

CLUSIT

Commissione di studio “Certificazioni di Sicurezza Informatica”

Linea guida per l’analisi di rischio

Codice doc.to: CS_CERT/SC1/T3

Stato: Draft

© CLUSIT 2002

Linea guida per l’analisi di rischio

INDICE

1. Introduzione.....	4
2. Scopo della presente linea guida.....	4
3. Introduzione al concetto di rischio.....	4
3.1. Fasi della gestione del rischio.....	5
3.2. Il processo di analisi di rischio.....	5
3.2.1. Classificazione delle informazioni e delle risorse informatiche.....	5
3.2.2. Identificazione delle minacce.....	5
3.2.3. Identificazione delle vulnerabilità.....	6
3.2.4. Identificazione del livello di rischio.....	6
4. Le caratteristiche da ricercare in una metodologia per l'analisi di rischio.....	6
4.1. Ripetibilità e riproducibilità.....	6
4.2. Comprensibilità.....	6
4.3. Condivisione.....	7
4.4. Coerenza.....	7
4.5. Attinenza al dominio.....	7
4.6. Riutilizzabilità.....	7
4.7. Adeguatezza al livello di consapevolezza in azienda.....	7
4.8. Fattibilità in termini temporali.....	7
4.9. Fattibilità in termini economici.....	7
4.10. Sintesi nei risultati.....	8
5. Riferimenti.....	8

1. Introduzione.

La Commissione di studio “certificazioni di sicurezza informatica” ha individuato, nella riunione dell’8 Luglio 2002, tra gli obiettivi di maggior utilità a breve, l’elaborazione di documenti “linee guida” utilizzabili nella realizzazione di sistemi di gestione della sicurezza delle informazioni. Uno dei passi che la norma BS 7799 parte 2 richiede per la creazione di un sistema di gestione certificabile è quello dell’effettuazione di un’analisi di rischio, da cui desumere le azioni da implementare per la gestione del rischio in modo consapevole e adeguato ai valori da proteggere, in termini di informazioni o servizi erogabili dal sistema informativo. Il processo di analisi di rischio, perché di vero processo continuo si tratta e non di operazione una tantum, è un processo di importanza capitale per le conseguenze che può avere nelle operazioni che da esso dipendono, nel senso che la qualità delle informazioni prodotte nell’ analisi di rischio influenzerà pesantemente la qualità dei processi che seguiranno in cascata (scelte di gestione del rischio, implementazione delle contromisure, etc..) non ultimo il risultato economico dell’intera gestione della sicurezza delle informazioni.

2. Scopo della presente linea guida.

Il presente documento ha lo scopo di definire le caratteristiche ideali che una metodologia per l’effettuazione di un’analisi di rischio deve avere, indipendentemente da come essa sia pensata e realizzata e non vuole stabilire una metodologia specifica, dovendo essa essere coerente con il livello culturale dell’azienda, integrabile come patrimonio di conoscenza. Esistono varie metodologie disponibili sia come documenti di pubblico dominio, sia come metodologie proprietarie a cui a volte si accompagnano strumenti software per la raccolta e l’elaborazione dei dati necessari all’analisi stessa. Lo scopo primario del presente documento è di aiutare l’azienda nell’identificare quali tra esse siano più adatte alle caratteristiche dell’azienda stessa, ai piani temporali che l’azienda si è data, ai budget di spesa allocati per l’attività.

3. Introduzione al concetto di rischio

Il rischio si può definire come il prodotto scalare tra la gravità delle conseguenze che un evento pericoloso determinerebbe e la probabilità che tale evento pericoloso (minaccia) si realizzi:

$$R = G \times P$$

Tale definizione generale nel contesto della sicurezza delle informazioni può essere raffinata considerando, per le minacce di tipo deliberato, la probabilità come una funzione delle vulnerabilità presenti nel sistema e delle motivazioni dell’attaccante, o livello della minaccia:

$$P = f(V, M) \text{ (per minacce di tipo deliberato)}$$

Per le minacce di tipo accidentale la probabilità che un sinistro si verifichi è funzione della vulnerabilità alla minaccia e della probabilità intrinseca di accadimento del sinistro p (esempio: probabilità intrinseca di eventi atmosferici, inondazioni, black-out, nella zona considerata)

$$P = f(V, p) \text{ (per minacce di tipo accidentale)}$$

La gravità delle conseguenze G è normalmente esprimibile in termini di danno economico subito dall'azienda coinvolta nel sinistro, quindi in valuta corrente o classi di danno individuate da limiti definiti in valuta corrente.

3.1. Fasi della gestione del rischio

La gestione del rischio è normalmente suddivisa in due fasi distinte, anch'esse previste dalla norma BS 7799 parte 2:

- L'analisi di rischio, in cui a valle della classificazione delle informazioni, fondamentale, e dell'identificazione delle minacce, si identifica il livello di rischio associabile a ciascuna classe di informazioni.
- Il controllo del rischio, in cui si identificano le modalità (es.: trasferimento del rischi a terzi, riduzione del valore dell'informazione, riduzione delle vulnerabilità, etc..) in cui l'azienda decide di gestire i rischi associati con la perdita di riservatezza o integrità di dati/informazioni o la perdita di disponibilità di informazioni o risorse informatiche.

Lo scopo del presente documento si limita a considerare la prima delle due fasi, cioè l'analisi di rischio propriamente detta.

3.2. Il processo di analisi di rischio

L'intero processo di analisi di rischio è suddivisibile in fasi, da compiersi in sequenza ordinata. Possono esistere varianti, in particolare nell'ordine in cui vengono eseguite le fasi relative all'identificazione delle vulnerabilità e all'identificazione delle minacce, che possono essere completate in ordine relativo diverso da come sono presentate nel seguito. Non esistono invece dubbi sul fatto che la classificazione delle informazioni sia il punto di partenza per l'attività.

3.2.1. Classificazione delle informazioni e delle risorse informatiche.

Scopo di questa fase è la ricognizione e classificazione delle informazioni gestite dal sistema informativo aziendale, siano esse prodotte e gestite attraverso sistemi informatici o attraverso altri mezzi. Le informazioni sono, in generale, un'aggregazione di dati, ai quali, singolarmente, potrebbe non essere attribuibile nessun valore. Al termine di questa fase si dovrebbe raggiungere la conoscenza di quali classi di informazioni contengono valore per l'azienda e le relazioni esistenti con i dati che le compongono. Le informazioni andranno considerate ai fini degli obiettivi di integrità, riservatezza e disponibilità previsti nella definizione delle politiche di alto livello. Accanto alle informazioni vanno considerate le risorse informatiche, in termini di processi vitali, banda dei canali di comunicazione, potenza di calcolo, supporti per la memorizzazione. Le risorse andranno considerate ai fini degli obiettivi di disponibilità.

3.2.2. Identificazione delle minacce

Minaccia è un evento potenziale, accidentale o deliberato, che, nel caso accadesse, produrrebbe un danno per l'azienda determinato dalla violazione di uno degli obiettivi di sicurezza. L'elenco delle minacce dovrebbe comprendere minacce derivanti da eventi accidentali, minacce derivanti da interventi umani di tipo volontario, minacce derivanti da errori accidentali compiuti dagli utenti del

sistema informativo. Le caratteristiche del modello di business e dell'attività dell'azienda, le caratteristiche del sistema informativo e del sistema informatico e la collocazione logistica delle strutture dell'azienda e del sistema informatico concorrono a determinare l'elenco delle minacce possibili da prendere in considerazione.

3.2.3. Identificazione delle vulnerabilità

Vulnerabilità è una debolezza intrinseca del sistema informativo o del sistema informatico che, qualora si realizzasse una minaccia che la sfrutti, si avrebbe una violazione di uno degli obiettivi di sicurezza. Esistono vulnerabilità dovute alla collocazione geografica del sistema informatico (es: ai terremoti), vulnerabilità dovute a errori sistematici presenti nell'hardware o nel software (errori di progettazione), vulnerabilità dovute a possibili malfunzionamenti accidentali dell'hardware, vulnerabilità dovute a deficienze nelle procedure di utilizzo da parte degli utenti. Anche qui le caratteristiche del sistema, la sua collocazione, il livello di competenza degli utenti concorrono a determinare un elenco di vulnerabilità.

3.2.4. Identificazione del livello di rischio

L'identificazione del livello di rischio viene effettuata elaborando i risultati prodotti dalle tre fasi precedenti e può assumere connotati diversi di complessità essendo possibili semplici classificazioni di tipo qualitativo come dettagliate classificazioni di tipo quantitativo in cui il livello è associato a perdite di percentuali di fatturato. Ancora una volta il livello di consapevolezza del problema della sicurezza delle informazioni in azienda deve guidare i criteri di scelta.

4. Le caratteristiche da ricercare in una metodologia per l'analisi di rischio.

Dato il processo sopra citato, il livello di dettaglio con cui possono essere svolte le singole fasi del processo può variare molto in funzione dei molti parametri che caratterizzano la singola azienda. Qui di seguito sono elencate le principali caratteristiche da ricercare in una metodologia per l'effettuazione di un'analisi di rischio che risulti utile, praticabile, affidabile nei risultati e rappresentativa della realtà.

4.1. Ripetibilità e riproducibilità.

Analisi di rischio è sinonimo di misura del rischio e le caratteristiche primarie di un'operazione di misura sono la possibilità di ripetere la misura ottenendo gli stessi risultati a parità di ogni condizione, sia da parte dello stesso operatore in un tempo successivo, sia da parte di operatori diversi.

4.2. Comprensibilità.

I criteri adottati nell'espressione dei parametri che compongono il rischio (probabilità di accadimento, valore delle informazioni, etc.) devono essere trasparenti e comprensibili. Questo al fine di consentire il riutilizzo dei risultati in operazioni seguenti (vedi 4.6 Riutilizzabilità). Analogamente comprensibili devono essere i risultati prodotti.

4.3. Condivisione.

I valori attribuiti alle informazioni devono essere condivisi tra le funzioni aziendali per l'attività delle quali dette informazioni sono funzionali.

4.4. Coerenza.

I valori attribuiti alle informazioni devono essere coerenti con quanto stabilito dalle politiche di sicurezza di alto livello, essendo la definizione delle politiche di alto livello a monte dell'operazione di analisi di rischio nell'ordine dei processi contemplati dalla BS7799 parte 2.

4.5. Attinenza al dominio.

La definizione del dominio di applicazione del sistema di gestione della sicurezza delle informazioni deve essere coerente con il dominio definito per l'analisi di rischio.

4.6. Riutilizzabilità.

I risultati intermedi o finali dell'attività di analisi di rischio devono poter essere riutilizzabili in caso di variazioni delle condizioni (valori delle informazioni, minacce, vulnerabilità, etc.). Questo per permettere economie in tutti i casi in cui l'analisi di rischio vada ripetuta in quanto le condizioni sono variate. Inoltre, implicito nel concetto di sistema di gestione c'è il concetto di miglioramento e la misura del miglioramento passa anche per la revisione dell'analisi di rischio.

4.7. Adeguatezza al livello di consapevolezza in azienda.

La complessità di una metodologia per l'analisi di rischio deve essere adeguata al livello di consapevolezza esistente in azienda sui temi relativi alla sicurezza delle informazioni. Ciò per evitare gli insuccessi derivanti dall'introduzione di sistemi di gestione e processi non recepiti e lasciati allo stato di evento occasionale avulso dalla cultura aziendale, attuati solo perché *la norma lo richiede*.

4.8. Fattibilità in termini temporali.

I risultati del processo di analisi di rischio devono essere disponibili in tempi utili, commisurati con il livello della minaccia e con il piano temporale predisposto per l'implementazione dell'intero sistema di gestione della sicurezza.

4.9. Fattibilità in termini economici.

Il budget allocato per l'implementazione del sistema di gestione della sicurezza contempla una porzione allocata per l'analisi di rischio, che è uno dei processi coinvolti. La complessità e il livello di dettaglio dell'analisi di rischio deve essere commisurato con la previsione di spesa.

4.10. Sintesi nei risultati.

I risultati prodotti dal processo di analisi di rischio devono essere sintetici e facilmente accessibili nel mettere in relazione le informazioni (o le classi di informazioni) e le risorse con il livello di rischio associabile ad esse.

5. Riferimenti

ISO/IEC 17799: 2000 Information security management - Code of Practice for information security management.

BS 7799-2: 1999 – Information security management – Part 2: Specifications for information security management systems.

ISO/IEC TR 13335-3: 1998 – Information technology – Guidelines for the management of IT Security – Part 3: Techniques for the management of IT Security.

