Information Security Performance

Uno slogan molto noto recita che ***è possibile migliorare solo ciò che si misura***. E’ chiaro quindi che la misurazione permette di comprendere meglio la gestione: occorre però istituire un processo aziendale organico e realmente integrato con gli altri processi aziendali, al fine di raggiungere gli obiettivi di misurazione e assicurare la convergenza delle misurazioni con i più generali obiettivi di business. Ogni organizzazione, sulla base dell’analisi del contesto organizzativo, dovrebbe quindi individuare gli indicatori pertinenti; dovrebbe raccogliere e validare i dati a supporto degli indicatori; dovrebbe rendere ricorrente il processo di misurazione e reporting. Queste attività sono del tutto indipendenti da un eventuale software di reporting già adottato dall’organizzazione. La strutturazione di un processo di misurazione delle performance, ha come indubbio risultato sia una maggior consapevolezza della reale direzione aziendale, sia il miglioramento della sicurezza delle informazioni. Nel presente articolo sono condivisi gli strumenti minimi per creare un primo set di indicatori, con particolare riferimento al mondo della sicurezza delle informazioni.

La scelta degli indicatori più utili dipende da diversi elementi e può essere guidata da tre dimensioni: **ambito**, **oggetto** ed **esigenza**.

Ambito di misurazione: il concetto di sicurezza delle informazioni, nelle sue proprietà di disponibilità, integrità e riservatezza, si può essenzialmente suddividere nelle sue componenti ***gestionale*** e ***tecnologica***. La somma di queste due parti si può ricondurre ad una visione di insieme che consente di avere il presidio dell’oggetto misurato.

Oggetto di misurazione: gli indicatori si basano su delle formule matematiche volte ad oggettivare aspetti che altrimenti potrebbero essere interpretati in modo soggettivo e non coerente. Queste formule dovrebbero individuare in modo inequivocabile i singoli elementi che concorrono alla misurazione.

Esigenza di misurazione: è pacifico che la misurazione non può essere fine a sé stessa e dovrebbe necessariamente essere supportata da una esplicita esigenza che trova fondamento nella formulazione degli obiettivi del business.

La definizione di uno schema di misurazione delle performance, affinché produca indicatori usabili e coerenti con gli obiettivi, dovrebbe tenere in considerazione che il sottostante processo debba essere organizzato su tre macro-fasi: monitoraggio, misurazione e valutazione delle performance. Lo schema seguente riporta una possibile definizione di ciascuna di queste tre fasi.



Figura 1: definizioni di Monitoraggio, Misurazione e Valutazione in ambito Information Security Performance

Il processo Information Security performance dovrebbe, inoltre, tenere in considerazione ulteriori aspetti. **Il metodo di monitoraggio, misurazione e analisi delle valutazioni**: per mantenere coerenza nel tempo, il processo dovrebbe mantenere lo stesso approccio alla misurazione sia in termini di input data, sia in termini di regole di calcolo della misurazione. L'istante temporale e, soprattutto, la **frequenza di misurazione**: indicatori diversi possono avere esigenze diverse di misurazione e reporting. Indicatori di sintesi possono essere misurati con cadenza annuale, indicatori di gestione con cadenza trimestrale e indicatori tecnologici potrebbero richiedere una frequenza mensile di misurazione. La frequenza di misurazione è determinata anche in funzione del

destinatario della misurazione stessa: in ottica piramidale, è facile intuire che un indicatore di sintesi può essere condiviso con il top management, un indicatore di gestione con il middle management ed un indicatore tecnologico con i professionisti informatici. I criteri di valutazione: definiscono delle **soglie** che permettono di valutare la bontà del risultato raggiunto rispetto gli obiettivi. È prassi diffusa definire i KPI con le consuete soglie "verde-giallo-rosso". Ogni organizzazione dovrebbe definire le proprie soglie di valutazione in funzione delle proprie priorità, risorse e contesto aziendale. Una proposta valida indipendentemente da tali considerazioni di contesto sarebbe fuorviante. Tutti questi elementi concorrono alla definizione di un indicatore, la cui importanza è tanto maggiore quanto più efficaci vogliono essere i risultati del processo di Information Security.

Nell'implementazione di questo processo è inevitabile imbattersi con aspetti operativi che vanno dalla raccolta dei dati necessari ai calcoli, fino all'automazione della misurazione. Tutti questi aspetti possono essere indirizzati solo dietro un esplicito *commitment* del top management che sponsorizzi le necessarie attività e chiarisca ruoli e responsabilità per eseguire le misurazioni, non tralasciando la congrua allocazione di risorse (umane, economiche e tecnologiche) necessarie per garantire il buon esito del processo.

Per raccogliere i dati è importante individuare gli attori aziendali che ne dispongono, i data owner, ed iniziare a fare misurazioni con un approccio che può anche essere "iterativo". La raccolta delle prime fonti dati sarà probabilmente incompleta o con dati non esaustivi, quindi sarà importante capire quali azioni saranno necessarie per avere dati completi in un formato usabile. Ad esempio, il "*Service Desk*", interno all'organizzazione o in outsourcing ad un fornitore esterno, è un interlocutore primario per indicatori riferiti ai

dispositivi assegnati ad utenti finali, mentre "*IT Operations*" è il punto principale di contatto per gli indicatori relativi all'architettura aziendale. "*L'Incident Manager*" è l'interlocutore di riferimento per gli indicatori relativi a ticket di servizio, eventi, incidenti e crisi. Per gli aspetti di conformità, la funzione "*Legal*" o "*Compliance*" sono certamente il primo contatto per la valutazione dei relativi indicatori.

La raccolta dei dati, che alimenta il processo di Information security performance, dovrebbe essere ricorrente al fine di garantire un presidio sull'oggetto misurato. **Assegnare** quindi la **responsabilità** del processo di misurazione complessivo ad un manager, **validare ownership** degli indicatori e loro frequenza di misurazione, **fissare** meeting di condivisione di risultati e, **soglie**, redigere un piano di miglioramento in caso di indicatori "rossi" con gli owner degli indicatori, sono esempi di azioni che possono supportare il raggiungimento degli obiettivi di misurazione e conseguentemente del processo di Information security performance. Eventuali incentivi, come premi di risultato, possono essere presi in considerazione al fine di stimolare il raggiungimento di determinati risultati ritenuti strategici per il top management.

Come anticipato in precedenza, la scelta degli indicatori può essere guidata secondo tre dimensioni. Le tabelle seguenti riportano alcuni esempi di definizione di un indicatore, specificando per ognuno di essi una possibile metrica di misurazione e valutazione.

Figura 2: esempi di indicatori descritti tramite tabella

Altri indicatori possono essere definiti, ad esempio, considerando il numero ed i giorni necessari per la gestione degli incidenti, il costo di gestione degli incidenti, i

sistemi correntemente sottoposti a backup, l’esercizio di test di disaster recovery, la frequenza di modifica delle password, il numero di sistemi con strong authentication ecc.

In conclusione, è possibile rimarcare come l’Information Security Performance sia un mezzo per migliorare la sicurezza delle informazioni aziendali. Il calcolo degli indicatori non deve essere fine a se stesso od all’implementazione di una nuova tecnologia, anche se fosse la moda del momento. Per evitare di investire tempo e denaro in misurazioni che non portano ad alcun miglioramento è fondamentale avere l’allineamento con gli obiettivi di sicurezza delle informazioni come perno centrale del sistema di monitoraggio, misurazione e valutazione.

E’ quindi più utile, per l’organizzazione, avere anche solo pochi indicatori, ma ben allineati con gli obiettivi di sicurezza, piuttosto che acquistare costose tecnologie da rendere giustificate con “montagne” di giornate di lavoro, perdendo il focus rispetto all’unica cosa che può contare: migliorare, in modo semplice se possibile, la sicurezza delle informazioni. Nel raggiungimento di questo macro obiettivo avere dipendenti o fornitori con competenze non improvvisate, costituisce un vantaggio oltre che un risparmio di tempo e denaro.

Articolo a cura di **Thomas Castagna** e **Luciano Quartarone**

L’articolo Information Security Performance proviene da ICT Security Magazine.

https://www.ictsecuritymagazine.com/articoli/information-security-performance/