LA GESTIONE DELLA SICUREZZA

Non solo tecnologia

Si sta affermando sempre più un concetto di sicurezza come elemento trasversale che permea, a vari livelli, i processi di business e che quindi va gestito in modo sinergico a essi. Il fatto poi che le informazioni siano sempre più distribuite sia l'interno che all'esterno del perimetro aziendale, verso clienti, partner e fornitori, incrementa la complessità e, di conseguenza, complicala gestione.

La tecnologia certamente aiuta a predisporre misure di difesa ma, da sola, non è in grado di assicurare un livello di sicurezza adeguato a ogni esigenza aziendale, anche perché le aziende rappresentano realtà dinamiche in continua evoluzione.

Si evidenzia da ciò la necessità di gestire opportunamente la security, prevedendo una continua rivisitazione del livello di protezione a fronte dell'evoluzione informatica e dei processi di business aziendali. Emerge, pertanto, l'esigenza di inquadrare i diversi aspetti di sicurezza all'interno di una strategia aziendale specifica e coordinata, sorretta da una serie di policy e di protocolli rivolti a delineare adeguate azioni che garantiscano il mantenimento dello standard di protezione prefissato.

Al fine di semplificare questo tipo di azioni, l'offerta dei vendor si orienta sempre più verso soluzioni integrate, non solo per quanto riguarda le tecnologie, ma soprattutto rispetto alla possibilità di gestione unificata e centralizzata.

Spesso la semplicità gestionale viene utilizzata come importante leva di marketing. Tuttavia non va dimenticato che gestire la sicurezza non è un compito semplice così come non si tratta di un risultato banale quello di individuare, all'interno di ogni specifica azienda, il corretto compromesso tra protezione, valore dell'informazione ed esigenze di continuità di business, che condiziona le scelte tecnologiche, strategiche e di spesa per la sicurezza.

La scelta di gestione interna della sicurezza implica, innanzitutto, che esista una figura deputata a occuparsene. Anche nelle realtà piccole, in cui la dimensione finanziaria non consente la presenza di una figura dedicata specifica (il security manager) è essenziale che esista, in ogni caso un responsabile: insomma qualcuno che abbia tra i propri compiti specifici quello di occuparsene. Ovviamente dovrà trattarsi di una persona con competenze tecnologiche adeguate e che abbia il tempo per aggiornarsi sulle nuove"macro" vulnerabilità e minacce e risorse sufficienti per affrontarle.

In ogni caso, per aziende anche minimamente strutturate, la figura del security manager si appresta a diventare irrinunciabile. La presenza di un firewall e un antivirus, per lungo tempo considerata esaustiva per assicurare la protezione aziendale, non deve essere

considerata più sufficiente, anche per le realtà piccole. Sono richiesti strumenti integrati, processi di assessment delle vulnerabilità e una gestione e un controllo costante e dinamico delle soluzioni e delle policy di protezione implementate.

Infatti, sempre più frequentemente, le PMI hanno lo stesso tipo di problematiche e le stesse esigenze delle aziende di livello enterprise, con l'inconveniente di disporre di risorse inferiori. D'altra parte l'offerta di mercato negli ultimi anni si è occupata molto delle esigenze delle aziende più piccole e sono ormai disponibili, anche a costi accessibili alle PMI, soluzioni di sicurezza con portata analoga a quelle di classe enterprise.

In molti casi, la consapevolezza da parte delle aziende dell'importanza della sicurezza e la contemporanea constatazione di non disporre degli strumenti adeguati per affrontarla in modo corretto internamente hanno indotto a indirizzarsi verso strutture esterne dedicate. I servizi di sicurezza gestiti sono certamente un trend in continuo aumento.

L'offerta di servizi è ampia e variegata e include la gestione e l'aggiornamento tecnologico nel tempo di firewall, antivirus, IP/VPN, intrusion detection, vulnerability assessment, filtraggio dei siti Web e reportistica su tutte le attività sospette e bloccate.

La più recente tendenza è legata alla gestione della business continuity, mano a mano che, come si diceva prima, questa si afferma come un aspetto trasversale tra sicurezza e business.

I vantaggi di affidarsi a una struttura esterna sono quelli tipici dell'outsourcing: la possibilità di avere una copertura 24x365 (essenziale per questi compiti), di potersi affidare a personale specializzato dotato di tecnologie all'avanguardia e costantemente in aggiornamento, che effettui un monitoraggio costante e riveda periodicamente l'esposizione al rischio dell'azienda. Un altro aspetto fondamentale è la capacità d'intervento rapido, in un ambito in cui la differenza tra fermare un attacco entro pochi minuti oppure lasciarlo proliferare per un'ora può fare una grandissima differenza.

La contropartita rispetto a questa serie di vantaggi risiede nell'affidarsi a un soggetto esterno e, in qualche modo, perdere una percentuale di controllo su alcuni aspetti gestionali o informativi. In conseguenza di ciò sta incontrando un crescente successo un approccio indirizzato all'outsourcing parziale, in cui l'azienda si affida a una struttura esterna per la verifica, il monitoraggio e l'impostazione di alcune azioni automatiche di protezione, mantenendo però il controllo sui propri apparati e sui processi gestionali afferenti alla sicurezza.

L'analisi del rischio

L'analisi del rischio è il punto di partenza del processo di pianificazione di un sistema di sicurezza IT aziendale. Prima di descrivere le fasi con cui si arriva alla sua valutazione, occorre, però, definire che cosa s'intende con rischio: esso è una misura del danno che consegue a un evento pericoloso, in funzione della probabilità che questo si verifichi effettivamente. Solo una corretta valutazione del rischio permette a un'azienda di stabilire quale piano di intervento sia opportuno implementare al suo interno.

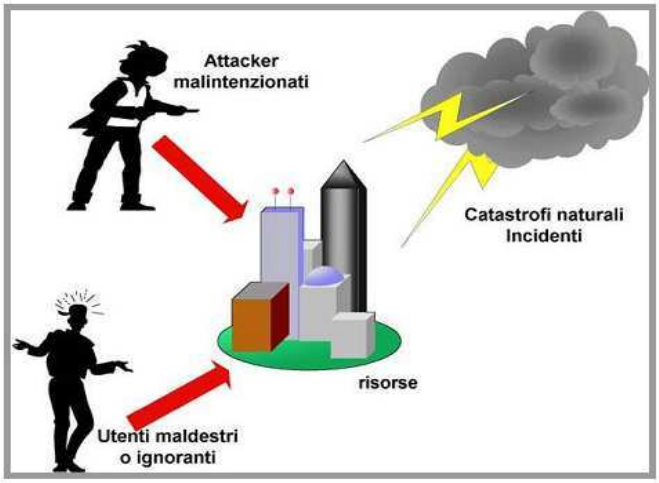
Tale analisi, inoltre, va ripetuta periodicamente perché l'entità dei danni dovuti a un

attacco informatico segue la dinamicità dell'azienda.

In altre parole, quest'ultima, nel corso della propria esistenza, evolvendo, modifica le proprie risorse e le esigenze di business (ad esempio attraverso fusioni o acquisizioni aziendali). D'altro canto, anche le condizioni esterne variano: gli hacker scoprono nuove vulnerabilità dei sistemi, inventano altre tecniche e via dicendo; di conseguenza cambia il rischio ed è necessario rimettere tutto in discussione.

Il rischio, dunque, è tanto più alto quanto più elevato è il valore della risorsa che si ritiene di dover proteggere e quanto maggiore è la minaccia che incombe su quella risorsa; un'azienda il cui asset principale è rappresentato dalle informazioni, potrebbe restare distrutta dalla perdita delle stesse (per esempio, si pensi a un'assicurazione che si vedesse cancellare tutti i dati relativi alle proprie polizze).

Le minacce sono tipicamente classificate in tre categorie:calamità naturali, minacce intenzionali e minacce involontarie.



Le tre origini del rischio

L'analisi del rischio può invece essere scomposto nelle seguenti fasi:

- identificazione o classificazione delle risorse da proteggere;
- identificazione delle minacce cui sono soggette le risorse (insieme e singolarmente);
- identificazione delle vulnerabilità (o vulnerability assessment, come è più comunemente indicata usando il termine inglese);
- valutazione del rischio.

Identificazione delle risorse

La prima fase consiste nella realizzazione di un inventario delle risorse informative. Vanno considerate, in questa analisi, sia tutte le informazioni che vengono prodotte in azienda, con qualsivoglia strumento, sia tutti i mezzi dell'infrastruttura IT (dai server alle workstation, dalle reti alla loro banda, fino ai dischi, ai nastri di backup, ai cavi e così via).

Per ciascuna risorsa, quindi, deve esserne calcolato il valore. In particolare, per quanto riguarda le informazioni, queste andranno confrontate con gli obiettivi primari della

sicurezza, vale a dire confidenzialità, integrità e disponibilità.

Le risorse informatiche e di comunicazione, invece, sono importanti essenzialmente ai fini della disponibilità e vanno valutate in funzione delle loro criticità all'interno dell'azienda. Un server, per esempio, è tipicamente più importante di una workstation, il router per il collegamento a Internet è normalmente più utile di quello che consente la connessione a un ufficio distaccato con poco personale part time, ma potrebbe essere vero il contrario se quest'ufficio è l'agenzia periferica di una banca che, attraverso quel router, effettuai resoconti giornalieri.

Ulteriori elementi che è opportuno considerare nella valutazione della specifica risorsa o tipologie di risorse sono i costi per la perdita o il suo danneggiamento, in termini di profitto, tempo perso ed esborso per eventuali riparazioni. Un inventario dovrebbe definire, per ciascuna risorsa, le seguenti classi di dati:

- tipo di risorsa (se si tratta di dati, hardware, software o altro);
- criticità (se è un sistema generico o mission critical);
- proprietà delle informazioni;
- posizione fisica o logica della risorsa;
- numero di inventario (nel caso sia disponibile);
- informazioni relative ai contratti di manutenzione in essere per la risorsa (in termini di livelli di servizio, garanzie, contatti, processo di sostituzione e così via).

Ai fini della protezione delle risorse (in particolare delle informazioni), che rimane il fine ultimo, il dato più importante è quello della criticità. Tanto che è opportuno essere piuttosto rigorosi nel definirla, ricorrendo eventualmente a una sorta di classificazione e dividendo, così, le informazioni in:

- Sensibili: Sono le risorse più importanti, che vanno protette da eliminazioni o modifiche non autorizzate, garantendone disponibilità e integrità, oltre che riservatezza. In generale, sono dati che devono essere protetti con più di una normale garanzia di accuratezza e completezza. Le transazioni finanziarie o le azioni legali dell'azienda sono due esempi di questo tipo di informazioni.

- Riservate: Anche in questo caso va assicurata la riservatezza. Si tratta perlopiù di dati destinati a essere rigorosamente utilizzati solo all'interno dell'impresa. Per questa categoria di informazioni il danno maggiore potrebbe derivare da una loro divulgazione non autorizzata. Per esempio, informazioni riguardanti i risultati finanziari o lo stato di salute di aziende private.

- Private: Per certi versi si potrebbe considerare una classe della categoria precedente. È opportuno, però, considerarla a parte perché vi rientrano i dati che sono soggetti alla normativa sulla privacy e che, conseguentemente, potrebbero portare a ripercussioni legali per il responsabile della sicurezza se divulgati senza autorizzazione. Vi appartengono, per esempio, tutti i dati sul

personale e sui clienti.

• Pubbliche: In questa categoria rientrano tutti i dati che non sono contemplati esplicitamente in una delle tre categorie precedenti. In generale, sono informazioni la cui divulgazione non avrebbe serie conseguenze.

Identificazione delle minacce

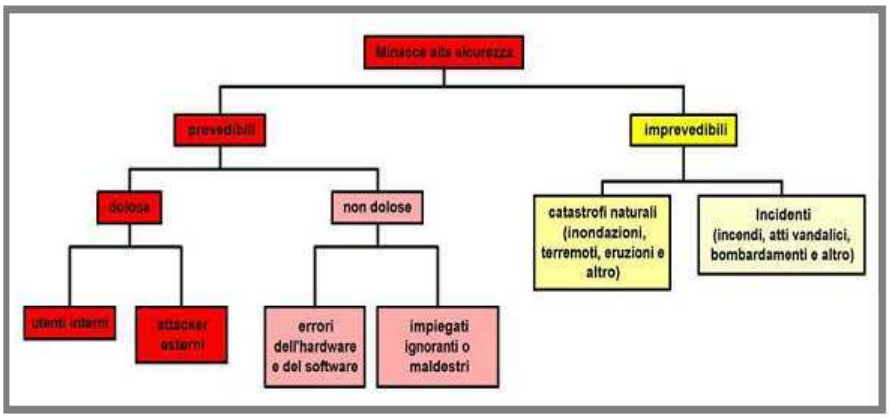
Le minacce possono essere di diversi tipi, che devono essere considerati in relazione con le caratteristiche dell'azienda. Queste vanno esaminate e valutate sia in termini di locazione geografica, sia (e soprattutto) in riferimento alle attività e al modello di business. Può essere abbastanza logico, ad esempio, che una banca sia maggiormente esposta a minacce di tipo volontario di quanto non lo sia una catena di ristoranti. Peraltro, in alcuni casi, possono entrare in gioco considerazioni di carattere socio politico che influenzano la valutazione della minaccia.

Ognuno dei modi in cui una risorsa può essere danneggiata, alterata, rubata, distrutta o resa inaccessibile, costituisce una minaccia. Tra questi bisogna considerare sia quelli volontari sia involontari, senza dimenticare le catastrofi, quali incendi, terremoti e inondazioni, che in molte zone d'Italia si presentano con una frequenza tutt'altro che trascurabile.

Vulnerability assessment

Come osservato in precedenza, le minacce possono essere di tipo imprevedibile, spesso riferite in letteratura anche come minacce "naturali". Rientrano in questa categoria catastrofi quali inondazioni e terremoti, ma anche, quindi con un'accezione più ampia, incendi, attentati e così via. La probabilità che queste minacce si verifichino non è regolabile con un sistema di sicurezza IT e dipende da condizioni essenzialmente esterne all'azienda. Vanno evidentemente considerate e possono essere misurate (la probabilità di un'eruzione alle pendici dell'Etna è ovviamente maggiore che sulla riva del Po, viceversa per un'inondazione). In questi casi le tecniche adottabili per la protezione delle informazioni sono quelle tipiche del disaster recovery.

La tipologia di minacce che invece sono generalmente indicate come di origine umana, ma che sono riferibili in senso più ampio come "prevedibili", in quanto vi rientrano anche guasti del software o dell'hardware, possono essere suddivise in "volontarie" (o "dolose") e "involontarie" (o "non dolose").



Classificazione delle minacce

Le minacce considerate involontarie sono, generalmente, quelle derivanti da un errore di un dipendente o alla sua ignoranza. Possono essere molto gravi, e causare danni ingenti direttamente (con l'eliminazione o la modifica di dati conseguente a un uso maldestro delle applicazioni) oppure indirettamente (con l'apertura di una falla nel sistema di sicurezza a causa del mancato adempimento delle policy per negligenza o disattenzione). Per ridurre il rischio di queste minacce è opportuno, innanzi tutto, condurre una campagna di sensibilizzazione interna alla sicurezza. È essenziale, in particolare, che i dipendenti siano a conoscenza delle conseguenze del loro comportamento scorretto non solo sul piano pratico ed economico, per quanto concerne l'azienda, ma anche su quello legale, che li potrebbe coinvolgere direttamente. Tra le minacce involontarie rientrano anche i guasti dell'hardware o i difetti del software, la cui probabilità di accadimento può essere calcolata, in funzione delle caratteristiche di partenza delle risorse (un server fault tollerance fornisce garanzie di affidabilità e disponibilità, come pure uno storage con supporto RAID e via dicendo) e misurata, con un controllo periodico del loro stato.

Le minacce volontarie o dolose sono certamente da considerare le più pericolose. Esse sono di natura umana e derivano da un attacco mirato che può provenire tanto dall'esterno quanto dall'interno dell'azienda. Tra i due casi, l'ultimo è presumibilmente il peggiore anche perché è più difficile da rilevare e prevedere. Questo tipo di minacce deriva da attacchi che sfruttano tipicamente le vulnerabilità del sistema di sicurezza o in maniera opportunistica (un hacker che "casualmente" durante scansioni "a pioggia" trova un buco in un sistema e vi entra) o mediante un'accurata pianificazione. Tra i metodi di attacco si ricordano: il social engineering (cioè una vera e propria attività spionistica, tesa a ottenere informazioni dirette dagli utenti, usando una falsa identità); virus, worm e cavalli di Troia; Denial of Service (che mette, per esempio, un server in condizioni di dover negare il servizio); rinvio dei pacchetti; modifica dei pacchetti; IP spoofing (tramite il quale l'hacker sostituisce l'indirizzo IP della propria macchina con un altro, tipicamente della rete che sta attaccando); password guessing (il tentativo di indovinare o calcolare una password).

Considerandole varie minacce (che peraltro possono essere anche di tipo misto), è possibile determinare quali vulnerabilità possono essere sfruttate. Le vulnerabilità sono, in generale, dovute a errori o trascuratezze di gestione: una configurazione superficiale, un bug del software, una versione non aggiornata dell'antivirus e così via. Si consideri, per esempio, il sistema operativo della macchina su cui è installato il firewall. Da esso dipende quest'ultimo, che può essere disabilitato facilmente se sul sistema operativo stesso non è stata disattivata la corrispondente funzione. Per quanto riguarda le modalità di gestione è importante tenere presente che, praticamente, tutti gli attacchi sfruttano delle vulnerabilità note che possono essere riparate, spesso, con largo anticipo rispetto al momento in cui può verificarsi un attacco. Il vulnerability assessment consiste in una serie di tecniche e tecnologie per il controllo dello stato di salute di tutte le risorse, comprese soprattutto tutte le soluzioni di sicurezza. Queste possono essere mantenute aggiornate effettuando una scansione periodica delle risorse e pianificandone l'evoluzione. Peraltro, sono sempre più comuni opzioni di aggiornamento automatico disponibili anche sotto forma di servizio.

La valutazione del rischio

Una volta ultimate le tre fasi precedentemente illustrate, occorre un lavoro di sintesi che

porti alla valutazione del rischio. Per questo è possibile operare in diversi modi, con scuole metodologiche diverse. I risultati possono essere classificati con un maggior o minor livello di dettaglio e la valutazione può essere sia di tipo qualitativo sia quantitativo, includendo, per esempio, valori numerici del rischio espressi in percentuali del fatturato. Una linea guida che sta assumendo un ruolo di standard nel settore è rappresentata dalla normativa ISO17799 / BS7799. Esistono in ogni caso delle caratteristiche fondamentali che è opportuno siano presenti in ogni analisi del rischio:

- riproducibilità e ripetitività: dato che occorre ripetere periodicamente il processo e al fine di ottenere risultati confrontabili con i precedenti è opportuno che l'analisi possa essere condotta con le stesse procedure;

- comprensibilità: il rischio deve essere espresso, qualitativamente o quantitativamente che sia, in forma chiara atta a definire la successiva strategia di protezione; condivisibilità: i risultati dell'analisi devono essere condivisi tra le diverse funzioni aziendali e deve essere condotta una campagna di sensibilizzazione interna, che costituisce la prima forma di protezione;

- consistenza: la valutazione del rischio è funzione delle policy di primo livello, per i cui i valori attribuiti alle risorse devono essere consistenti con gli obiettivi di riservatezza, integrità e disponibilità;

- riutilizzabilità: i risultati delle varie fasi devono poter essere reimpiegati, al fine di accelerare i successivi processi e consentire economie di scala (per esempio, il vulnerability assessment potrebbe essere condotto indipendentemente, più di frequente di tutto il processo di analisi del rischio);

- adeguatezza: la valutazione del rischio non può portare alla definizione di strumenti e policy di sicurezza incomprensibili per la cultura aziendale che, altrimenti, non sarebbero rispettivamente utilizzati e seguite;

- rapidità: i risultati dell'analisi devono essere disponibili in tempi utili per poter procedere alla fase di implementazione del sistema di sicurezza o del suo aggiornamento.