La Risk Analisys
L'approccio e le metodologie standard

ICTsystem
integration is now

Serie "Le MiniGuide" vol. 2406/2010

La Risk Analisys

Con questa Mini Guida si intende porre a confronto – seppure in maniera non esaustiva – le tecniche di analisi dei rischi standard con le metodiche proprietarie sempre più spesso sviluppate in maniera specifica e da esse derivate, per condurre attività di analisi dei rischi all'interno delle aziende, con l'obiettivo di evidenziare vantaggi e svantaggi dell'adozione di ciascuna.

L'analisi dei rischi: considerazioni generali

In generale, le metodologie applicabili per la conduzione di un procedimento di analisi dei rischi sono molteplici, spesso diverse tra loro per obiettivi primari e caratteristiche, ma tutte basate su elementi e passaggi procedurali comuni. Non è possibile affermare, ad oggi, che esista una tecnica migliore di altre, ma è piuttosto **dell'analisi**: si distinguono in quest'ambito un approccio concettuale importante comprendere quale sia l'approccio più idoneo al contesto, soprattutto con riferimento a:

- **livello di approfondimento** orientato all'organizzazione e un approccio operativo orientato al contesto tecnologico-infrastrutturale
- **modalità/criteri di assegnazione dei valori (sistema di misurazione) del rischio:** sono identificabili una misurazione di tipo quantitativo basata su elementi monetari e statistici, ed una misurazione di tipo qualitativo, basata sull'identificazione di macro-scenari di analisi
- **ripetibilità del processo di analisi:** si fa riferimento in quest'ambito ad approcci statici che realizzano una fotografia dello stato attuale della sicurezza e che richiedono revisioni periodiche, ed approcci dinamici che forniscono elementi per una gestione continuativa del rischio, inserendo la valutazione dei rischi come parte integrante di un qualsiasi processo di implementazione e manutenzione dei sistemi informativi.

Ciascuno degli approcci indicati e conseguentemente ciascuna delle metodologie standard note che a tali approcci si ispira (OCTAVE, CRAMM, …), presenta la sua indubbia validità. Ma ciascun approccio, quando non correttamente contestualizzato o contestualizzabile, può altresì introdurre considerevoli disagi, sino al punto di vanificare il risultato dell'analisi medesima.

Le più frequenti sorprese in senso negativo sono diretta conseguenza della complessità dei metodi di analisi, complessità che ne rende difficoltosa l'applicazione, ancor più in una realtà come quella italiana, caratterizzata da un tessuto economico fatto in prevalenza di medie imprese e da una cultura orientata a privilegiare più la creatività che il rigore metodologico.

Da un'attenta e valida comparazione delle diverse metodologie di analisi dei rischi effettuata qualche tempo fa dall'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione, è emerso da un lato, l'estremo rigore dei numerosi approcci che affrontano la problematica a tutto campo e con notevole livello di dettaglio; dall'altro, la complessità della loro applicazione pratica, primariamente nel settore PMI, al punto che alcune di queste metodologie sono state adattate proprio per ricavare un sottoinsieme di controlli orientati a contesti a minore complessità (es. OCTAVE).
Di fronte alla necessità di sottolineare le lacune macroscopiche di contesto per ottenere valido supporto dal top management ed avviare seri investimenti destinati al potenziamento dell'infrastruttura di sicurezza, il fatto di poter procedere all'analisi con tecniche ripetibili e rigorose, ma allo stesso tempo semplici e applicabili in tempi contenuti, costituisce senza dubbio un notevole vantaggio.

Per questa ragione, forse, sono emerse metodiche proprietarie semplificate che, pur ispirandosi ai dettami di noti standard internazionali (ISO 27001, ISO 15408, BSI IT Baseline Protection Manual, ecc.) si caratterizzano per la peculiarità di indirizzare, attraverso un procedimento di valutazione qualitativa, soltanto l'insieme dei processi di business ritenuti di maggiore rilevanza (strategici) o l'insieme degli asset (tecnologici e non) che detti processi supportano.

Si preferisce normalmente l'adozione di un metodo qualitativo di analisi che permetta di dare immediata evidenza agli scenari oggetto di investigazione e fornire una visione completa del quadro generale di analisi, rispetto ad un'analisi di tipo quantitativo che – se pure caratterizzata talvolta da maggiore precisione nelle valutazioni – spesso presenta enormi difficoltà nella rappresentazione oggettiva di rischi e potenziali perdite legati primariamente ad asset aziendali non tangibili (es. l'immagine dell'azienda).

Tali tipologie di analisi, in generale, presentano un approccio operativo focalizzato sull'ambito tecnologico-infrastrutturale (asset driven analysis) che prende in esame un sottoinsieme specifico delle componenti dell'infrastruttura ICT ed evidenzia per ciascuna di esse il livello di rischio al quale risulta esposta, con l'obiettivo ultimo di identificare le aree a maggior esposizione sulle quali intervenire.

Parallelamente a questo tipo di orientamento, inoltre, l'impostazione conferita alla tecnica di analisi si è posta l'obiettivo di identificare gli ambiti a maggior rischio tra quelli legati alla sicurezza fisica, logica, applicativa e organizzativa (fattore umano e/o meccanismi intrinseci di processo), evidenziando in questo caso, oltre all'insieme di criticità e correttivi puntuali determinati dal passaggio precedente, anche le aree più in generale meritevoli di ulteriori indagini.

Un possibile approccio metodologico

Schematizzando un possibile approccio metodologico potrebbe fare riferimento ai seguenti passaggi primari:

1. analisi preliminare di impatto, finalizzata alla caratterizzazione dei parametri di valutazione ai quali si farà riferimento per la successiva analisi di rischio;
2. identificazione degli asset primari;
3. identificazione degli ambiti di analisi e valutazione del rischio;
4. identificazione delle minacce che insistono sull'ambiente e sui contesti specifici;
5. identificazione delle contromisure esistenti, finalizzata all'attribuzione dei livelli globali di rischio;
6. analisi di impatto delle minacce sull'ambiente e sui contesti specifici;
7. valutazione dei rischi di esposizione alle minacce indicate per ciascuna componente dell'infrastruttura in esame;
8. identificazione degli ambiti di rischio a maggiore rilevanza, sia per ciò che riguarda gli elementi di infrastruttura tecnico-organizzativa da esaminare (componenti tecnologiche e organizzative – fattore umano), sia per quanto concerne gli elementi dell'infrastruttura stessa. (vedi Figg. 1 e 2 seguenti).

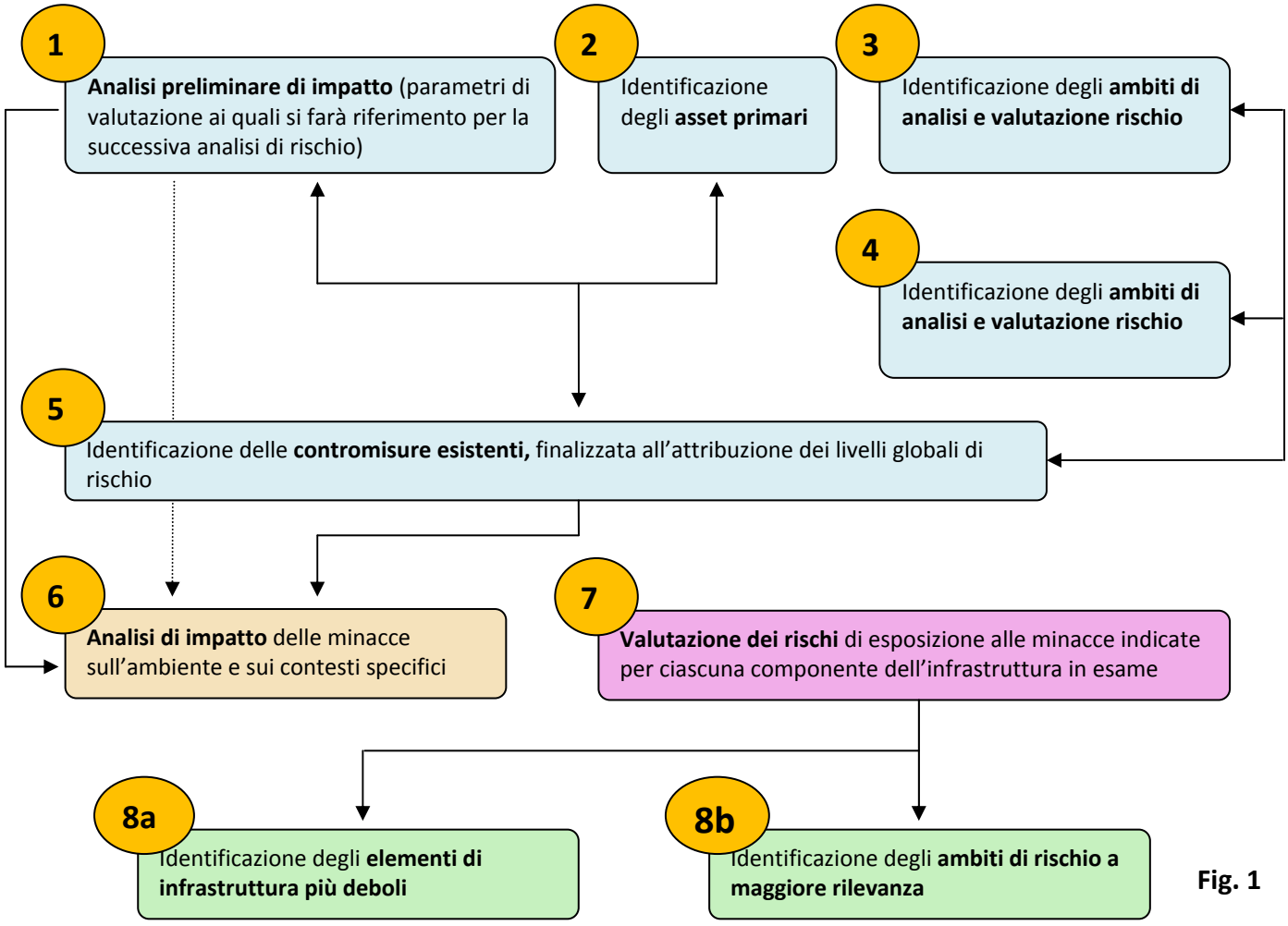

Fig. 1

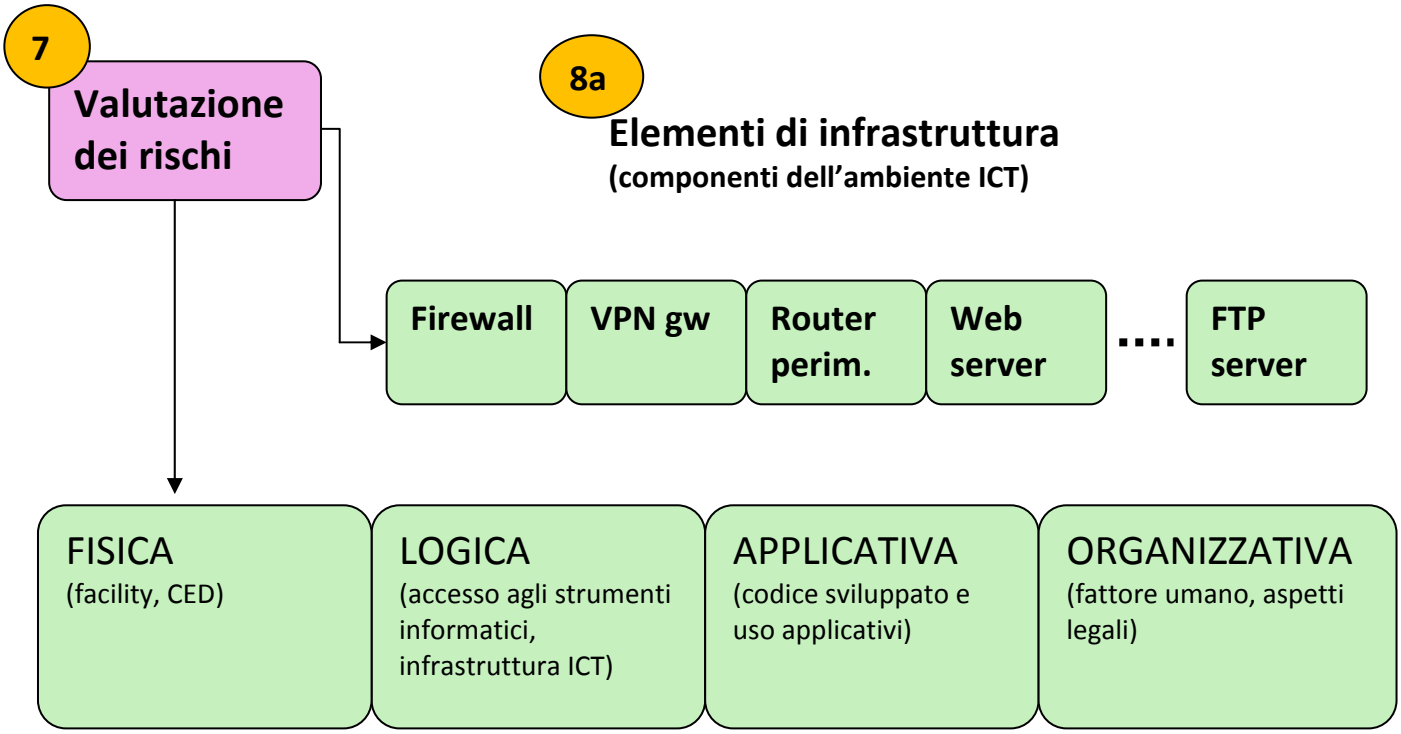

Fig. 2

I risultati conseguiti mediante tale procedimento di analisi dei rischi permette di studiare gli interventi correttivi concentrando l'attenzione su un set limitato di componenti infrastrutturali e con riferimento a contesti specifici, favorendo rapidità e semplicità nell'introduzione dei correttivi stessi, oltre che nella successiva gestione e revisione di tali misure.

La struttura del procedimento di analisi, inoltre, ha il vantaggio di consentire valutazioni e scelte immediate anche di fronte ad una eventuale molteplicità di soluzioni aderenti all'insieme dei requisiti indicati che si differenziano tuttavia per:

- **costo**: al crescere delle complessità e della qualità della soluzione adottata, anche la componente di costo evidenzia naturalmente una maggiore incidenza;
- **fruibilità**: variano gli elementi di automazione e facilità d'uso, spesso in diretta associazione con la componente di costo, dal momento che migliorie in tal senso richiedono la dotazione di strumenti tecnologici caratterizzati da maggiore sofisticazione;
- **completezza**: ciascuna soluzione, pur risultando in termini generali esaustiva rispetto ai requisiti – come si è detto – presenta caratteristiche tali da modificare l'entità dei rischi residui da gestire e si lega direttamente,

pertanto, alle politiche di risk management che l'azienda intende porre in essere.

Rispetto ai tre elementi citati, tale procedimento di analisi consente, infatti, proprio di dare risalto al legame di proporzionalità diretta tra l'investimento (costo) sostenuto e le garanzie di fruibilità e completezza della soluzione.
Gran parte della semplificazione ottenuta e della praticità del metodo descritto, sono il risultato dell'introduzione del passaggio n. 1, l'analisi preliminare di impatto, la quale si appoggia la concetto di macrodato, inteso come informazione in transito in ogni sua forma e associata ad uno specifico supporto.

Il core business dell'azienda in questione, infatti, è rappresentato dalla gestione di flussi informativi che costituiscono, come tali, il primo elemento di interesse per le valutazioni di rischio. In tal senso, quindi l'asset di riferimento è stata proprio l'informazione in transito (macrodato), per la quale si è ricercata la migliore modalità per la riduzione dell'esposizione ai rischi di compromissione e/o alterazione.

E' proprio seguendo il percorso dell'informazione nell'ambito dell'infrastruttura ICT ed esaminando le operazioni alle quali essa è soggetta è possibile identificare gli elementi infrastrutturali più deboli, così come i passaggi e gli ambiti di operatività maggiormente esposti a rischio. Il tutto, partendo dalla logica in base alla quale l'attribuzione delle probabilità di occorrenza (quantitative e qualitative) dipende dalle contromisure di protezione e prevenzione in essere al momento dell'analisi e dal valore che l'azienda attribuisce al macrodato – in termini di requisiti di riservatezza, integrità, disponibilità, autenticazione e non-ripudio. E' proprio quest'ultimo valore che può essere verificato mediante il criterio della valutazione preliminare di impatto, intesa come tipologia di danno alla quale si è soggetti nel caso di compromissione di uno dei requisiti indicati, e incidenza della perdita del requisito rispetto al danno globale previsto.

Osservazioni conclusive

Le considerazioni sin qui operate e il metodo illustrato permettono di conferire riconoscimenti ad una categoria di tecniche di analisi dei rischi (quelle proprietarie ricavate come semplificazione di passaggi procedurali derivati da tecniche standard "ufficiali") non sempre considerata per il valore reale che offre in fase operativa.

Resta naturalmente indiscutibile il riferimento generale alle metodiche standard più note e diffuse, ma è finalmente possibile affermare che, ogni volta che un contesto lo rende utile, opportuno o necessario, è possibile effettuare valutazioni di rischio anche con metodiche semplificate e sviluppate ad hoc, a patto – naturalmente – di chiarire sin dall'inizio il quadro operativo, i passaggi procedurali e gli obiettivi specifici che si intende raggiungere, facendo la massima attenzione all'obiettività e alla ripetibilità del processo attuato.