

La risk analysis tra metodologie standard e tecniche proprietarie (ICT Security - giugno 2007)

Con questo articolo intendiamo porre a confronto – seppure in maniera non esaustiva – le tecniche di analisi dei rischi standard con le metodiche proprietarie sempre più spesso sviluppate da società di consulenza e da security manager responsabili di condurre attività di analisi dei rischi all'interno della propria azienda, con l'obiettivo di evidenziare vantaggi e svantaggi dell'adozione di ciascuna. L'articolo nasce da una personale esperienza dell'autore effettuata presso AR Enterprise, società operante nel comparto dei servizi ICT per il mercato *finance* italiano, sia quale produttore di soluzioni software complete ed integrate per il mercato dell'intermediazione mobiliare, sia quale soggetto erogatore di servizi di *outsourcing e facility management* alla propria clientela.

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 importante comprendere quale sia l'approccio più idoneo al contesto, soprattutto con riferimento a:

- livello di approfondimento dell'analisi: si distinguono in quest'ambito un ***approccio concettuale*** 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, si diceva, 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.

Una valida comparazione delle diverse metodologie di analisi dei rischi viene fornita dalla sintesi dell'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione [1][2]: dalla lettura dei documenti emergono proprio, da un lato, l'estremo rigore di 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 in fase di "***adattamento***" 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, stanno emergendo 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 ¹, soltanto l'insieme dei processi di business ritenuti di maggiore rilevanza (strategici) o l'insieme degli asset (tecnologici e non) che detti processi supportano.

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.

Questo è proprio il tipo di approccio che ho ritenuto più corretto adottare nel corso dell'analisi dei rischi da me condotta, alla quale ho fatto riferimento in apertura.

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.

Il lavoro svolto, in sostanza, si pone l'obiettivo di conferire alla ricerca una valenza bidimensionale che tenga conto, da un lato, degli elementi di debolezza delle singole componenti di infrastruttura, e dall'altro, delle lacune di contesto legate alla tipologia e ai criteri di utilizzo dei supporti tecnologici disponibili in azienda.

Dal punto di vista della ripetibilità, poi, benché la tendenza attuale rileva una sempre maggiore diffusione di modelli dinamici, il criterio da me adottato è stato quello della staticità, nell'ottica di una semplificazione del governo delle procedure di analisi dei rischi che andasse incontro alle necessità aziendali della società di disporre di strumenti efficaci e al contempo governabili dal ridotto staff ICT impiegato.

L'approccio metodologico

Se dovessimo schematizzare l'approccio adottato nel corso del progetto citato in apertura, potremmo 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

¹ Si preferisce 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).

organizzative – fattore umano), sia per quanto concerne gli elementi dell’infrastruttura stessa – Figg. 1 e 2.

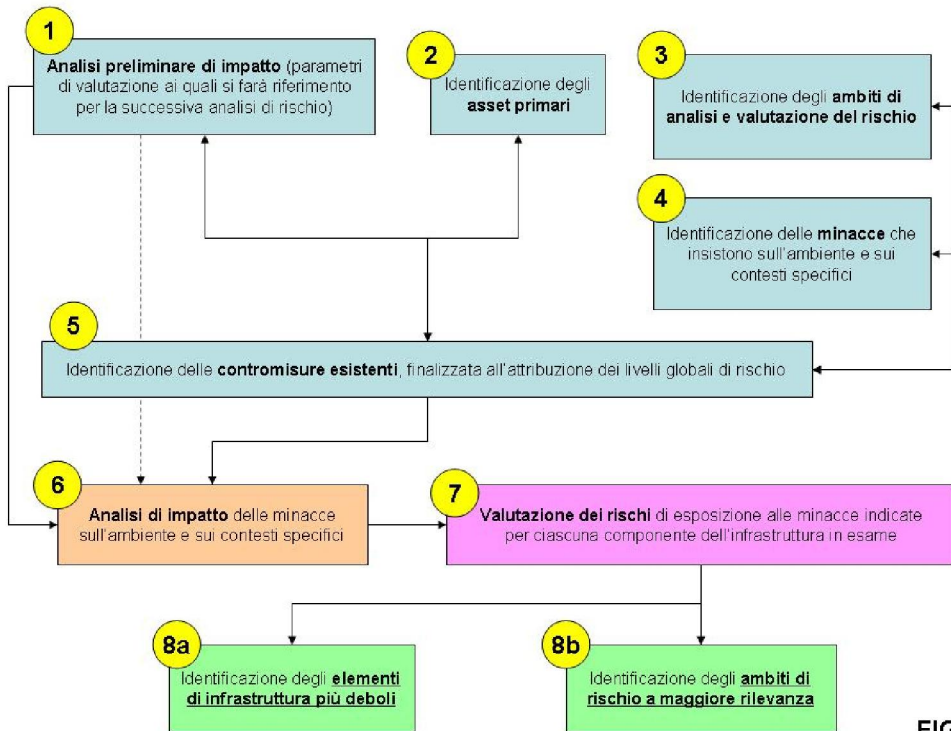


FIG. 1

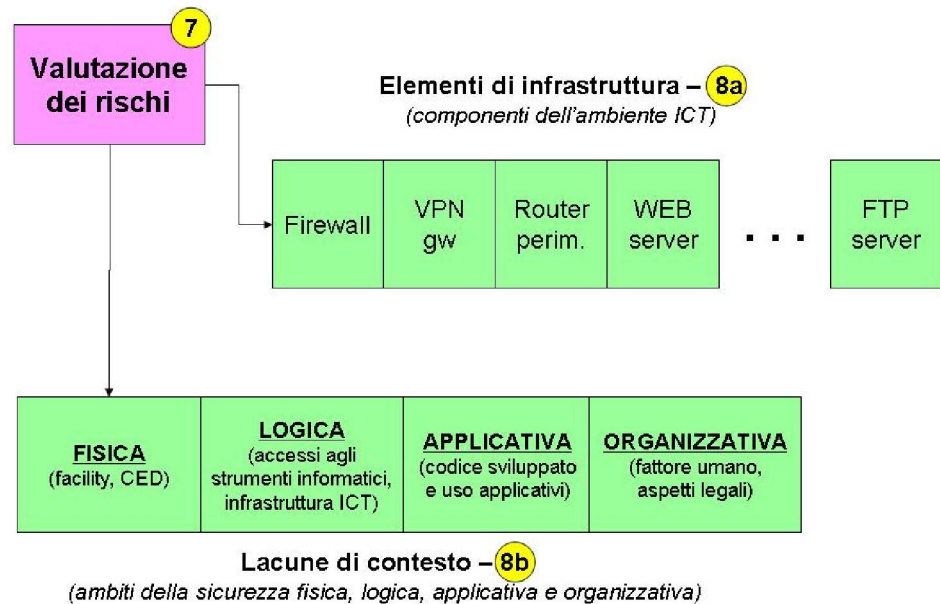


FIG. 2

I risultati conseguiti mediante il procedimento di analisi dei rischi adottato hanno permesso 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 (proprio come nel caso del lavoro svolto) 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 miglorie 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, il 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 al 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 che è stato 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 è stato 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 ci 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.

Riferimenti bibliografici

- [1] AA.VV. – ISCOM – La sicurezza delle reti - dall'analisi del rischio alle strategie di protezione – http://www.iscom.gov.it/documenti/files/news/pub_002_ita.pdf
- [2] AA.VV. – ISCOM – Risk Analysis: approfondimenti – http://www.iscom.gov.it/documenti/files/news/linee_guida_rischi_due.pdf
- [3] AA.VV., Introduction to the OCTAVE® Approach – http://www.cert.org/octave/approach_intro.pdf
- [4] How CRAMM works - <http://www.cramm.com/overview/howitworks.ht>
- [5] The Logic behind CRAMM's Assessment of Measures of Risk and Determination of Appropriate Countermeasures
<http://www.cramm.com/files/techpapers/CRAMM%20Countermeasure%20Determination%20and%20Calculation.pdf>
- [6] D. Bossi, E. Lando, M. Sem, S. Valerio – Il metodo PRO.FI.T.A.B.LE.: analisi dei rischi e identificazione delle misure correttive per la salvaguardia dei flussi dispositivi per il regolamento di operazioni su strumenti finanziari (tesi MIP – Corso Superiore di Formazione in Information Security Management – giugno 2006)