematerializzazione del posto di lavoro sono soprattutto a livello di organizzazione dei processi e di cultura aziendale.



Cosa serve a un virtual worker

Un'azienda che vuole iniziare un processo di dematerializzazione del lavoro deve essere in grado di mettere al centro delle priorità la persona stessa e i suoi bisogni. Questo perché il lavoratore deve avere a disposizione gli strumenti necessari per portare

avanti le sue attività e allo stesso tempo deve poter comunicare e interagire con altri membri del team di lavoro. A un virtual worker devono essere garantiti una serie di servizi che lo agevolino nelle sue attività, non solo di comunicazione, ma anche di socializzazione, come la partecipazione alle community aziendali, e di accesso alla conoscenza condivisa del patrimonio informativo dell'organizzazione. Un virtual worker deve avere la possibilità di collaborare e confrontarsi con altri colleghi e chiedere, se necessario, la consulenza o il parere di esperti.

In pratica è fondamentale creare un'ambiente di lavoro aperto e collaborativo, che sappia compensare la mancanza di interazione fisica (che comprende anche i segnali non verbali) e di sinergia che si crea nella

comunicazione faccia a faccia. Per questo i sistemi informativi devono essere ripensati nell'ottica di fornire supporto alla nuova struttura organizzativa nata dall'esigenza di abilitare un nuovo modo di lavorare, ma soprattutto creando le condizioni adatte a favorire l'operatività e l'interazione tra le persone che vi lavorano.

P. S.

Il crescente utilizzo di dispositivi mobili in azienda può creare difficoltà a chi deve gestire la migrazione di applicazioni da rete fissa a mobile. Il cloud può risolvere diversi problemi

NETWORKING

Una sinergia che migliora le applicazioni in rete



Qual è il futuro delle reti? E delle applicazioni? In che problemi possono incorrere CIO e manager quando in azienda si utilizzano applicazioni mobile in relazione ad ambienti cloud privati o pubblici? Sono domande che iniziano a porsi sempre più di frequente i responsabili aziendali alle prese con un'evoluzione dell'ICT che non accenna a rallentare e che con la continua immissione sul mercato di dispositivi mobili di vario tipo, dallo smartphone al netbook, all'iPAD o al tablet crea non pochi problemi a chi deve decidere come procedere con gli investimenti e a quali elementi porre attenzione.

Gli aspetti che si devono tenere presente quando si affronta il problema di una rete trasmissiva (sia di proprietà che acquisita sotto forma di servizio) e di come sia possibile utilizzare in modo proficuo dei dispositivi mobili per migliorare i propri processi di business, o far migrare le applicazioni disponibili agli utenti di rete fissa anche agli utenti mobile, sono di diversa natura ma sostanzialmente in buona parte riconducibili a problemi tecnologici.

Quello che ne deriva però, e in seguito vengono esplorati questi aspetti, è che quando li si considera nel loro complesso si delinea uno scenario in cui a trarne beneficio è il cloud, che appare in grado, se non di risolvere, perlomeno di mitigare molti dei problemi di rete che si incontrano quando un'applicazione fruita sino ad oggi sul proprio pc a livello di desktop viene fatta migrare anche sul dispositivo portatile.

La crescente tendenza all'utilizzo di applicazioni office in mobilità su un'ampia varietà di dispositivi va di pari passo con la diffusione di apparati tecnologicamente molto evoluti e dotati di schermi ad alta risoluzione e ampi che permettono di fruirne per innovative soluzioni di collaborazione o di immersive application. Ma tale evoluzione deve andare necessariamente di pari passo con le prestazioni e la disponibilità di reti in modo da garantire una accettabile user experience.

Qui però si incontrano dei problemi, perchè quando un'applicazione fruita inizialmente su rete fissa viene fatta migrare e resa disponibile in una rete mobile si sconta, a prescindere dal costo che pur ha la sua importanza, la forte differenza in termini di banda disponibile e di modalità stessa con cui una rete mobile è realizzata, e tale differenza si incrementa se si opera in un contesto internazionale dove intervengono anche i problemi connessi al roaming.

Quello che ci si chiede è se il cloud possa e come permettere di compensare perlomeno in parte tali differenze che, se si considerano i ritardi di trasmissione, il round trip, la latenza sulle diverse tratte di rete, eccetera, finisce con l'essere di certo significativa. Ad esempio, la latenza, uno dei parametri di riferimento più noti dalla letteratura tecnica, invece di pochi millisecondi o la decina di millisecondi può arrivare anche all'ordine dei 200 millisecondi, quanto basta per far sì che alcune applicazioni risultino ben lontane dall'assicurare un'adeguata user experience.

Gli elementi in gioco

Per capire se la risposta possa essere positiva si può analizzare quali sono gli elementi che influiscono sul comportamento di un'applicazione e sui tempi di risposta, e quindi sulla user experience. Sostanzialmente i fattori che entrano in gioco, iniziando dal dispositivo di utente (e cosa valida in generale sia per le reti fisse

che il processore), il fatto che i processori siano meno potenti di quelli di desktop, la limitata memoria interna disponibile e una limitata banda disponibile. La differenza è di numerosi fattori e, nel caso della banda, può arrivare anche ad un intero ordine di grandezza. Di certo un fattore dieci per la velocità di linea ha un profondo impatto sulla resa di un'applicazione.



che mobili), sono quattro: il tempo di elaborazione sul dispositivo di utente, il tempo di trasporto in rete dipendente dalla sua velocità e articolazione geografica, la latenza media della rete, il tempo di elaborazione presso il data center. In questo, poi, la rete impatta sia all'andata che al ritorno e cioè per quello che viene riferito in inglese come il "round trip".

Tempo richiesto per il trasporto dei dati e latenza sono i due elementi che maggiormente impattano sulla user experience di un utente mobile, soprattutto per applicazioni quali quelle di videocomunicazione o di tipo "immersive". Reti ad elevata latenza potrebbero portare a una riproduzione distorta del segnale video, un elemento sempre più presente nelle applicazioni UCC e quindi risultare del tutto inaccettabile per servizi di questo tipo.

In sostanza, poiché i problemi derivanti da una rete mobile sono noti, ma difficilmente affrontabili, i fattori su cui si può intervenire sono altri e cioè il disegnare un'applicazione direttamente per ambienti mobili, o adattarla opportunamente, in modo che tenga conto dei limiti esistenti. Non sempre questo è però possibile ed è qui che entra in gioco un ambiente private o pubblico cloud e il ruolo che può assumere nel mitigare le criticità di una rete o di un dispositivo mobile che presenta costruttivamente numerose differenze e limitazioni rispetto ad un dispositivo desk top.

Tra le differenze più evidenti e che impattano sull'efficienza ci sono aspetti come la ridotta energia disponibile con le batterie esistenti (che devono alimentare display ampi e le diverse interfacce di rete mobile, oltre

Spostare funzioni elaborative e di storage sul cloud

Il cloud può contribuire a risolvere diversi problemi di applicazioni e reti mobili. Ad esempio, un'applicazione può essere distribuita territorialmente ed erogata dal cloud mediante data center che sono prossimi all'utilizzatore mobile. Ciò apporta benefici sia in termini di capacità elaborativa risparmiata sul dispositivo sia per quanto concerne la latenza della rete, che è tanto più ridotta quanto più il tragitto percorso dai dati è breve.

Inoltre, diventa possibile disporre di memoria in quantità pressoché illimitata, eliminando uno dei maggiori limiti di un dispositivo mobile e riducendo ulteriormente le necessità energetiche. Ciò ovviamente richiede che un'applicazione sia adeguatamente bilanciata tra il dispositivo e i data center su cui risiede nel cloud, che ci sia un adeguato livello di sicurezza e che si disponga di funzionalità di monitoring dinamico che permettano di garantire in ogni istante e luogo il medesimo livello di servizio.

Un ruolo nell'ottimizzazione delle prestazioni e dei consumi lo può avere anche il tipo di rete. Applicazioni che possono riconoscere automaticamente le reti mobili disponibili verso il cloud e commutare automaticamente su quella più veloce o a minor consumo in base alle priorità applicative possono trarre beneficio dal fatto che ad esempio una connessione Wi-Fi richiede a livello di interfaccia meno energia, anche un terzo in meno, che non di quella necessaria per alimentare un'interfaccia GPRS.

G.S.

Video Wall e tavoli touch screen abilitano un'esperienza multimediale e interattiva che trasporta il visitatore in un mondo di storia, design e cultura

COMMUNICATION

Samsung racconta l'eccellenza di Campari



Un requisito fondamentale per la predisposizione del progetto era che fosse totalmente in linea con

l'immagine che Campari voleva trasmettere verso l'esterno: quella di un'azienda dinamica, attenta all'oggi ma proiettata verso il futuro. Inoltre, doveva essere un luogo di immagini ed emozioni in cui i contenuti multimediali fossero visualizzati con un livello di qualità allo stato dell'arte.

«Oggi viviamo in una società dell'immagine in cui l'elemento visivo è importantissimo - ha spiegato Paolo Cavallo, direttore della Galleria Campari -. Campari dispone di contenuti di immagine significativi che desiderava trasmettere in modo moderno e di qualità, affiancandoli a un'esperienza interattiva che consentisse al visitatore di sentirsi parte attiva della visita. Abbiamo identificato in Samsung il partner ideale per tradurre tecnicamente il progetto del Video Wall e del percorso interattivo per l'elevato livello qualitativo fornito dalle sue tecnologie di visualizzazione. Alla fine Samsung non è stato un semplice fornitore, ma si è rivelato un partner a valore che ci ha supportato in tutte le nostre esigenze».

Nel corso dei suoi oltre 150 anni di storia, Campari si è evoluta in un Gruppo che rappresenta una delle realtà più importanti nel settore del beverage a livello mondiale, presente in 190 Paesi con leadership nei mercati italiano e brasiliano e posizioni di primo piano negli USA, in Germania e in Svizzera e un fatturato netto consolidato nel 2010 di oltre 1.1 miliardi di Euro.

In occasione del 150° anno dalla sua fondazione, Campari ha avviato un progetto innovativo e multimediale per raccontare la propria storia, realizzando la permanente Galleria Campari ospitata presso la storica sede di Sesto San Giovanni, in provincia di Milano. Ad accompagnarla in questa avventura, fatta di innovazione e multimedialità, Campari ha chiamato Samsung che ha messo a disposizione le proprie competenze e tecnologie di visualizzazione.

Un progetto che unisce storia, arte e tecnologia

Galleria Campari è un luogo dinamico, multimediale e interattivo che racconta il percorso del marchio attraverso le espressioni artistiche che hanno caratterizzato i suoi 150 anni di storia.

Artisti di ogni genere si sono, infatti, cimentati nella rappresentazione dell'essenza del marchio realizzando un raro connubio tra cultura artistica e comunicazione industriale: da Fortunato Depero, personaggio principale del Futurismo, a Bruno Munari, geniale anticipatore della video arte; da Federico Fellini che firma nel 1984 il primo spot per Campari a Ugo Nespolo che, nel 1990, orchestra la pubblicità Campari per i Mondiali di Calcio '90. Gli spazi di Galleria Campari sono stati suddivisi in tre grandi aree tematiche: comunicazione, arte e produzione, ciascuna caratterizzate da un luogo distinto. Ad accogliere il visitatore vi è una parete Video Wall che proietta una selezione del ricco archivio delle campagne pubblicitarie Campari, affiancata da un'originale macchina del tempo realizzata con un monitor Samsung Lcd da 50", con cui è possibile accedere alle fondamentali tappe storiche del marchio. Un lungo ed elegante tavolo interattivo, realizzato anche questo con tecnologia Samsung, permette al visitatore di sfogliare la storia del marchio. Vi è poi una parete di 32 metri dove è proiettata una selezione dei contenuti delle tappe fondamentali della storia Campari e un percorso illuminato che accompagna il visitatore attraverso un'esperienza sensoriale fatta di suoni, immagini e profumi. «Il progetto Campari ha confermato l'eccellenza di Samsung nell'ambito delle tecnologie visuali – ha commentato Mario Levratto, Direttore Marketing della Divisione IT di Samsung Italia – mettendo in evidenza la capacità di progettazione ed esecuzione dei nostri professionisti e partner nell'ambito di progetti complessi che richiedono di coniugare elevata competenza con la capacità di adattarsi alle esigenze del cliente».

Soluzioni per un'esperienza visuale allo stato dell'arte

Per la realizzazione del Video Wall sono stati utilizzati 15 display Samsung Lcd da 40" che permettono di visualizzare ottimamente immagini di grandi dimensioni pur mantenendo una propria identità quando vengono utilizzati per mostrare contenuti indipendenti.

Questi display sono dotati di avanzate soluzioni tecnologiche che assicurano una qualità ottimale da ogni angolo di visuale, sia verticale sia orizzontale. Grazie al sistema DNle (Digital Natural Image enhancer) le immagini risultano più luminose e nitide, mentre gli ottimizzatori di movimento e di colore e gli intensificatori di

contrasto e dettaglio garantiscono la riproduzione dei filmati con una qualità visiva senza precedenti. Il tempo di risposta più rapido disponibile in commercio – solo 8 ms – permette ai monitor Samsung di offrire un'esperienza visiva piacevole e rilassante. Inoltre, grazie a una gamma di meccanismi di protezione (Screen Scroll, Pixel Type, Bar Type, Erase Type) i display Samsung non presentano alcun problema di persistenza delle immagini. Il tavolo interattivo utilizza 12 monitor Samsung Lcd da 32" e permette di consultare documenti, foto, libri digitalizzati, sfogliandoli in modo semplice e immediato grazie alla tecnologia sviluppata appositamente da Samsung che ha reso touchscreen il lungo pannello di vetro che sovrasta i display. «Samsung ha saputo rispondere alle nostre esigenze anche per i tavoli che noi chiamiamo "dell'approfondimento" – ha precisato Paolo Cavallo – consentendoci di predisporre una lunga lastra touchscreen interattiva non interrotta dalle cornici degli schermi. Anche la dimensione dei monitor è stata individuata insieme a Samsung per consentire un'ottimale visibilità da parte del visitatore in piedi».

«Il nostro livello di soddisfazione sul progetto e, nello specifico, per le realizzazioni che hanno coinvolto Samsung, è molto elevato – ha precisato Paolo Cavallo -. I risultati in termini di affluenza e gradimento della Galleria sono molto gratificanti. Negli ultimi nove mesi abbiamo avuto 7mila visitatori provenienti da ogni parte del mondo, che hanno espresso un forte apprezzamento per il modo in cui Campari è riuscita a raccontare la propria storia. Il successo ottenuto ci ha portato a decidere di ampliare la Galleria aggiungendo un nuovo piano per il quale abbiamo previsto di proseguire la partnership con Samsung». Questa nuova fase di sviluppo prevede un orientamento ancora più spinto all'interazione con il visitatore e sarà maggiormente indirizzata ad approfondire il legame che lega Campari al mondo del bere e al rapporto con il design, prevedendo anche monitor interattivi che trasmetteranno interviste con designer che hanno lavorato con il Gruppo.

«La Galleria Campari rappresenta anche un'opportunità per il nostro management – ha commentato Paolo Cavallo – che ha la possibilità di predisporre visite con partner commerciali e di comunicare l'azienda in un modo differente. Il connubio con le tecnologie digitali di Samsung rappresenta il complemento ideale tra due realtà proiettate verso il futuro all'insegna delle direttrici di qualità e design».

POP Channel rende la comunicazione nei punti vendita dinamica e misurabile

Una soluzione espositiva indirizzata alla GDO e al retail che coniuga il digital signage con tecnologie per misurare il ritorno della comunicazione

Si chiama POP Channel ed è una soluzione di nuova concezione, risultato di un progetto interamente italiano sviluppato da Majrani Group, azienda nata nel 1996 che si occupa di comunicazione per il punto vendita.

Si tratta di una soluzione espositiva adatta ad articoli di vario genere, che combina il ruolo di un espositore tradizionale con una comunicazione video trasmessa da un monitor integrato i cui contenuti cambiano in modo dinamico in base alle caratteristiche dell'osservatore; tutto ciò grazie a un software in grado di riconoscere alcuni tratti distintivi dell'osservatore partendo dall'immagine catturata da una videocamera.

Il sistema è dotato anche di un sensore che registra la presa del prodotto e che chiude il cerchio della misura dell'effetto del sistema di comunicazione sulla vendita effettiva.

«POP Channel viene posizionato come un espositore, ma è, in realtà, un media di nuovo tipo che si propone di introdurre un nuovo modello di vendita – ha commentato Riccardo Majrani, fondatore di Majrani Group -. È un progetto nato in Italia con ambizioni internazionali e che sarà presto esportato anche in Spagna, Svizzera e Brasile. Siamo partiti con un formato euro-pallett che comprende un modulo espositivo coerente con i modelli standardizzati della GDO. Il sistema è in grado di distinguere sesso, età e quattro diverse espressioni del consumatore che gli transita di fronte e di modificare, di conseguenza, la comunicazione video. Il dato viene acquisito in forma integrata e resta anonimo per non infrangere la privacy.



La soluzione POP Channel

Sull'espositore è riportato un avviso che precisa che il sistema non scatta fotografie né registra filmati». Il modello con cui viene proposto attualmente POP Channel è quello del noleggio con un bilancio di costi che i portavoce del progetto sostengono comparabili con quelli degli espositori statici. Attualmente non è previsto un meccanismo interattivo, sebbene tecnologicamente non presenti difficoltà di implementazione, poiché analisi di mercato indicano una scarsa propensione degli shopper all'interazione.

R.F.

Il backup Symantec fa un passo in avanti

Rilasciate le nuove versioni di Backup Exec e NetBackup, migliorate nell'interfaccia, nelle prestazioni e nel supporto della virtualizzazione

Arrivano sul mercato Backup Exec 2012 e NetBackup 7.5, le nuove versioni delle diffuse soluzioni Symantec per la protezione e il ripristino dei dati.

I miglioramenti apportati si inseriscono all'interno dei tre punti chiave che definiscono la proposizione di Symantec per affrontare con successo il tema del backup: controllo della crescita dei dati, unificazione delle piattaforme, semplificazione.

NetBackup 7.5 è in grado di interfacciarsi con i diversi sistemi operativi e con le piattaforme basate su open standard. I miglioramenti ap-

portati consentono di ridurre i tempi necessari per effettuare la copia dei dati, di ottimizzare l'uso della tecnologia snapshot all'interno dei processi di backup e di contrastare il backup illimitato e incontrollato delle informazioni inutili tramite un'indicizzazione e catalogazione dei dati in base al loro valore.

Backup Exec 2012 è la nuova versione della soluzione per la protezione in ambienti Windows. Integra la tecnologia di deduplicazione, prevede il supporto per la protezione di ambienti VMware e Microsoft Hyper-V ed è disponibile in versione con agente (per un backup più granulare) oppure agentless (per incrementare le prestazioni). Le principali novità ruotano attorno a tre aspetti.

Il primo è una semplificazione della configurazione e dell'interfaccia utente che è stata completamente ridisegnata. Il

secondo è il conseguimento dell'unificazione tra ambiente fisico e virtuale grazie all'introduzione della tecnologia V-Ray. Infine un recovery granulare per ogni tipologia di dato.

Backup Exec 2012 è disponibile come Small Business Edition per le esigenze di protezione onsite oppure in versione cloud. **R.F.**

Dimension Data con decisione nel cloud

Lazienda del Gruppo NTT ha reso disponibile a livello mondiale un'articolata gamma di servizi cloud

Dimension Data si propone con una nuova offerta di servizi per ambienti cloud pubblici e privati, molto articolata, che indirizza i molteplici requisiti richiesti a un'azienda nel suo passaggio verso il cloud e comprende:

- Cloud Enablement: servizi di consulenza per aiutare a comprendere la propria predisposizione cloud.
- Cloud e System Integration: servizi di integrazione attraverso sistemi IT tradizionali interni e cloud privati, pubblici e ibridi.
- Compute-as-a-Service (CaaS): server e storage virtuali offerti come un servizio in ambienti condivisi (pubblici) e dedicati (privati).
- Servizi Gestiti: una serie di servizi di supporto che includono la gestione delle patch, la configurazione dei dispositivi e il backup.
- Servizi Cloud Avanzati: servizi a valore aggiunto che includono backup e disaster recovery su cloud implementati sulla Managed Cloud Platform.
- Servizi Applicativi: applicazioni ospitate e operative sulla Managed Cloud Platform.

Nella strategia di servizi cloud di Dimension Data un ruolo primario lo ha la Managed Cloud Platform, una piattaforma di distribuzione cloud gestita e ospitata in un data center di Dimension Data o dei clienti. La piattaforma comprende un'infrastruttura cloud (server, storage, networking, virtualizzazione e software di sistema operativo) e Dimension Data CloudControl, un sistema per la gestione dell'ambiente cloud che fornisce il controllo e l'automazione delle funzioni di provisioning, amministrazione e fatturazione delle risorse cloud. Basato sul sistema di gestione cloud di OpSource, Dimension Data CloudControl è stato ulteriormente ampliato funzionalmente per un utilizzo all'interno di ambienti cloud pubblici e privati con un framework di gestione comune.

«Grazie alla disponibilità di un'unica piattaforma per distribuire tutti

Enrico Brunero, Line of Business manager Data Center, di Dimension Data



i Servizi Cloud di Dimension Data, i clienti sono in grado di migrare da modelli di cloud pubblici, privati e ibridi senza dover riprogettare e reintegrare l'infrastruttura di base, con un conseguente risparmio di tempo e costi» ha sottolineato Enrico Brunero, Line of Business Manager Data Center di Dimension Data. Peraltro, evidenzia sempre Brunero, i servizi Cloud offrono molteplici funzionalità, che includono: garanzie in termini di disponibilità, prestazioni e servizi.; un'interfaccia di amministrazione self-service basata su web e API; controllo della infrastruttura di rete per la configurazione di VLAN basate su cloud, firewall, load-balancing multicast e NAT. **G.S.**

Una nuova generazione di processori Intel

Più prestazioni e meno consumi per una famiglia di processori e chipset con tecnologia a 22 nm

Intel ha annunciato il rilascio della terza generazione della famiglia di processori Intel Core. Un annuncio che porta sul mercato un numero elevato di soluzioni.

Al mercato dei sistemi mobili sono indirizzati otto nuovi processori Intel Core i7 (i7-3820QM, i7-3720QM, i7-3612QM, 3610QM) e il processore Intel Core i7 Extreme Edition (i7-3920XM), quattro chipset (HM77, UM77, HM76, HM75) e cinque nuove opzioni wireless della gamma Intel Centrino (Advanced-N 6235, Wireless-N 2230, Wireless-N 2200, Wireless-N 135 e Wireless-N 105).

Al segmento desktop si indirizzano i processori i7-3770K e i7-3770, tre nuovi processori Intel Core i5 (i5-3570K, i5-3550, i5-3450) e sei nuove offerte di chipset (Z77, Z75, H77, Q77, Q75, B75).

Per i desktop a basso consumo arrivano le CPU siglate i7-3770T, i7-3770S, i5-3550S, i5-3450S.

I nuovi processori sono basati su tecnologia transistor 3D realizzata a 22nm, che consentono di ottenere una maggiore densità di elaborazione e nuove funzioni per la gestione del consumo energetico.

L'incremento delle prestazioni di CPU sfrutta le tecnologie Intel Turbo Boost Technology 2.0 e Intel Hyper-Threading Technology; la disponibilità di Cache condivisa con i processori per la grafica ottimizza il bilanciamento del carico. Miglioramenti anche nelle prestazioni di visualizzazione e nella connettività, con l'integrazione di USB 3.0 ad alta velocità, PCI di terza generazione e supporto per lo standard SATA 3.0 a 6 Gbps.

Migliorate anche le funzionalità indirizzate alla sicurezza con evoluzioni nelle tecnologie anti theft, identity protection e malware intrusion; inoltre è stato introdotto un nuovo generatore di numeri random basato su hardware based per rendere più performante il processo di cifratura. **R.F.**

Con i maker nasce la generazione del «fare»



Riccardo Florio

Li hanno chiamati maker e si stanno affacciando sul mondo dell'IT e non solo, fornendo interessanti spunti di interesse e riflessione. È la generazione che si vuole riappropriare del "fare", quella che ha un'idea e la realizza. Quello dei maker viene proposto come un fenomeno nuovo dai Media che, come sempre, puntano a ricondurre a un unico denominatore una serie di esperienze anche se nate indipendentemente le une dalle altre, in condizioni e modalità differenti. Trovato il movimento ecco allora che "scatta" l'esigenza di convocare raduni (il primo italiano si è svolto a febbraio), creare un'identità, stabilire definizione di cosa è maker e di cosa non è maker. Sta di fatto che ai maker si sta attribuendo una connotazione filosofica e di innovazione sociale, che si va a contrapporre come modello positivo all'immane nuova sigla (di cui il mondo anglosassone sembra proprio non poter fare a meno) dei NEET, acronimo di "Not in Education, Employment or Training" a indicare individui che non stanno ricevendo un'istruzione, non hanno un impiego o altre attività assimilabili (tirocini, lavori domestici e così via) e che non stanno cercando un'occupazione. In senso generale, l'idea dei maker è trasversale per settore di attività e riunisce fai da te, arte, moda, design, artigianato ma, soprattutto, ha una forte connotazione tecnologica e, in tal senso, offre un nuovo elemento di riscatto per i "nerd" tecnologici associandogli una connotazione che, per dirla all'americana, li rende "cool".

A prima vista tutto ciò non sembra molto diverso dal tradizionale concetto di imprenditoria ma l'IT, come già accaduto in passato, costituisce l'elemento differenziante. Già in passato il Web aveva offerto alle piccole aziende l'opportunità di presentarsi al mondo con un aspetto professionale, predisponendo uffici virtuali che si confrontavano sullo stesso piano di quelli delle grandi aziende. Lo sviluppo tecnologico mette ora a disposizione dell'imprenditoria nuove forme di artigia-

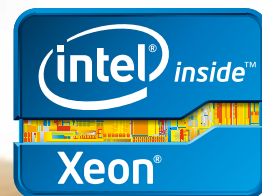
nato digitale che aprono orizzonti industriali potenzialmente rivoluzionari. Facciamo qualche esempio.

Tra le tecnologie che stanno alimentando il fenomeno maker vi sono le cosiddette stampanti 3D, dispositivi che permettono di realizzare la transizione dal digitale al fisico che finora mancava per chiudere il cerchio dell'imprenditorialità industriale. Si tratta di sistemi che, sulla base di progetti 3D creati al computer, permettono di realizzare fisicamente piccoli oggetti, utilizzando prevalentemente materiali plastici. L'elemento che abilita il carattere rivoluzionario è il costo di questi dispositivi, con soluzioni già disponibili a meno di mille Euro, che li ha proiettati nel mondo consumer. Per ora i tempi di realizzazione sono lunghi e le dimensioni degli oggetti ridotte ma le prevedibili rapide economie di scala lasciano prevedere che presto potrà essere disponibile a tutti l'equivalente di una macchina a controllo numerico, integrata, versatile e semplice per un uso domestico.

Le possibili ricadute di un approccio simile sono davvero rivoluzionarie.

C'è già chi prevede abitazioni dotate di sistemi per la creazione di oggetti che stravolgeranno i modelli di acquisto, almeno per una ampia classe di articoli. Se vorrò un vaso, un paio di scarpe da ginnastica o una sedia potrò scaricare da Internet un modello 3D da dare "in pasto" al sistema di creazione casalingo per vederlo realizzato all'interno delle mura domestiche con materiali e colori personalizzati. O ancora: avete rotto il contenitore del vostro smartphone? Potrete crearne uno nuovo semplicemente scaricando il modello 3D disponibile sul sito dell'azienda produttrice. Per chi conosce Star Trek, un telefilm che ha anticipato molte delle tecnologie che sono arrivate fino a noi - dalle porte che si aprono da sole al telefono cellulare - sembra che si giunta l'ora di dare il benvenuto a quello che sull'astronave Enterprise era chiamato il replicatore, in grado di produrre ogni tipo di oggetto semplicemente sulla base di un comando vocale.

Restiamo invece ancora in attesa del teletrasporto. ■



Make IT Dynamic

Come il tuo business.

Hai un'azienda di piccole o medie dimensioni che vuole sfruttare le sfide della globalizzazione migliorando l'efficienza? Sai che l'IT può fare la differenza, ma l'IT può sembrare molto complicata. Concentrati sul business, non preoccuparti dell'IT. Le offerte EASY solution di Fujitsu sono proprio quello che cerchi. Facili da acquistare, integrare e gestire: sono quindi l'ideale per aziende come la tua.

Fujitsu ti offre fino a 200€ di sconto, 3 anni di garanzia inclusi nel prezzo e fino al 31 Marzo 2012 monitor e tastiera /mouse wireless a solo 1€!¹

Il nuovo server PRIMERGY con processore Intel® Xeon® si ripaga grazie ai risparmi su consumi e manutenzione.



«Scopri i vantaggi
della supervalutazione
server sul tuo cellulare.»



PRIMERGY RX300 S6

INFO » it.fujitsu.com/makeitdynamic

NUMERO VERDE » 800 466 820

CAMBIA SERVER » cambiaserver.it

BLOG » <http://tech4green.it/>

Vieni a trovarci a SMAU Business:

ROMA 21, 22 marzo

PADOVA 18, 19 aprile

BOLOGNA 6, 7 giugno

1. Offerta valida solo per codici selezionati e consultabili su www.cambiaserver.it, lo sconto varia a seconda del modello, salvo esaurimento scorte. Fujitsu si riserva il diritto di sospendere la promozione in qualsiasi momento.

Intel, il Logo Intel, Xeon e Xeon Inside sono marchi registrati da Intel Corporation negli Stati Uniti e in altri Paesi.

shaping tomorrow with you



Virtualizza di più con WebSphere. O spendi di più con WebLogic.

Hai più di 400 ragioni, perfettamente logiche, di preferire IBM WebSphere® a Oracle WebLogic®:

1. Risparmi il 57% su licenze e supporto per il primo anno.
2. Puoi scegliere tra più opzioni di virtualizzazione (compresi VMware e Xen).
3. Paghi solo per i processori core che ti servono (cosa che non sempre succede con Oracle WebLogic).
- 4-404. Sei in buona compagnia (lo scorso anno oltre 400 clienti Oracle WebLogic hanno scelto IBM WebSphere).

ibm.com/fatti/it/websphere