LE RAGIONI DELLA SICUREZZA IT

L'atteggiamento un tempo più diffuso, quando in azienda si cominciava a parlare di sicurezza informatica, era quello che molte società del settore ancora oggi identificano come quello dello "struzzo". Una comprensibile ignoranza delle problematiche faceva ritenere che la probabilità di subire un attacco informatico fosse molto bassa e che, tipicamente, questi eventi accadessero a qualcun altro. Del resto, lo stesso atteggiamento, ancor oggi, si può osservare se si esaminano le procedure di sicurezza applicate in molte imprese, per esempio in materia di prevenzione degli incendio, in generale, degli incidenti sul lavoro.
Eppure la sicurezza è un concetto antico quanto quello stesso d'azienda. La protezione del patrimonio intellettuale, i brevetti, le barriere all'ingresso di una banca, i controlli all'uscita da una miniera di diamanti, le guardie giurate, sono tutti elementi volti a garantire la sicurezza aziendale. Si potrebbe andare ancora avanti a elencare altri provvedimenti per la sicurezza aziendale. La relativa giovinezza degli strumenti informatici e, soprattutto, la diffusione degli stessi, cresciuta nell'ultimo decennio con l'avvento di Internet, hanno posto una "questione culturale" sul fronte della protezione logica dei dati e delle informazioni: da un lato, si è avvertita e si avverte una scarsa percezione di quello che significa ICT security, dall'altro una mancanza di una reale percezione del rischio.
Oggi si parla dell'era dell'informazione, per mettere in risalto l'importanza crescente del patrimonio della conoscenza come reale valore di un'impresa. Un concetto sul quale si può facilmente essere tutti d'accordo, anche perché non è una novità. Lo spionaggio industriale non è stato inventato con l'avvento dei computer; eppure cos'è se non furto di informazioni e know-how? Sono cambiati però gli strumenti, mentre il paradigma dell'e-business, che vuole un'impresa affidare all'IT tutte le attività e tutti i processi di business, esalta il ruolo del sistema informativo, facendone il deposito di quelle informazioni e di quel know-how che, in precedenza, si poteva raggiungere solo violando archivi e casseforti.
L'estensione in rete dell'azienda, il successo di Internet, intranet ed extranet hanno favoritolo sviluppo di soluzioni e strumenti informatici, sia hardware sia software, che rispondono a esigenze di protezione differenti dal passato. Un mondo quindi completamente nuovo che coglie impreparate molte aziende: da un lato, c'è una scarsa percezione di quello che significa IT security, dall'altro manca una reale percezione del rischio.

Verso un'azienda aperta

Teoricamente, l'unico sistema completamente sicuro è quello totalmente isolato dal resto del mondo. Evidentemente, non può essere un sistema aziendale, che altrimenti risulterebbe asfittico. Certamente, se si pensa comunque al mondo informatico di qualche anno fa, ci si potrebbe chiedere quali sono le ragioni che portano ad aprire l'azienda verso l'esterno e, quindi, che obbligano all'introduzione di un più o meno accurato sistema di sicurezza.
Di fatto, volendo identificare con Internet la causa primaria di tutte le minacce alla sicurezza del sistema informativo aziendale, andare online può rappresentare un rischio elevato. Un rischio che non si può però fare a meno di correre: per restare al passo con i tempi, per sfruttare i vantaggi competitivi delle nuove tecnologie, per poter godere di particolari condizioni che una società può riservare ai partner commerciali comunicanti in intranet, per conseguire dei risparmi con le VPN (Virtual Private Network) su Internet, per migliorare la comunicazione aziendale, per fornire dei servizi ai propri clienti, per implementare un servizio di commercio elettronico e così via.
Non è obiettivo di questa tesi dimostrare quanto sia opportuno introdurre in azienda tecnologie di comunicazione e infrastrutture innovative, al solo scopo di giustificare il ricorso a un sistema di sicurezza. Resta il fatto che tutte queste spinte verso l'apertura dell'azienda all'esterno sono una tendenza incontrovertibile che presenta indubbi vantaggi per le imprese, anche a fronte di una maggiore esposizione al rischio di violazioni informatiche.
Si consideri l'esempio del commercio elettronico. Analisi di settore lasciano intravedere un crescente utilizzo di Internet come mezzo per compiere acquisti.

Quanto bisognerà aspettare prima che questo mercato diventi interessante è difficile da stabilire, ma che siano migliaia di miliardi di euro o cifre molto inferiori che si sposteranno sul commercio elettronico già nei prossimi anni, gli investimenti per la creazione di un sistema di e-commerce non cambiano molto.
Già oggi, peraltro, si può pensare di impostare la propria infrastruttura perché sia pronta a garantire in tempi rapidi quelle caratteristiche di resilienza, upgrade prestazionale, ridondanza e sicurezza che sono alla base di un sistema di servizi online.
Oltre a rappresentare una fetta di mercato interessante, gli utenti Web costituiscono un'opportunità per lo sviluppo di nuovi servizi e applicazioni. Senza contare altre forme di comunicazione emergenti, per le quali cresce l'esigenza di sviluppare servizi a valore aggiunto. Il riferimento è al mondo del wireless e della mobilità in generale, che pone altri e nuovi interrogativi nei riguardi della sicurezza, ma che rappresenta un percorso inevitabile per molte aziende moderne.

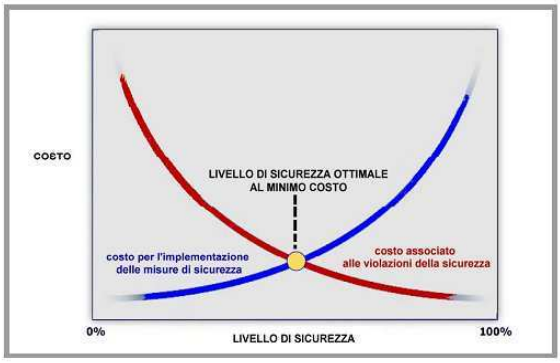
L'evoluzione delle infrastrutture

Realizzare un'infrastruttura che sia in grado di garantire servizi a valore aggiunto a clienti magari distribuiti sul globo o, meno ambiziosamente, mettere a disposizione della propria clientela un contact-center che soddisfi le esigenze di un dipartimento di customer care, non è comunque cosa da poco.
D'altronde, l'evoluzione stessa delle tecnologie sta portando verso l'implementazione di architetture di rete convergenti e all'emergere delle soluzioni di Virtual Private Network (VPN). Altre tendenze, quali la server e la storage consolidation, che portano al raggruppamento delle risorse in data center e alla riorganizzazione delle strutture aziendali, si sommano a quanto descritto, ponendo seri problemi intermini di management.
Aspetti che non devono agire come un freno, ma portare a un ripensamento complessivo della propria infrastruttura e ad adottare strategie architetturali e di piattaforma che tengano conto di fenomeni che sono in buona parte prevedibili e che, quindi, è opportuno far entrare nell'equazione progettuale.
È noto che le problematiche di gestione sono quelle che più di altre innalzano il cosiddetto total cost of ownership, ma risultano costi inevitabili quelli di gestione dell'informazione, elemento sempre più centrale e vero asset aziendale. Un'ottimizzazione in questo campo viene fornita anche dai sistemi di sicurezza. Un approccio globale al problema, infatti, prevede la realizzazione di policy molto precise e piuttosto rigide che consentono di aumentare il controllo su tutto il sistema e di aumentare l'efficienza oltre che la sicurezza delle informazioni.
Se qualche azienda ancora crede di poter fare a meno della sicurezza è perché ha evidentemente deciso di porsi fuori del mercato, chiudendo la propria impresa all'interazione e alla comunicazione diretta con partner e clienti. Ma anche se tale necessità non fosse sentita, una qualsiasi azienda con più di una sede si trova a dover affrontare il problema della comunicazione intra-aziendale. Fino a qualche anno fa, l'unica alternativa era quella di rivolgersi a un carrier (solo Telecom Italia fino al 1994) per affittare una linea dedicata.
Certamente una scelta sicura, ma anche costosa. Oggi, con Internet, esistono alternative molto più vantaggiose, ma che pongono un problema di sicurezza: ecco un primo esempio di trade off tra investimento in sicurezza e risparmio, con la possibilità di conseguire un vantaggio competitivo.
Soprattutto con le VPN (Reti Private Virtuali), l'evoluzione delle reti ha sostanzialmente modificato il rapporto tra rete trasmissiva e sicurezza. Inoltre, essa ha contribuito a esaltare i concetti di qualità del servizio, che di per sé è già un elemento di sicurezza, e a modificare l'architettura delle reti con l'affermazione di dispositivi specializzati, o appliance, volti ad accelerare le prestazioni all'interno della rete, e di apparati di comunicazione, i gateway, tesi a racchiudere la rete in una sorta di capsula che ingloba all'interno tutte le complessità architetturali e tecnologiche e semplifica l'interazione con l'esterno.

Dall'analisi di esigenze e risorse ai requisiti di protezione

Il "rischio" è il punto di partenza di ogni considerazione sulla sicurezza o, almeno, dovrebbe esserlo, anche perché è un concetto assolutamente radicato in un'impresa. I top manager, infatti, sono abituati a gestire il rischio, a misurarlo e a sfruttarlo a proprio favore.
Sotto questo punto di vista, la sicurezza informatica si può "banalmente" considerare

uno strumento di gestione del rischio. Peraltro, la complessità delle tecnologie rende il manager spesso incapace di comprendere quali siano le reali minacce e, quindi, di valutare correttamente quali asset aziendali siano in pericolo, nonché quanto sia grande tale pericolo.
Questo, però, non deve rimanere l'unico approccio alla sicurezza, altrimenti potrebbe limitare le scelte e le considerazioni all'ambito del threat management, cioè a proteggere l'azienda dalle minacce, esterne o interne, ma non consentirebbe di sfruttare alcuni elementi abilitanti della sicurezza. Le soluzioni di CRM (Customer Relationship Management) o di SCM (Supply
Chain Management), per esempio, sono un chiaro esempio di come si possano introdurre in azienda nuove tecnologie per estendere e ottimizzare i processi di business. Queste attività, peraltro, richiedono necessariamente l'impiego di tool di sicurezza al fine di garantire l'autenticità e l'integrità delle transazioni con clienti e partner. Anche qui esiste, in effetti, un rischio: per esempio, che un cliente non riconosca un ordine. Esistono vincoli legali che vanno rispettati, ma il governo italiano da tempo ha emesso leggi che consentono l'uso di strumenti informatici per autenticare transazioni elettroniche.
Solo considerando tutti gli aspetti della sicurezza e, quindi, i rischi e le opportunità che un'azienda deve fronteggiare, è possibile valutare correttamente quali soluzioni sono indispensabili, quali utili e quali probabilmente inutili. In ogni caso, è buona norma di business misurare il più accuratamente possibile il ROI (Return On Investment) della sicurezza, come di ogni altra spesa, assumendo, pertanto, che si tratti di investimenti e non di meri costi.
Ogni azienda deve quindi valutare le proprie esigenze in termini di sicurezza, identificando le aree di interesse e gli ambiti nei quali sarà opportuno adottare opportuni strumenti. È necessario studiare le infrastrutture utilizzate, le applicazioni e i processi aziendali, al fine di comprendere quali investimenti conviene effettuare.
Quello che emerge è una sorta di trade off tra l'investimento richiesto e il livello di protezione che si vuole o può ottenere.
In altre parole, il costo della sicurezza assoluta è certamente insostenibile per un'azienda: si può considerare che sia virtualmente tendente a infinito. Ma esiste anche un altro problema: troppa sicurezza, per assurdo, risulta controproducente, in quanto vincolerebbe così tanto l'azienda da rallentarne l'attività e diminuirne la produttività. Mentre, al contrario, un corretto livello di sicurezza garantisce lo svolgimento regolare e competitivo del business e, contemporaneamente, aumenta la produttività e la redditività dell'impresa.



L'evoluzione di tecniche e rischi

La gestione della sicurezza ha visto modifiche molto profonde negli ultimi anni. Il cambiamento delle modalità lavorative, e l'uso sempre maggiore di tecnologie di tipo online hanno aumentato in maniera radicale i rischi a cui si espone un'azienda.
In passato le problematiche della sicurezza venivano affrontate quando si era già verificato un problema e si cercava di rimediarvi nel più breve tempo possibile, mentre oggi si tende a privilegiare un approccio aziendale in cui ci sono risorse destinate a tempo pieno alla gestione della sicurezza.
Questa filosofia va estendendosi anche al cliente, dato che la crescente offerta di servizi online finisce per portare anche questa figura all'interno delle considerazioni generali della sicurezza aziendale.
Il grande numero di attacchi è legato in gran parte alla velocità e alla collaborazione. Nell'ultimo decennio la velocità è aumentata su due fronti: quello delle comunicazioni e quindi della possibilità di diffusione e di replicazione di virus e worm, e quello legato allo sviluppo del software, con tante nuove release ognuna delle quali può portarsi dietro delle vulnerabilità. Per quanto riguarda la collaborazione è difficile immaginare oggi un'azienda il cui lavoro non sia il frutto di cooperazione fra due o più dipendenti, se non di due o più reparti; il lato negativo, relativamente alla sicurezza è che più si mettono in condizione di collaborare due

utenti e più si dà spazio ad un uso illecito di questi strumenti.
Non bisogna dimenticare, infatti, che dagli Anni 90 ad oggi le conoscenze informatiche di chi effettua degli attacchi vanno decrescendo: mentre le prime incursioni richiedevano conoscenze avanzatissime dei sistemi e dei protocolli di comunicazione, oggi sono disponibili su internet tantissimi strumenti che spaziano da semplici script a evolutissime piattaforme in grado di decidere autonomamente quale attacco effettuare in base al sistema attaccato, che possono essere semplicemente scaricati e lanciare senza sapere quali vulnerabilità del software o dei protocolli sfruttino.
I cosiddetti "script-kiddies", ovvero le persone con conoscenze tecniche molto limitate che utilizzano questi strumenti quasi per gioco, hanno popolato le cronache dei giornali nel febbraio del 2000 quando vennero effettuati i più clamorosi attacchi di tipo Distributed Denial of Service ai server di Ebay, di Yahoo!, di Amazon e molti altri causando danni per milioni di dollari in mancati profitti. In particolare l'attacco a Yahoo! ha raggiunto punte di Gigabyte di traffico al secondo, mettendo bene in chiaro che un attacco DDOS ben orchestrato può mettere in ginocchio qualsiasi rete.
Si tratta di una tendenza in aumento, che renderà sempre più probabile essere vittima di attacchi e che sta mutando rispetto agli obiettivi, indirizzandosi sempre più verso una logica di profitto anziché di "sfida".
Tutto ciò porta verso un approccio integrato e olistico alla sicurezza. Negli Stati Uniti già dal Dicembre 2003 è stata introdotta una Task Force per la Corporate Governance sotto il controllo della National Cyber Security Partnership, il cui scopo è di sviluppare e promuovere un framework di gestione coerente, e guidare l'implementazione delle politiche di sicurezza per le aziende, le organizzazioni e gli istituti accademici.

Le minacce nell'era del Web 2.0

Le più recenti analisi concordano nell'evidenziare che non sono più i virus a preoccupare, ma minacce più sofisticate quali phishing, adware, spyware e botnet. Denominatore comune di questi termini, oggi alla ribalta, è il fatto che si tratta di azioni illegali orchestrate non più dai cosiddetti script kid, giovani in cerca di notorietà che si pongono obiettivi ambiziosi per mettere alla prova le proprie capacità, ma organizzazioni criminali vere e proprie, che utilizzano i ragazzi, spesso all'oscuro del disegno complessivo, come braccio armato per le loro malefatte. Obiettivo ultimo di queste organizzazioni è guadagnare soldi: attraverso il furto di identità, cioè sottraendo e utilizzando in modo fraudolento dati degli utenti, numeri di carta di credito, password e altro, oppure con il ricatto, per esempio minacciando un'organizzazione di mettere ko i suoi sistemi Internet, o ancora sfruttando l'ingenuità di chi riceve mail mascherate da richieste di beneficenza, pubblicità di prodotti super economici e via dicendo.
Ma c'è di più. Chi scrive malware oggi condivide informazioni con i "colleghi", mentre prima non accadeva. Ormai vengono seguite le stesse fasi di sviluppo del software normale, secondo il modello opensource, con il rilascio successivo di diverse versioni, il debug e via dicendo. Inoltre, esiste un vero e proprio mercato delle vulnerabilità: chi ne segnala una viene pagato, così come avviene per le liste di indirizzi e-mail. E per trovare le vulnerabilità non c'è bisogno di essere particolarmente competenti: esistono tecniche, chiamate "fuzzing", che permettono di effettuare lo scanning dei programmi in automatico. Questi speciali tool possono essere lanciati anche su un pc portatile, poiché non serve una macchina particolarmente potente. Il mercato delle vulnerabilità è ormai alla luce del sole, tanto che qualcuno, qualche mese fa, ne mise una relativa a Excel all'asta su eBay: il portale se ne accorse, e cancellò l'asta prima della fine. Come conseguenza di ciò, continua ad aumentare il numero di attacchi"zero day", che sfruttano vulnerabilità ancora non note e per le quali non sono disponibili patch, malgrado le software house stiano riducendo i cicli di rilascio delle patch, che, in molti casi, hanno ormai cadenza costante. Ciò fa sì che sia più breve il periodo di rischio cui sono esposti gli utenti.

I calo dei virus e l'aumento dello spam

La riduzione del numero di virus in circolazione è sotto gli occhi di qualunque utente di pc. Dati recenti parlano di una mail infetta ogni 337, pari allo 0, 3% del totale, e, in ogni caso, nessuno dei virus emersi nel 2006 ha causato un'epidemia, come avveniva in passato. Se da un lato, come accennato, questo calo si deve allo

spostamento delle energie degli hacker verso attività più redditizie, dall'altro non va dimenticato che ormai quasi tutti i pc sono protetti da antivirus costantemente aggiornati, che riducono significativamente le preoccupazioni e i danni. In effetti, sono oltre 200mila le varianti di virus attualmente in circolazione, ma i tool per l'individuazione e la rimozione sono diventati accurati e largamente disponibili.
Un problema in costante crescita è, invece, quello dello spam, che secondo alcune fonti raggiungerebbe oggi una percentuale pari all'80 90% del totale delle mail in circolazione. Il costo associato è notevolissimo, sia in termini di tempo perso per cancellare le mail sia perché lo spam rallenta i sistemi, intasando le reti trasmissive. Per non essere individuati, gli spammer ricorrono a trucchi come quello di utilizzare domini poco noti e che cambiano con una rapidità impressionante. Le tradizionali blacklist degli anti spam impiegano circa 20 minuti per bloccare un sito, ed è questo il ritmo tenuto dagli spammer nel modificare l'URL di provenienza. Dato che registrare un dominio costa pochi dollari, il vantaggio economico è comunque notevole. Inoltre, utilizzano i nomi di dominio di piccole isole, come quella di Man o quella minuscola di Tokelau, nel Pacifico, un fenomeno noto come"spam-Island hopping". Legato allo spam è il phishing, ovvero l'invio di mail che sembrano provenire da un'azienda reale, come una banca o un sito di e-commerce, con l'obiettivo di estorcere informazioni riservate. Nel 2006 ne sono stati censiti circa 17mila, secondo Secure Computing Research.
In effetti, oggi i tool necessari per attività di spamming e phishing sono pubblicamente disponibili su Internet, mentre è possibile acquistare elenchi di indirizzi validi con milioni di nominativi per poche decine di euro.

L'adware nuova fonte di reddito

Una delle principali fonti di profitto su Internet è l'adware, il software che si installa sul computer della macchina utente e lancia dei pop up pubblicitari mirati, in base a dati di marketing raccolti attraverso lo spyware. I due concetti, spyware e adware, sono, infatti, strettamente legati. Si tratta di una minaccia che non sarà debellata tanto facilmente nel prossimo futuro, perché ha un buon ritorno economico, considerati gli elevatissimi volumi su cui agiscono. Il modello dell'adware nasce in modo legale, ma gli hacker si introducono nei computer senza permesso, prendendo a volte denaro dalle società coinvolte, oppure dirottano i pagamenti verso di loro. Dati rilevati a maggio del 2006 parlano di 700 famiglie di adware con oltre 6000 varianti.
Le principali fonti di malware, cioè i siti che dispensano il software all'ignaro visitatore, sono quelli più gettonati, come quelli dei divi o di eventi sportivi molto seguiti: i mondiali di Germania, per esempio, hanno portato alla circolazione di un virus camuffato da foglio elettronico della classifica, e di uno spyware nascosto in un salvaschermo.

Web 2.0 e Bot net

La diffusione delle nuove minacce su Internet è oggi alimentata da due fenomeni. Il primo è quello delle cosiddette social network, o del Web 2.0. Ci si riferisce a quell'insieme di siti (da You Tube a Wikipedia) in cui i veri protagonisti sono gli utenti, che possono pubblicare direttamente i propri contenuti. Al successo di questo fenomeno si accompagna, secondo gli addetti ai lavori, un aumento delle problematiche di sicurezza, prima fra tutte il furto di identità: gli utenti si sentono fiduciosi e lasciano in rete non solo le generalità, ma anche i propri interessi e le informazioni sulla propria vita privata, tutti dati utili per truffe mirate.
Da ultimo, ma non per importanza, va citato l'emergere dei Bot net (termine derivato da Robot), universalmente considerati la principale minaccia del momento. Si tratta di una rete di computer che vengono di fatto "controllati" da un hacker, che li può utilizzare per inviare un attacco o uno spam su grande scala, senza che l'utente del computer si accorga di niente. Il fenomeno è in espansione e si prevede che in futuro le Bot net, e chi le governa, assumeranno il ruolo di centrali distribuite di comando e controllo. Inoltre, emergerà l'utilizzo di protocolli per il controllo diversi dai tradizionali IRC (Internet Relay Chat) o HTTP. Gli autori di Bot utilizzano sempre più tecniche di sviluppo open source, con la collaborazione fra diversi sviluppatori, e questo rappresenta un cambio importante nell'evoluzione del malware, poiché lo rende sempre più solido e affidabile. Si preannuncia, quindi, una crescita esplosiva del fenomeno.