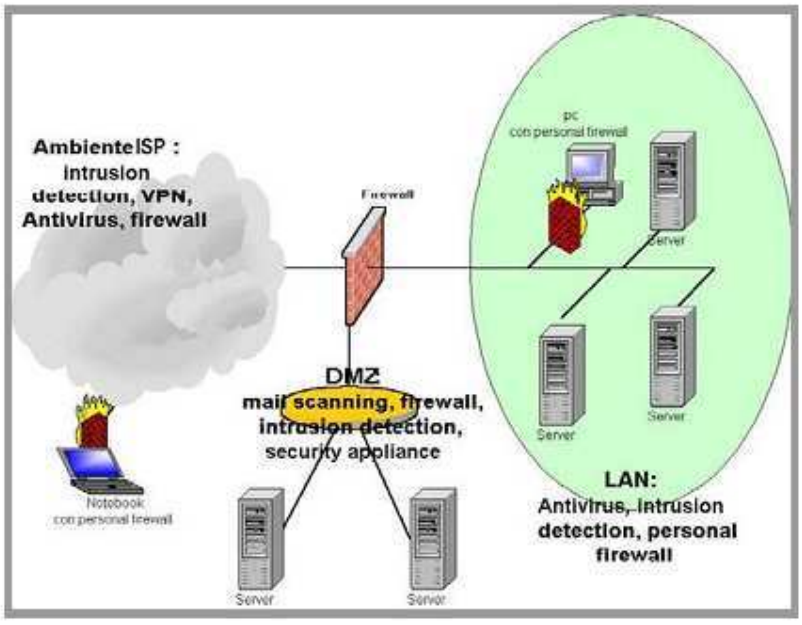
UN APPROCCIO INTEGRATO ALLA SICUREZZA

Le diverse soluzioni per la sicurezza si sono evolute nel corso degli anni al fine di indirizzare problematiche specifiche, andandosi così a posizionare in punti precisi dell'infrastruttura di elaborazione e comunicazione aziendale. Per esempio, l'autenticazione sugli host centrali, in un primo momento, e sui gateway di accesso, successivamente, oppure i firewall a protezione del perimetro applicativo e così via.

Questa visione rifletteva la natura delle minacce, che, però, hanno imboccato la strada di un'evoluzione convergente. Gli attacchi, infatti, adottano tecnologie ibride che richiedono strumenti altrettanto integrati se si vuole avere una ragionevole certezza che possano essere rilevati.

Quello che sta emergendo è uno scenario che vede l'affermarsi di un'architettura distribuita dei sistemi di sicurezza, con l'installazione di soluzioni in modalità client server e con l'integrazione di applicazioni inizialmente separate. Un esempio peculiare, a tale proposito, sono i sistemi di intrusion detection.

Nati per essere posti all'interno della rete, si stanno spostando in tutti gli elementi dell'architettura, posizionandosi su host, segmenti di rete e client, sia all'interno della LAN sia all'esterno del firewall, come pure nella DMZ. Ma, addirittura, tali sistemi sono anche in grado di colloquiare con analoghe soluzioni poste dagli Internet Service Provider a protezione delle connessioni di rete. Senza contare poi l'interazione degli stessi sistemi di IDS con i dispositivi di firewall.



L'evoluzione verso una sicurezza distribuita

Un esempio immediato dei vantaggi che può portare l'integrazione dei sistemi è quello dell'autenticazione. Nei sistemi informativi aziendali già di media dimensione ci si confronta con l'esistenza di directory multiple, che elencano gli utenti ciascuna secondo un proprio punto di vista. Sono directory organizzate da ogni dipartimento aziendale, che per ogni dipendente elabora particolari informazioni. Così come esistono directory impostate dalle particolari applicazioni che devono servire.

Questa situazione porta a due ordini di problemi. Il primo è vissuto dall'utente, che deve autenticarsi ogni volta che accede a un'applicazione, a un database o a un server diverso. Con tutte le difficoltà che questo comporta, quale il dover memorizzare più user ID e password. Alle volte le impostazioni delle applicazioni stesse impediscono di poter adottare lo stesso tipo di identificativi: per esempio, un mail server potrebbe essere stato configurato dal responsabile in modo che ogni account abbia come user ID "nome.cognome", che è difficilmente impostabile come entry di un sistema legacy.

Il secondo problema è di carattere gestionale, con una mole di dati che si replicano e sono difficili da mantenere aggiornati e consistenti. Si pensi all'impiegato che lascia il posto di lavoro: il suo account deve essere cancellato da tutti i sistemi singolarmente. La situazione tipica è che, in una buona percentuale dei sistemi, i privilegi di accesso del dipendente rimangono attivi anche a distanza di molti mesi dalle sue dimissioni o dal suo licenziamento. Per risolvere questi problemi, che possono essere alla base di criticità nella sicurezza aziendale, sono state sviluppate delle tecniche cosiddette di Single Sign On (SSO), tali per cui l'utente ha la necessità di autenticarsi una sola volta con un server centrale.

Sarà poi questo a effettuare le autenticazioni successive mano a mano che l'utente richiede l'accesso a un nuovo server o applicazione, facendosi in un qualche modo garante della sua identità.

Un approccio sistemico

Per poter realizzare l'integrazione delle soluzioni di sicurezza, tanto più quanto maggiore si vuole che sia il livello d'integrazione, è opportuno adottare un approccio sistemico, che abbracci l'insieme delle problematiche della sicurezza partendo dalle esigenze aziendali e traducendo le stesse in policy di sicurezza. Queste andranno poi opportunamente adattate e implementate nei vari sistemi in maniera consistente. Si ottiene, così, un sistema robusto in cui tutte le soluzioni collaborano alla protezione e alla prevenzione.

Un tale sistema, peraltro, non consiste solo in un insieme integrato di applicazioni, più o meno automatiche. Come già evidenziato, la sicurezza è anche una questione organizzativa.

Poco o nulla servono le precauzioni se, poi, nessuno le adotta. Le policy oltre che definite devono essere implementate. Molte di queste, però, non sono automatiche o, comunque, possono essere disattese dagli utenti, anche senza intenzioni dolose, ma semplicemente per accelerare il proprio lavoro (quanti hanno "voglia" o si ricordano di lanciare il backup periodicamente?).

Le policy diventano procedure e una certa attenzione è richiesta, come, per esempio, quella di non lasciare appuntate le password su foglietti (tipico il post-it giallo sotto la

tastiera).

A caratterizzare più di ogni altra cosa un approccio sistemico, peraltro, è la visione della sicurezza come processo continuo. Si è detto che il punto di partenza deve essere il rischio: comprendere quali sono le informazioni e le risorse che hanno bisogno di protezione e, soprattutto, quali sono i danni che si conseguirebbero in caso di perdita delle stesse. Si ottiene, così, una misura degli investimenti che sarà opportuno realizzare. Una volta progettato di conseguenza il sistema di sicurezza, questo va implementato con tutte le implicazioni di carattere organizzativo cui si è accennato, anche in termini di definizione di policy aziendali.

Il passo successivo è quello del controllo e della manutenzione del sistema. Questo, però, implica il continuo aggiornamento delle soluzioni, perché stiano al passo con l'evoluzione delle minacce, ma anche l'adeguamento di tutta l'architettura del sistema alle variazioni dello scenario complessivo. È la stessa azienda soggetta a cambiamenti: si pensi alle acquisizioni, all'istituzione di una nuova business-unit e a tutte quelle dinamicità che testimoniano il buon stato di salute di un'impresa.

Periodicamente, dunque, è necessario rimettere tutto in discussione, a partire dal rischio stesso cui è soggetta l'impresa, mantenendo sotto controllo il sistema di sicurezza per verificarne la robustezza (per esempio, con tecniche di vulnerability assessment) e l'adeguatezza.

La necessità di un responsabile

Un sistema del genere deve essere quindi gestito sia nell'operatività di tutti i giorni sia nella sua pianificazione complessiva. Entrambe sono fasi delicate, che richiedono un impegno crescente all'aumentare delle dimensioni aziendali, delle risorse messe sotto controllo e, ovviamente, delle soluzioni implementate.

La complessità che ne emerge, unitamente all'importanza dei sistemi di sicurezza, suggerisce la definizione di responsabilità ben precise, con la nomina di un responsabile della sicurezza. In Italia, alcune normative impongono la presenza di un responsabile della sicurezza IT in azienda (da non confondere con quello imposto dalla legge 626, che riguarda la sicurezza del posto di lavoro). Il security manager, come viene spesso indicato con dizione inglese, è preposto alla gestione del sistema di sicurezza e può essere perseguito anche penalmente (come prevede il DPR 318) in caso di danni causati da inadempienze alla sicurezza da parte dell'azienda. A seconda delle realtà, potrà essere necessario affiancare al responsabile uno staff, variamente composto. Alcuni studi indicano come ideale un rapporto 1 a 25, tra personale dedicato alla sicurezza e numero di postazioni (client, server e nodi di rete inclusi).

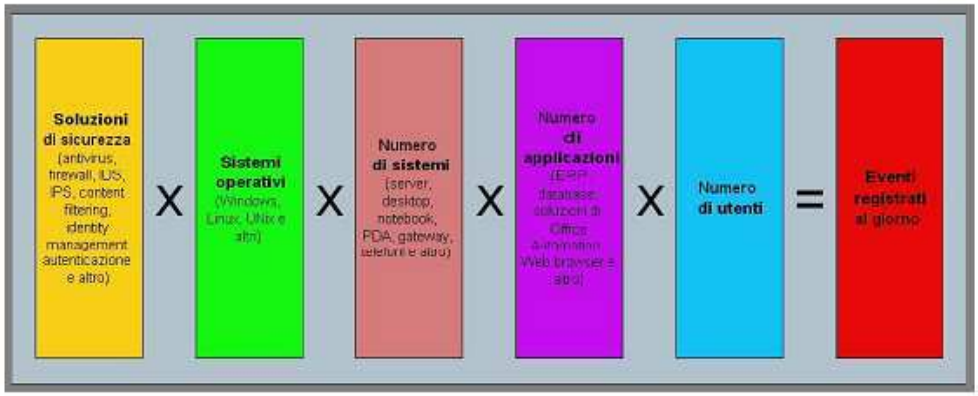
Nella realtà, naturalmente, sono i budget IT a dettare le regole per il dimensionamento dello staff.

Si consideri, però, che in un'azienda di medie dimensioni, dotata di un sistema già minimamente sofisticato, sarebbe opportuno poter contare almeno su un responsabile, un database manager, un addetto alla manutenzione e almeno un amministratore.

L'eccesso di informazioni

Un problema derivante dall'implementazione di un sistema integrato non supportato da un adeguato strumento di amministrazione è legato all'eccesso di informazioni che il security manager si trova a dover gestire.

Ogni soluzione del sistema, dall'antivirus al firewall, dai sistemi di rilevamento delle intrusioni a quelli per il controllo degli accessi, alle soluzioni per l'identity management, alle sessioni d'autenticazione e così via, genera delle informazioni, registrando gli eventi che sono tenute a monitorare. Si stima che solo il firewall di una media organizzazione, come potrebbe essere una banca, registra circa ventimila eventi al giorno.



Una formula per l'eccesso di informazioni sulla sicurezza (Fonte: Computer Associates)

La corretta introduzione delle policy di sicurezza in ogni dipartimento aziendale può comportare un ulteriore incremento della quantità di informazioni che vengono registrate, molte delle quali relative allo stesso evento che viene registrato su più fronti.

Sussiste, pertanto, un problema di integrazione, che, evidentemente, deve esser affrontato a monte, in fase di progettazione, prevedendo da subito uno strumento di integrazione delle diverse soluzioni, in modo da poter quantomeno raccogliere le informazioni su una base omogenea e su un'unica console di amministrazione centralizzata. Anche così, peraltro, non è pensabile gestire la mole di dati, se questa non viene preventivamente filtrata da un sistema di reportistica intelligente che consente di visualizzare le informazioni con formule di sintesi immediate, per esempio legate al rischio connesso con l'evento.

Nel caso prima esemplificato, peraltro, questo non sarebbe probabilmente sufficiente, se non in presenza di un motore di correlazione intelligente dei dati, che fornisce un primo elemento di supporto alle decisioni, di cui l'amministratore del sistema ha evidente bisogno, altrimenti non avrebbe le capacità gestionali per reagire alle situazioni che potrebbero compromettere processi e attività essenziali per l'azienda stessa. Senza contare che anche il semplice svolgimento delle attività quotidiane dell'amministratore potrebbe risultare problematico.

Anticipare gli attacchi

La varietà di minacce alla sicurezza informatica non cessa di sorprendere. Una recente notizia che giunge dagli Stati Uniti riporta che un hacker, dopo essere riuscito ad accedere al sistema informativo di un'azienda, ne ha cifrato alcuni contenuti, indirizzando successivamente all'utente una richiesta di denaro di 200 US-$ da depositare su un conto in Internet in cambio della chiave per sbloccare i file.

In realtà la richiesta di "riscatto"in cambio di dati informatici non rappresenta una novità assoluta e gli analisti, pur prevedendo possibili repliche di attacchi di questo tipo, non ritengono che si sia di fronte a un nuovo trend a larga diffusione.

Questo episodio rappresenta, tuttavia, un punto di partenza interessante per una riflessione sulla varietà delle minacce che continuamente le aziende si trovano a fronteggiare per proteggere le loro informazioni e dimostra che la "fantasia" degli hacker riesce ancora a superare le previsioni dei professionisti della sicurezza.

Ogni volta che si mette a punto una tecnica di difesa, compare un nuovo tipo di minaccia. È così che siamo passati dai virus, ai worm, ai trojan fino al più recente fenomeno dello spyware, ancora più difficile da controbattere poiché si colloca al confine tra lecito (o addirittura utile) e illecito.

Quando la battaglia sembra vinta sul piano delle tecnologie, lo scontro si sposta sull'interruzione di servizio, sull'estorsione di informazioni attraverso tecniche di social engineering o sul piano della truffa più tradizionale, come è il caso del phishing, con cui si riescono a carpire informazioni bancarie simulando false richieste via mail da parte degli istituti di credito. Non sono neppure mancati casi in cui gli hacker siano riusciti a sfruttare i comportamenti messi in atto dalle società che producono soluzioni per la sicurezza per testare e mettere a punto minacce particolarmente efficaci. Per queste ragioni, per esempio, le società che realizzano antivirus non diffondono mai informazioni su eventuali codici maligni individuati, prima di avere reso disponibile un sistema di protezione.

Un altro aspetto che colpisce è la facilità con cui è possibile condurre un attacco, anche da parte di chi non dispone di alcuna conoscenza specifica. Nell'esempio descritto prima, l'utente è stato contagiato dal virus accedendo a un sito Web, attraverso il quale l'attaccante, sfruttando una vulnerabilità nota di Internet Explorer, è riuscito a scaricare sulla sua macchina del codice ed eseguirlo. Per installare adware o spyware è, infatti, sufficiente predisporre l'exploit su un sito Web, caricare un eseguibile e indurre gli utenti ad accedervi. Su Web sono disponibili tutte le informazioni utili allo scopo, comprese quelle per copiare lo schema e adattarlo per frodi di svariato tipo.

Il caso citato mette in evidenza anche un altro tema interessante, per certi aspetti collegato alla facilità di lanciare un attacco. Si sta assistendo a un cambiamento negli obiettivi degli attacchi basati su codice malevolo che risultano non solo sempre più mirati, ma anche sempre più indirizzati a ottenere denaro. Sembrano, insomma, definitivamente terminati i tempi in cui gli hacker violavano i sistemi per il gusto di un'affermazione personale.

Protezione multilivello

Già da tempo la proliferazione delle minacce e la consapevolezza della protezione dei dati come elemento strategico hanno messo in evidenza che non è possibile gestire la sicurezza all'interno dell'azienda in modo "manuale" né, tanto meno, amatoriale. È necessario personale specializzato e dedicato e l'utilizzo di sistemi in grado di automatizzare le azioni protettive e la risposta agli attacchi.

Il passo successivo, che si evidenzia sempre più, non solo nei messaggi di marketing, ma anche nei prodotti resi disponibili dai vendor che operano nel settore dell'ITSecurity, è

che essere reattivi non basta più.

La prima ragione per cui l'approccio reattivo non sufficiente è legata alla rapidità con cui le minacce riescono a diffondersi e arrecare danni: si pensi che un virus può impiegare meno di 15 minuti per diffondersi, a livello mondale, su centinaia di migliaia di computer.

Anche nel caso in cui si riuscisse, intervenendo sulla tecnologia, ad accelerare i tempi di risposta, un sistema reattivo, basato sulla conoscenza della minaccia da cui difendersi, non potrebbe fare nulla rispetto a minacce di nuovo tipo, i cosiddetti attacchi del giorno zero.

Essere proattivi non è però facile e richiede una sinergia tra soluzioni tecnologiche adatte e il loro inserimento all'interno di una strategia specifica aziendale indirizzata alla sicurezza.

Da un punto di vista tecnologico la tendenza è quella di utilizzare una combinazione di tecniche differenti e di prevedere sistemi in grado di operare in modo coordinato a più livelli, in diversi punti della rete e capaci di intervenire in modo differenziato in funzione del livello di rischio.

La sicurezza è, infatti, sempre un compromesso tra obiettivi di business e requisiti operativi e nel caso in cui si segua un approccio proattivo, particolare attenzione va posta alla configurazione delle soluzioni e al loro corretto inserimento all'interno dell'infrastruttura, in modo da evitare la generazione di falsi positivi, in grado di spostare il delicato equilibrio tra vantaggi e svantaggi.

Un contributo importante per la realizzazione di un approccio proattivo è fornito dalle nuove tecniche di individuazione delle minacce basate sul riconoscimento delle anomalie di comportamento: per esempio un eccessivo e ingiustificato flusso di traffico su una certa porta, il comportamento di un protocollo oppure una chiamata alla rubrica da parte di un messaggio di posta elettronica.

Altrettanto importante, per un approccio proattivo di successo, è imparare dall'esperienza, prevedendo, all'interno del processo di protezione, lo spazio per un continuo feedback proveniente dall'analisi dei risultati prodotti dai comportamenti adottati in precedenza.

Gli aspetti strategici sono altrettanto importanti. Da una parte è opportuno predisporre un disegno architetturale e regole di accesso alla rete che consentano, ai non autorizzati, di raccogliere il minor numero di informazioni possibili. Dall'altro è necessario, come sempre, che venga diffusa una cultura della sicurezza tra il personale interno e che venga fatto comprendere come, per esempio, la divulgazione di un insieme di dati apparentemente non correlati e di poca importanza, possa rappresentare l'elemento abilitante per lanciare un attacco efficace o per diffondere informazioni riservate.

Per terminare, una nota positiva: l'utente è riuscito a sbloccare i file senza sottostare al ricatto, grazie a un reverse engineering del Trojan che ha permesso di capire le modalità di azione del (semplice) sistema di cifratura e di scrivere un decifratore adeguato.