Sicurezza informatica: ottenere il livello ottimale con una politica di gestione che punti sull’utente

Author : Salvatore Lombardo

Date : 30 maggio 2018

La messa in pratica di una strategia tale da garantire la sicurezza informatica di un sistema informativo si complica quanto più estesa risulta la rete aziendale. Per questo motivo è necessario definire un’adeguata gestione della sicurezza ICT (Information and Communication Technologies), che individui il rischio e le vulnerabilità del sistema, e che definisca le contromisure da adottare in caso di manifestazione di un evento di pericolo.

In tal senso, non si può prescindere dal non ricorrere ad un approccio basato sull’analisi del rischio, secondo quanto stabilito dallo standard ISO/IEC 27001.

Questa norma internazionale definisce i requisiti per impostare e gestire un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) e consente di analizzare la problematica sotto i punti di vista della sicurezza logica (protezione dei dati e delle informazioni), fisica (protezione delle persone e delle risorse) e organizzativa (politica del Personale).

Di seguito tratterò alcuni aspetti.

1. *Il ruolo dell’Amministratore di rete e la cultura della sicurezza informatica*
2. *Il livello di sicurezza informatica ottimale*
3. *La continuità operativa dei servizi*

Il ruolo dell’Amministratore di rete e la cultura della sicurezza informatica

La politica di sicurezza, riguardando tutti gli utenti del sistema, deve essere elaborata partendo dalla direzione dell’organizzazione interessata. Poiché i responsabili dirigenziali, in genere, non hanno competenze tecniche, l’amministratore di rete deve essere l’intermediario della comunicazione tra la dirigenza e gli utenti ed il punto di riferimento riguardo ai problemi e alle raccomandazioni della sicurezza ICT.

Il ruolo dell’Amministratore è quello di assicurare che le risorse informatiche e i permessi di

accesso siano coerenti con la politica di sicurezza definita, di mettere a conoscenza la dirigenza sulle informazioni riguardo alla sicurezza, e di consigliarla sulle strategie da attuare.

Il segreto principale per il successo di una politica di sicurezza è quello di riuscire a fornire agli impiegati, in quanto utenti del sistema informativo dell'organizzazione, una buona conoscenza delle regole attraverso delle azioni di sensibilizzazione e spesso anche di alfabetizzazione.

Gli ultimi fatti di cronaca riguardanti gli attacchi informatici rilevano infatti che la prima fonte di incidenti relativi alla sicurezza informatica è rappresentata dalla scarsa consapevolezza del rischio da parte delle vittime che cadono nelle trappole appositamente allestiste dai cyber criminali.

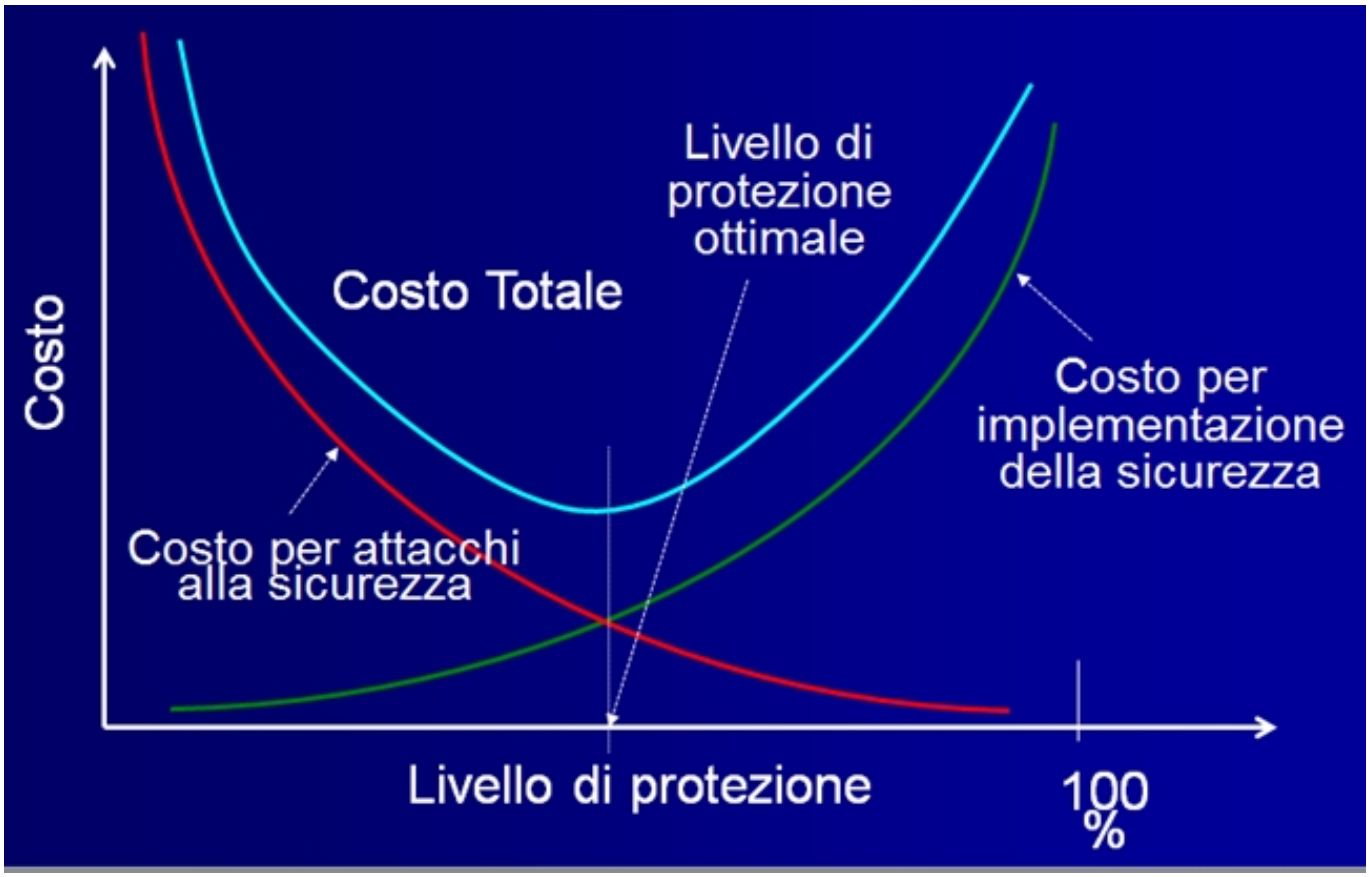
Risulta quindi di fondamentale importanza che le strutture amministrative diffondano al proprio interno una vera e propria cultura della sicurezza informatica, aiutando i centri di elaborazione dati nell'azione di prevenzione e difesa dalle potenziali minacce.

In quest'ottica sarebbe buona norma fornire consigli utili per la salvaguardia e la riservatezza delle informazioni sensibili. L'applicazione delle buone regole comportamentali in tema di sicurezza informatica può infatti diminuire le vulnerabilità ed essere d'ausilio a quelle tecniche convenzionalmente utilizzate per la protezione hardware/software (antivirus, firewall etc.).

Il livello di sicurezza informatica ottimale

Nelle fasi preliminari dello studio di un piano di sicurezza, un aspetto indispensabile, al fine di ottenere il massimo rendimento possibile con il minor costo, è la determinazione del livello ottimale del livello di sicurezza. Esso corrisponde al costo minimo totale, necessario a garantire un compromesso tra il costo per l'implementazione di un dispositivo di sicurezza efficiente e il costo relativo alle conseguenze di un attacco informatico.

Quanto detto è verificabile dal diagramma cartesiano *costo-livello di protezione* di figura, che di seguito si commenta.



Il costo per l'implementazione della sicurezza aumenta all'aumentare del livello di protezione (**curva verde**), mentre diminuisce di pari passo quello relativo alle conseguenze degli attacchi alla sicurezza (**curva rossa**). Il costo totale è rappresentato dalla curva superiore (**curva celeste**), ottenuta dalla somma punto per punto delle due curve precedenti. Nel punto più basso della curva somma si ottiene il minor costo possibile, a fronte di un livello ottimale di sicurezza. Per una corretta valutazione è di fondamentale importanza che le curve per ogni tipologia di costo si calcolino tracciando sul diagramma *costo – livello di protezione* l'insieme dei punti dati dalla serie storica dei dati disponibili. Maggiore sarà il numero di punti a disposizione, maggiore sarà l'attendibilità della curva del costo totale dato dalla somma dei due andamenti.

La continuità operativa dei servizi

Il piano di continuità operativa è il documento guida principale per le azioni da intraprendere nelle condizioni d'emergenza al fine di garantire la continuità dei servizi di una infrastruttura informatica, la cui stesura deve valutare opportunamente i costi e i rischi che un fermo attività può comportare.

Gli eventi che potenzialmente pregiudicano l'operatività dei servizi possono essere sommariamente raggruppati nel modo seguente:

- guasti elettrici, allagamenti, incendi;

- danneggiamento di strumenti hw/sw;
- errore umano;
- interruzione di servizi causa virus, introduzione involontaria di codice malevolo etc.

Pertanto, sarebbe auspicabile che tale piano venisse:

- recepito da tutto il personale;
- aggiornato periodicamente in funzione anche della continua evoluzione del settore ICT;
- adattato ad ogni possibile variazione subita dalla politica di sicurezza dell'amministrazione.

In ogni caso occorre tenere in considerazione per ridurre al minimo i danni causati dall'interruzione di un servizio, sia il tempo necessario per il ripristino dell'infrastruttura informativa che la distanza temporale che intercorre tra lo stato in cui il sistema si trovava prima del blocco e lo stato in cui viene ripristinato.

Quest'ultima prerogativa può essere garantita migliorando la ridondanza dei dati residenti su quei sistemi di riserva, solitamente remoti, pronti al subentro in caso di blocco del sistema principale. C'è da precisare che, in concomitanza con la fase di realizzazione della continuità operativa, deve essere studiata anche un'adeguata procedura di collaudo, per la verifica della validità delle soluzioni adottate. I risultati così ottenuti potranno dare un prezioso contributo per delineare una politica ottimale di Business Continuity.

Considerazioni finali

Purtroppo, per ovvi motivi, come per la sicurezza fisica nella vita reale, non è possibile garantire una sicurezza informatica assoluta, ma possiamo almeno, adottando anche delle regole di buona pratica, attenuare il rischio di esposizione alle minacce informatiche.

Penso che per raggiungere questo obiettivo sia fondamentale la collaborazione di tutti.

A tal proposito mi piace citare lo scrittore statunitense Robert Orben: *Errare è umano e dare la colpa al computer lo è anche di più*. Con questo intendo dire che nella gestione della sicurezza informatica l'approccio dell'uomo riveste un ruolo fondamentale.

Il compito di noi addetti ai lavori e di coloro che conoscono le tecnologie ed i rischi connessi al loro uso per incrementare in maniera sensibile il livello di sicurezza dovrebbe essere quello di mettere le nostre competenze al servizio della collettività ponendo gli utenti al centro del processo di prevenzione ed attenuazione del rischio.

Tutti gli accorgimenti e le soluzioni hardware e/o software sono necessari ma non sufficienti a garantire da soli la totale protezione dei sistemi informativi. Bisogna puntare sul continuo aggiornamento riguardo alle vulnerabilità degli strumenti di comunicazione telematica, alle nuove tecniche di attacco e alle possibili contromisure da adottare, allo scopo di diffondere una cultura digitale che consideri l'utente non finale ma punto centrale.

Sitografia

- https://it.wikipedia.org/wiki/ISO/IEC_27001
- https://it.ccm.net/contents/833-introduzione-alla-sicurezza-informatica
- https://it.safeandsavvy.f-secure.com/2015/12/04/sicurezza-informatica-dipendenti-attenzione-pericolo/

A cura di: **Salvatore Lombardo**