La Security Metrics:
misurare per conoscere, conoscere per gestire e prevenire.

- Published on May 23, 2018

Federica Mazzoleni

queste domande prende spunto il presente articolo, che mira a fornire una risposta a tale interrogativo e ad indagare da dove nasce l'esigenza di misurare nell'ambito della Sicurezza.

Già alla fine dell'800 era chiaro che una comprensione profonda di un fenomeno non poteva prescindere dalla sua misurazione.

"Quando puoi misurare ciò di cui stai parlando, ed esprimerlo in numeri, puoi affermare di saperne qualcosa; se però non puoi misurarlo, se non puoi esprimerlo con numeri, la tua conoscenza sarà povera cosa e insoddisfacente: forse un inizio di conoscenza, ma non abbastanza da far progredire il tuo pensiero fino allo stadio di scienza, qualsiasi possa essere l'argomento" (Lord Kelvin, 1883).

La misurazione si pone, quindi, come passo fondamentale nel processo di consolidamento della conoscenza di ogni materia, compresa, quindi, quella della Sicurezza.

La Metrics è quel processo di misurazione che non si focalizza su meri numeri, ma che si spinge oltre, misurando le performance di un processo e, nello specifico, la Security Metrics può essere definita come un insieme di misurazioni quantitative di aspetti identificabili delle attività di Sicurezza (Campbell, 2011).

Affinché la Security Metrics che si intende costruire non rimanga un conteggio privo di valore, ma costituisca una robusta base per le valutazioni del business, è necessario che essa sia SMART (Niehaus, 2014):

- Specifica, che indirizzi performance determinate;

- Misurabile, basata su dati precisi e completi;

- Attuabile, che sia di facile comprensione e che sia di aiuto nel capire quando e come agire;

- Rilevante: che misuri qualcosa di grande importanza per il raggiungimento degli obiettivi di business;

- Timely (puntuale), che i dati siano disponibili e accessibili in tempo utile.

La fondamentale differenza tra le performance di una qualsiasi delle attività che costituiscono il business di un'organizzazione e le performance della Sicurezza è che le prime tendenzialmente si esprimono e misurano in termini di ricavi, mentre le seconde di riduzione dei costi e/o delle perdite. Infatti, gli investimenti in ambito Sicurezza raramente generano un profitto economico, ma incrementano il business value in altri modi non meno cruciali, ad esempio riducendo le possibilità del verificarsi di incidenti di sicurezza, limitando i danni degli stessi o facilitandone e velocizzandone la soluzione (ISACA Journal, 2015).

In un contesto complesso come quello della realtà aziendale moderna, se non si misurano concretamente i risultati ottenuti attraverso le azioni e soluzioni implementate, risulta impossibile dimostrare il valore aggiunto apportato al business dal sistema sicurezza.

È qui che entra in gioco il RoSI, l'indice sul ritorno degli investimenti di sicurezza, che si misura come segue (SEC, 2006): RoSI : (Esposizione al Rischio % Rischio mitigato – Costo della soluzione)/Costo della soluzione Il RoSI fornisce un riscontro quantitativo e quindi oggettivo di quelli che sono i benefici apportati dall'attività di Sicurezza a fronte del budget impiegato per la stessa.

Il grande vantaggio di esprimere il valore di una soluzione di sicurezza tramite il RoSI si riscontra nel fatto che esso è immediatamente comprensibile anche per il top management, abituato ad esprimersi in termini di ROI delle soluzioni. Esprimendosi in questi termini, quindi, si adotta il linguaggio tipico del business e ciò garantisce la trasparenza e l'efficacia dei risultati che si intendono comunicare.

Per quanto riguarda il costo della soluzione di sicurezza, quando ci si trova a dover valutare l'opportunità di affrontare tale spesa è necessario tenere in considerazione che il risparmio a prescindere dal costo (Saving Money Regardless of Cost – SMRC) non è sempre una strategia vincente (ISACA, 2015). È utile domandarsi "risparmiare sì, ma a quale costo?". Un incidente di sicurezza che si verifica a seguito di una non adeguata adozione di misure preventive può comportare perdite finanziare dirette e indirette, diminuzione della produttività, implicazioni legali, danno reputazionale e ciò dovrebbe avere un peso critico nel momento della suddetta decisione.

La sicurezza si rivela, quindi, un'attività strategica ai fini della Business Continuity. Per questo motivo è necessario che il top management sia coinvolto nel Security Management attraverso la partecipazione alla formulazione degli obiettivi da raggiungere e all'analisi dei risultati ottenuti, da cui deve necessariamente risultare un esame delle debolezze legate alle tematiche di Sicurezza e, quindi, un piano di risoluzione delle stesse. Quest'attività si inserisce perfettamente nella logica del Ciclo di Deming o Ciclo PDCA – Plan, Do, Check, Act. Secondo la stessa le attività critiche per il

business come, nel nostro caso la sicurezza, devono essere in primo luogo pianificate (Plan) affinché risultino strumentali al business e, quindi, implementate (Do) secondo le modalità stabilite. In seguito è necessario controllare (Check) l'efficacia delle stesse, affinché eventuali carenze, non conformità o punti di inefficienza vengano identificati con prontezza e si possa agire (Act) nel modo più consono ai fini della risoluzione degli stessi, garantendo il miglioramento continuo delle performance.

Oggigiorno il business richiede prontezza e velocità di decisione affinché si possa tenere il passo con le esigenze di mercato e anticipare i competitors. Grazie ad un impiego corretto di una Security Metrics robusta e di strumenti che rendano facilmente comprensibili e disponibili i risultati ottenuti, si garantisce che i dati rilevanti relativi alla sicurezza siano immediatamente accessibili e chiari, trasformando la Metrics stessa in uno strumento chiave per il processo di decision-making e di monitoraggio e miglioramento delle performance del business. Inoltre, le potenzialità di analisi offerte dallo strumento della Metrics, quando efficacemente sfruttate nonché inserite in un'ottica di lesson learned, permettono una conoscenza approfondita dei trend di esposizione al rischio della propria organizzazione, permettendo di prevenire il concreto manifestarsi di minacce e quindi salvaguardare il business stesso, con evidenti economie di scala.

Per qualsiasi informazione, si prega di contattare: operations@shielddefensiveservices.com; consulting@shielddefensiveservices.com

Fonti:

Lord Kelvin, (1883), PLA, vol. 1, "Electrical Units of Measurement" Journal of Research and Practice in Information Technology, Vol. 38, N.1, Febbraio 2006, The Security Executive Council (SEC)

Campbell G.K., (2011), "Measures and Metrics in Corporate Security", Security Executive Council Publication Series

Campbell G.K., (2011), "Enterprise Security Metrics: A Snapshot Assessment of Practice" Security Executive Council Publication Series

Niehaus G., (2014), "Case Study: Risk Management and Security Metrics at Boeing", Journal of Applied Risk Management and Insurance, vol.2 N.1

ISACA Journal, Vol. 1 2015