MASTER UNIVERSITARIO di II Livello

in

HOMELAND SECURITY

Università Campus Bio-Medico – Roma

Consorzio NITEL

Quality Solutions

PROJECT WORK ABSTRACT

QSRA: una metodologia di Risk Assessment per l'Information Security

Candidato: Dott. Gabriele Mandelli

Tutor: Dott. Alessandro La Daga

ABSTRACT

La scelta dell'argomento per la stesura dell'elaborato finale è stata fatta grazie al coinvolgimento operativo del candidato da parte di **Quality Solutions**, ovvero grazie alla partecipazione in affiancamento ad un intervento di consulenza sull'intero processo di certificazione dei Sistemi di Gestione della Sicurezza delle Informazioni (ISO/IEC 27001:2005). Da qui, dunque, la decisione di concentrarsi sul dominio dell'Information Security e di presentare la peculiare metodologia di Risk Assessment concepita ed applicata da Quality Solutions in questo ambito.

Dopo un **capitolo introduttivo** a spiegazione del progetto formativo intrapreso dal candidato, il **secondo capitolo** prende in esame i concetti di Risk Analysis e Risk Assessment, concentrandosi in particolare sulla loro applicazione nell'Information Security.

L'importanza della **sicurezza delle informazioni** deriva dalla loro diffusione e dal ruolo che occupano nella collettività in quanto i governi, gli apparati militari, le aziende, le istituzioni finanziarie, gli ospedali, ecc. ne accumulano un gran numero, di natura per lo più riservata, circa i loro impiegati, clienti, prodotti/servizi, ricerche/progetti e stati finanziari; la maggior parte di queste è accumulata, elaborata e immagazzinata in computer e, per mezzo della rete, trasmessa ad altri computer. Se esse dovessero cadere nelle mani di delinquenti o di competitor, oppure essere perse a causa di un evento accidentale, una simile perdita porterebbe a potenziali conseguenze negative di svariata natura; la loro protezione è dunque un'attività molto importante ed in parecchi casi anche un requisito legale e/o etico. Per questi motivi la **Risk Analysis** costituisce un elemento essenziale per assicurare che i sistemi di protezione progettati siano effettivamente coerenti con le minacce pertinenti e le relative probabilità di accadimento; essa è definita come la valutazione delle vulnerabilità proprie di un sistema rispetto alle diverse possibili minacce e prevedibili conseguenze del danneggiamento o distruzione dello stesso. L'elaborato ne illustra pertanto i core criteria e la formula mediante la quale viene tradizionalmente applicata:

$$R = f(M, V, C)$$

Passaggio fondamentale del capitolo è dunque la descrizione della norma ISO/IEC27001:2005, dedicata ai **Sistemi di Gestione della Sicurezza delle**

Informazioni (SGSI o ISMS, Information Security Management System): il suo obiettivo è proprio quello di proteggere i dati e le informazioni da minacce di ogni tipo al fine di assicurarne la confidenzialità, l'integrità e la disponibilità e di fornire i requisiti per l'adozione di un adeguato SGSI a supporto di tale obiettivo. L'elaborato illustra in seguito la norma ISO/IEC 27005:2011, riguardante la **gestione del rischio della sicurezza delle informazioni**: essa fornisce le linee guida per la gestione dei rischi nel dominio dell'Information Security all'interno di un'organizzazione, in accordo con i requisiti specificati dalla ISO 27001 sia per l'implementazione che per l'operatività di un SGSI. Nello specifico, per l'ottenimento di tali scopi, amplia le prospettive della Risk Analysis mediante il concetto di **Risk Assessment**: l'analisi dei rischi non viene considerata alla stregua di un metodo analitico che da solo fornisce gli elementi necessari per procedere allo studio dei rischi, ma come una fase integrata in un processo valutativo più strutturato, per l'appunto il Risk Assessment (composto da Risk Identification, Risk Analysis e Risk Evaluation). Lo standard in questione, però, non fornisce alcuna metodologia di trattamento del rischio; definisce, invece, il framework di un processo strutturato, sistematico e rigoroso che va dall'identificazione dei rischi alla creazione di un piano di trattamento degli stessi

Da questi concetti prende le mosse il **terzo capitolo** dell'elaborato, il quale presenta la metodologia standardizzata e documentata di Risk Assessment per l'Information Security di cui Quality Solutions ha deciso di dotarsi, seguendo le linee guida dela ISO 27005 in termini di passaggi logico/funzionali e struttura. La **QSRA** (Quality Solutions Risk Assessment) mira ad ottenere una valutazione dei rischi relativi ai processi aziendali inerenti l'SGSI, considerando sia il valore degli asset interessati che le minacce a cui sono esposti; di conseguenza permette anche di definire i criteri per stabilire quali contromisure applicare e per valutarne l'adeguatezza. La QSRA procede identificando:

- *Cosa deve essere protetto*, attraverso un'analisi funzionale e strutturale del contesto di riferimento;
- *Quanto deve essere protetto*, attraverso la stima del valore degli asset e delle relative vulnerabilità;
- *Contro chi o cosa ci si deve proteggere*, attraverso l'analisidelle minacce che possono causare danni;

- *Come proteggersi in maniera appropriata*, attraverso la definizione di specifici livelli di efficacia delle contromisure, sulla base delle esigenze reali e dell'esperienza pregressa sempre in ambito di analisi dei rischi.

L'elaborato ne illustra la formula mediante la quale viene applicata:

$$\mathbf{LR_{(i;j)} = P_i \ x \ A_j \ x \ V_{ij}}$$

dove:

- $\mathbf{LR_{(i;j)}}$ è il Livello di Rischio di un asset associato ad una specifica minaccia;
- $\mathbf{P_i}$ è la probabilità di accadimento della minaccia "i";
- $\mathbf{A_j}$ è la criticità dell'asset "j";
- $\mathbf{V_{ij}}$ è il Livello di Vulnerabilità dell'asset "j" rispetto alla minaccia "i".

Se consideriamo con attenzione il ruolo centrale che le informazioni ricoprono nel business dei nostri tempi, possiamo concludere che la QSRA, in quanto strumento capace di assicurare la protezione delle informazioni più critiche per l'azienda attraverso l'analisi delle minacce, delle vulnerabilità e delle conseguenze sul patrimonio aziendale, non è solo uno strumento di valutazione dei rischi ma costituisce un importante strumento di business.