Key Impact Indicator e Key risk Indicator per la cyber risk evaluation

Date : 12 febbraio 2016

Una delle principali sfide dell'Information Security risiede nella capacità di misurare correttamente e coerentemente il costo economico della non sicurezza. L'identificazione di metriche accurate e l'utilizzo di indicatori significativi assume un ruolo fondamentale dal punto di vista strategico in quanto: migliorano il processo di risk assesment, facilitano l'identificazione di vulnerabilità e consentono un monitoraggio costante dei rischi.

Affinché le metriche e gli indicatori si possano considerare efficaci essi devono poter essere ripetibili e significative a tal punto da poter alimentare uno storico degli assessment (utile a comparare l'efficienza delle contromisure adottate), del ritorno sull'investimento (in termini di mancate perdite) e dei danni (anche a livello forense).

METODOLOGIE PER LA MISURAZIONE DEI RISCHI E DELLE PRESTAZIONI

1. **Key Performance Indicator (KPI)**
   Uno dei principi fondamentali nella gestione dell'impresa è la misurazione delle prestazioni. Essa è fondamentale in quanto da una parte facilita l'identificazione dei gap tra le prestazioni attuali e quelle desiderate e dall'altra migliora il monitoraggio delle prestazioni aziendali. I Key Performance Indicator (KPI), quando scelti accuratamente, aiutano ad identificare precisamente e accuratamente dove è necessario intervenire per migliorare la performance aziendale.
   Un KPI è un tipo di metrica solitamente impiegata da un'organizzazione per valutare la propria prestazione generale o quella dei singoli processi e/o attività che la compongono. In particolar modo, i KPI vengono spesso impiegati nella misurazione delle attività di business ritenute più importanti e a sostegno dei processi critici o strategici dell'azienda.
   Generalmente i KPI:
   • Offrono una visione in tempo reale dell'andamento delle prestazioni dell'azienda su base giornaliera, settimanale o mensile;
   • Misurano i gap di prestazione tra le attività in atto e l'obiettivo strategico da

raggiungere;
• Possono essere utilizzati per valutare l’efficacia delle contromisure di rischio e di sicurezza implementate dal processo di risk management;
• Possono essere impiegati nella costruzione di dashboard interattive che consentano un analisi puntuale e sintetica delle performance organizzative, economiche e finanziare dell’azienda.

2. **Key Risk Indicator (KRI)**
   Negli ultimi anni i Key Risk Indicator sono stati al centro dell’attenzione nell'ambito del risk management. Il dibattito si concentra principalmente nell'identificazione della metodologia più appropriata per la valutazione, monitoraggio e riduzione del rischio aziendale. In questo contesto i KRI assumono un’importanza fondamentale in quanto si dimostrano utili: al monitoraggio dell’andamento del rischio nel corso del tempo, nell’offrire un segnale di avvertimento nel caso di maggiore esposizione ad un determinato rischio, nella pianificazione di azioni correttive o delle contromisure.
   Un indicatore si ritiene chiave “*if it serves a very important statement and does it very well*” (Davis, 2006). I KRI sono “*statistiche o misurazioni in grado di offrire una prospettiva riguardo il posizionamento della compagnia rispetto al rischio*”, tendono ad essere rivisti periodicamente per assicurare la corretta ed eterogenea valutazione del rischio e “*segnalano alla compagnia quei cambiamenti che possono indicare l’emergere di un rischio*” (Coleman, 2009).
   I KRI vengono utilizzati per misurare il livello di incertezza di un progetto o di un qualsiasi processo/attività. Considerando la criticità del tempo di risposta nella gestione del rischio, diviene palese l’importanza ed utilità dei KRI. Infatti, più velocemente viene rilevato un rischio, più è facile l’identificazione e l’implementazione delle misure necessarie a gestire la situazione e garantire la continuità operativa.
   Mentre l’identificazione e sviluppo di appropriati KRI necessita specifiche capacità ed expertise, il loro impiego facilita il monitoraggio del rischio e può diminuire drasticamente i tempi di risposta e di approntamento delle contromisure. Per questo motivo è fondamentale che la persona incaricata della gestione del rischio aziendale identifichi e sviluppi un appropriato set di KRI.
3. **Le differenze tra KRI e KPI**
   Avendo analizzato sia i KPI che i KRI diviene ora importante identificare le principali differenze tra questi indicatori. Come detto in precedenza i KPI si concentrano sulla misurazione delle prestazioni mentre i KRI si focalizzano sui rischi. Di conseguenza mentre i KRI possono offrire adeguati “early warning indicator” riguardo rischi emergenti, i KPI non possono essere usati per questa funzione in quanto misurano principalmente i risultati aziendali.
   In altre parole, i KPI indicano la distanza dal raggiungimento di un predeterminato obiettivo mentre i KRI rappresentano l’evoluzione del rischio aziendale e, quindi, la probabilità di successo nel raggiungimento degli obiettivi aziendali. I KRI, offrendo leading-indicator riguardo rischi emergenti, possono segnalare preventivamente il peggioramento di determinate prestazioni aziendali.
   Di conseguenza, se utilizzati congiuntamente ai KPI, facilitano e migliorano l’identificazione preventiva delle aree e processi di business che, per garantire la continuità del livello di prestazioni, necessitano un aumento di risorse ed energia.

UN APPROCCIO ALLA MISURAZIONE DEGLI IMPATTI: I KEY IMPACT INDICATOR (KII)

Nei paragrafi precedenti si è esplorato il ruolo ricoperto dai KPI e KRI all'interno della valutazione e monitoraggio dei rischi e delle prestazioni di un intero processo di gestione del rischio e delle contromisure adottate.

In questo paragrafo ci concentreremo su un aspetto chiave del processo di risk assessment: l'identificazione e misurazione degli impatti. Una valutazione erronea può influenzare negativamente la percezione, categorizzazione e classificazione dei rischi da parte del management. Ciò è ancor più significativo nel campo dei rischi informatici il cui impatto è inerentemente più difficile da valutare e prevedere. Le principali difficoltà sono, da un lato, una non chiara definizione di ciò che si vuol misurare e, dall'altro, l'assenza di un set di riferimento di indicatori di impatto.

Nel processo di gestione del rischio, un buon punto di partenza per la valutazione degli impatti è il momento in cui un'organizzazione stabilisce le strategie per raggiungere gli obiettivi strategici di business. A seguire, gli obiettivi operativi vengono stabiliti per ciascuna strategia.

Solitamente, in questo momento, una società dovrebbe definire le metriche per quantificare e monitorare gli obiettivi, la risk appetite[1] di partenza e la risk tolerance[2] nel cercare di raggiungerli.

Secondo la metodologia del COSO Enterprise Risk Management, se gli obiettivi operativi o le strategie non sono allineate con il livello di risk appetite, esse dovrebbero essere riviste dal management. Questo avviene quando il rischio associato ad una strategia eccede la risk appetite o quando il livello del rischio viene ritenuto troppo basso rispetto la risk appetite per raggiungere un dato obiettivo.

Le metriche degli obiettivi sono utilizzate per definire le soglie ed i rispettivi livelli di tolleranza al rischio.
Entrambi gli elementi, le metriche e le soglie, divengono utili sia nella valutazione degli aspetti che influenzano l'impatto del rischio che nello stabilire le linee che non devono essere superate da questo.

Valutare l'impatto significa definire il tipo di perdita in cui si incorre e trovare la giusta "unità di misura" per quantificarla nel momento in cui il rischio si palesa. Secondo la definizione data dallo standard ISO 31000:2009, l'impatto è una combinazione tra l'esposizione e le conseguenze, dove la prima è la misura in cui un'organizzazione e/o stakeholder è soggetta ad un evento, mentre la seconda rappresenta il risultato di un evento che colpisce gli obiettivi di un'organizzazione. Le conseguenze possono degenerare attraverso un effetto a catena ed avere sia degli effetti positivi che negativi a loro volta descrivibili qualitativamente o quantitativamente.

Pertanto è utile considerare sia metriche qualitative che quantitative quando si vanno ad

analizzare gli impatti dei rischi.
Solitamente, le principali categorie di impatto considerate sono:

- **Economico**: essa valuta l'effetto del rischio in termini di incremento dei costi o i minori ricavi per un'organizzazione. Questo criterio può essere applicato a tutti i rischi che colpiscono, in modo quantitativo, il fatturato di una società. Le soglie qui possono essere stabilite utilizzando i costi, i ricavi e i margini come punti di riferimento.
- **Mercato**: qui l'impatto è rappresentato dalla perdita di quote di mercato come conseguenza di un rischio legato all'incapacità di soddisfare i bisogni dei consumatori in termini di servizi o prodotti.
- **Reputazione**: questa categoria è spesso caratterizzata da scale di misura qualitative con le quali si valuta lo svolgersi di eventi che colpiscono l'immagine dell'organizzazione.
- **Vantaggio competitivo**: esso valuta l'impatto in termini di perdita da parte dell'organizzazione del vantaggio competitivo rispetto ai propri competitor.

Il Ponemon Institute è un centro di ricerca specializzato e punto di riferimento in questo campo: esso ha concepito una metodologia attraverso la quale quantificare il costo dei data breach a seguito di un attacco informatico. Innanzitutto il think tank ha fornito una definizione di "data breach" inteso quindi come un evento in cui un nome di una persona, una cartella clinica e /o una transazione finanziaria o una carta di debito viene posta ad un potenziale rischio, che sia in formato elettronico che cartaceo. In un loro recente studio[3], in collaborazione con IBM, essi hanno identificato tre principali cause di un data breach: un attacco criminale/malintenzionato, un errore di sistema o un errore umano. In base ai loro studi, i costi di un data breach possono variare soprattutto in relazione alle cause e alle misure di sicurezza al tempo adottate.

Per calcolare il costo dei data breach il Ponemon Institute adotta una metodologia di costing chiamata activity-based costing (ABC), già conosciuta e diffusa nelle pratiche del Project Management. Questa metodologia identifica le attività di progetto alle quali vengono assegnati dei costi in base al reale utilizzo. Per calcolare il costo medio di un data breach, essi raccolgono sia i costi diretti che indiretti sostenuti dall'organizzazione.

I costi diretti includono l'ingaggio di investigatori esperti (forensic), una linea per il supporto esterno diretto e la fornitura di abbonamenti gratuiti e sconti su futuri prodotti e servizi ai clienti danneggiati. Queste tipologie di costi sono collegate alle spese dirette sostenute per determinate attività (come ad esempio detection, response e recovery post incidente).

I costi indiretti includono invece sia le investigazioni e le comunicazioni interne che il valore della clientela persa ottenuto dal fatturato o dalla diminuzione del tasso di acquisizione clienti. Questi rappresentano il totale di tempo, di impegno e di altre risorse impiegate dall'organizzazione senza un esborso diretto. Infine, il Ponemon Institute considera anche il costo opportunità.

Questo viene definito come il costo risultante dalle opportunità di business perdute a seguito degli effetti negativi di immagine ottenuti dalla comunicazione dell'evento alle vittime (e quindi reso pubblico ai media). Esso può essere misurato attraverso il turnover della clientela esistente

e dal numero stimato di clienti che dimostreranno l’interesse a chiudere la relazione contrattuale a seguito dell’incidente informatico. Il Ponemon Institute ha inoltre definito i fattori che influenzano l’incremento o diminuzione dei costi di un data breach. Tra i primi: la perdita od il furto dei dispositivi, il coinvolgimento di una terza parte nella violazione, l’immediata notifica e coinvolgimento di consulenti esterni.

Tra i fattori che diminuiscono i costi compaiono: una forte organizzazione della sicurezza, la presenza ed applicazione sia di un business continuity plan che di un incident response plan e la designazione di uno Chief information Security Officer.

Considerato quanto finora detto, abbiamo provato ad avanzare una proposta di set di Key Impact Indicator che possono essere applicati agli aspetti informatici, organizzativi e fisici della sicurezza di un’organizzazione. Il nostro obiettivo è di identificare un set di indicatori di impatto che, a prescindere dalla natura del rischio, potrebbero essere impiegati per migliorare il processo di risk management. Inoltre, abbiamo identificato una serie di indicatori che possono essere facilmente quantificati economicamente e quindi facilitare il risk manager nel suo processo decisionale.

Di seguito la lista dei KII:

- Profit loss;
- EBITDA loss;
- Reputation damage;
- Emerging damage - legal expenditure;
- Incident handling cost (remuneration per days of skilled technicians);
- Mean Time To Repair cost (MTTR);
- Cost of unused people or unable to work (remuneration per days and machine stop);
- Cost of technologies or equipment to be replaced;
- Fines due to Service Level Agreement infringements;
- Economic value of the disclosure, unavailability and compromising of data/information;

Le metriche che potrebbero essere adottate per la misurazione di ciascun KII:

- Profit loss:
  - Importo al giorno
- EBITDA loss
  - Importo al giorno
- Reputation damage;
  - Ammontare quotidiano di citazioni su giornali, blog, post, ecc raccolti su canali social/siti web/media predefiniti;
  - Perdita di mercato / anno (mese)
  - Perdita di clienti / anno (mese)
  - Delta sulla percezione del brand sulla base di sondaggi.
- Emerging damage - legal expenditure;
  - Importo totale per evento (azione)
- Incident handling cost;

- Remunerazione / giorno di un tecnico altamente qualificato * totale di tecnici coinvolti * giornate.

- Mean Time To Repair cost (MTTR);
  - Remunerazione / giorno di un tecnico altamente qualificato * totale di tecnici coinvolti * giornate di MTTR
  - Costi non di HR per la recovery / giorno * giornate di MTTR
- Cost of unused people or unable to work;
  - Remunerazione giornate lavoro * tempo di arresto della macchina/ sistema
- Cost of technologies or equipment to be replaced;
  - Totale per apparecchiature/sistemi (inclusi costi di installazione + costi logistici) * numero di apparecchiature/ sistemi coinvolti.
- Fines due to Service Level Agreement infringements;
  - Totale delle penali / giorno per contratto * giorni di violazione * numero di contratti violati
- Economic value of the disclosure, unavailability and compromising of data/information;
  Importo del valore totale dei dati determinato in:
  - Costo totale per la riacquisizione dei dati persi;
  - Utile stimato sull'uso (se non precedentemente considerato) /year
  - Perdita di profitto a causa dei dati compromessi (se non precedentemente considerata) /anno
  - Sanzioni o danni causati dalla divulgazione (se non precedentemente considerata)
  - Perdita di mercato (se non precedentemente considerata)
  - Perdita di reputazione (se non precedentemente considerata) (rif. precedenti metriche reputazionali).

Il processo di valutazione, affinché sia completo ed efficace, dovrebbe tenere in considerazione anche l’impatto sulle altre organizzazioni causato dal disservizio. A tal fine, per ogni cliente dell’organizzazione “colpita” dovremmo replicare il calcolo dei KII escludendo i rimborsi (inclusi nelle penali previste dagli SLA). Infine, per ottenere una valutazione quantitativa ed il più possibile comprensiva degli aspetti dell’impatto di un rischio sul business, dovremmo sommare tutti i nostri KII stimati con il valore totale dei KII dei nostri clienti.

CONCLUSIONI

Questo articolo ha illustrato come l’utilizzo di KRI e KPI possa facilitare il processo di gestione dei rischi e delle minacce. Questi indicatori possono essere utilizzati come una base informativa su cui costruire un analisi dei rischi e delle minacce capace di individuare, sia ex-ante che expost, le migliori contromisure da adottare. Partendo da una chiara definizione della propensione al rischio dell’azienda e dei livelli di prestazione desiderati, monitorando i KRI e KPI, possiamo ridurre le incertezze, garantire i risultati e mitigare gli impatti negativi sull'azienda. Infine abbiamo visto come l’identificazione e l’utilizzo di KII possa facilitare l’analisi dei rischi e delle minacce migliorando l’accuratezza e la precisione con cui i possibili

impatti vengono calcolati.

BIBLIOGRAFIA

- Jonathan Davies, Mike Finlay, Tara McLenaghen, Duncan Wilsonm 2006, Key Risk Indicators – Their Role in Operational Risk Management and Measurement. Risk Business International Limited.
- Les Coleman 2009, Risk Strategies – Dialling up Optimum Firm Risk. Gower e-Book, Publishing, Burlington, USA.
- Ann Bostrom, Steven P. French, Sara J. Gotllieb 2008, Risk Assessment Modeling and Decision Support . Springer Publishing, Berlin.
- Aravind Immaneni, Chris Mastro and Michael Haubenstock 2004 , A Structured Approach to Building Predictive Key Risk Indicators p 42- 47, in Operational Risk: A Special Edition of The RMA Journal , The Risk Manager Association ,Journal {Available online at: https://subscriber.riskbusiness.com/InterestingReading/42-47.pdf 25/11/2014}.
- Ponemon Institute and IBM, 2014 Cost of Data Breach Study: Global Analysis, Benchmark research sponsored by IBM Independently conducted by Ponemon Institute LLC May 2014.
- ISO 31000:2009 – Risk Management.
- ISO ISO GUIDE 73:2009 - Risk Management Vocabulary.
- Scarlat, Emil, Nora Chirita, and Ioana-Alexandra Bradea. “Indicators and Metrics Used in the Enterprise Risk Management (ERM).” Economic Computation and Economic Cybernetics Studies and Research 2012: pag 5-18.
- University of California and U.S. Department of Energy, Oak Ridge Associated Universities, http://www.orau.gov/pbm/documents/overview/uc.html

NOTE

1. Risk Appetite is the amount and type of risk that an organization is willing to pursue or retain (ISO GUIDE 73:2009).
2. Risk Tolerance is the organization’s or stakeholder’s readiness to bear the risk after risk treatment in order to achieve its objectives (ISO GUIDE 73:2009).
3. Ponemon Institute and IBM, 2014 Cost of Data Breach Study: Global Analysis, Benchmark research sponsored by IBM Independently conducted by Ponemon Institute LLC May 2014.

A cura di:
Luisa Franchina
Michele Kidane Mariam
Federico Ruzzi

Articolo pubblicato sulla rivista ICT Security – Maggio 2015