

Vulnerabilità dello storage: un rischio da evitare

IL TEMA È DI QUELLI CALDI E LE AZIENDE SONO SEMPRE PIÙ ATTENTE ALLA SICUREZZA DELLE INFRASTRUTTURE IT AFFINCHÉ SI POSSA DEFINIRE IL PROFILO DI RISCHIO E LE CORRETTE MODALITÀ PER OTTIMIZZARE LE RISORSE INTERNE E GARANTIRE UNA EFFICACE STRATEGIA DEL RISCHIO INFORMatico. MA LA SITUAZIONE RISULTA ESSERE ANCORA PARECCHIO DISOMOGENEA TRA I SETTORI AZIENDALI.

Un recente studio di Harris Interactive, evidenzia che la maggioranza degli Americani adulti (57%) ritiene che il contenuto dei file archiviati sul loro computer valga più del PC stesso. Nonostante questo, i consumatori e le PMI continuano a non proteggere i propri dati. Forrester Research ha intervistato 600 decisori di PMI europee e altrettanti di grandi aziende per fare il punto sullo stato dell'IT Security. Il risultato emerso è che la sicurezza rimane una priorità alta nelle grandi aziende mentre le piccole imprese privilegiano l'aggiornamento dei PC e una migliore integrazione tra le applicazioni.

Una recente indagine condotta su un campione di 108 aziende

italiane da NetConsulting evidenzia che la motivazione primaria che giustifica l'investimento in sicurezza, per l'81% degli intervistati, è la compliance alle normative, mentre solo il 9% ha dichiarato di aver subito attacchi informatici.

Ma allora, qual'è lo scenario e la sensibilità mostrata dalle aziende italiane in rapporto al livello di vulnerabilità riscontrato?

Lo abbiamo chiesto ai principali fornitori di tecnologie storage e servizi di sicurezza, di seguito potete leggere come hanno risposto.

Giuseppe Russo, Chief Technologist, Principal Engineer & Security Ambassador di **Sun**, evidenzia che le aziende non dispongono ancora di un approccio sistemico e complessivo. In particolare sono ancora poche le aziende che affrontano metodologicamente il problema della classificazione delle informazioni. "La mancata adozione di politiche di classificazione dei dati" - prosegue Russo - congiuntamente alla scarsa adozione di sistemi operativi (o applicativi) capaci di implementare sistemi multilivello, non impedisce che informazioni aziendali classificate o riservate transitino tra le mani o sui computer di chi non ha diritto a leggerle".

Dello stesso parere è Paolo Votta - Product Marketing Manager StorageWorks Division di **HP** che sottolinea quanto le aziende abbiano affrontato principalmente le tematiche relative alla protezione del business, costruendo infrastrutture resilienti e provvedendo a soluzioni di backup. La sicurezza è stata applicata al perimetro o utilizzando i metodi di protezione degli accessi inclusi nei dispositivi (amministrazione a livelli, mascheratura dei volumi). "L'attenzione comunque inizia a spostarsi sui rischi di appropriazione indebita delle informazioni" - sottolinea Votta - "come nel caso più semplice del backup su nastro quando il media generato può essere sottratto o perso. Sono previsti infatti sistemi di encryption che consentono la rilettura solo al possessore delle chiavi di de-encryption, così come si possono aggiungere moduli software

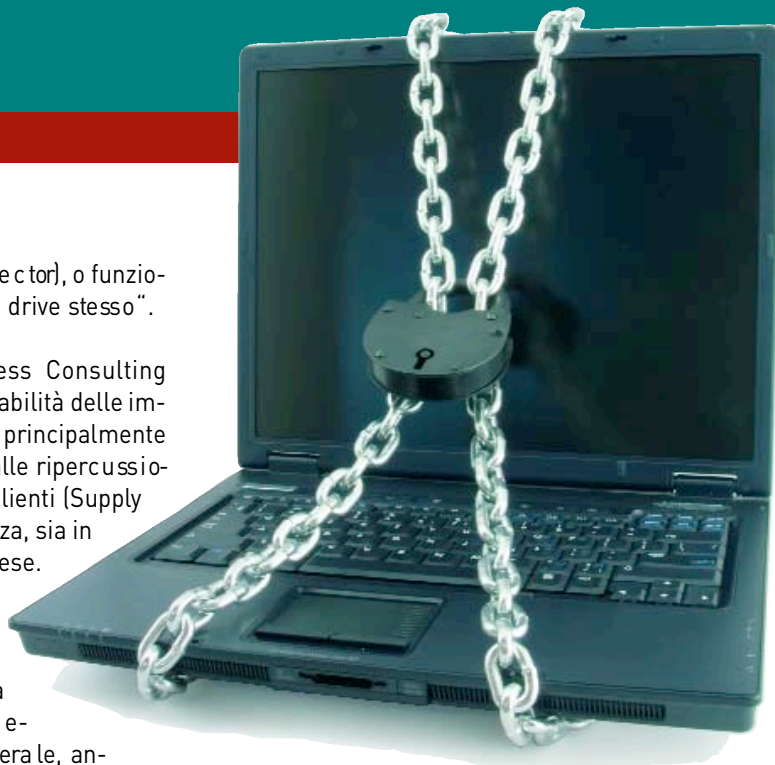


all'applicativi di backup (Data Protector), o funzionalità native di encryption nel tape drive stesso".

Per Giuseppe Fortunato, Business Consulting Principal di **HDS**, il livello di vulnerabilità delle imprese Italiane è ancora molto alto, principalmente a causa di una scarsa attenzione alle ripercussioni che le relazioni con fornitori e clienti (Supply Chain) possono avere sulla sicurezza, sia in ambito PMI che nelle grandi imprese. Da non sottovalutare anche la quasi totale mancanza, da parte dell'autorità, di controlli periodici sul rispetto delle normative e la consapevolezza che i sistemi di e-mail sono i più esposti ma, in generale, anche i meno protetti. Infine, nella P.A. esiste una normativa stringente che individua ruoli e responsabilità, ma mancano le risorse economiche per avviare le iniziative.

Per Roberto Mircoli, BDM Security & Wireless Networking di **Cisco** le minacce informatiche non tramontano mai, piuttosto si trasformano, si specializzano e a quelle conosciute se ne aggiungono di nuove. Tra le minacce più diffuse rimangono i worm e ciò che viene definito malware in senso lato: spyware, codici maligni in grado di auto-propagarsi e incorporare meccanismi di attacco multiplo. Proprio per questa connotazione polimorfica e metamorfica, il malware e le altre tecniche di infezione e di attacco continuano ad avere un'efficacia allarmante nell'eludere le protezioni circoscritte a singole tecnologie e prodotti orientati a mitigare specifiche vulnerabilità.

Lello Marra, Responsabile della BU Security di **Magirus** evidenzia che una soluzione completa di sicurezza dell'infrastruttura IT deve prevedere molteplici funzionalità, come ad esempio un sistema di firewalling in alta affidabilità, un sistema di intrusion protection, un sistema anti-spam e anti-spyware e, non ultimo, un sistema anti-virus. Recenti normative prevedono l'implementazione di questi sistemi, ma difficilmente ne definiscono le caratteristiche peculiari e tecnologiche affinché possano risultare realmente efficaci. Se a questo fattore aggiungiamo altre problematiche come i costi, sia di implementazione che di gestione, e la scarsa conoscenza delle tecnologie, ne risulta un ridotto livello di sicurezza dei dati, specialmente in quelle realtà dove non è assegnato alcun budget di spesa.



"Dell - ci racconta Ugo Moreero, Brand Manager Enterprise di **Dell** - ha analizzato un problema concreto di vulnerabilità che molte aziende si trovano ad affrontare: la gestione della posta elettronica". Un utente medio di posta elettronica elabora 10Mb di dati al giorno, secondo i dati IDC, e la mole di messaggi scambiati in posta elettronica crescerà del 25/30 per cento entro il 2009, secondo quanto dice Gartner, spamming escluso. La posta infatti si utilizza per comunicare tra colleghi, dipendenti, partner e clienti, quindi richiede una disponibilità 24x7.

Per Valerio Fabrizi, Security Practice Manager di **Unisys** le aziende Italiane oggi subiscono un numero di attacchi alla sicurezza di tipo malware e intrusioni in rete sempre crescente, in particolare dall'interno stesso dell'azienda. Negli ultimi tempi si è verificato, inoltre, un forte incremento di furti di identità digitale (quali ad esempio credenziali e fenomeni di phishing) dovuti in particolar modo alla scarsa sensibilizzazione sui temi della sicurezza che ancora sussiste da parte degli utenti italiani. Proprio tale mancanza di attenzione rappresenta ancora oggi l'anello debole per un sistema di sicurezza informatico.

Ma come si stanno muovendo le imprese italiane rispetto allo scenario europeo?

Mauro Cicognini, Responsabile Security Business Development di **I.NET** rileva che in Italia permane un'attenzione insufficiente da parte delle aziende alla sicurezza informatica, elemento derivante dai



security assessment gestiti. A fronte di questo livello medio di vulnerabilità abbastanza elevato, non si registrano grossi casi di eventi malevoli: evidentemente oggi le aziende italiane, per le loro dimensioni o caratteristiche, non sono ancora un bersaglio interessante.

Rispetto allo scenario europeo - molto variegato - il nostro Paese, come spesa destinata alla sicurezza dalle aziende, intesa in quantità ed efficacia, si colloca insieme alla Spagna ad un livello medio-basso. Al vertice c'è il Regno Unito, per cultura molto vicino agli Stati Uniti, seguono Francia e Germania, dove le aziende sono comunque ben organizzate.

Russo di **SUN** ribadisce che le aziende italiane stanno prima di tutto cercando di mettersi in regola con le normative: dalla legge sulla privacy (DL 196/2003) alle misure Minime di Sicurezza, dal decreto Pisanu (L155/2005) a Basilea 2 e a molte altre. Si aggiunga a questo la presa di coscienza di molte aziende di essere parte integrante delle cosiddette Infrastrutture Critiche Nazionali. In tal senso il Consiglio dell'Unione Europea ha emanato lo scorso dicembre una direttiva secondo la quale le aziende devono prendere coscienza di far parte di una rete europea e di conseguenza devono attrezzarsi per implementare corrette contro-

misure di sicurezza a fronte di una adeguata analisi del rischio.

Per Elio Molteni, Executive Security Advisor di **CA**, oltre ad una differenziazione rispetto allo scenario europeo, vale la pena comparare i vari settori merceologici all'interno del mercato italiano. In effetti, alcuni settori merceologici, come ad esempio le Banche e le Telco, sono molto più "attenti" alla sicurezza, rispetto ad altri. Un'attenzione confermata dalla percentuale relativa all'adozione di strumenti di Intrusion Detection che vede valori nettamente superiori in questi due settori. La nuova soluzione di CA denominata CA HIPS (Host Intrusion Prevention System) contribuisce a impedire l'ingresso nella rete di minacce note e ignote quali malware, spyware, adware e altro software dannoso.

Anche Sergio Resch, BDM System Storage di **IBM**, evidenzia grandi differenze tra i settori, identificando le aziende bancarie come le imprese che hanno investito e continuano ad investire in soluzioni avanzate di sicurezza e che rappresentano dei casi di eccellenza organizzativa e tecnologica. Altri settori invece, come la PMI devono ancora affrontare il tema in maniera strutturata e risultano essere estremamente arretrati rispetto agli altri



paesi europei. IBM è molto presente nel settore bancario ed è coinvolta in parecchi progetti sul tema della sicurezza e protezione del patrimonio informativo. Per sensibilizzare la PMI italiana negli ultimi anni sono state intraprese diverse attività di sensibilizzazione verso gli utenti finali, i Business Partner IBM e le associazioni di categoria.

Mircoli di **Cisco** rileva che le aziende che operano nei servizi finanziari, già da anni sono molto attente alle tematiche sulla sicurezza e hanno compreso che per fare fronte a tali minacce occorre difendere non solo il perimetro della propria rete, le LAN, la WAN, ma anche le applicazioni e i sistemi, gli accessi remoti, il Data Center. Occorre inoltre sottolineare che nessun singolo prodotto o sistema oggi disponibile può essere considerato sufficiente e adeguato ad indirizzare le esigenze di sicurezza delle organizzazioni, e che l'approccio più efficace è quello a livello di sistema. Cisco ha realizzato un portafoglio tecnologico completo per realizzare reti intrinsecamente sicure capaci di autodifendersi rispetto a minacce note o ancora sconosciute.

Per Fortunato di **HDS** si assiste ad una situazione di grave ritardo. Circa il 50% delle grandi imprese italiane non ha ancora un piano di sicurezza fisica completo per i propri dati aziendali. L'atteggiamento delle imprese verso le tematiche di sicurezza è ancora quello di chi affronta un problema di secondo ordine (a più bassa priorità rispetto alla generazione di nuovo business ed al contenimento dei costi produttivi) che richiede interventi difficili da giustificare in termini di costi.

Secondo Paolo Ardemagni, Regional Director Southern Europe di **Check Point** le aziende italiane sono in ritardo rispetto allo scenario europeo principalmente perché sono più restie a cedere i propri dati a terzi, e ad avvalersi così di servizi di sicurezza che permetterebbero loro di demandare ad altri la sicurezza della propria azienda. È un ritardo culturale prima che tecnologico: sul mercato internazionale, le realtà medie e grandi, in particolari britanniche e statunitensi, hanno immediatamente riconosciuto il ruolo strategico che i fornitori di servizi gestiti di sicurezza possono avere per il loro business. Fin quando le piccole e medie imprese italiane, classicamente lo specchio della nostra economia, non vinceranno questa remora, il ritardo rimarrà, ed anzi, tenderà ad aumentare.

Per Maurizio Desiderio, Regional Sales Director EMEA di **Imprivata**, ci sono alcuni settori che dimostrano di essere più sensibili nei confronti di questa problematica e sono quello sanitario e bancario. Anche il mercato delle assicurazioni sta mostrando un forte interesse data la necessità di ge-

stire identità e accessi delle numerose terze parti affiliate. Una soluzione di access management e single sign-on come OneSign di Imprivata rappresenta un ottimo mezzo per ridurre i problemi di vulnerabilità, semplificare la gestione delle password e controllare gli accessi. Si tratta di una soluzione che si installa in pochi giorni, assicura ritorni immediati senza richiedere investimenti ingenti e può rappresentare il primo passo verso un progetto più completo di identity management.

Microsoft propone una offerta tecnologica e di processo che ha l'obiettivo di stimolare le aziende ad assumere un approccio integrato ed esteso verso la Sicurezza IT. Gestire la sicurezza delle reti è diventato un compito molto complesso e, per fornire una risposta efficace alle necessità delle aziende, Microsoft propone la nuova linea di prodotti per la sicurezza: Microsoft Forefront. Questa famiglia raccoglie strumenti di protezione perimetrale, delle applicazioni di messaggistica e collaborazione e dei sistemi operativi fortemente integrati fra loro e con la piattaforma.

Secondo Stefano Torri, Director Southern Europe e Middle East di **Plasmon Data**, da anni il mercato offre soluzioni efficaci e a costi decisamente contenuti per eliminare la perdita accidentale dei dati o vere e proprie "incursioni" esterne. È il caso delle tecnologie Ottiche True WORM, del tutto impermeabili ad hacker e virus, ma anche all'errore umano. Il problema della vulnerabilità viene acuito per quelle tipologie di dati che vanno conservati per periodi particolarmente lunghi. Perché migrare dati che vanno conservati 10-15 anni ogni 3-4 anni, a causa del ciclo di obsolescenza della tecnologia SATA ad esempio? Meglio considerare tecnologie con un ciclo di vita più esteso come l'UDO (50 anni di ritenzione, 12-15 anni di ciclo di vita). Grazie ai suoi supporti removibili, è inoltre possibile avere a costi moderati un sistema di disaster recovery efficace, mantenendo una seconda copia offline in cassaforte o in un armadio ignifugo. ■

