Sicurezza

[*Di questi tempi si parla sempre più frequentemente di sicurezza o security in campo informatico e spesso anche in modo non appropriato. Il sottoscritto, dopo avere subito una serie di attacchi via internet e dopo essersi visto espropriare il firewall da ignoti ha affrontato il tema in maniera formale e quelle che seguono sono alcune considerazioni derivate da quest'esperienza.*]

Quando ho iniziato a scrivere quest'articolo volevo dargli un taglio molto "pratico" ma rileggendolo mi sono reso conto che l'argomento richiedeva un'introduzione e delle premesse iniziali. Spero quindi che il risultato non Vi sia noioso, ma credo che i concetti espressi non siano poi così ovvi a tutti.

Leggendo vari articoli sulla sicurezza e sentendone così spesso parlare ho avuto la netta impressione che oggi giorno questo termine stia assumendo la stessa valenza che, nel tempo, ho visto assumere a termini come multimediale, in altre parole dei vocaboli utilizzati in maniera vaga e inadeguata allo scopo di "vendere" prodotti o soluzioni. Non a caso molte delle persone da me contattate sull'argomento mostravano una pura e semplice volontà/capacità di installare un firewall a prezzi più o meno adeguati.
E` molto importante avere chiaro che il termine sicurezza non si risolve né in termini di oggetti come un firewall né in termini di decreti più o meno adeguati.
La sicurezza è, un modus operandi che, tramite delle regole accettate da tutti coloro che ne sono coinvolti, permette di arrivare a delle situazioni che l'azienda definisce sicure e può arrivare a stravolgere l'operatività e i flussi documentali dell'azienda stessa.
E` importante tenere presente che è impossibile implementare alcuna politica di sicurezza (policy) se non viene deciso che cosa viene protetto e da chi. Sicuramente ci sono alcune tipologie di dati che sono considerati oggettivamente riservati e che vanno tutelati per legge (DPR 675/96, ecc.). Aldilà di questi non sempre ciò che, in un'azienda, viene considerato un dato da proteggere, ha la stessa valenza in un'altra azienda. Inoltre si deve considerare che alcune informazioni, a volte, sono da difendere solo rispetto all'esterno dell'azienda, ma devono circolare liberamente all'interno della stessa in quanto possono rappresentare delle procedure di lavoro o di comportamento che devono essere comuni a tutti i membri dell'azienda stessa. Da qui la necessità di molto buon senso: sicuramente si deve avere sufficiente paranoia da desiderare di difendere i propri dati da accessi non consentiti; ma è anche necessario tanto buon senso per capire quando determinate misure di sicurezza sono eccessive o addirittura dannose.
E` necessario,quindi, stendere un elenco, di che cosa viene considerato disponibile e che cosa viene considerato protetto in base al quale prendere ogni decisione sulla security. La policy dovrebbe decidere, inoltre, quale atteggiamento prendere nei confronti delle violazioni alle normative stese. Gli argomenti da considerare per la stesura di tale elenco dipendono interamente dalla definizione aziendale di "sicurezza". Ci si dovrebbe essenzialmente chiedere:

- Come l'azienda classifica i dati in confidenziali o sensibili?
- Il sistema contiene informazioni confidenziali o sensibili?
- Da chi ci si sta cercando di difendere?
- C'è reale necessità di accessi remoti al sistema?
- Un sistema di password o cifratura può essere sufficiente come protezione?
- Si necessita dell'accesso a Internet?
- Quanto deve essere accessibile il sistema da Internet?
- Quale azione verrà intrapresa in caso di scoperta di violazione di sicurezza?

Qualsiasi policy dovrebbe essere un compromesso fra l'usabilità dei dati e la necessità di proteggerli e deve tenere conto della fiducia concessa al personale aziendale. Risulta inoltre inutile qualsiasi soluzione tecnica se in precedenza il personale non viene preventivamente educato alla sicurezza e tale processo potrebbe richiedere una modifica dell'operatività per alcuni settori. Una cosa che spesso si trascura in fase di analisi è che non tutte le informazioni sono registrate su supporto elettronico e che spesso sono proprio le informazioni cartacee le più facili da interpretare. Ha poco senso quindi installare un buon firewall in azienda e poi permettere che gli impiegati gettino copia stampata del bilancio o dei progetti senza avere passato i fogli in una macina-carta.

Chiaramente nell'analisi che segue cercherò di focalizzare in particolare le problematiche legate al trattamento elettronico del dato tralasciando i dettagli riguardanti la parte cartacea.

Cominciando a rendere concreto il discorso, quindi, il primo passo da fare durante un'analisi di sicurezza è

a) l'individuazione e la classificazione delle risorse da difendere

sarà dunque opportuno creare un elenco di tutte le tipologie di documento/dato gestite in azienda e, a fianco di ogni voce, indicare dove risiede fisicamente: in quali calcolatori, in quali unità di backup e se ne esiste una copia cartacea. Si compila l'elenco completo delle basi dati, delle persone responsabili al trattamento di tali dati, dei destinatari dei dati e della "profondità di accesso ai dati stessi". Una cosa spesso dimenticata è l'opportunità di elencare eventuali linee di comunicazione/tragitti fisici coinvolti durante il trasferimento/manipolazione dei dati. Non di rado, infatti, è il mezzo trasmissivo ad essere oggetto di intercettazione.

Dopo avere individuato che cosa va difeso e da chi va difeso si passa ad analizzare chi e come potrebbe trafugare, rovinare o rendere indisponibile il dato. Tale fase è

b) l'individuazione dei rischi

si elencano quali sono i rischi logici e fisici che potrebbero rendere indisponibile il dato per esempio:
debolezze vulnerabilità dei sistemi operativi dei calcolatori in cui risiede il dato
debolezze del database contenente il dato
accessibilità al furto fisico
deterioramento fisico nel tempo del supporto che contiene il dato (è ormai noto che i nastri tendono a smagnetizzarsi ed i cd a perdere la leggibilità)
possibilità di intercettazione del dato lungo le linee di trasmissione
guasto del calcolatore (un alimentatore non ridondante, una motherboard o un controller che si guastano possono renderlo indisponibile)

Segue **c) l'individuazione delle responsabilità**

non solo nel senso inteso dalla legge (ovvero di chi è la colpa nel caso in cui...) ma cercando di capire chi è responsabile dell'integrità e disponibilità del dato. Rendendo noto a tutti chi è il responsabile di un dato si riducono i tempi e si migliora la qualità dell'intervento di ripristino qualora esso divenisse necessario. Questa individuazione è sicuramente molto facile in una piccola azienda ma in una grossa realtà richiede un'analisi dei flussi documentali e delle procedure informatiche che coinvolgono tale tipo di documento/dato.

Si deve quindi passare

d) all'analisi delle contromisure

Si provvede alla classificazione delle aree aziendali e, nei casi più drastici, ad applicare una riduzione della mobilità in modo da garantire che le persone non sconfinino dall'area a loro assegnata. Per applicare tali misure chiaramente si rende necessario un sistema di sorveglianza.
Si devono prevedere sicuramente un sistema antincendio e un buon piano di ripristino per fare fronte a disastri fisici. Si dovranno implementare (eccole finalmente) delle difese antivirus e dei firewalls ed eventualmente una cifratura delle trasmissioni (VPN).
Sarà necessario migliorare la sicurezza delle workstation cercando dei sistemi operativi realmente protetti da password (colgo l'occasione per ricordare che MS Windows 3.x e 9.X non offrono di fatto nessuna protezione tramite password) Bisognerà applicare le dovute patch ai S.O. /programmi in accordo con quanto segnalato nei vari siti o bollettini sulla sicurezza.

Alla fine di tutto questo è opportuno ricordarsi che la creazione di una situazione sicura non è un processo statico ma un'operazione continuata nel tempo. Si devono quindi mettere in bilancio una serie di attività di mantenimento che hanno oltre tutto una certa onerosità soprattutto in termini di ore lavoro. Non si deve dimenticare

- una verifica periodica e cancellazione degli UID non più validi
- una verifica giornaliera dei log dei programmi
- le attività legate alla gestione degli accessi e alla modifica periodica delle password
- la verifica periodica dei backup e test di ripristino (ho visto sistemisti in lacrime di fronte ad un nastro irrecuperabile)
- la lettura costante dei bollettini di sicurezza e l'applicazione delle patch ai programmi

oltre a ciò bisogna pensare che il pirata informatico è anch'esso un beneficiario della costante crescita tecnologica dei PC e dei software e quindi può sfruttare tale potenziale per i suoi fini (basta pensare agli algoritmi di protezione ormai divenuti inutili di fronte al numero di tentativi di breack per ogni unita di tempo che sono possibili grazie alla accresciuta potenza delle CPU). Non si deve perciò trascurare di aggiornare costantemente i propri sistemi allo stato dell'arte delle soluzioni.

Tutte queste considerazioni crollano di fronte alla disponibilità economica di un'azienda che chiaramente non può dilapidare il proprio patrimonio per la difesa informatica. Il limite logico è che il costo della difesa del dato non deve essere maggiore del valore (diretto o indiretto) del dato stesso. E' pertanto utile già nella fase iniziale una valutazione costo beneficio che ponga la perdita del bene, o indisponibilità, contro il valore dello stesso. Ne emergerà una cifra da tradurre in budget disponibile per la difesa del dato.

di Rudi Giacomini Pilon

Referimenti:

1. D.P.R. 675/96 tutela delle persone e altri soggetti rispetto al trattamento dei dati personali. (Gazzetta Ufficiale n.107 del 10/05/1997)
2. Linee Guida per la definizione di un piano per la sicurezza... (AIPA - www.aipa.it)
3. Linux Security How-to
4. Securing and optimizing Linux: by Gerhard Mourani