



Analisi e gestione del rischio

ing. Daniele Perucchini
Fondazione Ugo Bordoni
dperucchini@fub.it



ISCOM e infrastrutture critiche



www.iscom.gov.it



Premessa

Prima di iniziare qualsiasi considerazione sull'analisi e gestione del rischio è opportuno evidenziare alcuni **presupposti** che caratterizzano il **sistema di gestione della sicurezza** che, se verificati correttamente, consentiranno di approntare un efficace sistema di protezione. Questi presupposti sono indicati in svariate normative internazionali, best practices, linee guida del Cnipa, etc.

(OCSE, ISO27001/17799, lo "Standard of Good Practice" dell'Information Security Forum, "Enterprise Risk Management", CobiT; ITIL, gli standard ITSEC e "CommonCriteria", le linee Guida del CNIPA etc).



Presupposti per la analisi e la gestione del rischio

1. Sensibilizzazione
2. Organizzazione e governo
3. **Analisi dei rischi**
4. Politiche e procedure
5. Costante monitoraggio e allineamento del sistema di protezione



3) Analisi dei rischi

L'analisi dei rischi è fondamentale per acquisire conoscenza delle minacce e delle vulnerabilità che incombono sull'organizzazione e per poter **dirigere sforzi e risorse** (per definizione limitati) a difesa delle aree più a rischio.



L'importanza dell'analisi dei rischi

- le reti sono sempre più complesse ed il loro modificarsi genera sempre nuovi rischi
- la tecnica di protezione è fortemente dipendente dal rischio relativo
- la protezione completa (a volte **eccessiva**) potrebbe implicare un utilizzo restrittivo e rallentato delle risorse
- i costi per implementare un livello di sicurezza che vada oltre il necessario o l'ottimale o che si estenda ad elementi a basso impatto, possono diventare **proibitivi** per la maggior parte delle organizzazioni.



Finalità dell'analisi dei rischi

- individuare quali siano le **minacce** informatiche a cui si è esposti
- individuare le **vulnerabilità** del proprio sistema informativo
- valutare **l'impatto** nel caso in cui le minacce si concretizzino
- definire ed implementare contromisure (tecniche, procedurali, organizzative) adeguate a **mitigare il rischio** con un impegno commisurato ai potenziali impatti
- accettare consapevolmente il **rischio residuo**



In altre parole

- In definitiva l'analisi dei rischi pone le basi perché si possano scegliere le contromisure **senza provare a indovinare**, e si possano bilanciare tali contromisure rispetto ai rischi e ai costi delle stesse.
- *Il processo di analisi dei rischi è richiesto, direttamente o indirettamente, da normative comunitarie e nazionali e dai principali standard di riferimento (Standard ISO 17799 - ISO27001, ISF Standard of Good Practice, CobiT ("Control Objectives of IT Governance" dell' ISACA), GMITS ("Guidelines for the Management of IT Security"))*



Elementi comuni

A prescindere dalla metodologia utilizzata, esistono molti elementi e passaggi del processo di analisi dei rischi comuni a tutte le metodologie:

- individuare, classificare e valorizzare i beni da proteggere
- individuare e valutare gli agenti ostili, minacce, vulnerabilità e il rischio
- definire quali minacce vanno fronteggiate e con quali contromisure (tecniche e non)
- calcolare il rischio residuo, valutarne i livelli accettabili e definire le contromisure che permettono di mantenere il rischio entro questi livelli.



Varie metodologie di analisi dei rischi

- Le metodologie esistenti in merito alla conduzione di un'analisi dei rischi sono molteplici e spesso si presentano con differenti obiettivi o caratteristiche, anche se si basano su alcuni concetti, elementi e passaggi procedurali comuni.
- Nessuna è particolarmente migliore dell'altra. Però è importante comprendere quale tipologia di approccio sia più idonea utilizzare.

Caratteristiche:

- livello di approfondimento dell'analisi
- modalità di assegnazione dei valori (sistema di misurazione dei rischi)
- ripetibilità e frequenza del processo di analisi.



Livello di approfondimento

Se si considera il livello di approfondimento con cui si conduce un'analisi dei rischi, essa può essere

- **concettuale**, quando è destinata al management ed è orientata all'organizzazione e ai processi
- **operativo**, quando è destinata allo specialista o al responsabile dei sistemi informatici, e orientata, quindi, alla singole tecnologie e al contesto, appunto, operativo.



Approfondimento concettuale

Una valutazione di tipo concettuale - ad alto livello - dei rischi consente

- di individuare il **profilo di rischio** a livello **strategico e organizzativo**
- di definire le minacce all'organizzazione e quindi individuare le **macro aree di criticità** o contesti di rischio su cui intervenire nel tempo
- di definire un piano di **interventi immediati** a livello di Organizzazione
- di definire la **politica generale della sicurezza**.



Approfondimento operativo

Un'analisi di tipo operativo è più orientata alla valutazione dettagliata e approfondita della sicurezza delle singole tecnologie, sistemi e specifici ambiti di rete e si prefigge di (ad esempio):

- comprendere le vulnerabilità, minacce e rischi a cui sono esposte le singole tecnologie e le informazioni trattate
- definire architetture e standard tecnologici di sicurezza
- proporre percorsi operativi per la correzione delle debolezze riscontrate

Modalità di assegnazione dei valori del rischio



Nello scegliere una metodologia è importante scegliere una metrica

- La misurazione di tipo **quantitativo** si basa su elementi monetari e statistici
- Le metodologie **qualitative** in generale non richiedono dati statistici, e si basano su una scala di valori (basso, medio, alto, vitale, critico). Tali approcci, apparentemente più superficiali e meno precisi, in realtà si rivelano spesso più onesti
- La metodologia **quantitativa apparente** ovvero **semiquantitativa** è un mix delle precedenti



Ripetibilità e frequenza del processo di analisi

A seconda della ripetibilità/frequenza del processo di analisi dei rischi, si possono distinguere le metodologie esistenti fra approcci **statici** e approcci **dinamici/continuativi**.



Gli approcci dinamici/continuativi

- non fotografano la situazione della sicurezza in un dato momento, ma danno gli elementi per analizzare e gestire **continuamente** e **dinamicamente** il rischio
- la valutazione e gestione dei rischi diventa parte integrante dei processi di implementazione, manutenzione e monitoraggio dei sistemi informativi
- comportano un **decentramento** in termini di responsabilità nella gestione dei rischi, con il coinvolgimento di tutte le funzioni aziendali a più livelli, e richiedono un mandato che parte dal **Top-Management** e che coinvolge tutta l'Organizzazione



Gli approcci statici

Gli approcci statici

- realizzano una fotografia dello stato attuale della sicurezza
- richiedono revisioni periodiche, con scadenze temporali diverse, a seconda del livello di profondità dell'analisi
- normalmente sono gestiti sotto la responsabilità di funzioni aziendali specifiche, in genere in ambito ICT (ICT Manager, Security Officer, Comitato per la Sicurezza, ecc.); quindi le altre funzioni aziendali sono coinvolte solo passivamente.



Tendenza attuale

La tendenza attuale rileva una sempre più crescente diffusione di approcci e modelli di analisi e gestione dei rischi di tipo **dinamico e continuativo**, orientati al business aziendale e integrati con tutte le restanti attività di analisi dei rischi aziendali (rischi operativi, di credito, finanziari, ecc.)



La gestione dei rischi

L'analisi dei rischi consente di definire le opportune contromisure da adottare. L'effettiva adozione delle contromisure, la gestione e il monitoraggio nel tempo dell'effettivo stato della sicurezza, costituiscono il **Sistema di gestione della sicurezza**



Sistema di Gestione della Sicurezza

L'effettiva salvaguardia della sicurezza delle informazioni attraverso un'attenta gestione dei rischi richiede la realizzazione di un adeguato **Sistema di Gestione della Sicurezza** (SGS) sviluppato secondo le tre dimensioni del problema:

- processi
- organizzazione
- tecnologie.



Sistema di Gestione della Sicurezza

Lo scopo fondamentale di un Sistema di Gestione della Sicurezza è, quindi, quello di attuare un ragionevole compromesso **consapevole** tra il **costo della sicurezza** e i **costi della non sicurezza** e il suo obiettivo principale consiste nel mantenere nel tempo uno stabile e ottimale livello di protezione.



Conclusioni

- Individuare le persone che devono gestire la sicurezza
- effettuare una adeguata analisi dei rischi
- adottare un sistema di gestione della sicurezza
- gestire i cambiamenti nel corso del tempo
- formazione di tutti i soggetti coinvolti (anche il Top Management)



Grazie

Daniele Perucchini
Fondazione Ugo Bordoni

dperucchini@fub.it