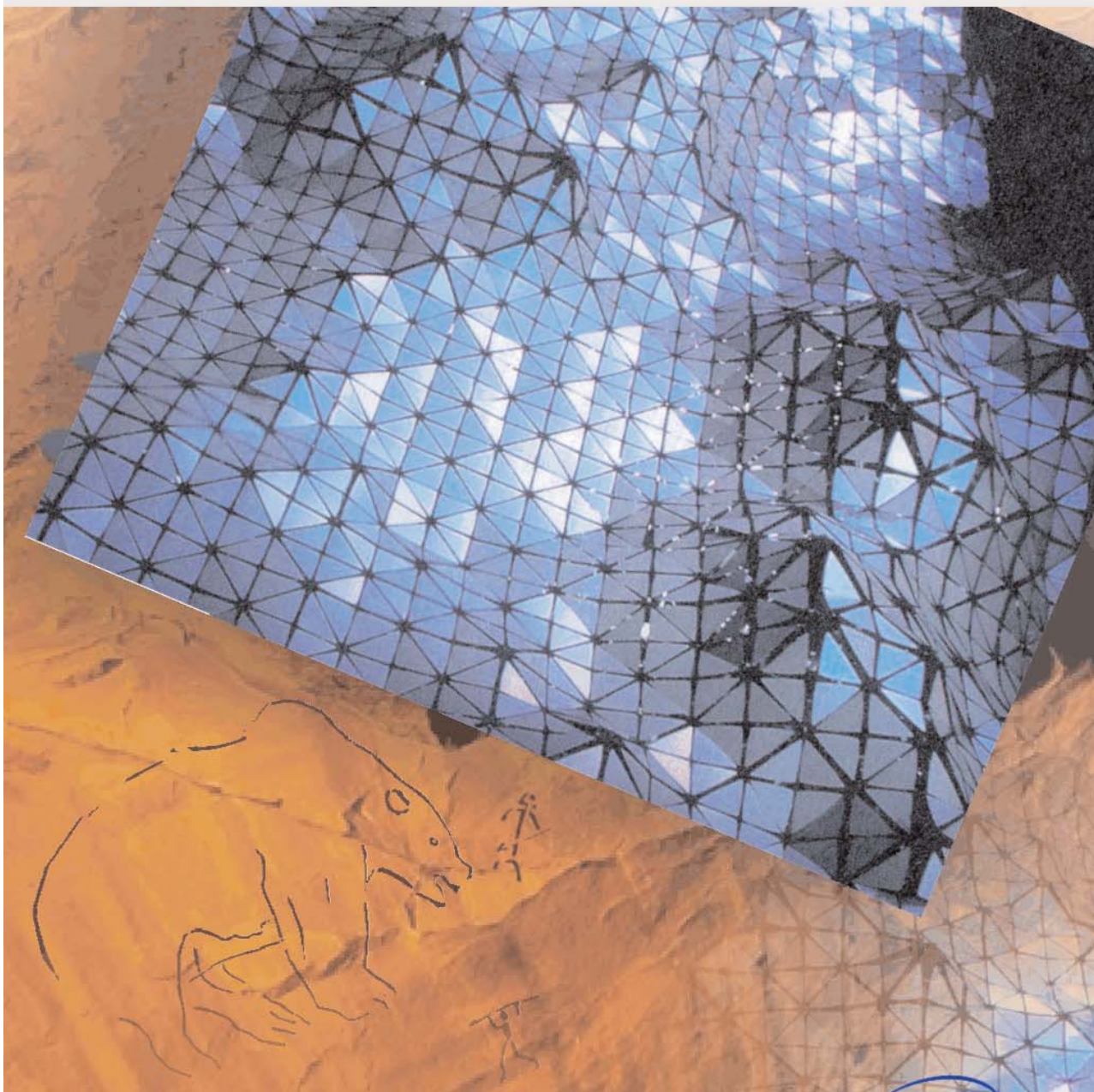




Ministero delle Comunicazioni



RISK ANALYSIS APPROFONDIMENTI



Linee Guida 

Le opinioni e le considerazioni espresse in questo volume, nonché le proposte avanzate, sono da considerarsi come personali dei singoli partecipanti e non riflettono necessariamente la posizione dei rispettivi Enti e Società d'appartenenza.

Il contenuto del presente volume è da considerarsi unicamente come studio tecnico/scientifico orientativo delle problematiche inerenti la sicurezza delle reti e la tutela delle comunicazioni.

Pertanto nessuna responsabilità potrà essere attribuita agli autori o all'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione, che cura questa pubblicazione, per ogni eventuale conseguenza derivante da qualsivoglia utilizzo dei contenuti del presente testo.

Le citazioni di specifici marchi o nomi di prodotti presenti nel documento sono riportati a mero scopo esemplificativo, non esauriscono il novero di prodotti esistenti sul mercato e in nessun caso costituiscono elemento di valutazione o di raccomandazione per l'utilizzo dei prodotti stessi.

La presente pubblicazione è diffusa a titolo gratuito e gli autori hanno ceduto all'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione gratuitamente e a tempo indeterminato i diritti di autore.



RISK ANALYSIS

Approfondimenti

Indice

Introduzione	3
Guida alla Lettura	5
Parte Prima	
Capitolo 1: Generalità	
<i>Genesi e storia dell'analisi del rischio nel contesto delle aziende e delle organizzazioni</i>	8
<i>L'analisi e la gestione dei rischi nel contesto più ampio della Security Governance</i>	9
<i>Vantaggi di un processo di analisi dei rischi in azienda</i>	12
<i>L'analisi dei rischi e lo scenario normativo</i>	13
Capitolo 2: Peculiarità e similitudini delle metodologie e degli strumenti di analisi del rischio	
<i>Approccio all'analisi dei rischi</i>	16
<i>Concetti comuni</i>	17
<i>Rischio</i>	17
<i>Minaccia</i>	17
<i>Vulnerabilità</i>	18
<i>Danno</i>	18
<i>Impatto</i>	19
<i>Fasi e passi dell'analisi dei rischi</i>	19
<i>Preparazione e pianificazione</i>	19

<i>Identificazione e stima dei rischi</i>	20
<i>Valutazione dei rischi</i>	21
Capitolo 3: L'analisi dei rischi in pratica	
<i>Gli strumenti per l'analisi dei rischi</i>	22
<i>Grado di maturità delle organizzazioni e self-assessment</i>	24
<i>Ambito, ruoli e responsabilità</i>	25
<i>Modellizzazione e valutazione in pratica</i>	27
<i>Risultati dell'analisi</i>	28
<i>Strategie di gestione del rischio</i>	29
Parte seconda - schede descrittive	31
<i>AS/NZS 4360:2004 RISK MANAGEMENT</i>	32
<i>BSA – Baseline Security Assessment</i>	39
<i>Ce.TRA - Continuous e.Business Threat and Risk Analysis</i>	42
<i>CRAMM</i>	47
<i>Defender Manager</i>	51
<i>EBIOS</i>	55
<i>ERAM - Enterprise Risk Assessment and Management</i>	64
<i>FIRM (Fundamental Information Risk Management)</i>	70
<i>ISA – Information Security Assessment</i>	76
<i>ISO/IEC 21827 - System Security Engineering, Capability Maturity Model 80</i>	
<i>NET.RISK</i>	80
<i>NORA - Network Oriented Risk Analysis methodology</i>	86
<i>OCTAVE® - Operationally Critical Threat, Asset, and Vulnerability EvaluationSM</i>	91
<i>OSSTMM – Open Source Security Testing Methodology Manual</i>	96
<i>PRA – Psychological Risk Assessment</i>	99
<i>RAF - Risk Analysis Facility</i>	102
<i>RISKWATCH (versione per l'Italia)</i>	106
<i>SARA - Simple to Apply Risk Analysis</i>	112
<i>SPRINT – Simplified Process for Risk Identification</i>	117
<i>SSM - Scalable Security Model</i>	122



RISK ANALYSIS

Approfondimenti

Introduzione

La presente pubblicazione si inquadra in una serie di attività svolte da un gruppo di esperti volontari appartenenti al settore pubblico e privato nel corso del 2005 e relative alla realizzazione di linee guida su:

Gestione delle emergenze locali

Risk analysis approfondimenti

Qualità del servizio su UMTS

Qualità dei servizi per le PMI su reti fisse a larga banda

Certificazione della sicurezza ICT

Outsourcing della sicurezza ICT

Si coglie volentieri l'occasione per ringraziare quanti hanno, con entusiasmo e professionalità, collaborato alla redazione e alla revisione del presente documento:

Gabriella Attanasio (Vem Sistemi S.p.A.), Roberta Bruzzone (International Crime Analysis Association), Marco Bubani (Vem Sistemi S.p.A.), Giulio Carducci (Securteam S.r.l. – Elsag), Giancarlo Caroti (Terna S.p.A.), Francesca Di Massimo (Microsoft Italia), Francesco Gentile (Gfi Ois S.p.A.), Nicola Mancini (GRTN S.p.A.), Roberto Margherita (Banksiel S.p.A.), Simona Napoli (KPMG S.p.A.), Claudio Pace (Aspasiel S.r.l.), Armando Perugini (CV AN (R) Consulente. Amm.ne Difesa-TELEDIFE-SE.PRO TE.CSAS), Alberto Piamonte (Wise Map - Gruppo Adfor S.p.A.), Massimo Piccirilli (Ministero delle Comunicazioni), Giovanna Ricci (RFI S.p.A.), Federico Sandrucci (C. Amm. (Aus) Consulente Amm.ne Difesa TELEDIFE-SE.PRO TE.CSAS), Giampaolo Scafuro (RETIS Consulting S.r.l.), Ugo Spaziani (ISACA Roma).

Si ringraziano ancora, per il loro apporto e i loro suggerimenti: Luca Boselli (KPMG S.p.A.), Stefania Caporalini - Ajello (Datamat S.p.A.), Raoul Chiesa (@Mediaservice.net Srl - ISECOM Italia), Luca Corciulo (PricewaterhouseCoopers Advisory S.r.l.), Sebastian D'Amore (PricewaterhouseCoopers Advisory S.r.l.), Renzo Dell'Agnello (Studio Dell'Agnello S.r.l.), Andrea Mariotti (KPMG S.p.A.), Carlo Mazza (Elea S.p.a.).

Roma, luglio 2006

Il Direttore
dell'Istituto Superiore delle Comunicazioni
e delle Tecnologie dell'Informazione

Ing. Luisa Franchina



RISK ANALYSIS

Approfondimenti

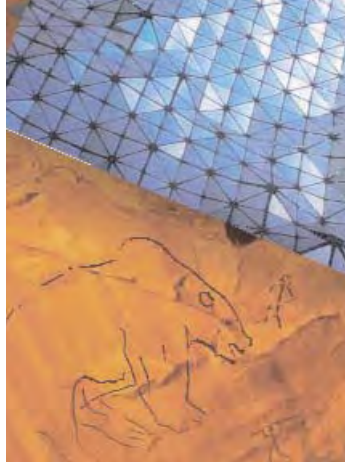
Guida alla lettura

Questo documento tratta di analisi dei rischi nell'ambito della protezione delle informazioni aziendali, al fine di assicurarne l'integrità, la disponibilità ed evitarne indebiti utilizzi. In particolare ci si riferirà agli aspetti di protezione delle informazioni, come elemento specifico del patrimonio aziendale, quando queste vengono elaborate, conservate e trasmesse attraverso strumenti ICT.

Il documento nasce dalla condivisione di esperienze maturate nell'applicazione dell'analisi dei rischi e parte dall'esame e dalla descrizione delle metodologie e, più in generale, degli strumenti utilizzati in tale ambito. Le metodologie e gli strumenti considerati sono pertanto quelli che ricadono in tali specifiche esperienze e non intendono esaurire il panorama di quanto disponibile e neanche essere necessariamente rappresentative dell'intero quadro metodologico nazionale e internazionale. Tuttavia il numero delle metodologie e degli strumenti analizzati, nonché la varietà in termini di approcci a effettive esperienze applicative di origine concettuale, hanno consentito di trarre alcune indicazioni generali sull'argomento.

Il documento si compone pertanto di due parti:

- la prima parte contiene le indicazioni generali emerse dalle attività sopradescritte e si pone l'obiettivo di fornire elementi utili a chi volesse avvicinarsi all'analisi dei rischi in ambito ICT, sia fornendo una panoramica generale della materia, sia esponendo alcune nozioni di base e indicazioni pratiche derivanti dall'esperienza nell'applicazione delle metodologie di analisi;
- la successiva seconda parte, composta da schede che descrivono le metodologie e gli strumenti considerati, vuole invece porsi come punto iniziale di approfondimento di alcune tra le diverse alternative disponibili per l'attuazione di una analisi dei rischi.



RISK ANALYSIS

Approfondimenti

PARTE PRIMA

CAPITOLI

- 1 - Generalità**
- 2 - Peculiarità e similitudini delle metodologie e degli strumenti di analisi del rischio**
- 3 - Analisi dei rischi in pratica**

Capitolo 1: Generalità

Genesi e storia dell'analisi del rischio nel contesto delle aziende e delle organizzazioni.

Giova iniziare ricordando che il concetto di rischio e la sua trattazione razionale è estremamente ampia e diversificata.

Il concetto di rischio appartiene alla sfera stessa delle attività umane, costituendo da sempre un fattore di riferimento nella vita personale, nelle guerre, nelle attività commerciali, nell'impresa e in molti altri aspetti dell'esistenza. Esso indica, in generale, l'eventualità di subire un danno.

Limitando l'argomento agli aspetti di gestione del rischio in ambito aziendale, il concetto di rischio si applica ad una molteplicità di riferimenti: si parla di rischio di progetto, di cambio delle valute, della salute dei lavoratori, e così via.

La trattazione razionale di tale concetto risale ad alcuni personaggi di scienza del passato, quali Fibonacci e Cartesio, che si sono occupati del rischio soprattutto in termini probabilistici, studiando la connessione tra rischio e gioco (nel senso delle probabilità di vittoria rispetto a quelle di perdita).

Il rischio ha costituito un elemento dello studio delle probabilità fino alla metà del secolo scorso, quando è stato introdotto nella più generale teoria dell'organizzazione aziendale. Infatti, nel corso della fine del 1800 e della prima metà del 1900 i vari pionieri del management burocratico, amministrativo, scientifico, umanistico (da Max Weber a Frederick Taylor, dai coniugi Gilbreth a Henri Fayol a Elton Mayo) non si erano preoccupati più di tanto di analizzare le componenti del rischio nell'organizzazione. E' solo con l'introduzione, intorno al 1950, successivamente alla conclusione e anche tramite l'esperienza della Seconda Guerra Mondiale, dei principi di indeterminazione e di contingenza, della teoria del caso e dei sistemi complessi nella teorizzazione dell'organizzazione aziendale, che la trattazione dell'analisi e della gestione dei rischi cominciano a trovare spazio.

In tale ambito, dall'accezione iniziale, in cui il rischio indica l'eventualità di subire una perdita, si è più recentemente passati, nell'ambito degli studi sulla gestione d'impresa e degli sviluppi delle scienze statistiche applicate all'economia aziendale, ad una connotazione non necessariamente negativa, in cui il rischio indica un evento di cui è incerto il verificarsi e che potrebbe avere conseguenze negative o positive, rappresentando pertanto una opportunità. Tipica situazione di questo genere è quella di chi si dedichi a operazioni finanziarie sul mercato delle azioni o delle valute (rischio di perdite finanziarie in relazione alla possibilità di ottenere guadagni). Questa suddivisione in situazioni dove il vantaggio del correre un rischio risulta evidente e motivante rispetto a quelle in cui il vantaggio non appare ben chiaro costituisce la base della suddivisione moderna, molto usata in ambito aziendale, tra rischi puri (legati a eventi con conseguenze negative) e rischi speculativi (in cui le conseguenze positive sono speculari rispetto a quelle negative).

Nell'ambito più specifico dei sistemi informatici, occorre attendere gli anni 1970-80 perché i sistemi distribuiti, le reti e infine Internet pongano in primo piano le esigenze di sicurezza e, di converso, l'opportunità di attività di analisi dei rischi, intese soprattutto come prerequisito per una progettazione razionale dei sistemi di protezione.

L'analisi e la gestione dei rischi nel contesto più ampio della Security Governance

Il concetto di Governance, a proposito di organizzazione e gestione d'azienda, è di recente introduzione, al pari di quello di analisi e gestione dei rischi.

Dal 1960 in poi, parallelamente al consolidamento della corrente di pensiero che considerava l'azienda come un sistema complesso e al riconoscimento del ruolo crescente che rivestivano per l'azienda non solo i dipendenti, ma anche tutte le parti che con l'azienda intrattenevano rapporti (e quindi fornitori, clienti, azionisti di minoranza, ecc., cioè i cosiddetti stakeholder), veniva a profilarsi e a consolidarsi presso le maggiori aziende la cosiddetta Corporate Governance, articolata in seguito in varie componenti (Financial, Operational, Security, ecc.).

Il concetto di Governance in azienda sta ad indicare quella qualità, in tutti gli aspetti della gestione, che garantisce correttezza, trasparenza, legalità, controllo e verificabilità finalizzate non solo alla salvaguardia degli interessi degli azionisti di riferimento, ma anche di tutti gli stakeholder sopra indicati. Nell'ambito delle componenti della Governance, l'analisi dei rischi assume ben presto un ruolo di rilievo. Qualsiasi decisione strategica importante, quale l'apertura di nuovi mercati o l'istituzione di nuovi insediamenti all'estero, le innovazioni che possono influenzare la qualità della vita dei dipendenti, i progetti d'ingegneria complessi, devono essere accompagnati da un processo di analisi dei rischi connessi e da una valutazione dei possibili danni che colpirebbero, come si è visto, non solo gli azionisti di riferimento, ma anche altre categorie di interessati.

Nel suo specifico dominio, la Sicurezza richiede anch'essa, per i fini sopra esposti, una componente di Governance. Anche di questa componente di Governance l'analisi dei rischi costituisce un elemento essenziale per assicurare che i sistemi di protezione progettati e attuati siano, in effetti, coerenti con le minacce pertinenti e le relative probabilità di accadimento, nonché con i vincoli legali esistenti.

E' in tale ambito che si colloca l'implementazione di un sistema di gestione della sicurezza delle informazioni ¹(ISMS - Information Security Management System²). Tali sistemi di gestione possono infatti essere considerati elementi abilitanti della Governance della sicurezza: essi mettono a disposizione un sistema organico che costituisce la trama operativa in grado di correlare - secondo prassi consolidate - obiettivi, attività e strumenti, facilitando le attività di gestione, coordinamento e controllo della sicurezza. La Governance viene quindi abilitata dal fatto che le decisioni possono essere prese sulla base di informazioni che risultano consistenti ed affidabili proprio in quanto originate da processi noti, stabili e misurabili.

I passi per adottare un ISMS sono i seguenti:

- censire ed elevare a valore gli Information Asset;
- analizzare i rischi;
- identificare le misure di sicurezza e predisporre un piano di implementazione delle stesse;

- creare consapevolezza e diffondere la cultura della sicurezza;
- formare il personale ed informarlo con continuità;
- verificare le misure di sicurezza in essere ed adeguarle;
- eseguire attività di reporting, monitoraggio e auditing.

Le attività sopra elencate sono collegate l'una all'altra a cascata; di conseguenza risulta subito evidente che l'analisi dei rischi è il fulcro su cui fanno perno tutte le successive attività: si tratta pertanto di una fase fondamentale per l'implementazione del sistema di controllo.

Tale analisi non deve essere centrata sull'IT e pensata prevalentemente con riferimento al controllo accessi (logico e fisico).

Le linee guida di Corporate Governance si indirizzano, con maggior forza, sull'identificazione di più ampie aree di rischio, cercando di includere tutti gli eventi relativi a violazioni della sicurezza delle informazioni che potrebbero avere conseguenze sull'azienda.

1 Le informazioni riportate nel seguito sono tratte da "White paper - Information Security Management System - Un valore aggiunto per le Aziende" realizzato dal gruppo di lavoro AIEA sugli ISMS.

2 L'ISMS è composto da:

- *politica di sicurezza, che fornisce le direttive aziendali per la sicurezza delle informazioni;*
- *organizzazione, che assicura la corretta gestione della sicurezza delle informazioni all'interno dell'organizzazione;*
- *classificazione e controllo del patrimonio, che assicura l'identificazione dei beni aziendali (dove per beni si intendono anche le informazioni) e la definizione e applicazione di misure di protezione adeguate al loro valore;*
- *sicurezza del personale, per ridurre il rischio di errori, furti, frodi, ecc.;*
- *sicurezza fisica e ambientale, per prevenire accessi non autorizzati, danni e incidenti;*
- *gestione operativa e delle comunicazioni, che assicura una gestione operativa corretta e sicura delle elaborazioni e delle macchine;*
- *controllo degli accessi alle informazioni;*
- *sviluppo e manutenzione delle applicazioni, che assicura che la sicurezza sia incorporata nei sistemi informativi gestione della continuità operativa, che assicura una tempestiva reazione ad interruzioni operative e la protezione delle attività critiche da disastri e incidenti rilevanti;*
- *conformità con la legge, che assicura di ottemperare a leggi e a regolamenti pertinenti.*

Esse definiscono inoltre un modello di controllo del rischio basato su una costante attività di monitoraggio e di re-assessment dei rischi (ciò che costituisce un rischio oggi potrebbe non esserlo domani, mentre nuovi rischi sono generati dall'emergere di nuove tipologie di minacce o da cambiamenti nell'ambiente interno o esterno all'azienda).

Vantaggi di un processo di analisi dei rischi in azienda

L'approccio definito dalla Governance si contrappone ad una prassi ampiamente diffusa che vede l'implementazione della sicurezza basarsi sulla realizzazione di misure di protezione "standard", per cui firewall, intrusion detection system, antivirus, ecc., vengono installati perché costituiscono una sorta di "norma igienica" ormai consolidata.

Tale modo di procedere, se da un lato costituisce una sorta di "zoccolo minimo", dall'altro può suscitare un falso senso di sicurezza, perché le contromisure così implementate possono non essere in grado di controllare e ridurre tutte le vulnerabilità di sistemi ormai complessi e fortemente correlati tra loro. Ricordiamo la regola che la sicurezza complessiva di un sistema è data dalla sicurezza "dell'anello più debole della catena".

Infatti, anche se può esistere la sensazione che le minacce, le contromisure, le componenti tecnologiche che costituiscono reti e sistemi informatici siano sempre un po' le stesse, e che quindi una semplice check-list sia più che sufficiente per gestire la sicurezza, in realtà la progettazione di un valido sistema di protezione non è così semplice.

Occorre anzitutto considerare il numero ormai veramente alto, in continua evoluzione, di minacce e, soprattutto, di attacchi potenziali.

Inoltre le informazioni che si intende proteggere hanno valore diverso:

- l'esigenza di autenticazione certa per un determinato tipo di posta elettronica può essere assai maggiore rispetto a quella

- relativa alla diffusione degli elenchi di telefono interni;
- un determinato segmento di rete può richiedere caratteristiche di protezione assai più stringenti, magari anche a costo di qualche sacrificio in termini di generalità di servizio e di efficienza nel volume delle transazioni praticabile.

Solo un processo sistematico di analisi dei rischi consente di considerare gli elementi descritti e di definire in modo proattivo le misure da adottare.

Infine, un processo costantemente attivo di analisi dei rischi consente di avere sempre disponibile l'evidenza della consistenza del sistema di protezione attuato e di poterlo presentare ad eventuali interlocutori autorizzati, elevando il grado di fiducia nell'utilizzo delle transazioni elettroniche.

L'analisi dei rischi e lo scenario normativo

Come già ricordato, tra gli obiettivi della Governance vi è anche quello di assicurare il rispetto delle norme di legge vigenti. In tale contesto l'analisi dei rischi deve considerare i vincoli imposti da leggi e norme che, in taluni casi, prevedono responsabilità anche di carattere penale per i contravventori.

Vale la pena ricordare:

- la tutela della Privacy regolamentata dal Codice in Materia di Protezione dei Dati Personali (D. Lgs. 196/2003) che dispone di importanti misure per la tutela dei dati personali;
- il D. Lgs. 231/2001 in materia di responsabilità amministrativa;
- la legislazione in materia di diritto di autore (D. Lgs. 518/92, D. Lgs. 70/2003, L. 128/2004 'Decreto Urbani') ;
- la normativa Banca d'Italia con:
 - le istruzioni di Vigilanza per le Banche, Titolo IV, capitolo 11, Sezione II Sistema dei Controlli Interni, con particolare riferimento al paragrafo 4 sui Sistemi Informativi;
 - le Istruzioni di Vigilanza per gli Intermediari Finanziari iscritti nell' "Elenco Speciale", Capitolo VI "Organizzazione amministrativa e contabile e controlli interni", con particolare riferi-

mento ai paragrafi relativi ai sistemi informativi ed all'esternalizzazione di funzioni aziendali (outsourcing);

- e ancora, per il settore bancario, gli accordi di Basilea (vedi sito www.bis.org).

Nel contempo, tra tutte le normative citate, l'unica che impone esplicitamente l'effettuazione e la documentazione di una analisi dei rischi è il Codice in Materia di Protezione dei Dati Personali, che al punto 19 dell'Allegato B ("Disciplinare Tecnico in Materia di Misure Minime di Sicurezza") sancisce l'obbligatorietà della redazione di "un documento programmatico sulla sicurezza contenente idonee informazioni riguardo", tra l'altro, "l'analisi dei rischi che incombono sui dati" (punto 19.3).

Si osservi che i dati a cui si riferisce la norma sono i dati personali³ di cui l'azienda è titolare⁴ e che tali dati nella maggioranza dei casi non coincideranno completamente con le informazioni aziendali da proteggere, in quanto critiche per l'azienda stessa.

Inoltre i rischi da considerare nell'ambito della legge differiscono da quelli considerati a fini aziendali. Infatti l'obiettivo del Codice, come definito all'art.1, è quello di garantire il "rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali."

Pertanto i rischi considerati dalla legge sono quelli che potreb-

³ Il Codice, all'art.4, comma 1, sub b), definisce "dato personale", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

⁴ Il Codice, all'art.4, comma 1, sub f), definisce "titolare", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

bero ledere tali diritti e, specificatamente, come definito all'art. 31:

- di distruzione o perdita, anche accidentale, dei dati stessi;
- di accesso non autorizzato;
- di trattamento non consentito o non conforme alle finalità della raccolta.

Appare pertanto evidente come il rispetto del Codice e l'analisi dei rischi, contenuta nel documento programmatico sulla sicurezza, da esso previsto, non comporti l'effettuazione di una analisi dei rischi completa ed esaustiva ai fini aziendali.

Nel contempo, va altresì sottolineato che, in virtù dell'ampio contesto di applicazione dell'analisi dei rischi delle informazioni derivante dai concetti di Governance, sopra esposti, gli stessi rischi dovranno essere considerati in ambito aziendale, per le ripercussioni che potrebbero avere sull'azienda stessa, in termini di sanzioni, amministrative, civile e penali, ma anche, ad esempio, di danni di immagine.

Capitolo 2: Peculiarità e similitudini delle metodologie e degli strumenti di analisi del rischio

Approccio all'analisi dei rischi

I diversi metodi e strumenti di analisi dei rischi possono essere distinti, in base al metodo di valutazione dei rischi utilizzato, nelle seguenti tre categorie:

- qualitativo;
- quantitativo;
- semi-quantitativo.

Il primo approccio prevede una valutazione del rischio su una scala qualitativa (ad esempio alto, medio, basso).

Il secondo approccio, invece, riconduce le valutazioni ad un valore numerico puntuale, spesso inteso come la perdita economica derivante dal verificarsi del rischio. Si tratta di un approccio più difficile ed oneroso del primo perché costringe ad un censimento ed una valorizzazione degli asset e ad una valorizzazione delle perdite che si avrebbero in caso di incidente.

Il terzo approccio è un compromesso fra i primi due, nel quale le valutazioni sono effettuate in termini qualitativi e, successivamente, trasformate in numeri per poterle elaborare attraverso algoritmi di calcolo, come se si trattasse di valutazioni quantitative.

Solo FIRM, tra le metodologie di analisi considerate nel presente lavoro, utilizza metriche di calcolo del rischio sia di tipo quantitativo sia qualitativo, basate sul concetto di scorecard, che offrono una visione d'insieme e a diversi livelli di profondità. Tutte le altre metodologie e gli altri strumenti analizzati, nella seconda parte di questo documento, sono riconducibili ad approcci di tipo qualitativo o semi-quantitativo.

Concetti comuni

Le metodologie e gli strumenti di analisi dei rischi disponibili, anche limitando l'analisi a quelli applicabili in ambito ICT, sono numerosi. Attraverso l'analisi comparata dei concetti che ciascuno di essi utilizza è possibile identificare gli elementi "universalmente" riconosciuti come parte integrante dell'analisi dei rischi e che, quindi, dovranno comunque essere considerati e con i quali si dovrà avere dimestichezza nel momento in cui si intenda effettuare un'analisi dei rischi.

Nel seguito saranno pertanto descritti i principali concetti comuni, nonché quelli specifici, così come emersi dall'analisi delle metodologie e degli strumenti descritti nella seconda parte di questo documento. Ovviamente l'esame di ulteriori metodologie, qui non considerate per le ragioni descritte nella Guida alla Lettura, potrebbe arricchire di ulteriori elementi l'analisi riportata.

Rischio

La concettualizzazione più generale, condivisa praticamente da tutte le metodologie, identifica il rischio come l'eventualità che una minaccia possa trasformarsi realmente in danno, comportando così un determinato impatto.

Unica peculiarità si ritrova in Net.Risk che identifica il "rischio reale" come rischio potenziale (livello di esposizione ad una minaccia) messo in relazione alla criticità di un dato asset.

Le altre metodologie utilizzano i concetti di "rischio potenziale" o "intrinseco", come il livello di rischio a prescindere dalle contromisure in essere, e di "rischio effettivo" o "residuo" come il livello di rischio, tenuto conto le contromisure implementate.

Minaccia

La minaccia viene definita come un evento di natura dolosa o accidentale che, sfruttando una vulnerabilità del sistema, potrebbe provocare un danno. Su questa definizione tutte le metodologie prese in esame sono concordi. Non si riscontrano quindi peculiarità nella definizione, ma piuttosto nella modalità di gestione delle minacce offerte dai diversi strumenti: alcuni rendono disponibili cataloghi di minacce personalizzabili, altri ne forniscono solo il concetto lasciando all'analista il compito di individuarle.

Vulnerabilità

La vulnerabilità non viene sempre definita esplicitamente nelle metodologie/strumenti considerati e presenta diverse sfumature.

La definizione generale la identifica come una debolezza, intrinseca o dovuta a condizioni di esercizio, che possa essere sfruttata da una minaccia per arrecare danno.

Tuttavia, mentre alcune metodologie danno maggior rilievo al concetto di vulnerabilità, altre lo considerano in modo implicito. Ad esempio, CRAMM evidenzia anche il concetto di assenza di controlli e non solo quello di debolezza, FIRM enfatizza il fatto che la presenza di vulnerabilità aumenta la probabilità di accadimento di una minaccia, mentre AS/NZS 4360 non considera direttamente le vulnerabilità (l'eliminazione o la riduzione delle vulnerabilità viene considerata una strategia di trattamento dei rischi, ma esse non sono considerate nell'ambito dell'analisi degli stessi). Anche Defender Manager e Net.Risk non esprimono direttamente il concetto di vulnerabilità, ma lo considerano rispettivamente attraverso il "livello di esposizione" (il livello di esposizione di un componente a una determinata minaccia) e il "rischio potenziale" (valutazione delle vulnerabilità di un dato sottosistema alle minacce presenti).

Danno

Il danno è la conseguenza negativa del verificarsi di un rischio o dell'attuarsi di una minaccia. Tali conseguenze vengono spesso identificate da una perdita di riservatezza, integrità e/o disponibilità dell'informazione.

In alcuni casi, questa definizione condivisa viene però ulteriormente specificata. Ad esempio ISO 21827 distingue il danno in "tangibile" (danno monetario provocato sul sistema) e "intangibile" (danno di immagine o comunque immateriale), mentre SARA e SPRINT differenziano il danno in "business consequence" (frodi o attacchi informatici andati a buon fine) e "security breach" (perdita di disponibilità, integrità, riservatezza dovuti ad un incidente, come un guasto agli elaboratori).

CRAMM non definisce direttamente il concetto di danno, ma indirettamente attraverso scenari di impatto. ISA, EBIOS, FIRM,

NORA, OCTAVE, RAF e Net.Risk non utilizzano il termine, preferendo invece il concetto di impatto.

Impatto

Questo concetto è presente nella maggior parte degli strumenti/metodologie analizzate, ma la sua definizione spesso si sovrappone a quella di danno. E' il caso, ad esempio, di Defender Manager dove impatto e danno vengono considerati sinonimi a tutti gli effetti.

Alcuni strumenti/metodologie, come ERAM, FIRM, Risk Watch, associano il concetto di impatto a quello di misura o entità del danno, ma la definizione che accomuna la maggior parte di essi (ISA, CRAMM, EBIOS, ISO21827, OCTAVE, RAF, SARA, SPRINT e CETRA) vede l'impatto come effetto sull'azienda o ente e sul suo business del verificarsi di una minaccia, quindi l'effetto reale del danno sul sistema. CETRA esplicita come l'impatto deve tenere conto ad esempio anche di possibili responsabilità civili o penali (presenti ad esempio nel D. Lgs. 196/2003).

Fasi e passi dell'analisi dei rischi

Analogamente a quanto fatto più sopra per i concetti alla base dell'analisi dei rischi, è possibile identificare, attraverso l'esame comparato di alcune metodologie e strumenti, le fasi e i passi necessari per effettuare un'analisi dei rischi in ambito ICT.

Preparazione e pianificazione

Preliminarmente all'avvio delle fasi operative dell'analisi, sembra opportuna, sebbene non esplicitamente prevista da tutte le metodologie/strumenti considerati, una prima attività di pianificazione dell'analisi stessa, volta a definire con precisione il perimetro o ambito della stessa, nonché ad acquisire ogni elemento già disponibile e rilevante ai fini dell'analisi stessa. In tale fase sarà definito con chiarezza anche l'obiettivo che si intende raggiungere e i risultati attesi.

Nei casi in cui la metodologia lo richieda, tale fase di avvio può avere contenuti più operativi, comportando la scelta del modello concettuale atto a rappresentare la realtà aziendale nei successivi passi dell'analisi.

A titolo esemplificativo, è possibile considerare la metodologia CRAMM, che prevede che nelle fasi iniziali dell'analisi vengano identificati gli asset (dati e informazioni) da proteggere e di conseguenza il perimetro di analisi (architettura di rete, asset fisici, applicativi e processi aziendali). Attività analoghe sono previste anche da Defender Manager, FIRM, NORA, ISA, Net.Risk, ecc..

Identificazione e stima dei rischi

Una volta stabilito l'ambito dell'analisi e, dove previsto, scelto il modello della realtà aziendale da utilizzare, metodologie e strumenti prevedono l'esecuzione di una o più fasi volte a "popolare" il modello individuato.

Innanzitutto saranno determinate le minacce che incombono sulle informazioni che si intende proteggere e quali sarebbero le conseguenze del concretizzarsi di tali eventi.

In questa fase vengono inoltre considerate, ove previsto, le vulnerabilità degli ambienti e degli strumenti utilizzati per l'elaborazione e la trasmissione delle informazioni da proteggere.

In taluni casi questa fase può comprendere anche l'identificazione delle misure di sicurezza già implementate a protezione delle minacce considerate.

L'attività di stima dei rischi coinvolge, poi, più fattori, più o meno numerosi a secondo della metodologia o dello strumento considerati. Ad esempio Ce.TRA considera il rischio come una funzione del bene o asset che può subire un danno, della Minaccia (valutata in base alla Motivazione ed alla Capacità dell'agente latore della minaccia nel portare l'attacco) che incombe su tale asset e della Vulnerabilità (valutata in base alla Severità della stessa e l'Esposizione dell'asset al danneggiamento) degli strumenti utilizzati.

Tali attività sono ovviamente fortemente dipendenti dagli aspetti specifici della metodologia o dello strumento che si sta utilizzando. La maggior parte degli approcci considerati propone questionari o check-list da utilizzare in tale ambito.

Molto utili si possono rivelare liste predefinite, anche se tali liste non possono essere per loro natura esaustive ed è pertanto sempre richiesto l'intervento della conoscenza diretta del contesto che si

intende analizzare ed esperienza nell'applicazione dell'analisi dei rischi.

Valutazione dei rischi

Le informazioni raccolte nella fase precedente sono elaborate, attraverso gli algoritmi propri di ciascuna metodologia, al fine di ottenere una valutazione dei rischi stessi, che permetta di classificarne la gravità o la criticità, al fine di guidare le successive fasi di implementazione delle misure di protezione più appropriate.

Alcune delle metodologie e degli strumenti esaminati prevedono in questa fase anche l'identificazione delle misure di sicurezza da implementare. Si tratta di misure di sicurezza applicabili allo specifico rischio individuato, ma che occorrerà comunque sempre sottoporre al giudizio professionale di chi conduce l'analisi al fine di adattare alle specifiche esigenze e allo specifico contesto aziendale.

Capitolo 3 - Analisi dei rischi in pratica

Gli strumenti per l'analisi dei rischi

Nel capitolo precedente e soprattutto nel seguito di questo documento è analizzato l'approccio metodologico all'analisi dei rischi, ma perché la metodologia diventi un processo concreto è necessario allocare risorse che la mettano in pratica, costantemente, utilizzando gli strumenti messi a disposizione della metodologia stessa.

Gli strumenti messi a disposizione dalle metodologie hanno la funzione di guidare il team di analisi in ogni stadio del processo, fornendo un collettore unico per raccogliere, valutare, interpretare le informazioni. Compiere attività quali la modellizzazione di asset, la valutazione delle variabili che contribuiscono al grado di esposizione al rischio, la scelta delle metriche e la stima degli scostamenti rispetto ad obiettivi attesi o sperati, fornendo altresì una rappresentazione sintetica del tutto, richiederebbe, senza strumenti, uno sforzo non indifferente.

Non bisogna tuttavia attendersi da tali strumenti l'impossibile. È fuor di dubbio che sarebbe certamente interessante conoscere ogni anno quanto accantonare come spesa in sicurezza per i rischi concernenti i sistemi informativi per l'anno successivo. Ma per poter ottenere tale risultato si dovrebbero raccogliere le valutazioni dell'impatto dei rischi in termini quantitativi (economici), partendo da una valorizzazione puntuale degli asset minacciati (per es. calcolando il costo di ripristino, la mancanza di produttività del personale, e così via). Sarebbe inoltre necessario calcolare il valore di beni intangibili, come la perdita d'immagine, o la perdita di competitività.

Il pericolo di attribuire valutazioni soggettive, ma percepite come oggettive in quanto quantitative, è in questi ambiti concreto ed ha evidenti ripercussioni sulla qualità dei risultati ottenibili. Si pensi ad esempio alla difficoltà per una società quotata di dover valutare, sulla base di un approccio quantitativo, la perdita in punti percentuali sui mercati azionari conseguente a un incidente.

La valutazione dei beni intangibili potrebbe inoltre richiedere competenze specialistiche *ad hoc* e comportare la dilatazione di tempi e

costi dell'analisi, per la ricerca degli elementi oggettivi necessari alla valutazione. Ma questo vale anche per altri passi di tutto il processo (si pensi, ad esempio, alle valutazioni delle vulnerabilità di tipo tecnico).

Le metodologie qualitative o semiquantitative hanno oggi, dalla loro, una snellezza che meglio consente di rappresentare in tempi ragionevoli scenari di rischio di organizzazioni di diverse dimensioni e settori di attività, senza comunque escludere in linea di principio forme di integrazione con altri risultati.

Per contro la principale limitazione dell'approccio qualitativo e semi-quantitativo è rappresentato dalla necessità di considerare con cautela la confrontabilità dei risultati tra analisi condotte su realtà diverse o, sulla stessa realtà, in tempi diversi.

Indipendentemente dal tipo di approccio adottato, sia esso qualitativo o quantitativo, bisogna comunque considerare che metodi e strumenti di analisi hanno lo scopo di raccogliere e sistematizzare conoscenze distribuite tra *business owner*, *service manager*, referenti applicativi, ufficio gestione crisi, sistemisti e così via, che già provvedono a forme di sotto-analisi per altra via e con finalità più contingenti (la stesura del Documento Programmatico sulla Sicurezza, la profilazione degli accessi logici alle risorse, le attività periodiche di *vulnerability assessment*, la definizione dei livelli di servizio, ecc.).

La competenza del team incaricato dell'analisi non risiede quindi tanto nella conoscenza specialistica delle problematiche coinvolte, quanto nella capacità di integrare le informazioni e le conoscenze disponibili, vincendo, talvolta, anche alcune resistenze organizzative derivanti dalla divisione delle responsabilità tra i diversi uffici dell'azienda.

La scelta di metodo e strumenti dovrebbe essere comunque successiva alla necessità di darsi obiettivi di analisi del rischio ragionevolmente perseguibili, anche in funzione del grado di maturità in questo ambito della organizzazione/istituzione che intende condurre l'analisi.

Grado di maturità delle organizzazioni e self-assessment

È conveniente che una organizzazione affronti l'analisi del rischio per gradi, specie se "giovane" sul tema.

Anche nei casi in cui si persegue l'obiettivo della certificazione del sistema di gestione, l'approccio per gradi è applicabile e si realizzerà tarando, magari verso il basso, i servizi certificabili in prima battuta, adeguando cioè l'ambito della analisi in funzione dell'ambito del certificato.

Sembra generalmente trovare il favore delle organizzazioni iniziare con attività di *self-assessment* di alto livello, a prescindere da una definizione puntuale dell'ambito dell'analisi, che obbligherebbe da subito a confrontarsi con la raccolta di informazioni di dettaglio, come quelle necessarie per il censimento e la valutazione degli *asset*.

Come noto, il *self-assessment* consiste in un'auto-valutazione che permette di capire il livello attuale al quale si trova l'organizzazione, per derivarne indicazioni utili sul livello di sforzo necessario per implementare un processo di gestione del rischio, e pianificare parallelamente un approccio graduale all'evoluzione del sistema informativo e dei processi interni diretti a supportarlo⁵.

Un vantaggio indiretto che si ricava con questo tipo di approccio è inoltre quello di riuscire a coinvolgere sui temi dell'*information security* funzioni diverse a livelli diversi (dirigenti, middle-management, operativi), spesso producendo risultati inattesi su temi importanti, come quello della divisione delle responsabilità.

Un modo pratico di realizzare il *self-assessment* è quello di allestire un questionario sulla intranet aziendale, distribuendo le domande in ragione delle mansioni e del ruolo degli intervistati, e dando loro il tempo di completare le risposte, magari a più riprese, entro una scadenza.

Le domande affrontano temi classici della sicurezza delle informazioni (per es., partendo da un questionario ottenuto girando in forma di domanda la ISO17799) senza tralasciare mai gli aspetti orga-

⁵ cfr. "Guida Microsoft alla gestione dei Rischi"
<http://www.microsoft.com/italy/technet/security/guidance/secrisk/default.aspx>

nizzativi sottesi a quelli più tecnici (ad esempio, le domande sulle modalità di autenticazione sono affiancate da quelle concernenti le modalità di gestione del ciclo di vita delle credenziali degli utenti).

Alcuni esempi di domande:

- le *policy* e le procedure di sicurezza sono chiare, concise, ben documentate, complete, immediatamente accessibili?
- viene mantenuto e aggiornato un inventario di tutti gli *asset*, quali i dati, i beni hardware e quelli software?
- sono implementati meccanismi per il *delivery* automatico delle *patch* per tutte le tipologie di sistemi e di programmi in uso all'interno dell'organizzazione?
- e' stato costituito un *incident response team* con il mandato di svolgere attività di *incident management* e *forensic analysis*?

Le risposte sono graduate, in modo che i punteggi attribuiti alle risposte si collochino in fasce che consentono di valutare l'attitudine e il grado di maturità dell'organizzazione rispetto al *risk management*.

Il *self-assessment* dovrebbe riuscire a rappresentare risultati ragionevoli e non macroscopicamente contraddittori, magari suddivisi anche per funzioni di appartenenza dell'intervistato o dominio di indagine. Se fondato poi su uno standard, deve consentire di mettere in evidenza il grado di scostamento da quanto raccomandato da quello standard.

Ambito, ruoli e responsabilità

Tale approccio per gradi potrebbe essere consigliabile anche nell'attuazione di una analisi più completa, non limitata cioè al *self-assessment*, specie se bisogna ancora acquisire dimestichezza con il processo di analisi dei rischi in tutte le sue fasi.

In tal senso si può definire un ambito di partenza funzionale ad alcuni rami di business o attività a supporto, ed ampliarlo in tempi successivi.

Si tratta insomma di definire un primo progetto pilota con un ambito ragionevolmente ristretto. Ad esempio per una *software factory* esso potrebbe essere costituito dai documenti di analisi funzionali, i *tool*

e i server di sviluppo, i *backup* dei sorgenti, gli strumenti di controllo del versioning.

Per una società commerciale, l'attenzione potrebbe porsi sul processo di vendita, dall'acquisizione del cliente fino all'incasso della fattura, e sui sistemi che supportano tali attività, comprendendo i rischi legati alla riservatezza dei dati sulla clientela, fino alla continuità dei processi di consegna e fatturazione.

Una società di produzione potrebbe considerare la continuità dei sistemi di controllo della produzione, includendo gli aspetti della protezione delle aree e della sicurezza fisica del data center, del *change management*, ecc.

Come si vede, ambiti diversi genereranno modelli di analisi diversamente "popolati" e a diversi livelli di profondità, chi più orientato agli aspetti di sicurezza logica e agli asset di natura software, chi a quelli di sicurezza fisica e di gestione operativa.

In ogni caso, deve essere posta attenzione alla definizione dell'ambito (si veda a tal proposito anche quanto detto nel Capitolo 2): se l'ambito è troppo generico costringerà a "popolare" più modelli di analisi, rendendo necessario effettuare molteplici valutazioni volte ridondanti; viceversa un ambito troppo ristretto, rischia di non far emergere situazioni di rischio orizzontali, offrendo una rappresentazione parziale.

Inoltre, modificare l'ambito dell'analisi, una volta avviata, non sempre è una attività agevole, sia a causa di rigidità presenti in alcuni degli strumenti di analisi, sia perché eventuali modifiche potrebbero portare a ri-valutare aspetti già considerati.

Dalla definizione dell'ambito discende, inoltre, la definizione degli aspetti organizzativi dell'analisi stessa. Pertanto esso deve avere un sufficiente livello di dettaglio da consentire l'attribuzione di ruoli e responsabilità della sicurezza degli *asset* che vi ricadono a funzioni/uffici/società ben definiti.

Tale attività può non limitarsi all'analisi dell'organigramma aziendale. Potrebbe essere necessario identificare le attività svolte da ciascun ufficio e individuare le corrispondenti responsabilità. Se parliamo poi di terze parti l'attività deve avere un richiamo al contratto di forn-

tura o di *outsourcing*. È utile predisporre *ad hoc* un documento sui ruoli e le responsabilità, in modo da avere un unico punto di riferimento da tenere aggiornato.

Modellizzazione e valutazione in pratica

Naturalmente dalla definizione dell'ambito derivano anche gli elementi di partenza per il popolamento del modello di analisi. In questa fase l'attenzione principale dovrà essere posta nella definizione del livello di dettaglio più opportuno: una entità generica "LAN" può andare bene per la rete di un CED, connessa a poche reti di clienti, tutte non pubbliche, sotto la completa gestione del CED stesso, anche per quanto attiene alla configurazione degli apparati attivi che permettono la comunicazione. Diversamente essa potrà essere differenziata in sottoreti, VLAN, *firewall*, ecc..

Potrebbe inoltre essere importante che il modello consenta di considerare anche i processi e non solo gli *asset*. Talvolta il rischio non è infatti legato a un "oggetto" fisico o logico, ma piuttosto ad una attività che viene effettuata su tale oggetto.

Ad esempio, rimanendo al solo livello tecnico, si consideri il rischio sull'integrità dei dati relativo a un disallineamento tra dati dovuto alla presenza di procedure di trasferimento da un sistema A ad un sistema B. Il rischio non è intrinseco della base dati A piuttosto che della base dati B, ma è della procedura di trasformazione dei dati che interviene tra A e B.

Come detto, le minacce/vulnerabilità non sono sempre elementi intrinseci degli oggetti in quanto tali, ma perché essi, in un preciso punto del processo, presentano un rischio, come una modalità debole con cui gli utenti sono autorizzati all'uso di risorse, o un canale informale impiegato per comunicare con altre funzioni o fornitori, o nel fatto che un controllo non è ciclico, o perché non è prevista una conferma della ricezione e così via.

Il team di analisi del rischio dovrebbe essere composto da persone che hanno dimestichezza con i processi aziendali e non solo esperti tecnologici, che devono cioè avere l'abilità di sondare quale è il business, quali le attività e le sotto-attività di cui è composto e come

l'esecuzione di tali attività debba avvenire in sicurezza, perché dall'input fornito venga prodotto l'output atteso.

Per quanto riguarda invece le metriche e le valutazioni necessarie per lo svolgimento dell'analisi, occorre sottolineare come sia fondamentale la loro conoscenza, per un utilizzo corretto della metodologia. Lo stesso discorso vale, a maggior ragione, per l'algoritmo che sta alla base del calcolo del rischio, da cui di fatto dipende tutta l'analisi.

Le valutazioni possono essere ottenute tramite interviste ai referenti e attività di auditing sul campo. La soluzione qualitativamente migliore, pur richiedendo tempi e costi maggiori, si ottiene da una combinazione delle due. Le interviste da sole potrebbero offrire valutazioni troppo soggettive, specie se rivolte ad un solo intervistato.

Risultati dell'analisi

L'analisi dei rischi ha un'altra fase fondamentale nella interpretazione dei risultati.

Il semplice calcolo del rischio, inteso come applicazione dell'algoritmo, non è sufficiente a produrre il risultato finale dell'analisi. La conclusione dell'analisi non dovrebbe infatti limitarsi alla illustrazione, comunque necessaria, in una rappresentazione di facile lettura, della mappa dei rischi emersa dall'analisi.

Occorre accompagnare tale mappa con opportuni ragionamenti atti ad individuare le ragioni organizzative ed aziendali per cui certe aree presentano un livello di rischio palesemente superiore alla media, ovvero perché una certa minaccia continua a insistere su valori alti rispetto all'analisi di sei mesi fa, ecc..

Obiettivo di tale tipo di analisi non è solo quello di illustrare compiutamente i risultati dell'intera attività, ma anche quello di confermare le valutazioni fatte.

Potrebbe infatti emergere che non è possibile trovare una giustificazione plausibile a un rischio elevato e che si è in realtà commesso un errore di valutazione o interpretazione del metodo nelle fasi precedenti.

Ovviamente questa fase può essere complessa: alcune volte le ragioni di un determinato risultato potrebbero trovarsi in punti “distanti” nella catena del modello.

Naturalmente, l'importanza dell'interpretazione si riflette anche sugli strumenti, che devono offrire funzionalità di reportistica raffinate quanto più possibile, onde consentire al team di concentrarsi non sulle forme di rappresentazione dei numeri, ma sul loro significato complessivo.

Strategie di gestione del rischio

Conosciuti i livelli di rischio cui sono esposti gli *asset* (o i processi, a seconda della vista offerta dalla metodologia) l'organizzazione/istituzione si trova a dover prendere decisioni sul “se” e sul “come” gestirli.

A livello macroscopico, la scelta cade di norma tra i due estremi di accettare i rischi o ridurli.

Nell'uno e nell'altro caso la decisione si fonda su una valutazione costi/benefici. Il rischio si accetta perché implementare adeguate contromisure/controlli non comporta un incremento conveniente in termini di maggiore protezione. Viceversa, si decide di ridurlo, predisponendo adeguate misure preventive o reattive.

L'analisi costi/benefici fa parte del lavoro di razionalizzazione del team di analisi al pari dell'attività di interpretazione dei risultati sopra descritta. Gli strumenti di analisi possono, in generale, essere utilizzati per fornire elementi per valutare l'efficacia di una determinata misura di sicurezza.

Per la valutazione del costo di una determinata misura di sicurezza occorrerà poi considerare diverse variabili. Ad esempio potrebbero essere considerati i seguenti aspetti: grado di competenza richiesta per mettere in piedi la misura, tempo necessario per implementarla, numero di utenti interessati, costo della licenza e della infrastruttura che dovrebbe ospitarla, ecc.

Successivamente, conclusa l'analisi e prese le decisioni di gestione dei rischi, occorre verificare se le misure implementate siano

effettivamente quelle giuste, misurandone l'efficacia.

Tale misurazione, che può essere basata sui concetti propri dei sistemi di qualità, può utilizzare gli strumenti messi a disposizione dagli strumenti di sicurezza stessi: log, alert, ecc.. Occorrerà però dotarsi di competenze specifiche e di strumenti software in grado di analizzare i dati prodotti da tali strumenti⁶.

Inoltre le misurazioni dovrebbero essere estese agli aspetti organizzativo/procedurali. La verifica di presa visione di una politica di sicurezza pubblicata sulla intranet, o di un *warning anti-phishing* via mail, piuttosto che di una campagna di *awareness* resa disponibile con una animazione on-line sulla home page, potrebbero fornire i dati necessari per calcolare tali tipi di indicatori.

L'obiettivo da raggiungere potrebbe essere quello di definire un *tableau de board*, alimentato anche dagli eventi di basso livello osservati dalla linea operativa, concentrata sugli esiti delle sonde di *intrusion detection*, piuttosto che sui tempi di risposta del server che ospita la *revocation authority*.

⁶ Alcuni esempi di indicatori di natura tecnica possono essere i seguenti:

- per la sicurezza delle applicazioni:
numero pagine vulnerabili al SQL injection/ totale pagine applicative, frequenza deploy sorgenti negli ambienti del ciclo di vita software, numero errori applicativi rilevati/ mese, numero interventi correttivi/ numero errori rilevati;
- per la sicurezza fisica:
numero guasti ai tornelli/ anno, numero guasti al sistema di condizionamento delle sale server/ anno, numero di black-out, numero furti per anno, numero prove di recovery da disastro, tempo medio di recovery da disastro, numero rilevatori antifumo per metri cubi, numero interventi di manutenzione per anno, tempo medio di intervento di manutenzione;
- per la sicurezza di rete:
frequenza scansioni di rete/ anno, numero di sistemi oggetto di scansione/ totale sistemi, frequenza di aggiornamento dei pattern delle vulnerabilità, frequenza di revisione delle regole dei firewall, frequenza aggiornamento antivirus, numero di virus rilevati, numero attacchi bloccati/ totale attacchi rilevati.



RISK ANALYSIS

Approfondimenti

PARTE SECONDA SCHEDE DESCRITTIVE

Nelle pagine che seguono, come già illustrato nella Guida alla Lettura di questo documento, sono riportate le schede descrittive di alcune metodologie e strumenti per l'analisi dei rischi ICT, che intendono costituire un punto di partenza per chi volesse approfondire le diverse alternative disponibili per l'attuazione di una analisi dei rischi.

Le schede sono state predisposte secondo un formato standard, in modo da consentire una esposizione schematica di quelli che sono sembrati, a parere di chi ha partecipato alla stesura di questo documento, gli aspetti più rilevanti da conoscere nel momento in cui si intendesse acquisire una conoscenza preliminare di una metodologia o uno strumento di analisi. Inoltre l'utilizzo di un formato consistente dovrebbe consentire la possibilità di una lettura comparata delle diverse schede.

E' necessario sottolineare, come già fatto nell'introduzione, che le metodologie e gli strumenti considerati rappresentano le metodologie e gli strumenti noti a coloro che hanno compilato le schede e non vogliono in alcun modo esaurire le diverse possibilità esistenti, né essere rappresentative del panorama attuale. Si tratta semplicemente, come detto, di un punto di partenza per il lettore che intendesse approfondire la tematica.

Inoltre anche all'interno delle singole schede, le informazioni riportate sono quelle note a chi le ha predisposte e potrebbero pertanto esistere ulteriori aspetti in esse non riportati.

AS/NZS 4360:2004 RISK MANAGEMENT

Informazioni fornite da Simona Napoli di KPMG

Ambito di applicazione:

Lo standard propone una guida generale alla gestione del rischio, descrivendo in tale ambito anche il processo di *risk assessment*, come insieme delle attività di *risk identification* (identificazione di cosa, dove, quando, perchè e come un evento potrebbe accadere), *risk analysis* (comprensione sistematica della natura e del livello di rischio) e *risk evaluation* (comparazione tra il livello di rischio e i criteri di valutazione dello stesso).

Poiché si tratta di una guida generale, lo standard può essere applicato a un'estesa varietà di attività, decisioni o operazioni da enti pubblici, imprese, associazioni o individui. E' indipendente da specifici settori industriali ed economici. Può essere applicato in tutte le fasi di vita di un'attività, una funzione, un progetto, un prodotto o un bene.

Esso inoltre, proprio perché di natura generale, può essere applicato sia ai rischi (cioè gli eventi che hanno un effetto negativo) sia alle opportunità (cioè gli eventi che hanno un effetto positivo). In questa scheda si sono considerati gli aspetti relativi ai rischi, tralasciando le considerazioni specifiche relative alle opportunità.

Standard di riferimento

La metodologia presentata è essa stessa uno standard (*Joint Standards Australia/ Standards New Zealand Committee*) emesso dall'ente normatore australiano SAI (*Standards Australia International* – www.standards.com.au).

Approccio alla misurazione dei rischi:

qualitativo quantitativo semi-quantitativo

Poiché AS/NZS ha l'obiettivo di definire il processo di *risk management* in modo generale (vedi "Ambito di applicazione") identifica e definisce tutte le diverse tipologie di approccio alla misurazione dei rischi

misurazione sia del rischio potenziale o intrinseco (cioè a prescindere dalle contromisure) sia del rischio effettivo o residuo (cioè tenendo conto delle contromisure poste in essere)

misurazione del rischio effettivo o residuo (cioè il rischio relativo alla situazione in essere, comprese le contromisure implementate)

misurazione del rischio potenziale o intrinseco (cioè a prescindere dalle contromisure adottate)

Concetti e definizioni chiave:

- RISCHIO:** [*Risk*] La possibilità che succeda qualcosa che abbia un impatto sugli obiettivi.
- MINACCIA:** [*Hazard*] Una fonte di danno potenziale.
- VULNERABILITA'¹:** Non utilizzato.
- DANNO:** [*Loss*] Qualunque conseguenza o effetto negativo, finanziario o di altra natura.
- IMPATTO:** Non utilizzato.
- CONSEGUENZE:** [*Consequence*] Risultato o impatto di un evento.

Altre definizioni:

CONTROLLO: [*Control*] Un processo, una *policy*, un apparato, una prassi o qualunque azione posta in essere per minimizzare i rischi.

EVENTO: [*Event*] Verificarsi di una particolare situazione.

FREQUENZA: [*Frequency*] Una misura del numero di occorrenze per unità temporale.

PROBABILITA': [*Probability*] La misura delle probabilità di accadimento espressa con un numero compreso tra 0 e 1.

RISCHIO RESIDUO: [*Residual risk*] Il rischio che resta dopo l'implementazione del "trattamento" del rischio.

"TRATTAMENTO" DEL RISCHIO: [*Risk treatment*] Il processo di selezione e implementazione delle misure finalizzate a cambiare la natura o il livello del rischio.

PARTI COINVOLTE: [*Stakeholders*] Le persone o le organizzazioni che potrebbero influenzare, essere influenzate o percepirsi come influenzate da una decisione, un'attività o un rischio.

¹ Le vulnerabilità non sono direttamente considerate nell'ambito dell'analisi dei rischi. Esse vengono considerate a valle dell'analisi, nell'ambito della fase di "trattamento" dei rischi (ricordiamo che lo standard in oggetto si riferisce all'intero processo di risk management, identificando l'analisi dei rischi come una parte dello stesso). In tale ambito un possibile "trattamento" consiste nel ridurre la vulnerabilità al rischio identificato. Anche nell'ambito del "trattamento" le vulnerabilità non sono direttamente menzionate: si parla piuttosto di riduzione del danno o riduzione della probabilità.

Elementi della Metodologia di misurazione dei rischi:

Come indicato in “ambito di applicazione”, lo standard descrive in modo generale il processo di *risk assessment* e in tale ambito l’attività di analisi dei rischi (comprensione sistematica della natura e del livello di rischio).

Il livello di rischio viene misurato come la combinazione tra le conseguenze e la possibilità che un evento si verifichi.

Lo standard identifica poi diverse modalità di valutazione di conseguenze e possibilità e in base a ciò classifica i diversi tipi di analisi dei rischi:

- l’analisi qualitativa utilizza parole per descrivere le conseguenze potenziali e la possibilità che tali conseguenze si concretizzino. Tale tipo di analisi può essere utilizzato:
 - per una valutazione iniziale finalizzata a identificare i rischi che richiedono analisi più approfondite;
 - nei casi in cui tale analisi è sufficiente per supportare le decisioni;oppure
 - se i dati quantitativi o le risorse disponibili sono inadeguate per un’analisi quantitativa;
- L’analisi semi-quantitativa utilizza scale qualitative come quelle descritte sopra, associandovi dei valori numerici. L’obiettivo è quello di produrre una scala per la classificazione dei rischi, non quello di ottenere un valore realistico del rischio, come nell’analisi quantitativa.
- L’analisi quantitativa utilizza valori numerici (e non scale descrittive, come nell’analisi qualitativa e semi-quantitativa) sia per le conseguenze sia per la possibilità, utilizzando dati provenienti da fonti diverse. La qualità dell’analisi dipende dall’accuratezza e dalla completezza dei valori numerici e dalla validità dei modelli utilizzati.

VALUTAZIONE DELLE RISORSE:

- | | | |
|-------------------------------------|--|---------------------------------------|
| <input type="checkbox"/> Dati | <input type="checkbox"/> Tecnologia | <input type="checkbox"/> Applicazioni |
| <input type="checkbox"/> Facilities | <input type="checkbox"/> Risorse umane | |

La valutazione delle risorse non viene direttamente considerata. Tuttavia essa è considerata in modo indiretto nella definizione dei criteri di valutazione dei rischi, cioè dei criteri che devono essere utilizzati per stabilire se intervenire a fronte di un certo rischio. Tali criteri possono essere di natura operativa, tecnica, finanziaria, legale, sociale, ambientale, umanitaria, ecc..

La valutazione del rischio viene pertanto effettuata confrontando il livello di rischio (conseguenze x possibilità) con i criteri di valutazione.

VALUTAZIONE DELL'IMPATTO:

- | | | |
|---------------------------------------|---|--|
| <input type="checkbox"/> Riservatezza | <input type="checkbox"/> Integrità | <input type="checkbox"/> Disponibilità |
| <input type="checkbox"/> Conformità | <input type="checkbox"/> Efficienza operativa | <input type="checkbox"/> Efficacia operativa |

Poiché si tratta di uno standard generale non vengono date indicazioni specifiche.

VALUTAZIONE DELLA PROBABILITA':

Poiché si tratta di uno standard generale non vengono date indicazioni specifiche.

VALUTAZIONE DELLE CONTROMISURE:

Lo standard indica che la valutazione di conseguenze e possibilità viene effettuata tenendo conto dell'efficacia delle strategie e dei controlli in essere.

Lo standard identifica quindi i diversi "trattamenti" del rischio:

- evitare il rischio decidendo di non iniziare o non proseguire l'attività che comporta il rischio;
- modificare la possibilità che un rischio si verifichi, riducendola
- modificare le conseguenze di un rischio, riducendone i danni
- condividere il rischio, coinvolgendo un altro soggetto, ad esempio attraverso contratti, assicurazioni, partnership, *joint venture*
- accettare il rischio

Lo standard indica che la scelta del "trattamento" più appropriato deve considerare il costo di implementazione del "trattamento" rispetto ai benefici che ne derivano.

- | | | |
|---|-------------------------------------|--|
| <input checked="" type="checkbox"/> riduzione probabilità | <input type="checkbox"/> preventive | <input type="checkbox"/> disegno della contromisura |
| <input checked="" type="checkbox"/> riduzione conseguenze | <input type="checkbox"/> reattive | <input type="checkbox"/> applicazione della contromisura |
| <input checked="" type="checkbox"/> evitare il rischio | | |
| <input checked="" type="checkbox"/> trasferire il rischio | | |
| <input checked="" type="checkbox"/> accettare il rischio | | |

Approccio:

La metodologia prevede l'applicazione dell'analisi dei rischi su:

- | | | |
|--|---|--|
| <input checked="" type="checkbox"/> processi | <input checked="" type="checkbox"/> risorse di business | <input checked="" type="checkbox"/> risorse tecnologiche |
|--|---|--|

Si tratta di uno standard generale applicabile a qualunque "oggetto".

Passi metodologici :

Lo standard descrive il più complesso processo di *risk management* suddividendolo nelle seguenti fasi (quelle in neretto fanno parte del *risk assessment*):

- 1 **Comunicazione e condivisione:**
Comunicazione e condivisione con le parti coinvolte, interne ed esterne, in ogni fase del processo di *risk management* e nel processo di *risk management* nel suo complesso.
- 2 **Definizione del contesto:**
Identificazione del contesto interno ed esterno e di quello di gestione dei rischi, al fine di definire i criteri in base ai quali valutare i rischi e la “struttura” dell’analisi che si intende effettuare
- 3 **Identificazione dei rischi**
Indicazione su dove, quando, perché e come il verificarsi di un evento potrebbe comportare un degrado, un ritardo o un miglioramento degli obiettivi.
- 4 **Analisi dei rischi**
Identificazione e valutazione dei controlli esistenti. Determinazione delle conseguenze e delle possibilità e, quindi, del livello di un rischio. L’analisi considera diverse conseguenze potenziali e come queste potrebbero verificarsi.
- 5 **Valutazione dei rischi**
Confronto dei livelli stimati di rischio con i criteri di valutazione definiti considerando sia i potenziali benefici sia le conseguenze negative. La valutazione dei rischi consente di decidere sull’estensione e sulla natura dei “trattamenti” richiesti e di definire le priorità.
- 6 **“Trattamento” dei rischi**
Sviluppo e implementare specifiche strategie e piani di azione per aumentare i potenziali benefici o ridurre i potenziali danni.
- 7 **Monitoraggio e miglioramento**
E’ necessario monitorare l’efficacia di tutte le attività del processo di *risk management*, in un’ottica di miglioramento continuo. Inoltre i rischi e l’efficacia dei “trattamenti” devono essere monitorati per assicurare che i cambiamenti non comportino priorità diverse.

Tool a supporto: software

Per molti tool software di supporto al *Risk Management* i produttori dichiarano la conformità allo standard AS/NZS 4360

 questionari/ *check-list*, ecc. manuali e linee guida

- “AS/NZS 4360:2004 Risk management” è lo standard pubblicato dal SAI.
- “HB 436:2004 Risk Management Guidelines - Companion to AS/NZS 4360:2004”
Si tratta di una guida pubblicata dal SAI e fornisce linee guida per l'applicazione dello standard, fornendo esempi e indicazioni, per ciascuna delle sette fasi previste dallo standard stesso
- Esistono poi altre guide di altri autori (non pubblicate direttamente dal SAI)

 disponibilità training

- Online Training Course
Corso sviluppato dal SAI Global and Catalyst Communications and Training, è un corso base che illustra il modello di risk management definito dallo standard AS/NZS 4360:2004

 disponibilità aggiornamenti periodici

Lo standard viene aggiornato dal SAI, secondo esigenza (non periodicamente). La versione disponibile è stata aggiornata nel 2004.

 possibilità di personalizzazioni

Nessuna informazione specifica da segnalare.

Risultati ottenibili :

L'obiettivo di questo standard è quello di fornire una guida alle imprese pubbliche e private, a gruppi ed individui per ottenere:

- una base più affidabile e rigorosa per prendere decisioni e per la pianificazione;
- una migliore identificazione delle opportunità e delle minacce;
- un guadagno a partire dall'incertezza e dalla variabilità;
- una gestione preventiva piuttosto che reattiva;
- una più efficace allocazione ed utilizzo delle risorse;
- una migliore gestione degli incidenti ed una riduzione delle perdite e del costo del rischio, inclusi i premi per le assicurazioni;
- un innalzamento della fiducia degli stakeholder;
- un incremento nell'aderenza della legislazione rilevante;
- un miglior governo dell'impresa.

Lingua

Italiano

Inglese

Altro _____

BSA Baseline Security Assessment*Informazioni fornite da Roberta Bruzzone di ICAA (International Crime Analysis Association)***Ambito di applicazione :**

Il metodo BSA permette di valutare i rischi pertinenti ai sistemi informativi aziendali. La definizione e la presentazione degli indici di rischio avviene tramite un report suddiviso in cinque "security domains". L'executive summary dei risultati si basa su grafici e risulta adatto per agevolare la lettura dei risultati anche al management non esperto sulle problematiche di information security. L'analisi BSA risulta particolarmente adatta ad organizzazioni caratterizzate da complessità media/medio-alta.

Standard di riferimento:

ISO/IEC 17799; Common Criteria ISO/IEC 15408; D.Lgs. 196/03

Approccio alla misurazione dei rischi :

qualitativo quantitativo semi-quantitativo

misurazione sia del rischio potenziale o intrinseco (cioè a prescindere dalle contromisure) sia del rischio effettivo o residuo (cioè tenendo conto delle contromisure poste in essere)

misurazione del rischio effettivo o residuo (cioè il rischio relativo alla situazione in essere, comprese le contromisure implementate)

misurazione del rischio potenziale o intrinseco (cioè a prescindere dalle contromisure adottate)

Concetti e definizioni chiave :

RISCHIO: Indice numerico normalizzato che definisce la probabilità che si verifichi una perdita di qualità delle informazioni (confidenzialità, integrità, disponibilità) a seguito di un evento/azione. Il rischio viene pesato in base al livello protezione garantito dalle contromisure già adottate ed all'importanza che il singolo ambito/asset ha nel contesto dell'organizzazione (business related value). Il rischio residuo rappresenta il livello di rischio normalizzato calcolato in seguito all'applicazione delle contromisure critiche o di tutte le contromisure indicate.

MINACCIA: L'esistenza di fattori avversi che possano avere interesse, capacità ed intenzione di compromettere informazioni, attività, organizzazione o sistemi critici; la minaccia può nascere da fattori fisici, ambientali e da azioni intenzionali perpetrate o meno ad opera di soggetti terzi.

VULNERABILITA': Rappresentano punti deboli dell'infrastruttura a diversi livelli (fisico, sistema operativo, applicazioni, audit, procedure, policy, formazione, controlli, network, ecc.) che possono facilitare la violazione dolosa, colposa o accidentale di una o più componenti del sistema informativo.

DANNO: Non utilizzato IMPATTO: Non utilizzato CONSEGUENZE: Non utilizzato

Elementi della Metodologia di misurazione dei rischi :

I fattori presi in considerazione durante l'analisi sono:

- organizzazione del reparto IT: la struttura preposta all'erogazione dei servizi IT rappresenta un punto di partenza fondamentale per valutare gli aspetti relativi al security management ed alle best practice adottate quotidianamente nella gestione dei servizi;
- struttura informatica esistente: l'analisi dell'architettura informativa intesa come:
 - struttura e topologia della rete (Intranet/Internet/ Extranet)
 - piattaforme hardware e software adottate
 - applicazioni di business e produttività generale
 - requisiti ed esigenze di disponibilità del prodotto IT aziendale;
- contromisure implementate e/o in corso di realizzazione: valutazione dell'infrastruttura di sicurezza e dei livelli di contromisure raggiunti per classi omogenee di minacce;
- security assessment precedenti: valutazione delle vulnerabilità e delle contromisure già individuate per ogni ambito tecnologico di riferimento;
- principali servizi e processi aziendali legati al Sistema Informativo Aziendale (SIA): censimento dei principali servizi erogati nell'ambito del SIA;
- organizzazione aziendale e valutazione del core -business: censimento dei processi e dei servizi critici rispetto al core -business aziendale, necessari ad una corretta valutazione dei rischi aziendali.

VALUTAZIONE DELLE RISORSE:

- | | | |
|--|--|--|
| <input checked="" type="checkbox"/> Dati | <input checked="" type="checkbox"/> Tecnologia | <input checked="" type="checkbox"/> Applicazioni |
| <input checked="" type="checkbox"/> Facilities | <input type="checkbox"/> Risorse umane | |

VALUTAZIONE DELL'IMPATTO:

- | | | |
|--|---|---|
| <input checked="" type="checkbox"/> Riservatezza | <input checked="" type="checkbox"/> Integrità | <input checked="" type="checkbox"/> Disponibilità |
| <input checked="" type="checkbox"/> Conformità | <input type="checkbox"/> Efficienza operativa | <input type="checkbox"/> Efficacia operativa |

L'analisi viene condotta sulle aree critiche e sulla capacità di ciascuna di rispettare i requisiti di riservatezza, integrità e disponibilità

VALUTAZIONE DELLE CONTROMISURE:

- | | | |
|--|-------------------------------------|--|
| <input type="checkbox"/> riduzione probabilità | <input type="checkbox"/> preventive | <input type="checkbox"/> disegno della contromisura |
| <input type="checkbox"/> riduzione conseguenze | <input type="checkbox"/> reattive | |
| <input type="checkbox"/> evitare il rischio | | <input type="checkbox"/> applicazione della contromisura |
| <input type="checkbox"/> trasferire il rischio | | |
| <input type="checkbox"/> accettare il rischio | | |

La criticità delle contromisure, intesa come livello di mitigazione del rischio appurato rispetto al costo, viene misurata su una scala con cinque livelli: critica, elevata, media, medio-bassa, bassa.

Approccio:

La metodologia prevede l'applicazione dell'analisi dei rischi su:

processi risorse di business risorse tecnologiche

L'analisi viene condotta anche con riferimento alla documentazione ufficiale.

Passi metodologici:

- Familiarizzazione
Valutazione globale dei rischi nell'ottica di una "baseline -security". Prevede una rilevazione delle vulnerabilità, effettuata in modo strumentale (a campione) sull'infrastruttura oggetto della BSA ed attraverso l'utilizzo di interviste semi - strutturate. In questa fase viene acquisita ed analizzata la documentazione prodotta in termini di policy, standard/guidelines, procedure e privacy.
- Analisi del rischio
Generazione di un report finale detto "mappa del rischio" nel quale sono sintetizzati i livelli di con tromisure attuali ed il rischio residuo per ciascun ambito di indagine.
- Security Roadmap
Illustrazione delle priorità degli investimenti considerando, oltre le minacce tecnologiche, anche gli aspetti legati al core -business ed all'organizzazione aziendale

Tool a supporto:

- software
- questionari/ check -list, ecc.
- Questionario semi -strutturato BSA.
- manuali e linee guida
- disponibilità training
- disponibilità aggiornamenti periodici
- possibilità di personalizzazioni

Contestualizzabile in base a lle peculiarità dell'organizzazione analizzata.

Risultati ottenibili:

Un'istantanea sullo stato della sicurezza del sistema informativo aziendale.

Lingua

Italiano Inglese Altro _____

Ce.TRA - Continuous e.Business Threat and Risk Analysis

Informazioni fornite da Federico Sandrucci del Ministero della Difesa

<u>Ambito di applicazione :</u>
La metodologia è utilizzabile per l'analisi e la gestione dei rischi cui sono esposte le informazioni trattate mediante sistemi informatici o anche non automatizzati.
<u>Standard di riferimento</u> ISO/IEC 17799; CRAMM (<i>Computer Risk Analysis Management Methodology</i>). La formulazione di Ce.TRA è una derivazione del modello adottato dal CSE (<i>Communication Security Establishment</i>) Government of Canada; assicura la piena aderenza ai requisiti richiesti dalla legge 196/03 ed in particolare al punto 19 dell'Allegato B in tema di Analisi dei Rischi.
<u>Approccio alla misurazione dei rischi</u> <input type="checkbox"/> qualitativo <input type="checkbox"/> quantitativo <input checked="" type="checkbox"/> semi-quantitativo
<input checked="" type="checkbox"/> misurazione sia del rischio potenziale o intrinseco (cioè a prescindere dalle contromisure) sia del rischio effettivo o residuo (cioè tenendo conto delle contromisure poste in essere) <input type="checkbox"/> misurazione del rischio effettivo o residuo (cioè il rischio relativo alla situazione in essere, comprese le contromisure implementate) <input type="checkbox"/> misurazione del rischio potenziale o intrinseco (cioè a prescindere dalle contromisure adottate)
<u>Concetti e definizioni chiave :</u>
<input checked="" type="checkbox"/> RISCHIO: Esposizione dell'azienda a perdite di varia natura (economiche, di immagine, ecc) che possono concretizzarsi a causa di agenti esterni in grado di sfruttare le vulnerabilità dei processi, delle risorse e dei sistemi adibiti al trattamento delle informazioni.
<input checked="" type="checkbox"/> MINACCIA: Un evento potenziale che sfruttando le vulnerabilità dei sistemi può produrre un danno alle informazioni.
<input checked="" type="checkbox"/> VULNERABILITA': Punti deboli dei sistemi che possono essere sfruttati da un agente per portare una minaccia.
<input checked="" type="checkbox"/> DANNO: Violazione della riservatezza, dell'integrità o della disponibilità delle informazioni.
<input checked="" type="checkbox"/> IMPATTO: È il danno concreto per l'azienda in termini di Responsabilità Penale, Responsabilità Civile, perdita di Immagine, disservizi nei confronti dell'utenza, danni economici indotti dalla violazione della sicurezza delle informazioni.
<input type="checkbox"/> CONSEGUENZE: Non utilizzato.

Altre definizioni:

AGENTE: Latore di una minaccia

BENE (ASSET): Le informazioni dell'Organizzazione

SCENARIO: La quadrupla (rischio, minaccia, bene, vulnerabilità) che denota una possibile combinazione di una minaccia che sfruttando una vulnerabilità dei sistemi può attaccare una informazione e portare ad un rischio di violazione della riservatezza, dell'integrità o della disponibilità delle informazioni

Elementi della Metodologia di misurazione dei rischi

Per ciascuno scenario si misurano le grandezze fondamentali bene, minaccia e vulnerabilità; il rischio è una grandezza derivata:

- minaccia: è valutata in base alla motivazione (M) ed alla capacità (C) dell'agente nel portare l'attacco. La motivazione e la capacità, sono misurati con una scala a tre valori, la minaccia con una scala a cinque valori;
- vulnerabilità: è valutata in base alla severità (S) della vulnerabilità e all'esposizione (E) del bene al danneggiamento a causa della vulnerabilità. La severità e l'esposizione sono misurati su una scala a tre valori, la vulnerabilità con una scala a cinque valori;
- la probabilità di accadimento di uno Scenario è una grandezza derivata ottenuta dalla combinazione della vulnerabilità del sistema sfruttabile dalla minaccia, secondo il principio che maggiori sono la minaccia e la vulnerabilità maggiore sarà la probabilità;
- il danno inerente ad uno scenario è una grandezza derivata ottenuta dalla combinazione della minaccia con il bene esposto a danno, secondo il principio che maggiori sono la minaccia ed il bene maggiore sarà il danno.

Sia il danno sia la probabilità sono misurati su una scala a nove valori riconducibili a tre classi basso medio e alto.

Il rischio per ciascuno degli scenari valorizzati è valutato come il prodotto aritmetico della probabilità di accadimento di un evento dannoso (Minaccia) per il danno potenziale che la minaccia può causare. Probabilità e danno sono convertiti in indicatori numerici ed il rischio assume un insieme discreto di valori da 1 a 81.

VALUTAZIONE DELLE RISORSE:

- | | | |
|--|--|---------------------------------------|
| <input checked="" type="checkbox"/> Dati | <input type="checkbox"/> Tecnologia | <input type="checkbox"/> Applicazioni |
| <input type="checkbox"/> Facilities | <input type="checkbox"/> Risorse umane | |

VALUTAZIONE DELL'IMPATTO:

- | | | |
|--|---|---|
| <input checked="" type="checkbox"/> Riservatezza | <input checked="" type="checkbox"/> Integrità | <input checked="" type="checkbox"/> Disponibilità |
| <input type="checkbox"/> Conformità | <input type="checkbox"/> Efficienza operativa | <input type="checkbox"/> Efficacia operativa |

I requisiti di riservatezza, integrità e disponibilità delle informazioni sono misurati con una scala a cinque livelli.

VALUTAZIONE DELLA PROBABILITA':

E' indicata in Elementi della Metodologia di misurazione dei rischi

VALUTAZIONE DELLE CONTROMISURE:

Una rappresentazione dei rischi per ciascun singolo bene o scenario su un diagramma probabilità/danno (diagramma Pb/D), consente di illustrare graficamente i criteri con cui determinare la strategia di abbattimento del rischio.

- | | | |
|---|-------------------------------------|--|
| <input checked="" type="checkbox"/> riduzione probabilità | <input type="checkbox"/> preventive | <input checked="" type="checkbox"/> disegno della contromisura |
| <input type="checkbox"/> riduzione conseguenze | <input type="checkbox"/> reattive | <input type="checkbox"/> applicazione della contromisura |
| <input checked="" type="checkbox"/> evitare il rischio | | |
| <input checked="" type="checkbox"/> trasferire il rischio | | |
| <input checked="" type="checkbox"/> accettare il rischio | | |

Approccio:

La metodologia prevede l'applicazione dell'analisi dei rischi su:

- | | | |
|--|---|--|
| <input checked="" type="checkbox"/> processi | <input checked="" type="checkbox"/> risorse di business | <input checked="" type="checkbox"/> risorse tecnologiche |
|--|---|--|

Tali elementi sono considerati in quanto costituenti l'infrastruttura adibita alla gestione e trattamento delle informazioni. L'analisi consiste nell'identificare e nello stimare le loro vulnerabilità.

Passi metodologici :

- 1 **Preparazione e Pianificazione**
In questa fase si determinano gli obiettivi del TRA e si definisce il perimetro di intervento. Si individuano le informazioni oggetto dell'analisi e si procede alla descrizione dei processi, delle risorse, e dei sistemi adibiti al trattamento delle informazioni, si costituisce il gruppo di lavoro, si stabiliscono i valori di soglia del rischio accettabile e del rischio limite, si formula il piano di lavoro.
- 2 **Raccolta dati**
In questa fase sono identificate le minacce e le vulnerabilità reali del sistema sulla base dei cataloghi propri della metodologia. La raccolta dati inizia con una collezione della documentazione inerente il sistema ed è poi completata con la tecnica dell'auditing, mediante intervista delle persone che rivestono un ruolo nella gestione del sistema, la somministrazione di questionari, la visita dei siti.
- 3 **Definizione degli Scenari**
In questa fase sono individuati gli scenari. Per ciascuna tipologia di informazioni, mediante una matrice di correlazione che associa ciascuna minaccia alle vulnerabilità sfruttabili ed ai rischi di violazione della riservatezza, dell'integrità e della disponibilità dell'informazione, si individuano le quadruple (rischio, bene, minaccia, vulnerabilità) significative.
- 4 **Analisi della criticità delle Informazioni**
In questa fase avviene la valutazione della criticità delle informazioni oggetto dell'analisi e sono identificate le informazioni maggiormente sensibili per il business aziendale.
- 5 **Analisi delle Minacce e delle Vulnerabilità**
In questa fase sono valutate le minacce e le vulnerabilità identificate con la Raccolta dati.
- 6 **Analisi dei Rischi**
In questa fase si procede alla valutazione della probabilità di accadimento, del danno potenziale e del rischio per ciascuno scenario.
Gli scenari sono raggruppati per tipologia di rischio e, per ciascun gruppo, è calcolato il rischio medio; tali valori sono poi confrontati con i valori di soglia del rischio accettabile e del rischio limite.
Si ottiene per risultato una classifica che evidenzia i maggiori rischi, le informazioni più esposte a danno, le minacce più pericolose e le vulnerabilità maggiormente sfruttabili.
- 7 **Gestione dei Rischi**
Mediante una simulazione della riduzione del rischio, che si ottiene agendo sul valore stimato dei beni, delle minacce e delle vulnerabilità, si individua la migliore strategia per ricondurre il rischio al di sotto della soglia del rischio accettabile.
Al termine della simulazione si ha un quadro preciso di quali siano i rischi accettabili e quali invece possano essere evitati, ridotti e trasferiti.

Tool a supporto :

software

Suite Microsoft Office

questionari/ check -list, ecc.

La metodologia fa uso di cataloghi di minacce e vulnerabilità standard aggiornati sulla base di *alert advisory bulletin* . Le minacce e le vulnerabilità catalogate sono messe in corrispondenza in una matrice di correlazione. La metodologia include anche un questionario per il censimento delle informazioni.

manuali e linee guida

disponibilità training

disponibilità aggiornamenti periodici

possibilità di personalizzazioni

Risultati ottenibili :

Non sono emersi elementi specifici

Lingua

Italiano

Inglese

Altro _____

CRAMM

Informazioni fornite da Francesco Gentile di Gfi Ois e Giampaolo Scafuro di RETIS Consulting

Ambito di applicazione:

Il metodo permette di valutare i rischi relativi ai sistemi informativi aziendali.

Standard di riferimento

British Standard on Information Security Management (BS 7799); Information Technology Security Evaluation Criteria (ITSEC); Computer Security Evaluation Criteria (TCSEC) and Common Criteria; HMG Manual of Protective Security; HMG Infosec Standards; CESG Memoranda; CISCO's white paper on setting up routers; Fred Cohen's paper Protecting against Distributed Denial of Service Attacks

Approccio alla misurazione dei rischi:

- qualitativo quantitativo semi-quantitativo
- misurazione sia del rischio potenziale o intrinseco (cioè a prescindere dalle contromisure) sia del rischio effettivo o residuo (cioè tenendo conto delle contromisure poste in essere)
- misurazione del rischio effettivo o residuo (cioè il rischio relativo alla situazione in essere, comprese le contromisure implementate)
- misurazione del rischio potenziale o intrinseco (cioè a prescindere dalle contromisure adottate)

Concetti e definizioni chiave:

- RISCHIO:** misura dell'esposizione di un sistema alla terna impatti, minacce, vulnerabilità
- MINACCIA:** Potenziale violazione di un requisito di sicurezza. E' indagata attraverso questionari.
- VULNERABILITA':** Una debolezza o una carenza di controlli che potrebbe portare ad una attuazione della minaccia verso un asset o un gruppo di asset. E' indagata attraverso questionari.
- DANNO:** Il danno non ha autonoma definizione. E' indagato indirettamente attraverso il concetto di impatto e scenari di impatto.
- IMPATTO:** L'effetto di una violazione di un requisito di sicurezza (disponibilità, integrità, riservatezza)
- CONSEGUENZE:** Non utilizzato

Elementi della Metodologia di misurazione dei rischi:

Il rischio è una grandezza derivata, funzione di *asset*, minaccia e vulnerabilità

Gli *asset* (dati, servizi/processi, dispositivi hardware e software, sito geografico) sono valutati in termini di valore intrinseco (se noto) e/o di impatti a seguito di una indisponibilità, mancanza di riservatezza o di integrità. Essi sono poi messi in relazione attraverso modelli (*asset model*), sempre a partire dai dati: in questo senso la metodologia è *data oriented*.

Il set di minacce e vulnerabilità è fisso e guidato dal tipo di *asset*.

Il rischio assoluto è espresso, attraverso un'opportuna matrice, come funzione di impatto/minaccia/vulnerabilità.

Le contromisure sono selezionate in base al loro stato di implementazione ed in relazione al loro peso complessivo nell'abbattimento del rischio; la valutazione dipende a sua volta da diversi parametri (costo, grado di efficacia, assenza di misure alternative e altri), personalizzabili secondo le esigenze.

VALUTAZIONE DELLE RISORSE:

La metodologia è "data centrica": l'informazione è il bene da proteggere.

Si crea un modello che schematizza le relazioni tra i dati, i processi che li utilizzano e le apparecchiature hardware e software tramite le quali vengono elaborati. Di un certo dato si sa quindi su quale server risiede, quali dispositivi di rete utilizza per essere trasmesso, quali utenti lo possono consultare o trattare, ecc..

- | | | |
|--|--|--|
| <input checked="" type="checkbox"/> Dati | <input checked="" type="checkbox"/> Tecnologia | <input checked="" type="checkbox"/> Applicazioni |
| <input type="checkbox"/> Facilities | <input type="checkbox"/> Risorse umane | |

VALUTAZIONE DELL'IMPATTO:

La valutazione degli impatti è effettuata su una scala di 10 valori.

- | | | |
|--|---|---|
| <input checked="" type="checkbox"/> Riservatezza | <input checked="" type="checkbox"/> Integrità | <input checked="" type="checkbox"/> Disponibilità |
| <input type="checkbox"/> Conformità | <input type="checkbox"/> Efficienza operativa | <input type="checkbox"/> Efficacia operativa |

VALUTAZIONE DELLA PROBABILITA':

La probabilità viene derivata dalla valutazione delle vulnerabilità (su una scala da 1 a 3) e delle minacce (su una scala da 1 a 5). Sulla base di tali valutazioni il software CRAMM calcola la misura del rischio.

VALUTAZIONE DELLE CONTROMISURE:

- | | | |
|---|--|--|
| <input checked="" type="checkbox"/> riduzione probabilità | <input checked="" type="checkbox"/> preventive | <input type="checkbox"/> disegno della contromisura |
| <input checked="" type="checkbox"/> riduzione conseguenze | <input checked="" type="checkbox"/> reattive | <input type="checkbox"/> applicazione della contromisura |
| <input checked="" type="checkbox"/> evitare il rischio | | |
| <input checked="" type="checkbox"/> trasferire il rischio | | |
| <input checked="" type="checkbox"/> accettare il rischio | | |

Le contromisure individuate dal software CRAMM considerano tutti i fattori sopra indicati, con opportuni pesi.

ALTRI ELEMENTI: E' definito il Fattore di Costo associato alla contromisura (Basso, Medio, Alto) e la tipologia della contromisura: procedurale, software, hardware, comunicazione, fisico.

Per ogni contromisura il software CRAMM indica su quali e quante minacce la stessa contromisura impatta.

Approccio:

La metodologia prevede l'applicazione dell'analisi dei rischi su:

processi risorse di business risorse tecnologiche

Passi metodologici:

- 1 Avvio
Raccolta di informazioni sull'ambito dell'analisi e gli *owner* da coinvolgere.
- 2 Identificazione e valutazione degli *asset*
 - a. Individuazione dei dati e delle informazioni da proteggere (secondo il core business dell'organizzazione) e definizione del perimetro di analisi, dell'architettura di rete, degli *asset* fisici, degli applicativi e dei processi aziendali.
 - b. Associazione degli *asset* (*asset modeling*) con indicazioni sulle relazioni che esistono tra dati, processi, applicativi, software e hardware.
 - c. Valutazione degli impatti, tramite questionari da sottoporre all'organizzazione.
- 3 *Assessment* sulle minacce e vulnerabilità
Rilevazione del grado di vulnerabilità e minaccia, attraverso questionari da sottoporre all'organizzazione.
- 4 *Risk analysis*
Calcolo dell'esposizione al rischio da parte del software CRAMM, una volta inseriti i valori dei questionari su vulnerabilità e minacce.
- 5 *Risk management*
Il software CRAMM elabora e propone le contromisure che possono successivamente essere analizzate e rielaborate e personalizzate dall'analista.

Tool a supporto:

- software
CRAMM per l'analisi dei rischi, interfaccia grafica facile da utilizzare se si conosce bene la metodologia.
- questionari/ check-list, ecc.
- manuali e linee guida
Esiste il manuale per l'utilizzo in CRAMM, in lingua inglese con riferimenti specifici allo standard BS 7799
- disponibilità training
- disponibilità aggiornamenti periodici
Gli aggiornamenti del tool CRAMM, le nuove versioni, sono inviati all'acquirente al loro rilascio
- possibilità di personalizzazioni

Risultati ottenibili :

Si ottiene una vista a vari livelli di dettaglio dei rischi sugli asset dell'organizzazione. La reportistica generata dallo strumento è completa ma in inglese, il che può anche costituire un ostacolo.

Lo strumento consente ad utilizzatori esperti di personalizzare funzionalità e tabelle.

Lingua

Italiano

Inglese

Altro _____

Defender Manager

Informazioni fornite da Giulio Carducci di Securteam -Elsag

<u>Ambito di applicazione :</u>
<p>Il metodo permette, in un'ottica intrinsecamente preventiva, di valutare i rischi pertinenti le risorse di business (segnatamente informazioni) e le risorse asservite alle stesse per il loro trattamento (risorse tecnologiche). Il metodo è efficacemente adottato anche per la valutazione dei rischi pertinenti i processi aziendali attraverso l'analisi dei relativi macrodati interessati.</p> <p>Può essere particolarmente adatto ad aziende con complessità medio/grande e gruppi industriali.</p>
<u>Standard di riferimento</u>
<p>BS7799</p> <p>E' possibile riferirsi a qualsiasi altro standard, modificando adeguatamente la base di conoscenza editabile.</p>
<u>Approccio alla misurazione dei rischi :</u>
<p><input checked="" type="checkbox"/> qualitativo <input type="checkbox"/> quantitativo <input type="checkbox"/> semi-quantitativo</p>
<p><input checked="" type="checkbox"/> misurazione sia del rischio potenziale o intrinseco (cioè a prescindere dalle contromisure) sia del rischio effettivo o residuo (cioè tenendo conto delle contromisure poste in essere)</p> <p><input type="checkbox"/> misurazione del rischio effettivo o residuo (cioè il rischio relativo alla situazione in essere, comprese le contromisure implementate)</p> <p><input type="checkbox"/> misurazione del rischio potenziale o intrinseco (cioè a prescindere dalle contromisure adottate)</p>
<u>Concetti e definizioni chiave :</u>
<input checked="" type="checkbox"/> RISCHIO: Rispetto a una certa minaccia è il prodotto logico tra la probabilità di accadimento della stessa e il danno arrecabile.
<input checked="" type="checkbox"/> MINACCIA: Evento potenzialmente dannoso
<input type="checkbox"/> VULNERABILITA': Questo concetto non compare esplicitamente nella metodologia, essendo compreso nel concetto di "livello di esposizione a una determinata minaccia di un determinato componente".
<input checked="" type="checkbox"/> DANNO: Risultanza negativa dell'attuazione di una minaccia per il tramite di un attacco che ha successo. Viene valutato qualitativamente.
<input type="checkbox"/> IMPATTO: Sinonimo di "danno", il termine non compare nella metodologia.
<input checked="" type="checkbox"/> CONSEGUENZE: Un insieme di "conseguenze dannose" sono considerate nei questionari che conducono alla valutazione del grado di criticità dei componenti.

Altre definizioni:

COMPONENTE: Lo scenario da analizzare è descritto come un insieme di componenti (rete, server, clients, software, etc.). Un componente di particolari caratteristiche è costituito dalle informazioni.

LIVELLO DI ESPOSIZIONE: Di un determinato componente, il suo livello di esposizione (alto, medio, basso) a una determinata minaccia.

ATTACCO: Modalità con cui si attua una certa minaccia.

CRITICITA': Qualità riferita ai dati e, per eredità da questi, anche ai componenti; essa "pilota" l'esigenza di protezione e i livelli di robustezza delle contromisure.

CONTROMISURE: Difese da adottare per contrastare gli attacchi in funzione della criticità dei componenti rilevata. Sono specificate a due livelli di astrazione, denominati "specifiche funzionali" e "specifiche attuative".

Elementi della Metodologia di misurazione dei rischi :

L'analisi dei rischi viene effettuata per ciascun componente, in funzione della sua criticità e del suo livello di esposizione a ciascuna minaccia prevista e pertinente.

La metrica adottata è fondamentalmente di tipo qualitativo.

Il livello finale di rischio viene determinato tramite il prodotto logico di indici numerici tarabili (che possono essere relativi alla criticità del componente, al suo livello di esposizione a un certo attacco o alla severità dell'attacco stesso) ed è utilizzato per "pilotare" le adeguate contromisure con l'opportuno livello di robustezza.

VALUTAZIONE DELLE RISORSE:

- | | | |
|--|---|---------------------------------------|
| <input checked="" type="checkbox"/> Dati | <input checked="" type="checkbox"/> Tecnologia | <input type="checkbox"/> Applicazioni |
| <input type="checkbox"/> Facilities | <input checked="" type="checkbox"/> Risorse umane | |

I dati sono l'elemento di riferimento per la valutazione della criticità, articolata nei valori alto-medio-basso riferita a ciascuno dei tre parametri Riservatezza -Integrità-Disponibilità. Ai fini della valutazione, i dati sono raggruppati in macrodati, concetto inteso come insieme di dati omogenei per supporto fisico utilizzato ed esigenze di protezione.

Nella definizione dello scenario, oltre ai dati sono presi in considerazione altri componenti, quali reti, server, client, risorse umane, ecc. Tali componenti ereditano la criticità in funzione della criticità dei macrodati che vengono trattati.

VALUTAZIONE DELL'IMPATTO:

- | | | |
|--|---|---|
| <input checked="" type="checkbox"/> Riservatezza | <input checked="" type="checkbox"/> Integrità | <input checked="" type="checkbox"/> Disponibilità |
| <input type="checkbox"/> Conformità | <input type="checkbox"/> Efficienza operativa | <input type="checkbox"/> Efficacia operativa |

VALUTAZIONE DELLA PROBABILITA':

Il concetto di probabilità viene inteso come livello di esposizione a un determinato attacco e misurato qualitativamente con la terna Alto -Medio-Basso.

VALUTAZIONE DELLE CONTROMISURE:

Il disegno della contromisura è specificato a due livelli di astrazione: specifica funzionale e specifica attuativa.

- | | | |
|---|--|--|
| <input checked="" type="checkbox"/> riduzione probabilità | <input checked="" type="checkbox"/> preventive | <input checked="" type="checkbox"/> disegno della contromisura |
| <input type="checkbox"/> riduzione conseguenze | <input checked="" type="checkbox"/> reattive | <input type="checkbox"/> applicazione della contromisura |
| <input type="checkbox"/> evitare il rischio | | |
| <input type="checkbox"/> trasferire il rischio | | |
| <input type="checkbox"/> accettare il rischio | | |

Approccio:

La metodologia prevede l'applicazione dell'analisi dei rischi su:

- | | | |
|-----------------------------------|---|--|
| <input type="checkbox"/> processi | <input checked="" type="checkbox"/> risorse di business | <input checked="" type="checkbox"/> risorse tecnologiche |
|-----------------------------------|---|--|

Passi metodologici:

- 1 Individuazione dello scenario di riferimento da analizzare
- 2 Individuazione dei macrodati e dei componenti tecnologici e organizzativi asserviti al loro trattamento.
- 3 Classificazione della criticità dei macrodati e, per eredità da questi, dei componenti utilizzati nel loro trattamento.
- 4 Stima del livello di esposizione, per ciascun componente, ai diversi attacchi previsti nella base di conoscenza.
- 5 Calcolo automatico dei livelli di rischio, per componente, sistema, scenario e individuazione delle pertinenti suggerite contromisure, con l'adeguato livello di robustezza.
- 6 Accettazione o rifiuto delle misure suggerite.
- 7 Calcolo del corrispondente livello residuo di rischio.
- 8 Consolidamento del piano di protezione definitivo e accesso alla fase di gestione dell'installazione delle contromisure.

Tool a supporto :

software

La metodologia è totalmente istanziata in un software applicativo, denominato appunto "Defender Manager".

questionari/ check -list, ecc.

Nel software applicativo sono inclusi i questionari per supportare la classificazione dei macrodati .

manuali e linee guida

Manuale d'uso per l'utente.

disponibilità training

E' previsto un training personalizzato fino alla realizzazione di un progetto prototipale.

disponibilità aggiornamenti periodici

Previsti, sia per il codice e che per la base di conoscenza.

possibilità di personalizzazioni

Il software può essere personalizzato anche negli aspetti riguardanti la tipologia della base di conoscenza.

Risultati ottenibili :

- il livello di rischio intrinseco calcolato per componente, sistema, scenario;
- i profili di protezione suggeriti, con indicazione delle diverse contromisure a livello di specifica sia funzionale che attuativa;
- il livello di rischio residuo in modalità "what if" per componente, sistema, scenario;
- l'indice del livello di rischio residuo di scenario, al variare delle contromisure adottate;
- il piano aggiornabile di installazione delle contromisure con la gestione del budget relativo.

Lingua

Italiano

Inglese

Altro _____

EBIOS

Informazioni fornite da Francesca Di Massimo di Microsoft Italia

Ambito di applicazione:

Il metodo EBIOS è utilizzato per valutare e trattare i rischi relativi alla sicurezza dei sistemi informativi (Information Systems Security – ISS) e costituisce un valido supporto nel processo di gestione dei rischi.

EBIOS® é ampiamente utilizzato in molti paesi, sia nel settore pubblico (ministeri ed enti sotto la loro amministrazione) che nel settore privato (società di consulenza, piccole e grandi imprese).

Standard di riferimento

ISO 13335 (GMITS); ISO 15408 (Common Criteria); ISO 17799.

Approccio alla misurazione dei rischi:

- qualitativo quantitativo semi-quantitativo
- misurazione sia del rischio potenziale o intrinseco (cioè a prescindere dalle contromisure) sia del rischio effettivo o residuo (cioè tenendo conto delle contromisure poste in essere)
- misurazione del rischio effettivo o residuo (cioè il rischio relativo alla situazione in essere, comprese le contromisure implementate)
- misurazione del rischio potenziale o intrinseco (cioè a prescindere dalle contromisure adottate)

Concetti e definizioni chiave:

- RISCHIO:** Esposizione dell'organizzazione a perdite di varia natura che possono concretizzarsi a causa di un latore di minaccia in grado di sfruttare le vulnerabilità dei processi, delle risorse e dei sistemi adibiti al trattamento delle informazioni.
- MINACCIA:** Possibile attacco di un latore di minaccia ai beni.
- VULNERABILITA':** Punti deboli di un'entità che possono essere sfruttati da un latore di minaccia.
- DANNO:**
- IMPATTO:** Conseguenze per un'organizzazione nel caso di una minaccia portata a termine.
- CONSEGUENZE:** Non utilizzato.

Altre definizioni:

RISCHIO RESIDUO: Rischio che persiste dopo il trattamento dei rischi.

LATORE DI MINACCIA: Una azione umana, un elemento naturale o ambientale che ha conseguenze potenzialmente negative sul sistema. Può essere caratterizzato dal tipo (naturale, umano o ambientale) e dalla causa (accidentale o intenzionale).

La causa accidentale può essere ulteriormente caratterizzata da esposizione e risorse disponibili, mentre quella intenzionale da esperienza, risorse disponibili e motivazione.

ENTITA': Un bene quale un'organizzazione, un sito, il personale, l'equipaggiamento, la rete, il software, il sistema.

OBIETTIVO DI SICUREZZA: Espressione dell'intenzione di contrastare le minacce o i rischi identificati (a seconda del contesto) e/o di aderire alle politiche e gli assunti organizzativi in merito alla sicurezza; un obiettivo può riguardare un sistema, il suo ambiente di sviluppo o quello di esercizio.

REQUISITO DI SICUREZZA: Specifica funzionale o di *assurance* riguardante il "sistema informativo" o il suo ambiente, che tratta dei meccanismi di sicurezza che devono essere implementati in relazione a uno o più obiettivi di sicurezza.

Elementi della Metodologia di misurazione dei rischi :

Espressione delle esigenze in fatto di sicurezza:

- **Creazione dei "fogli delle esigenze" (*needs sheets*)**

Lo scopo di questa attività è quello di creare le tabelle richieste per l'espressione delle esigenze in fatto di sicurezza da parte degli utenti. Queste consentiranno agli utenti di fornire un'obiettiva e consistente espressione delle esigenze in fatto di sicurezza per gli elementi che normalmente gestiscono nel loro contesto lavorativo. Questa attività è di aiuto nella stima del rischio e nella definizione dei criteri di rischio nel processo di gestione dei rischi.

- **Sintesi delle esigenze in fatto di sicurezza**

Lo scopo di questa attività è quello di assegnare le esigenze nell'ambito della sicurezza che risultano dal sunto dei valori ascritti dagli utenti agli elementi essenziali. Questa attività fornirà una visione obiettiva e consistente delle esigenze in ambito sicurezza. Contribuisce alla valutazione del rischio nel processo di gestione dei rischi.

Studio delle minacce

- **Studio delle fonti di minaccia**

Lo scopo di questa attività è di selezionare i metodi di attacco che sono rilevanti per il sistema da proteggere. Ogni metodo di attacco è caratterizzato dai criteri di sicurezza che può andare a colpire e (disponibilità, integrità, riservatezza, ecc.) ed è associato con i latori di minaccia. Questi latori di minaccia sono caratterizzati dal loro tipo (naturale, umano o ambientale) e dalla loro possibile causa (accidentale, deliberata). Questa caratterizzazione può essere riassunta nella forma di un attacco potenziale. Se i metodi di attacco costituiscono un rischio reale per il sistema da proteggere, il livello delle misure di sicurezza deve essere consistente con questo attacco potenziale. Questa attività corrisponde all'identificazione delle fonti nel processo di gestione dei rischi.

- **Studio delle vulnerabilità**

Lo scopo di questa attività è quello di determinare le vulnerabilità specifiche del sistema da proteggere e, dove appropriato, di caratterizzarle in termini di livello. Queste vulnerabilità intrinseche del sistema nascono dalle caratteristiche delle entità che contiene. Queste vulnerabilità possono essere sfruttate per attaccare il sistema di sicurezza; lo scopo essenziale degli obiettivi di sicurezza sarà, perciò, quello di ridurle. Questa attività contribuisce alla stima del rischio nel processo di gestione dei rischi.

- **Formalizzazione delle minacce**

Lo scopo di questa attività è quello di determinare le minacce che potrebbero colpire il sistema da proteggere. Tali minacce risultano dall'unione dei metodi di attacco (usati dai latori di minaccia identificati) con quelle che sono le vulnerabilità del sistema (sulla base delle entità identificate). Questa attività fornirà una visione obiettiva ed esauriente delle minacce che affliggono il sistema da proteggere. Questa attività contribuisce alla valutazione del rischio nel processo di gestione dei rischi.

- **Confronto delle minacce con le esigenze**

Lo scopo di questa attività è quello di determinare il reale rischio che può affliggere il sistema da proteggere. Attraverso il confronto delle minacce con le esigenze di sicurezza è possibile decidere quali rischi possono verosimilmente minacciare gli elementi essenziali così che possano essere ritenuti e ordinati in base ad una priorità. Tutti questi rischi devono essere valutati poiché molti di loro avranno bisogno di essere coperti da obiettivi di sicurezza. Questa attività contribuisce alla valutazione del rischio nel processo di gestione dei rischi.

VALUTAZIONE DELLE RISORSE:

- | | | |
|-------------------------------------|--|---------------------------------------|
| <input type="checkbox"/> Dati | <input type="checkbox"/> Tecnologia | <input type="checkbox"/> Applicazioni |
| <input type="checkbox"/> Facilities | <input type="checkbox"/> Risorse umane | |

VALUTAZIONE DELL'IMPATTO:

- | | | |
|--|---|---|
| <input checked="" type="checkbox"/> Riservatezza | <input checked="" type="checkbox"/> Integrità | <input checked="" type="checkbox"/> Disponibilità |
| <input type="checkbox"/> Conformità | <input type="checkbox"/> Efficienza operativa | <input type="checkbox"/> Efficacia operativa |

VALUTAZIONE DELLA PROBABILITÀ:

Non sono emersi elementi da riportare.

VALUTAZIONE DELLE CONTROMISURE:

- | | | |
|---|-------------------------------------|--|
| <input checked="" type="checkbox"/> riduzione probabilità | <input type="checkbox"/> preventive | <input type="checkbox"/> disegno della contromisura |
| <input checked="" type="checkbox"/> riduzione conseguenze | <input type="checkbox"/> reattive | <input type="checkbox"/> applicazione della contromisura |
| <input checked="" type="checkbox"/> evitare il rischio | | |
| <input checked="" type="checkbox"/> trasferire il rischio | | |
| <input checked="" type="checkbox"/> accettare il rischio | | |

Approccio:

La metodologia prevede l'applicazione dell'analisi dei rischi su:

- | | | |
|--|---|--|
| <input checked="" type="checkbox"/> processi | <input checked="" type="checkbox"/> risorse di business | <input checked="" type="checkbox"/> risorse tecnologiche |
|--|---|--|

Passi metodologici:

- 1 Identificazione dell'ambiente, e degli elementi essenziali e delle entità su cui esso è basato.
- 2 Valutazione dei rischi (stima del rischio e definizione dei criteri di rischio)
Consente di valutare le esigenze di sicurezza degli elementi essenziali in termini di disponibilità, integrità e riservatezza e di formalizzare gli impatti.
- 3 Analisi dei rischi
Consiste nell'identificazione e nella descrizione delle minacce che incombono sul sistema attraverso lo studio dei metodi di attacco dei fattori di minaccia e delle vulnerabilità.
- 4 Definizione del valore al rischio.
I rischi reali correlati al sistema sono formalizzati attraverso il confronto tra le minacce e le esigenze di sicurezza.
- 5 Trattamento del rischio.
Determinazione dei requisiti funzionali che consentono di raggiungere gli obiettivi di sicurezza e dei requisiti di *assurance* che consentono di accrescere il livello di fiducia nel loro raggiungimento.

Tool a supporto :

software

É disponibile gratuitamente sul sito del DCSSI

<http://www.ssi.gouv.fr/en/confidence/ebiospresentation.html#pratiquer>

questionari/ check -list, ecc.

manuali e linee guida

<http://www.ssi.gouv.fr/en/confidence/ebiospresentation.html#pratiquer>

disponibilità training

<http://www.ssi.gouv.fr/en/confidence/ebiospresentation.html#pratiquer>

disponibilità aggiornamenti periodici

possibilità di personalizzazioni

Risultati ottenibili :

Non sono emersi elementi specifici

Lingua

Italiano

Inglese

Altro _____

ERAM - Enterprise Risk Assessment and Management

Informazioni fornite da Federico Sandrucci del Ministero della Difesa

<p><u>Ambito di applicazione :</u></p> <p>E' uno strumento informatico, basato su una metodologia che permette di valutare e quantificare il rischio e di gestire la sicurezza in azienda.</p> <p>E' strutturato in modo da offrire una visione integrata e unitaria di aspetti che tradizionalmente sono gestiti in modi profondamente diversi tra loro.</p> <p>Copre tutti gli aspetti legati alla sicurezza aziendale.</p>
<p><u>Standard di riferimento</u></p> <p>ISO 17799; Busensant fur Sicherheit in der Informationstechnik (BSI)</p> <p>E' stata pensata per offrire un modello informatizzato a supporto di un sistema di gestione del rischio e della sicurezza al servizio del <i>Security Manager</i></p>
<p><u>Approccio alla misurazione dei rischi :</u></p> <p><input type="checkbox"/> qualitativo <input type="checkbox"/> quantitativo <input checked="" type="checkbox"/> semi-quantitativo</p>
<p>La metodologia esprime il valore delle risorse e dei processi in termini monetari e calcola in modo quantitativo il danno.</p>
<p><input checked="" type="checkbox"/> misurazione sia del rischio potenziale o intrinseco (cioè a prescindere dalle contromisure) sia del rischio effettivo o residuo (cioè tenendo conto delle contromisure poste in essere)</p> <p><input type="checkbox"/> misurazione del rischio effettivo o residuo (cioè il rischio relativo alla situazione in essere, comprese le contromisure implementate)</p> <p><input type="checkbox"/> misurazione del rischio potenziale o intrinseco (cioè a prescindere dalle contromisure adottate)</p>
<p><u>Concetti e definizioni chiave :</u></p>
<p><input checked="" type="checkbox"/> RISCHIO: E' definito come il prodotto fra la probabilità che una risorsa venga aggredita e il danno provocato.</p>
<p><input checked="" type="checkbox"/> MINACCIA: Evento potenziale o manifesto capace di compromettere l'integrità delle risorse e dei processi aziendali.</p>
<p><input type="checkbox"/> VULNERABILITA': Non utilizzato.</p>
<p><input checked="" type="checkbox"/> DANNO: Perdite monetizzabili prevedibili e/o calcolate in caso di aggressione delle minacce sia per le risorse (danno diretto) sia per i processi (danno indiretto).</p>
<p><input checked="" type="checkbox"/> IMPATTO: Danno percentuale sul valore attribuito alle risorse e ai processi.</p>

CONSEGUENZE: Non utilizzato.

Elementi della Metodologia di misurazione dei rischi :

VALUTAZIONE DELLE RISORSE:

Dati Tecnologia Applicazioni
 Facilities Risorse umane

VALUTAZIONE DELL'IMPATTO:

Riservatezza Integrità Disponibilità
 Conformità Efficienza operativa Efficacia operativa

VALUTAZIONE DELLA PROBABILITA':

Il sistema usa percentuali e valori e non scale.

La probabilità è calcolata in funzione della frequenza attesa e della percentuale di risorse colpite all'interno di una data popolazione.

VALUTAZIONE DELLE CONTROMISURE:

Il sistema usa percentuali e valori e non scale.

Le contromisure sono valutate in base alla riduzione attesa provocata da danni diretti, indiretti, consequenziali e stati di crisi ed espresse in termini quantitativi

riduzione probabilità preventive disegno della contromisura
 riduzione conseguenze reattive applicazione della contromisura
 evitare il rischio
 trasferire il rischio
 accettare il rischio

Approccio:

La metodologia prevede l'applicazione dell'analisi dei rischi su:

processi risorse di business risorse tecnologiche

Passi metodologici :

- 1 Identificazione e valorizzazione dei processi e dei sottoprocessi
Ogni processo è caratterizzato dai sottoprocessi, in cui si può scomporre senza limiti di alberatura, e dalle risorse necessarie.
Determinazione, per ogni risorsa utilizzata, del danno a carico del processo derivato dall'indisponibilità della risorsa stessa (in % rispetto alla disponibilità attesa) e della conseguente riduzione del livello di servizio.
- 2 Identificazione e classificazione di risorse, macrorisorse e minacce
Per ogni risorsa e per una data minaccia si specifica il numero di eventi attesi nell'unità di tempo, la percentuale della popolazione di risorse colpite, la riduzione di disponibilità attesa, il tempo di ripristino.
Il sistema calcola il danno diretto sulla risorsa e il danno indiretto su tutti i processi che ne fanno uso.
- 3 Identificazione e classificazione delle misure di sicurezza
Si creano scenari alternativi e si variano i parametri attesi relativi alle minacce, in funzione dell'applicazione delle misure di sicurezza.
Il sistema calcola i danni diretti (sulle risorse) e indiretti (sui processi) conseguenti
Si possono attribuire costi di applicazione e di gestione alle misure di sicurezza per valutare la convenienza delle singole soluzioni rispetto ai risultati attesi.
- 4 Creazione del modello
Si crea un modello, inizialmente semplificato, della realtà aziendale e orientato allo studio delle aree considerate più critiche; è possibile dettagliare il modello nel tempo secondo le necessità.
- 5 Gestione del modello
Si mantiene aggiornato il modello attraverso campagne di rilevazione della situazione esistente e dei cambiamenti strutturali, organizzativi e tecnici.
Il sistema stampa per ogni area, processo e risorsa i questionari a supporto.

Tool a supporto : software

MS-ACCESS con il data base in access o in SQLServer (può essere portato in oracle con una personalizzazione)

 questionari/ check -list, ecc.

Vengono generati dal programma in funzione della modellazione effettuata

 manuali e linee guida

Esiste un manuale on line comprendente sia le norme operative che gli aspetti funzionali

 disponibilità training

Possibilità di training sull'utilizzo della metodologia e del tool

 disponibilità aggiornamenti periodici

Tutte le nuove funz ioni implementate vengono rese disponibili all'interno del contratto di manutenzione

 possibilità di personalizzazioni

Personalizzazioni nella reportistica sono incluse nella fase di installazione.

Personalizzazioni funzionali possono essere analizzate caso per caso

Risultati ottenibili :

Il sistema consente di creare un modello che rispecchia le caratteristiche dell'azienda, di confrontarlo con un modello di riferimento e conseguentemente di valutare gli elementi di scostamento, simulare scenari alternativi, individuare le misure di sicurezza da mettere in atto, gestire progetti di applicazione delle norme di sicurezza adatte, rilevare e valutare gli incidenti.

Lingua Italiano Inglese Altro _____

FIRM - Fundamental Information Risk Management -

Informazioni fornite da Luca Corciulo di PricewaterhouseCoopers

<p><u>Ambito di applicazione :</u></p> <p>La metodologia FIRM viene utilizzata per condurre un assessment dei livelli di rischio associati a un determinato numero di “<i>Information Resource</i>” (vedere sezione concetti e definizioni chiave); i relativi rischi vengono accorpati per determinare il livello di rischio per l'intera organizzazione (<i>enterprise</i>).</p>
<p><u>Standard di riferimento</u></p> <p>E' una metodologia standard definita dall'Information Security Forum</p>
<p><u>Approccio alla misurazione dei rischi :</u></p> <p><input type="checkbox"/> qualitativo <input type="checkbox"/> quantitativo <input checked="" type="checkbox"/> semi-quantitativo</p> <p>La metodologia costituisce un approccio di analisi dei rischi di tipo dinamico, utilizza metriche di calcolo del rischio, sia di tipo quantitativo che qualitativo, basate sul concetto di scorecard, che offrono una visione d'insieme e ai diversi livelli di profondità.</p> <p><input checked="" type="checkbox"/> misurazione sia del rischio potenziale o intrinseco (cioè a prescindere dalle contromisure) sia del rischio effettivo o residuo (cioè tenendo conto delle contromisure poste in essere)</p> <p><input type="checkbox"/> misurazione del rischio effettivo o residuo (cioè il rischio relativo alla situazione in essere, comprese le contromisure implementate)</p> <p><input type="checkbox"/> misurazione del rischio potenziale o intrinseco (cioè a prescindere dalle contromisure adottate)</p>
<p><u>Concetti e definizioni chiave :</u></p> <p><input checked="" type="checkbox"/> RISCHIO: [<i>Information Risk</i>] Il rischio rappresenta l'eventualità o la probabilità di subire danni per il business in seguito a perdite di Riservatezza, Integrità o Disponibilità di informazioni. Il livello di rischio associato ad una risorsa informativa può essere valutato misurando:</p> <ul style="list-style-type: none"> • la criticità della risorsa informativa nell'ottica del business; • debolezze nei controlli che interessano la risorsa informativa; • eventi straordinari che interessano la risorsa informativa; • il <i>business impact</i> dovuto a incidenti informatici per un determinato periodo.

- MINACCIA:** [*Threat*] La minaccia può essere definita come il modo attraverso il quale la Riservatezza (o confidenzialità), l'Integrità e la Disponibilità di informazioni potrebbero essere compromesse. Le categorie di minacce che influenzano il rischio includono:
- malfunzionamenti di hardware o software;
 - effetti imprevisi seguenti a cambiamenti;
 - sovraccarichi;
 - errori umani;
 - violazioni di accesso.
- VULNERABILITA':** [*Vulnerability*] Le vulnerabilità possono essere definite come le circostanze che aumentano la probabilità che una minaccia si manifesti.
- DANNO:** Non utilizzato.
- IMPATTO:** [*Business impact*] L'impatto è un valore o una stima che indica la natura e il livello di danno che l'azienda può subire, espresso come risultato di una effettiva perdita di Riservatezza, Integrità o Disponibilità di informazioni.

Altre definizioni:

RISORSA INFORMATIVA: [*Information resource*] Termine utilizzato per rappresentare l'informazione e i servizi (facility) associati, necessari per il "processing" dell'informazione; i servizi più rilevanti sono le applicazioni di business, gli apparati, le reti di comunicazione e le capacità di "system development".

CRITICITA': [*Criticality*] La criticità è un valore o una stima che indica l'importanza di una risorsa informativa per un'azienda, basata sul massimo livello di danno che potrebbe sorgere se la Riservatezza, Integrità o Disponibilità delle informazioni venisse compromessa, tenendo conto anche del tempo di indisponibilità della risorsa.

DEBOLEZZA NEI CONTROLLI: [*Control weakness*] Si parla di debolezza nei controlli quando un controllo necessario non è stato implementato oppure non è applicato in tutte le situazioni che lo richiedono.

CONDIZIONE PARTICOLARE: [*Special circumstance*] E' una situazione che influenza la probabilità che una minaccia si manifesti, differente da quella introdotta da una debolezza nei controlli (es. Alto grado di cambiamento, complessità, accessibilità da parte di terze parti).

LIVELLO DI MINACCIA: [*Level of Threat*] Indica la probabilità che una minaccia o una categoria di minaccia possa verificarsi. Può essere valutato basandosi sullo storico relativo agli incidenti informatici verificatesi.

INCIDENTE INFORMATICO: [*Information incident*] E' un evento (o catena di eventi) che compromette la Riservatezza, Integrità o Disponibilità delle informazioni relative al business. Le categorie di incidenti informatici che influenzano il rischio includono quelli già citati nella definizione di minaccia.

RISCHIO ACCETTABILE: [*Acceptable risk*] E' il livello di rischio considerato accettabile dal top management di un business. Quantificando il rischio accettabile negli stessi termini del rischio effettivo, l'attenzione può essere focalizzata sulle risorse informative che posizionano il livello di rischio al di là di quello ritenuto accettabile.

Il rischio accettabile può essere esplicitato quantitativamente impostando:

- le componenti controllabili del rischio (debolezze nei controlli, livello di minaccia e impatto) con valori ritenuti accettabili dal top management;
- le componenti non controllabili del rischio (criticità e condizioni particolari) con valori limite.

Elementi della Metodologia di misurazione dei rischi:

Il concetto di base della metodologia è dato dall'Information Resource (la risorsa informativa) che evidenzia la correlazione tra dati, informazioni, applicazioni e sistemi informativi (Architetture, piattaforme ed apparati).

Primaria attività di FIRM è quindi il censimento e la classificazione delle "risorse informative" che costituiscono poi il contesto di protezione.

Da qui si procede con approccio sistematico a:

- definire ambito e scopo del monitoraggio: in particolare l'obiettivo è quello di tenere pienamente informato il top management sull'evolversi del livello di rischio informatico, interno all'organizzazione, e incoraggiare gli 'owners' ad abbassare il rischio a un livello ritenuto accettabile dal top-management;
- definire coerentemente ruoli, responsabilità e linee di comunicazione in seno all'azienda; ogni linea aziendale (dall'owner al Top Management, passando dai coordinatori e custodi del processo di monitoraggio), ricopre determinate ruoli e si assume precise responsabilità, utilizzando standard e protocolli di comunicazione predeterminati;
- predisporre i "sound fact-gathering tools" per l'analisi e la gestione dei rischi; (balance scorecard per la valutazione dei rischi, questionario di assessment degli incidenti, ecc.);
- realizzare e gestire un processo dinamico (costruttivo e continuativo) di misurazione e monitoraggio;
- predisporre report e presentazioni concise per il Top-Management.

Passi metodologici:

- 1 Censimento e classificazione delle “risorse informative” che costituiscono poi il contesto di protezione. Da qui si procede con approccio sistematico alle altre e seguenti fasi della metodologia.
- 2 Definizione ambito e scopo del monitoraggio:
L'obiettivo principale di tale passo è quello di tenere pienamente informato il top management sull'evolversi del livello di rischio informatico, interno all'organizzazione, e incoraggiare gli 'owners' ad abbassare il rischio a un livello ritenuto accettabile dal top-management.
- 3 Definizione coerente di ruoli e responsabilità e linee di comunicazione in seno all'azienda:
Ogni linea aziendale (dall'*owner* al Top Management, passando dai coordinatori e custodi del processo di monitoraggio), deve ricoprire determinati ruoli e si assume precise responsabilità, utilizzando standard e protocolli di comunicazione predeterminati.
- 4 Predisposizione dei “*sound fact-gathering tools*” per l'analisi e la gestione dei rischi:
Predisposizione e compilazione di *tool* quali *balance scorecard* per la valutazione dei rischi, questionario di *assessment* degli incidenti, ecc..
- 5 Realizzazione e gestione di un processo dinamico (costruttivo e continuativo) di misurazione e monitoraggio dei rischi.
- 6 Predisposizione di report e presentazioni concise per il Top-Management.

Tool a supporto:

software

Citicus One:

Un web Tool che consente di gestire tutte le fasi del processo attraverso appositi cruscotti informatizzati.

questionari/ check-list, ecc.

Sound fact-gathering tools:

- *Information risk scorecard:*
Balanced Scorecard Form, compilato dall'*owner* dell'*Information Resource*, che comprova:
 - tutti i fattori di rischio;
 - le contromisure;
 - *ownership* dell'*Information Resource*
- *Incident assessment forms:*
Form per la gestione dinamica e continuativa degli incidenti.

manuali e linee guida

“FIRM Methodology - User guide” costituisce il manuale descrittivo della metodologia e riporta linee guida per la conduzione dell’attività di *risk analysis*.

disponibilità training

Sono disponibili corsi di formazione, seminari e convegni sul tema organizzati dai membri e dagli agente dell’ISF.

disponibilità aggiornamenti periodici

ISF predispone aggiornamenti della metodologia, mettendoli a disposizione dei suoi membri.

possibilità di personalizzazioni

E’ possibile predisporre personalizzazioni della metodologia in base a specifiche esigenze.

Risultati ottenibili :

I risultati ottenibili sono già espressi nella sezione di “Passi metodologici”.

Lingua

Italiano

Inglese

Altro _____

ISA – Information Security Assessment

Informazioni fornite da *Andrea Mariotti e Luca Boselli di KPMG*

Ambito di applicazione :

L'obiettivo principale che si intende perseguire attraverso l'applicazione della metodologia ISA è la protezione del patrimonio informativo aziendale: la metodologia può essere applicata in tutte le fasi di vita di un'attività, una funzione, un progetto, un processo, un prodotto o un bene; è indipendente rispetto a specifici settori industriali ed economici.

Ad esempio, la metodologia ISA può essere utilizzata nel caso di sviluppo di nuove soluzioni infrastrutturali o applicative, consentendo di:

- valutare la criticità dei macrodati e definire i requisiti di sicurezza per la loro protezione;
- definire le contromisure da implementare, al fine di ridurre al minimo le vulnerabilità e minimizzare il rischio associato.

Standard di riferimento

La metodologia è stata sviluppata da KPMG (www.kpmg.com) sulla base di *best practice* e standard di settore (BS77 99, ISO/TR 13335, standard NIST, ecc.)

Approccio alla misurazione dei rischi :

- qualitativo quantitativo semi-quantitativo
- misurazione sia del rischio potenziale o intrinseco (cioè a prescindere dalle contromisure) sia del rischio effettivo o residuo (cioè tenendo conto delle contromisure poste in essere)
- misurazione del rischio effettivo o residuo (cioè il rischio relativo alla situazione in essere, comprese le contromisure implementate)
- misurazione del rischio potenziale o intrinseco (cioè a prescindere dalle contromisure adottate)

Concetti e definizioni chiave :

- RISCHIO:** La possibilità che una minaccia sfrutti una o più vulnerabilità e comprometta il patrimonio informativo dell'azienda.
- MINACCIA:** Evento in grado di compromettere il patrimonio informativo dell'azienda.
- VULNERABILITA':** Debolezza intrinseca o dovuta alle condizioni di esercizio, che può essere sfruttate dalle minacce.
- DANNO:** Non utilizzato.
- IMPATTO:** Il risultato di un'azione o di un evento indesiderato.
- CONSEGUENZE:** Non utilizzato.

Altre definizioni:

SUSCETTIBILITA': La suscettibilità è un indicatore che rappresenta in maniera sintetica la correlazione tra le minacce potenziali e la loro capacità di sfruttare le vulnerabilità presenti.

MACRODATO: Per macrodato si intende un insieme minimo di informazioni o un aggregato di dati, tali da costituire un raggruppamento omogeneo per l'applicazione delle misure di protezione.

Elementi della Metodologia di misurazione dei rischi :

La criticità di ogni macrodato dipende dal valore che lo stesso ha in termini di riservatezza, integrità e disponibilità all'interno del processo cui concorre, indipendentemente dal tipo, dal formato e dai supporti di memorizzazione utilizzati.

Il livello di rischio viene definito in funzione del valore dei macrodati, delle minacce cui sono sottoposti e delle vulnerabilità degli strumenti e delle infrastrutture di supporto che li gestiscono:

$$\text{Rischio} = f(\text{Valore}, \text{Minacce}, \text{Vulnerabilità})$$

VALUTAZIONE DELLE RISORSE:

La probabilità di accadimento delle minacce e il loro impatto viene applicato ai macrodati per determinare il rischio.

Le minacce e le vulnerabilità vengono a loro volta valutate in riferimento a tutta l'infrastruttura tecnologica (applicazioni, architetture hardware, infrastrutture di rete). Tale valutazione tiene conto anche dell'ubicazione fisica delle infrastrutture stesse.

- | | | |
|--|--|--|
| <input checked="" type="checkbox"/> Dati | <input checked="" type="checkbox"/> Tecnologia | <input checked="" type="checkbox"/> Applicazioni |
| <input checked="" type="checkbox"/> Facilities | <input type="checkbox"/> Risorse umane | |

VALUTAZIONE DELL'IMPATTO:

- | | | |
|--|---|---|
| <input checked="" type="checkbox"/> Riservatezza | <input checked="" type="checkbox"/> Integrità | <input checked="" type="checkbox"/> Disponibilità |
| <input type="checkbox"/> Conformità | <input type="checkbox"/> Efficienza operativa | <input type="checkbox"/> Efficacia operativa |

VALUTAZIONE DELLA PROBABILITA':

La valutazione della probabilità di accadimento delle minacce viene effettuata distinguendo categorie di minacce risultanti dalla combinazione delle seguenti variabili:

- **Fonte della minaccia :** descrive la fonte dalla quale un attacco potenziale può essere originato. Può essere interna (oltre ai dipendenti include anche il caso di outsourcer che gestiscono informazioni aziendali) o esterna a seconda dell'appartenenza o meno di colui che effettua l'attacco all'azienda.
- **Intenzionalità della minaccia :** descrive la natura dell'intenzione sottostante alla minaccia. Può essere sia intenzionale che non intenzionale (accidentale).

- **Struttura della minaccia:** descrive la struttura delle minacce in termini della complessità o del livello di conoscenza richiesto o della sofisticazione degli strumenti utilizzabili.

La stima viene effettuata in base alla percezione della possibilità di accadimento della minaccia, sia dai referenti di processo sia dai referenti tecnologici.

Anche in questo caso, le valutazioni sono effettuate in base ad una scala qualitativa di valori (da 'minaccia inesistente' a 'minaccia certa', convertita in scala numerica).

VALUTAZIONE DELLE CONTROMISURE: Non utilizzata

- | | | |
|--|-------------------------------------|--|
| <input type="checkbox"/> riduzione probabilità | <input type="checkbox"/> preventive | <input type="checkbox"/> disegno della contromisura |
| <input type="checkbox"/> riduzione conseguenze | <input type="checkbox"/> reattive | <input type="checkbox"/> applicazione della contromisura |
| <input type="checkbox"/> evitare il rischio | | |
| <input type="checkbox"/> trasferire il rischio | | |
| <input type="checkbox"/> accettare il rischio | | |

ALTRI ELEMENTI:

Analisi delle vulnerabilità

Le vulnerabilità analizzate dalla metodologia prevedono sia aspetti di natura tecnica, legati alla sicurezza logica o fisica degli strumenti e delle infrastrutture di supporto, sia aspetti di natura organizzativa, legati ad esempio alle procedure di lavoro o alle responsabilità del personale.

Le vulnerabilità, a secondo del tipo di strumenti e infrastrutture di supporto considerati, sono aggregate secondo le seguenti categorie:

- vulnerabilità delle applicazioni derivanti dall'assenza o da un'inadeguata gestione dei controlli di sicurezza;
- vulnerabilità delle architetture tecnologiche derivanti dall'assenza o da un'inadeguata gestione dei controlli di sicurezza;
- vulnerabilità delle infrastrutture di rete derivanti dall'assenza o da un'inadeguata gestione dei controlli di sicurezza;
- vulnerabilità delle ubicazioni derivanti dall'assenza o da un'inadeguata gestione dei controlli di sicurezza;

Ad ogni vulnerabilità delle precedenti categorie è associato un peso che rappresenta la gravità della stessa in relazione alle altre vulnerabilità: tale valore concorre alla determinazione del livello di rischio per i macrodati, in base alla presenza o meno della vulnerabilità stessa.

Approccio:

La metodologia prevede l'applicazione dell'analisi dei rischi su:

processi risorse di business risorse tecnologiche

Passi metodologici:

Al fine di individuare i macrodati che costituiscono il patrimonio informativo aziendale, valutarne la criticità e la relativa esposizione al rischio e definire le contromisure di sicurezza da adottare, devono essere svolte le seguenti fasi:

- 1 Individuazione dei macrodati e dei processi aziendali:
Per individuare i macrodati del patrimonio informativo da tutelare ed effettuare l'analisi dei rischi, è necessario in primo luogo identificare i processi aziendali ed i relativi responsabili: questi hanno l'obiettivo di assicurare un adeguato livello di protezione delle informazioni gestite, tramite l'adozione di opportune misure di sicurezza che non compromettano comunque l'efficienza e l'efficacia dei processi. I processi sono scomposti in sottoprocessi e per ciascuno di essi sono individuati i macrodati gestiti ed i relativi supporti di memorizzazione utilizzati (cartacei piuttosto che elettronici).
- 2 Mappatura degli strumenti e delle infrastrutture di supporto:
Al fine di determinare il livello di rischio che grava sui macrodati, devono essere identificati gli strumenti e le infrastrutture di supporto utilizzati per l'elaborazione e la trasmissione delle informazioni. L'associazione dei macrodati alle catene tecnologiche ed infrastrutturali da cui dipendono, permette ai referenti tecnologici di individuare le relative vulnerabilità che concorrono alla determinazione del livello di rischio.
- 3 Valutazione del valore e classificazione dei macrodati:
La classificazione dei macrodati, intesa come determinazione del valore che hanno per l'azienda, è elemento primario per il sistema di gestione della sicurezza. I referenti di processo stimano la criticità delle informazioni di propria competenza in relazione al livello di riservatezza, integrità e disponibilità delle stesse. La stima è effettuata esprimendo un giudizio qualitativo sui una serie di impatti provocati da eventi che comportano accessi non autorizzati/divulgazioni indebite, alterazioni ed indisponibilità delle informazioni.
- 4 Valutazione delle minacce
La valutazione delle minacce è il processo che porta all'identificazione degli eventi che possono compromettere il patrimonio informativo dell'azienda.
La stima viene effettuata in base alla percezione della possibilità di accadimento della minaccia, sia dai referenti di processo sia dai referenti tecnologici. Anche in questo caso, le valutazioni sono effettuate in base ad una scala qualitativa di valori, convertita in scala numerica.

5 Analisi delle vulnerabilità

Ai fini del calcolo del rischio cui sono sottoposti i macrodati, è necessario valutare le vulnerabilità degli strumenti e delle infrastrutture che li gestiscono, ossia archivi cartacei, applicazioni, architetture, infrastrutture di rete ed ubicazioni fisiche, come indicato nel modello di riferimento della metodologia. I referenti tecnologici, ognuno per le proprie responsabilità, valutano la presenza delle vulnerabilità identificando anche l'applicabilità delle stesse al contesto di riferimento.

Le vulnerabilità analizzate dalla metodologia prevedono sia aspetti di natura tecnica, legati alla sicurezza logica o fisica degli strumenti e delle infrastrutture di supporto, sia aspetti di natura organizzativa, legati ad esempio alle procedure di lavoro o alle responsabilità del personale.

6 Calcolo del livello di rischio:

La metodologia prevede l'esecuzione di un algoritmo di calcolo comune con cui, per ognuno dei singoli *asset*, viene calcolato un valore di suscettibilità: aggregando tali valori, si giunge alla definizione di un singolo valore di suscettibilità, utilizzato nella formula di calcolo finale del rischio del macrodato.

Il livello di rischio per ogni macrodato è, infine, definito nel seguente modo:

$$\text{Rischio del macrodato} = \text{Valore} * \text{Suscettibilità}$$

Tool a supporto: software

A supporto della metodologia viene utilizzato un'applicazione *web-based*, denominata **KARISMA** (Kpmg Advanced RISK Management).

 questionari/ check-list, ecc.

Sono disponibili questionari e check-list per poter utilizzare la metodologia senza l'aiuto diretto dell'applicazione KARISMA.

 manuali e linee guida

Sono disponibili sia manuali metodologici sia manuali sull'utilizzo dell'applicazione.

 disponibilità training

Sono disponibili corsi che illustrano la metodologia e altri che illustrano l'utilizzo dello strumento software.

 disponibilità aggiornamenti periodici

La metodologia viene aggiornata periodicamente.

 possibilità di personalizzazioni

Alcuni aspetti della metodologia possono essere personalizzati a secondo dello specifico ambito di applicazione del modello (ad es. rispetto al modello di classificazione delle informazioni, alla tipologia delle minacce e soprattutto alle specifiche vulnerabilità). Tali personalizzazioni possono essere riportate anche all'interno del tool KARISMA, in parte direttamente da parte degli utenti, in parte tramite modifiche al software.

Risultati ottenibili :

L'individuazione del livello di rischio relativo ai singoli macrodati all'interno dei processi aziendali consente ai responsabili di processo di stabilire la priorità negli interventi per la protezione delle informazioni e le modalità di gestione del rischio (accettazione, trasferimento, mitigazione), in base ai propri livelli di autonomia e di ambito, ed in base alle politiche di sicurezza adottate.

Inoltre l'analisi delle vulnerabilità consente ai referenti tecnologici di predisporre i piani di implementazione delle contromisure in base alle politiche di sicurezza adottate ed alle priorità stabilite dall'analisi dei rischi nel suo complesso.

Uno dei principali benefici della metodologia è quello di poter fornire, al termine delle attività, un quadro completo delle aree di criticità dei processi aziendali relativamente alla protezione del patrimonio informativo, definendo le priorità di intervento sulla base di requisiti che comprendono sia aspetti di business (valore delle informazioni) sia aspetti tecnologici (minacce e vulnerabilità). Tali interventi di gestione del rischio potranno perciò essere di natura differente e riguardare aspetti di sicurezza organizzativa, logica o fisica.

Lingua Italiano Inglese Altro _____

ISO/IEC 21827 - System Security Engineering, Capability Maturity Model

Informazioni fornite da Stefania Caporalini-Ajello di Datamat

Ambito di applicazione:

SSE-CMM consente di valutare lo stato di maturità dei processi, sulla base della verifica di una serie di *practice* che debbono essere seguite, e di riportare il risultato di questa analisi su una scala quantitativa. I processi a cui si applica tale valutazione sono quelli di sviluppo software e di gestione della sicurezza dei sistemi.

Nell'ambito delle *Security Base Practices* è considerata anche l'analisi dei rischi.

Standard di riferimento

Progettato e sviluppato, nel corso degli anni '90 in seno ad una organizzazione internazionale denominata ISSEA (*International Systems Security Engineering Association*), l'SSE-CMM è una metodologia adottata dalla *National Security Agency* statunitense ed è standard ISO dal 2002 con l'identificazione ISO/IEC 21827.

Approccio alla misurazione dei rischi:

- qualitativo quantitativo semi-quantitativo
- misurazione sia del rischio potenziale o intrinseco (cioè a prescindere dalle contromisure) sia del rischio effettivo o residuo (cioè tenendo conto delle contromisure poste in essere)
- misurazione del rischio effettivo o residuo (cioè il rischio relativo alla situazione in essere, comprese le contromisure implementate)
- misurazione del rischio potenziale o intrinseco (cioè a prescindere dalle contromisure adottate)

Concetti e definizioni chiave:

- RISCHIO:** Identificazione e valutazione della probabilità che la combinazione di una minaccia e di una vulnerabilità, in rapporto ad un determinato impatto, possano causare un danno significativo.
- MINACCIA:** L'esistenza di fattori avversi che possano avere interesse, capacità ed intenzione di compromettere informazioni, attività, personale o sistemi critici; la minaccia può anche nascere da fattori fisici, ambientali e da azioni intenzionali perpetrate o meno ad opera di soggetti terzi.
- VULNERABILITA':** Debolezze sfruttabili; le vulnerabilità individuano punti di *fault* che possono essere sfruttati da soggetti avversari al fine di portare a termine una minaccia; le vulnerabilità possono essere raggruppate in modo tale da rendere la presentazione dei risultati più chiara ed intuitiva.
- DANNO:** direttamente connesso con il valore dei beni e di due tipologie:
- tangibile: valore monetario del bene critico, impegno economico di ripristino, perdita economica nel periodo di ripristino (dipende dal valore dell'informazione e dagli impianti tecnologici);
 - intangibile: dipende dal compito istituzionale dell'organizzazione, valore legato alla perdita di immagine.

IMPATTO: Per impatto si intende la gravità degli effetti che un dato evento indesiderabile ed inaspettato può causare al patrimonio informativo in funzione del valore dei beni soggetti a compromissione; esempi di eventi indesiderabili possono includere la riduzione di efficienza della rete, la manomissione di dati, la perdita di integrità del sistema (affidabilità, sicurezza, accuratezza, ecc.).

CONSEGUENZE: Non utilizzato.

Elementi della Metodologia di misurazione dei rischi:

Trattandosi di una metodologia generale non prevede specifiche indicazioni su come misurare il rischi, ma da piuttosto indicazioni circa i passi da seguire per eseguire una analisi dei rischi.

Essa fornisce indicazioni su come misurare l'efficacia dell'analisi dei rischi attraverso:

- la descrizione dei processi essenziali di ingegneria della sicurezza dei sistemi e di gestione del rischio che un'organizzazione dovrebbe eseguire;
- la definizione di uno strumento di misura;
- la definizione di una guida per il miglioramento.

In particolare il processo di analisi dei rischi è riconducibile a quattro *process area*: PA2 – *Assess Impact*, PA3 – *Assess Security Risk*, PA4 – *Assess Threat*, PA5 – *Assess Vulnerability*.

VALUTAZIONE DELLE RISORSE:

- | | | |
|-------------------------------------|--|---------------------------------------|
| <input type="checkbox"/> Dati | <input type="checkbox"/> Tecnologia | <input type="checkbox"/> Applicazioni |
| <input type="checkbox"/> Facilities | <input type="checkbox"/> Risorse umane | |

VALUTAZIONE DELL'IMPATTO:

- | | | |
|--|---|---|
| <input checked="" type="checkbox"/> Riservatezza | <input checked="" type="checkbox"/> Integrità | <input checked="" type="checkbox"/> Disponibilità |
| <input type="checkbox"/> Conformità | <input type="checkbox"/> Efficienza operativa | <input type="checkbox"/> Efficacia operativa |

VALUTAZIONE DELLA PROBABILITA':

Trattandosi di una metodologia che descrive i passi e le attività dell'analisi dei rischi, non vengono definiti specifici metodi di valutazione della probabilità, ma viene esclusivamente definito come la probabilità sia un elemento da considerare nella valutazione dei rischi.

VALUTAZIONE DELLE CONTROMISURE:

- | | | |
|--|-------------------------------------|--|
| <input type="checkbox"/> riduzione probabilità | <input type="checkbox"/> preventive | <input type="checkbox"/> disegno della contromisura |
| <input type="checkbox"/> riduzione conseguenze | <input type="checkbox"/> reattive | <input type="checkbox"/> applicazione della contromisura |
| <input type="checkbox"/> evitare il rischio | | |
| <input type="checkbox"/> trasferire il rischio | | |
| <input type="checkbox"/> accettare il rischio | | |

Approccio:

La metodologia prevede l'applicazione dell'analisi dei rischi su:

- processi risorse di business risorse tecnologiche

Passi metodologici:

La metodologia considera le seguenti *process area*:

1 PA02 – *Assess Impact*

L'obiettivo di questo processo è di identificare gli impatti che potrebbero riguardare il sistema e di valutare la probabilità che l'impatto si verifichi. L'impatto può essere tangibile, come mancati ricavi o penali monetarie, oppure intangibili, come una perdita di reputazione.

2 PA03 – *Assess Security Risk*

L'obiettivo di questo processo è di identificare i rischi sulla sicurezza relativi all'affidabilità di un sistema in un determinato ambiente.

Il processo si focalizza sulla determinazione di tali rischi sulla base di una determinata comprensione di come le funzionalità e gli *asset* possono essere vulnerabili a determinate minacce. In particolare, queste attività consistono nell'identificare e valutare la probabilità di accadimento di una *exposure*.

Per *exposure* si intende la combinazione di una minaccia, una vulnerabilità e un impatto che può causare un danno rilevante.

3 PA04 – *Assess Threat*

L'obiettivo di questo processo è di identificare le minacce alla sicurezza e le loro proprietà e caratteristiche.

4 PA05 – *Assess Vulnerability*

L'obiettivo di questo processo è di identificare e descrivere le vulnerabilità della sicurezza di un sistema. Esso comprende le attività di analisi degli *asset* di sistema, definizione di vulnerabilità specifiche e valutazione della vulnerabilità del sistema nel suo complesso.

In questo contesto per vulnerabilità si intende un aspetto di un sistema che potrebbe essere utilizzato con obiettivi diversi da quelli per cui era stato originariamente inteso; una debolezza, un "baco" o un errore di implementazione che potrebbe essere sfruttato da una minaccia. In tal senso le vulnerabilità sono indipendenti da specifiche minacce o attacchi.

Tool a supporto:

- software
- questionari/check -list, ecc.
- manuali e linee guida
- disponibilità training
- disponibilità aggiornamenti periodici
- possibilità di personalizzazioni

Risultati ottenibili:

Come detto è possibile valutare, in un'ottica di miglioramento, la maturità dei processi di sviluppo del software e gestione della sicurezza, ivi inclusa l'analisi dei rischi.

Lingua

- Italiano
- Inglese
- Altro _____

NET.RISK

Informazioni fornite da Marco Bubani di Vem Sistemi

Ambito di applicazione :

Net.Risk è un uno strumento, fruibile via web, in grado di coadiuvare i responsabili della sicurezza in tutti i passi necessari alla gestione della sicurezza informatica.

Tramite il servizio è possibile, infatti, gestire tutte le fasi del processo di sicurezza integrando anche la documentazione richiesta dalla legge 196/03.

Standard di riferimento

British Standard on Information Security Management (BS 7799) - Parte 2

Approccio alla misurazione dei rischi :

qualitativo quantitativo semi-quantitativo

misurazione sia del rischio potenziale o intrinseco (cioè a prescindere dalle contromisure) sia del rischio effettivo o residuo (cioè tenendo conto delle contromisure poste in essere)

misurazione del rischio effettivo o residuo (cioè il rischio relativo alla situazione in essere, comprese le contromisure implementate)

misurazione del rischio potenziale o intrinseco (cioè a prescindere dalle contromisure adottate)

Concetti e definizioni chiave :

RISCHIO: Sono definiti i concetti di Rischio Potenziale e Rischio Reale:

- Rischio Potenziale: valutazione delle vulnerabilità di un dato sottosistema alle minacce presenti. La valutazione è effettuata mediante specifici controlli catalogati e il loro valore pesato in funzione della minaccia;
- Rischio Reale: rischio potenziale pesato in funzione del valore di criticità dell'*asset* su cui insiste.

MINACCIA: E' prevista la valutazione del rischio, in funzione di un catalogo predefinito di minacce

VULNERABILITA': Non compare esplicitamente ma viene considerato nell'analisi attraverso il rischio potenziale

DANNO: Non utilizzato.

IMPATTO: Non utilizzato.

CONSEGUENZE: Non utilizzato.

Elementi della Metodologia di misurazione dei rischi:

Net.Risk suddivide il processo di gestione della sicurezza in diversi passi di seguito schematizzati:

- definizione della politica di sicurezza: la redazione di Policy che regolino azioni e comportamenti da adottare, sono alla base del Sistema di Gestione della Sicurezza Informatica;
- identificazione dell'ambito di applicazione: si identifica COSA si vuole proteggere, è in questa fase che sono inventariati e catalogati gli ASSET del sistema, gli OGGETTI che dovranno essere analizzati per la valutazione del rischio e viene calcolato l'INDICE di CRITICITA' di ogni Asset;
- analisi del rischio: si compone di due fasi, la valutazione e la gestione del rischio:
 - valutazione del rischio: è necessario effettuare una serie di controlli per determinare i rischi a cui gli asset sono sottoposti;
 - gestione del rischio: Gestire il Rischio significa portare il suo valore sotto una soglia accettabile; definendo il Rischio Accettabile verrà presentata una matrice semplificata che mostra solo i problemi inaccettabili;
- azioni correttive: per tutti i valori di rischio superiori a quello accettabile, dovranno essere pianificate delle Azioni Correttive con lo scopo di ridurlo oppure trasferirlo.

VALUTAZIONE DELLE RISORSE:

- | | | |
|--|--|--|
| <input checked="" type="checkbox"/> Dati | <input checked="" type="checkbox"/> Tecnologia | <input checked="" type="checkbox"/> Applicazioni |
| <input checked="" type="checkbox"/> Facilities | <input type="checkbox"/> Risorse umane | |

VALUTAZIONE DELL'IMPATTO:

- | | | |
|--|---|---|
| <input checked="" type="checkbox"/> Riservatezza | <input checked="" type="checkbox"/> Integrità | <input checked="" type="checkbox"/> Disponibilità |
| <input type="checkbox"/> Conformità | <input type="checkbox"/> Efficienza operativa | <input type="checkbox"/> Efficacia operativa |

Il valore di RID (Riservatezza/Integrità e Disponibilità) coincide con il valore di criticità dell'*asset* e viene identificato, su una scala da 1 a 4, basandosi su una serie di interviste da rivolgere ai responsabili di settore.

VALUTAZIONE DELLA PROBABILITA':

Non è attualmente gestito.

VALUTAZIONE DELLE CONTROMISURE:

E' possibile tenere traccia delle contromisure previste per ridurre il rischio residuo

- | | | |
|---|-------------------------------------|--|
| <input type="checkbox"/> riduzione probabilità | <input type="checkbox"/> preventive | <input checked="" type="checkbox"/> disegno della contromisura |
| <input checked="" type="checkbox"/> riduzione conseguenze | <input type="checkbox"/> reattive | <input type="checkbox"/> applicazione della contromisura |
| <input type="checkbox"/> evitare il rischio | | |
| <input type="checkbox"/> trasferire il rischio | | |
| <input checked="" type="checkbox"/> accettare il rischio | | |

Approccio:

La metodologia prevede l'applicazione dell'analisi dei rischi su:

- | | | |
|-----------------------------------|---|--|
| <input type="checkbox"/> processi | <input checked="" type="checkbox"/> risorse di business | <input checked="" type="checkbox"/> risorse tecnologiche |
|-----------------------------------|---|--|

Passi metodologici:

- 1 Definizione della politica di sicurezza
Attraverso il servizio Net.Risk è possibile inserire i documenti che descrivono la Policy aziendale e le Procedure Operative utilizzate dagli incaricati della gestione e manutenzione dei sistemi informatici, centralizzandole in un punto raggiungibile via Web.
- 2 Identificazione dell'ambito di applicazione
In questa fase si definisce il perimetro di intervento al quale verrà applicato il processo. In sostanza il processo potrà essere applicato all'intero sistema informativo o ad una parte di esso.
Individuato il perimetro si effettuerà una catalogazione di tutte le componenti del sistema da analizzare raccogliendo informazioni su:
 - sedi;
 - edifici;
 - aree ed uffici;
 - oggetti (quali router, switch e quant'altro concorra al funzionamento del sistema informativo);
 - *asset* (quali server o archivi cartacei depositari delle informazioni).

In questa fase, oltre ad inventariare tutti gli oggetti sono stati definiti i seguenti step da seguire per determinare la criticità di un *asset*:

- individuare la struttura organizzativa (organigramma);
- individuare applicazioni e banche dati utilizzate da ogni area aziendale;
- determinare l'impatto sul business dovuto ad una perdita di RID (riservatezza Integrità e disponibilità) su dati e applicazioni per ogni area aziendale;
- mappare banche dati e applicazioni sul sistema informativo (quali server applicativi ed archivi elettronico/cartacei)

Il massimo valore di impatto sul business determina l'Indice di Criticità dell'Asset (IdC)

3 Analisi del Rischio

In questa fase Net.Risk ha adottato un sistema proprio che tiene conto dei seguenti fattori:

- catalogazione delle minacce al sistema informativo;
- valutazione delle vulnerabilità a queste minacce mediante controlli sul sistema (rischio potenziale);
- impatto che il verificarsi di una minaccia provoca sul business (rischio reale calcolato come prodotto del rischio potenziale per l'indice di criticità).

Le aree sulle quali vengono effettuati i controlli sono:

- perimetro fisico e logico;
- rete geografica;
- rete locale;
- sistema di cablaggio;
- continuità elettrica;
- archivi cartacei e sale macchine;
- archivi elettronici;
- contratti di outsourcing;
- procedure e policy.

Sono state considerate più di 30 minacce, oltre 60 controlli e più di 250 voci di dettaglio

Incrociando gli Asset ed il loro Indice di Criticità con il valore di Rischio Potenziale per ogni minaccia si ottiene la MATRICE DI RISCHIO.

Sono stati studiate queste logiche distinte della matrice di rischio, in modo da renderla facilmente consultabile, e un grafico complessivo suddiviso per le diverse aree, in modo da avere una visione immediata di quelle su cui lavorare maggiormente

Con la Gestione del Rischio è possibile visualizzare una matrice semplificata che mostra solo i problemi inaccettabili, ossia quelli che superano il livello di soglia considerato accettabile. In questo modo è possibile evidenziare solo le minacce su cui dover agire con azioni correttive, come descritto nel paragrafo successivo.

4 Gestione del Rischio

In questa fase il rischio viene catalogato in *rischio accettabile*, livello di rischi o ritenuto non critico per il Sistema Informativo e *rischio residuo*, livello di rischio per il quale occorre definire un'azione correttiva volta a portarne il valore sotto il livello accettabile.

Il rischio residuo può essere ridotto mettendo in campo una delle seguenti strategie:

- soluzione tecnologica;
- soluzione organizzativa;
- trasferimento di rischio ad un ente terzo (contratti di assistenza o assicurazioni).

E' in questa fase che si determinano le soluzioni di tipo tecnico ed organizzativo, volte a migliorare il sistema di gestione della sicurezza e ad elevarne il livello.

Tool a supporto:

- software
- questionari/ check -list, ecc.
- manuali e linee guida
- disponibilità training
- disponibilità aggiornamenti periodici
- possibilità di personalizzazioni

Risultati ottenibili:

- Calcolo del livello di rischio per area
- Calcolo del livello di rischio per minaccia
- Calcolo del livello di rischio per Asset
- Documenti per la redazione del DPSS (dlgs 196/03)
- Definizione Piano delle Contromisure per ridurre il livello di rischio ad un valore accettabile

Lingua

- Italiano Inglese Altro _____

NORA - Network Oriented Risk Analysis methodology

Informazioni fornite da Luca Corciulo di PricewaterhouseCoopers

Ambito di applicazione:

La metodologia NORA punta l'attenzione sui contesti di rete di comunicazione come ambito di applicazione dell'analisi del rischio,.

In particolare la "risorsa base" che viene definita nella prima fase della metodologia e intorno alla quale ruoterà tutto il processo di analisi del rischio, è costituita dal *NAP* (*Network Access Path*), ossia la descrizione dei percorsi di accesso alla rete in termini di client, server e funzione di rete (O&M, Billing, etc.).

Standard di riferimento

La metodologia è uno standard di PricewaterhouseCoopers per l'analisi dei rischi orientata alle reti (network).

Approccio alla misurazione dei rischi:

- qualitativo quantitativo semi-quantitativo
- misurazione sia del rischio potenziale o intrinseco (cioè a prescindere dalle contromisure) sia del rischio effettivo o residuo (cioè tenendo conto delle contromisure poste in essere)
- misurazione del rischio effettivo o residuo (cioè il rischio relativo alla situazione in essere, comprese le contromisure implementate)
- misurazione del rischio potenziale o intrinseco (cioè a prescindere dalle contromisure adottate)

Concetti e definizioni chiave:

- RISCHIO:** Il rischio è un termine utilizzato per esprimere la potenzialità che una minaccia (threat) si possa materializzare e trasformare in danno. Questa potenzialità è funzione dei controlli esistenti. L'impatto è ovviamente legato al bene considerato a rischio.
- MINACCIA:** [*Tbrear*] Una minaccia è un'azione che esula dal controllo e che può tradursi in un danno. Ogni minaccia ha associata una probabilità inerente al suo manifestarsi.
- Alcune minacce hanno associata una probabilità relativamente elevata, quali la probabilità che una linea P.T.O. degradi; altre, quali l'intercettazione o i tentativi di intrusione da parte di hacker sfruttando la rete pubblica, hanno associata una probabilità relativamente bassa.
- Ovviamente, questa probabilità è funzione del livello di attrazione e interesse suscitato dall'organizzazione. L'esistenza di una minaccia non è soggetto a controlli. Si è distinto il concetto di "minaccia" da quello di "rischio", poichè si è voluto dissociare quello che può succedere (minaccia) da quello potenziale che effettivamente si manifesta (il rischio); quando si verificherà, ci sarà un impatto reale, associato al rischio.

- VULNERABILITA'**: Non utilizzato.
- DANNO**: Non utilizzato.
- IMPATTO**: Non utilizzato.
- CONSEGUENZE**: Non utilizzato.

Altre definizioni:

CONTROLLO: [*Control*] Un controllo è un elemento che decrementa la potenzialità (o rischio) che una minaccia si manifesti. I controlli possono essere classificati come preventivi, rivelatori o correttivi.

RISCHIO RESIDUO E GRAVITA': Il rischio residuo è la parte del rischio che rimane dopo l'applicazione dei controlli.

I controlli possono influenzare sia la probabilità che l'impatto. La stima finale della probabilità e dell'impatto ha come output la 'gravità' stabilita utilizzando una matrice di gravità.

Il rischio residuo può essere strutturato in due categorie:

- il rischio di business residuo è quella parte di rischio rimanente che riguarda il conseguimento degli obiettivi di business;
- il rischio IT residuo è quella parte di rischio rimanente che riguarda la distribuzione di servizi IT

NORA si concentra sul rischio IT.

Elementi della Metodologia di misurazione dei rischi:

I seguenti elementi di base sono utilizzati dalla metodologia per il processo di analisi dei rischi:

- *Network Access Path*: descrizione dei percorsi di accesso alla rete in termini di client, server e funzioni di rete (O&M, Billing, etc.)
- *Threat Scenario* (scenario delle minacce): elaborati sulla base di scenari individuati all'interno dei sistemi informativi; NORA dispone di predefiniti "Threat Scenario", che devono poi essere mappati sulla specifica situazione della realtà aziendale oggetto di analisi, determinata dai NAP;
- *Matrice NSC* (Nap/Scenario Combination): determinata dalla correlazione fra NAP e Threat scenario;
- *Impact Criteria*: criteri di valutazione degli impatti (definiti su scala da A ad E, in ordine decrescente di impatto) sugli scenari delle minacce, rispetto ai parametri RID (Riservatezza Integrità Disponibilità);
- *Probability Scale*: valutazione della probabilità di attuazione delle minacce (su scala da 1 a 5);
- *Gravity Matrix*: combinazione di *Impact Criteria* e *Probability Scale* per dare valori di gravità.

VALUTAZIONE DELLE RISORSE:

La metodologia, nella prima fase di “Inizializzazione”, identifica i beni tangibili (fisici, come ad esempio computer, edifici, e/o logici, come software, sistemi IT, database, ecc.) che rientrano nei Percorsi di accesso alle reti (NAP); quest’ultimi costituiscono l’elemento base di tutto il processo di analisi dei rischi.

- | | | |
|--|--|--|
| <input type="checkbox"/> Dati | <input checked="" type="checkbox"/> Tecnologia | <input checked="" type="checkbox"/> Applicazioni |
| <input checked="" type="checkbox"/> Facilities | <input type="checkbox"/> Risorse umane | |

VALUTAZIONE DELL’IMPATTO:

I criteri della valutazione dell’impatto sono riportati nel precedente punto dove si descrivono gli elementi della metodologia di valutazione dei rischi.

- | | | |
|--|---|---|
| <input checked="" type="checkbox"/> Riservatezza | <input checked="" type="checkbox"/> Integrità | <input checked="" type="checkbox"/> Disponibilità |
| <input type="checkbox"/> Conformità | <input type="checkbox"/> Efficienza operativa | <input type="checkbox"/> Efficacia operativa |

VALUTAZIONE DELLA PROBABILITA’:

I criteri della valutazione della probabilità di attuazione delle minacce sono riportati nel precedente punto dove si descrivono gli elementi della metodologia di valutazione dei rischi.

VALUTAZIONE DELLE CONTROMISURE:

La metodologia prevede la valutazione delle contromisure da adottare al fine di mitigare i rischi, sulla base dei risultati definiti nella “Gravity Matrix”, come combinazione dei valori di “Impact Criteria” e “Probability Scale” (ricavati dalle fasi precedenti della metodologia)

Nella terza e ultima fase della metodologia, si prevede la definizione di un piano d’azione sulla base di soluzioni generiche e della valutazione di quanto offre il mercato (i.e. stato dell’arte); tale piano è tipicamente strutturato su 3 livelli così definiti:

- *Legacy systems/ Critical actions*, per mitigare i rischi con gravità elevate;
- *Legacy systems/ Complementary actions*, per mitigare i rischi che si intende indirizzare a medio-lungo termine
- *The Way Forward*, per la pianificazione pro-attiva delle misure di sicurezza a fronte di sviluppi futuri di rete.

- | | | |
|---|--|--|
| <input checked="" type="checkbox"/> riduzione probabilità | <input checked="" type="checkbox"/> preventive | <input type="checkbox"/> disegno della contromisura |
| <input checked="" type="checkbox"/> riduzione conseguenze | <input type="checkbox"/> reattive | <input type="checkbox"/> applicazione della contromisura |
| <input type="checkbox"/> evitare il rischio | | |
| <input type="checkbox"/> trasferire il rischio | | |
| <input type="checkbox"/> accettare il rischio | | |

Approccio:

La metodologia prevede l'applicazione dell'analisi dei rischi su:

- processi risorse di business risorse tecnologiche

Passi metodologici:

1 Inizializzazione:

- Rilevazione di tutti i link di rete.
- Rilevazione della struttura organizzativa (organizzazione a supporto della rete).
- Rilevazione delle piattaforme tecnologiche di rete.
- Raccolta di altre informazioni utili ai fini dell'avvio del processo di analisi (es. minacce e vulnerabilità di rete già conosciute, business drivers).
- Inventario della documentazione di rete.

Questa fase permette di rilevare l'ambiente tecnologico e organizzativo di riferimento, nonché di inventariare la documentazione dei beni di rete, tramite:

- *Network Documentation Questionnaire* (NDQ, sezione 1 e 2);
- altre interviste a completamento della fase di raccolta delle informazioni (esempio: tipologia dei servizi offerti, previsione dei volumi di traffico, incidenti di rete avvenuti).

2 Analisi

a. Analisi dei rischi:

- Mappatura delle "Business communication" sui NAP.
- Definizione delle combinazioni possibili fra "Threat Scenario" e NAP, in base a matrice di NSC (Nap/Scenario Combination).
- Valutazione dei possibili impatti sugli scenari delle minacce, rispetto ai parametri RID, determinati in base agli "Impact Criteria".

b. Analisi delle vulnerabilità

- "Analisi delle vulnerabilità", condotta tramite programmi di audit, che consente di determinare la probabilità di accadimento di un determinato scenario di minacce (in base a probability scale), al fine di determinare la matrice di gravità (la Gravity Matrix, ricavata come combinazione di impatto e probabilità di accadimento).

c. Sviluppi futuri

- Valutazione di sviluppi futuri sulle tecnologie.
- Valutazione degli impatti sulla sicurezza che tali sviluppi possono comportare.

3 Action Plan

Definizione di un piano d'azione sulla base di soluzioni generiche e della valutazione di quanto offre il mercato (i.e. stato dell'arte); è tipicamente strutturato sui 3 livelli definiti nel precedente punto "Valutazione delle contromisure".

Tool a supporto:

software

questionari/ check-list, ecc.

- Questionario per la documentazione e inventariamento degli asset di rete (fisici, logici, ecc.) denominato “Network Documentation Questionnaire”;
- Tabelle per la definizione dei NAP (Network Access Paths Matrix);
- Tabella di scenari predefiniti di minacce (Threat Scenario matrix), che devono poi essere mappati sulla specifica situazione della realtà aziendale oggetto di analisi, determinata dai NAP (vedere punto successivo);
- Matrice NSC (combinazione di NAP con “Threat Scenario”);
- Gravity Matrix

manuali e linee guida

disponibilità training

Sono disponibili corsi di formazione e seminari/convegni sul tema.

disponibilità aggiornamenti periodici

La metodologia viene aggiornata periodicamente.

possibilità di personalizzazioni

Possono essere predisposte personalizzazioni della metodologia in base a eventuali specifiche esigenze.

Risultati ottenibili:

Il processo di analisi del rischio ha come output una lista di rischi, classificata secondo il rischio residuo.

Lingua

Italiano

Inglese

Altro _____

OCTAVE® - Operationally Critical Threat, Asset, and Vulnerability EvaluationSM

Informazioni fornite da Francesca Di Massimo di Microsoft Italia

Ambito di applicazione :

OCTAVE è stata progettata per le grandi organizzazioni, mentre è in corso di definizione OCTAVE-S, specifica per le piccole organizzazioni

Standard di riferimento

Gli elementi essenziali, o requisiti, dell'approccio OCTAVE si esplicitano in un insieme di criteri, con cui possono essere consistenti molti metodi differenti.

Il Software Engineering Institute ha sviluppato due metodi che aderiscono ai criteri OCTAVE.

Anche altre organizzazioni stanno sviluppando le loro versioni di metodi consistenti con OCTAVE.

Questo può avvenire per specifici settori come per esempio la sanità oppure specifico per uno standard come l'ISO 17799, oppure possono incorporare strumenti e processi aggiuntivi che espandono l'area di competenza di OCTAVE.

Approccio alla misurazione dei rischi :

qualitativo

quantitativo

semi-quantitativo

misurazione sia del rischio potenziale o intrinseco (cioè a prescindere dalle contromisure) sia del rischio effettivo o residuo (cioè tenendo conto delle contromisure poste in essere)

misurazione del rischio effettivo o residuo (cioè il rischio relativo alla situazione in essere, comprese le contromisure implementate)

misurazione del rischio potenziale o intrinseco (cioè a prescindere dalle contromisure adottate)

Concetti e definizioni chiave :

RISCHIO: La possibilità di essere vittima di perdita o danneggiamento. Il concetto di rischio si riferisce a situazioni nelle quali una persona o un evento possono generare un danno e quindi avere impatti e conseguenze negative. Un rischio è composto da:

- evento;
- incertezza;
- conseguenza.

Nell'ambito della sicurezza dell'informazione, l'evento scatenante è la minaccia.

MINACCIA: È l'indicazione di un evento potenzialmente dannoso. Una minaccia si riferisce ad una situazione nella quale una persona (come ad esempio una persona che inizia un attacco di tipo denial of service contro il server mail di una organizzazione) o un evento (come ad esempio un incendio che danneggia hardware del sistema informativo di un'organizzazione) possono generare un danno.

VULNERABILITA': Non utilizzato.

DANNO: Non utilizzato.

IMPATTO: L'impatto è l'effetto negativo di una minaccia sulla missione e sugli obiettivi di business di un'organizzazione.

I criteri di valutazione dell'impatto devono essere usati per valutare l'impatto di ogni minaccia sulla missione e sugli obiettivi di business dell'organizzazione. E' necessario che i criteri scelti vengano applicati alle seguenti aree:

- reputazione/ fiducia dei clienti;
- incolumità/ salute delle persone;
- impatti e/o sanzioni legali;
- impatti finanziari;
- produttività;
- altro.

CONSEGUENZE: Non utilizzato.

Altre definizioni:

ASSET: ciò che rappresenta un valore per l'azienda. Gli asset di Information technology sono la combinazione di asset logici e fisici e sono raggruppati in classi specifiche (informazioni, sistemi, Servizi e applicazioni, personale)

ASSET CRITICI – gli asset più importanti per l'organizzazione, l'organizzazione subirebbe un impatto fortemente negativo nei seguenti casi :

- un asset critico viene rivelato a persone non autorizzate;
- un asset critico viene modificato senza autorizzazione;
- un asset critico viene perso o distrutto;
- l'accesso ad un asset critico viene interrotto.

PROBABILITA': la possibilità che un evento si verifichi

TEMPO TRA DUE EVENTI: la stima della frequenza con cui un evento può verificarsi (esempio: settimanalmente, una volta ogni due anni)

FREQUENZA ANNUALIZZATA: la proiezione annuale della possibilità che una minaccia si concretizzi in un dato anno.

PRATICHE DI SICUREZZA: gruppi di pratiche che possono essere sia strategiche che operazionali. Le pratiche di sicurezza strategiche hanno tipicamente un raggio d'azione molto ampio e indirizzano equamente tutti i rischi relativi a tutti gli asset critici (esempio: documentare un insieme di procedure di sicurezza) . Le pratiche operazionali sono invece focalizzate su attività giornaliere e possono essere indirizzate mitigando specifici rischi su specifici asset (esempio: controllare i default account di un sistema)

Elementi della Metodologia di misurazione dei rischi :

In OCTAVE, si valuta solo l'impatto di un rischio. La misura qualitativa nei tre livelli di alto, medio, basso è il metodo più semplice per assegnare un valore all'impatto del rischio. Questa misura fornisce un metro di paragone adeguato per confrontare i diversi impatti che incombono sui beni critici.

VALUTAZIONE DELLE RISORSE:

- | | | |
|--|---|--|
| <input checked="" type="checkbox"/> Dati | <input checked="" type="checkbox"/> Tecnologia | <input checked="" type="checkbox"/> Applicazioni |
| <input checked="" type="checkbox"/> Facilities | <input checked="" type="checkbox"/> Risorse umane | |

VALUTAZIONE DELL'IMPATTO:

Utilizzando l'approccio OCTAVE, un'organizzazione prende le decisioni riguardanti la protezione delle informazioni sulla base dei rischi di riservatezza, integrità e disponibilità degli asset relativi alle informazioni critiche.

- | | | |
|--|---|---|
| <input checked="" type="checkbox"/> Riservatezza | <input checked="" type="checkbox"/> Integrità | <input checked="" type="checkbox"/> Disponibilità |
| <input type="checkbox"/> Conformità | <input type="checkbox"/> Efficienza operativa | <input type="checkbox"/> Efficacia operativa |

VALUTAZIONE DELLA PROBABILITA':

Le probabilità delle minacce vengono stimate usando una combinazione di dati oggettivi, dell'esperienza soggettiva e dell'expertise.

Chi usa OCTAVE per la prima volta, non avrà dati oggettivi relativi alle minacce. Ma poiché spesso anche l'esperienza soggettiva e l'expertise mancano, in OCTAVE - *La probabilità è considerata a opzionale*. Ogni team deciderà se e come usare il concetto di probabilità.

VALUTAZIONE DELLE CONTROMISURE:

Per strategia di protezione si intende il modo in cui un'organizzazione intende alzare o mantenere il livello di sicurezza esistente. Il suo obiettivo è di indirizzare gli sforzi futuri legati alla sicurezza e di trovare una soluzione immediata a ogni vulnerabilità.

La strategia di protezione è strutturata in due aree di azione.

- *aree strategiche:*
 - sensibilizzazione e training;
 - strategie di sicurezza;
 - gestione della sicurezza;
 - procedure e norme di sicurezza;
 - gestione collaborative della sicurezza;
- *aree operative:*
 - controllo degli accessi fisici;
 - monitoraggio e auditing della sicurezza fisica;
 - gestione rete e sistemi;
 - autenticazione e autorizzazione;
 - gestione delle vulnerabilità;
 - crittografia;
 - progettazione della sicurezza e architetture;
 - gestione degli incidenti.

- | | | |
|---|--|---|
| <input checked="" type="checkbox"/> riduzione probabilità | <input checked="" type="checkbox"/> preventive | <input checked="" type="checkbox"/> disegno della contromisura |
| <input checked="" type="checkbox"/> riduzione conseguenze | <input type="checkbox"/> reattive | <input checked="" type="checkbox"/> applicazione della contromisura |
| <input type="checkbox"/> evitare il rischio | | |
| <input type="checkbox"/> trasferire il rischio | | |
| <input checked="" type="checkbox"/> accettare il rischio | | |

Approccio:

La metodologia prevede l'applicazione dell'analisi dei rischi su:

- | | | |
|--|---|--|
| <input checked="" type="checkbox"/> processi | <input checked="" type="checkbox"/> risorse di business | <input checked="" type="checkbox"/> risorse tecnologiche |
|--|---|--|

Passi metodologici :

OCTAVE è una attività di valutazione e non un processo continuo: periodicamente, un'organizzazione dovrà applicare nuovamente la metodologia OCTAVE.

OCTAVE valuta i rischi di sicurezza a livello organizzativo, tecnologico e di analisi tramite un approccio in tre fasi.

- 1 Costruire i profili delle minacce per singolo asset
 Questa valutazione è organizzativa. Il team di analisi definisce cosa è importante per l'organizzazione (asset informativi) e cosa l'organizzazione fa per proteggere questi asset .
 Il team seleziona quindi gli asset di importanza critica per l'organizzazione (asset critici) e descrive i requisiti di sicurezza per ognuno di essi. Alla fine, identifica le minacce ad ogni asset critico che contribuisce a creare il profilo delle minacce per quell'asset.
- 2 Identificare le vulnerabilità dell'infrastruttura
 Questa è una valutazione dell'infrastruttura informativa. Il team di analisi esamina i percorsi di accesso alla rete, identifica classi di componenti tecnologici relative ad ogni asset critico . Il team determina la misura in cui ogni classe è in grado di resistere agli attacchi alla rete.
- 3 Sviluppare una strategia e un piano di sicurezza
 Durante questa parte di valutazione, il team di analisi identifica i rischi dell'organizzazione sugli asset critici e decide cosa fare . Il team crea una strategia di protezione per l'organizzazione e un piano di mitigazione per indirizzare i rischi sugli asset critici , sulla base dell'analisi delle informazioni raccolte.

Tool a supporto :

- | |
|--|
| <input type="checkbox"/> software |
| <input type="checkbox"/> questionari/ check -list, ecc. |
| <input checked="" type="checkbox"/> manuali e linee guida |
| Scaricabili da http://www.cert.org/octave |
| <input checked="" type="checkbox"/> disponibilità training |
| Scaricabili da http://www.cert.org/octave |
| <input type="checkbox"/> disponibilità aggiornamenti periodici |
| <input type="checkbox"/> possibilità di personalizzazioni |

Risultati ottenibili:

OCTAVE crea una vista organizzativa dei rischi della sicurezza informatica ai quali è esposta l'organizzazione, fornendo una sorta di linea di base che può essere utilizzata per focalizzare le attività di mitigazione del rischio e miglioramento organizzativo.

Con l'utilizzo di OCTAVE, l'attività del team di analisi può essere così suddivisa:

- identificazione dei rischi di sicurezza informatica dell'organizzazione;
- analisi dei rischi al fine di determinare le priorità;
- pianificazione: sviluppo di una strategia di protezione per ottenere miglioramenti organizzativi e di un piano di mitigazione dei rischi per ridurre i rischi sugli asset critici per l'organizzazione.

Lingua

Italiano

Inglese

Altro _____

OSSTMM – Open Source Security Testing Methodology Manual

Informazioni fornite da Raoul Chiesa – Board of Directors Member CLUSIT, ISECOM, TSTF

Ambito di applicazione:

Open Source Security Testing Methodology Manual (OSSTMM) è una metodologia per l'esecuzione di test sulla sicurezza e una metrica per la misurazione dei risultati. Quest'ultima è denominata RAVs (*Risk Assessment Values*). I casi di test definiti dalla metodologia sono raggruppati in cinque sezioni (*channels*) che, nel loro insieme, si riferiscono a:

- livello di consapevolezza del personale sulla sicurezza;
- siti fisici, quali edifici, barriere fisiche e confini, basi militari;
- sicurezza degli accessi fisici;
- reti di elaboratori e per le telecomunicazioni;
- informazioni e dati;
- processi di gestione della sicurezza;
- apparati wireless e mobili;
- frodi e *social engineering*.

Standard di riferimento

OSSTMM – Open Source Security Testing Methodology Manual
(<http://www.osstmm.org>, <http://www.isecom.org>, <http://osstmm.mediaservice.net>)
dell'ISECOM, Institute for Security and Open Methodologies (USA, EU:
<http://www.isecom.org>).

Approccio alla misurazione dei rischi:

- qualitativo quantitativo semi-quantitativo
- misurazione sia del rischio potenziale o intrinseco (cioè a prescindere dalle contromisure) sia del rischio effettivo o residuo (cioè tenendo conto delle contromisure poste in essere)
- misurazione del rischio effettivo o residuo (cioè il rischio relativo alla situazione in essere, comprese le contromisure implementate)
- misurazione del rischio potenziale o intrinseco (cioè a prescindere dalle contromisure adottate)

Concetti e definizioni chiave:

- RISCHIO:** Una limitazione della sicurezza che ha un effetto negativo su persone, cultura, informazioni, processi, *business*, immagine, proprietà e capitale intellettuale.
- MINACCIA:** Non utilizzato.
- VULNERABILITA':** [*Vulnerability*] Una falla insita nello stesso meccanismo di sicurezza o un "meccanismo" che può essere sfruttato per aggirare le misure di sicurezza e ottenere un accesso privilegiato.
- DANNO:** Non utilizzato.
- IMPATTO:** Non utilizzato.

Elementi della Metodologia di misurazione dei rischi:

La metodologia OSSTMM affronta il problema dell'analisi dei rischi adottando un approccio orientato ad un'analisi diretta degli asset informatici.

Pur non essendo una metodologia di risk assessment di per sè, un test di sicurezza OSSTMM unito all'applicazione dei RAVs può fornire una base effettiva per un'analisi dei rischi e degli investimenti nella gestione della sicurezza, collegandosi quindi ai processi di Risk Analysis.

VALUTAZIONE DELLE RISORSE:

- | | | |
|--|---|--|
| <input type="checkbox"/> Dati | <input checked="" type="checkbox"/> Tecnologia | <input checked="" type="checkbox"/> Applicazioni |
| <input checked="" type="checkbox"/> Facilities | <input checked="" type="checkbox"/> Risorse umane | |

VALUTAZIONE DELL'IMPATTO:

- | | | |
|--|---|---|
| <input checked="" type="checkbox"/> Riservatezza | <input checked="" type="checkbox"/> Integrità | <input checked="" type="checkbox"/> Disponibilità |
| <input checked="" type="checkbox"/> Conformità | <input type="checkbox"/> Efficienza operativa | <input checked="" type="checkbox"/> Efficacia operativa |

VALUTAZIONE DELLA PROBABILITA':

OSSTMM non definisce una scala, ma fornisce gli elementi per farlo.

VALUTAZIONE DELLE CONTROMISURE:

- | | | |
|---|--|---|
| <input type="checkbox"/> riduzione probabilità | <input checked="" type="checkbox"/> preventive | <input checked="" type="checkbox"/> disegno della contromisura |
| <input checked="" type="checkbox"/> riduzione conseguenze | <input checked="" type="checkbox"/> reattive | |
| <input checked="" type="checkbox"/> evitare il rischio | | <input checked="" type="checkbox"/> applicazione della contromisura |
| <input type="checkbox"/> trasferire il rischio | | |
| <input checked="" type="checkbox"/> accettare il rischio | | |

<p>ALTRI ELEMENTI:</p> <p>OSSTMM definisce i requisiti operativi utili per collocare un elemento nel c.d. “spazio della sicurezza”.</p>
<p><u>Approccio:</u></p> <p>La metodologia prevede l'applicazione dell'analisi dei rischi su:</p> <p><input type="checkbox"/> processi <input checked="" type="checkbox"/> risorse di business <input checked="" type="checkbox"/> risorse tecnologiche</p>
<p><u>Passi metodologici:</u></p> <ol style="list-style-type: none"> 1 <i>Penetration Testing</i> per la raccolta sul campo dei dati. 2 Verifica incrociata con questionari, modelli di intervista e moduli di raccolta dati. 3 Correlazione dei dati raccolti direttamente sul campo e quelli dichiarati dai responsabili aziendali. 4 Applicazione dei RAVs.
<p><u>Tool a supporto:</u></p> <p><input type="checkbox"/> software</p> <p><input checked="" type="checkbox"/> questionari/ check-list, ecc.</p> <p><input checked="" type="checkbox"/> manuali e linee guida</p> <p>Disponibili in più lingue.</p> <p><input checked="" type="checkbox"/> disponibilità training</p> <p>A livello nazionale ed internazionale.</p> <p><input checked="" type="checkbox"/> disponibilità aggiornamenti periodici</p> <p><input checked="" type="checkbox"/> possibilità di personalizzazioni</p>
<p><u>Risultati ottenibili:</u></p> <p>Si riassumono di seguito i principali risultati ottenibili:</p> <ul style="list-style-type: none"> • misurazione in scala assoluta del livello di sicurezza (<i>Actual Security</i>); • controllo sui sistemi di mitigazione del danno; • previsione dei <i>down-time</i> applicabili ai differenti asset: <i>Data Networks Security</i>, <i>Physical Security</i>, <i>Personnel Security</i>, ecc.; • gestione degli investimenti sugli elementi di sicurezza; • interfacciamento, integrazione e <i>compliance</i> con i principali standard e metodologie (ISO 17799, ISO27001, BS7799, GAO, FISCAM, NIST, SOX, ecc.).
<p><u>Lingua</u></p> <p><input checked="" type="checkbox"/> Italiano <input checked="" type="checkbox"/> Inglese <input checked="" type="checkbox"/> Altro: Cinese, Giapponese, Spagnolo (altre lingue in corso di sviluppo)</p>

PRA Psychological Risk Assessment

Informazioni fornite da Roberta Bruzzone di ICAA (International Crime Analysis Association)

<u>Ambito di applicazione:</u>		
Risorse umane di organizzazioni pubbliche e private di tutte le dimensioni, compreso il singolo utente.		
<u>Standard di riferimento</u>		
La metodologia è stata creata dall' <i>International Crime Analysis Association</i> (www.criminologia.org e www.icaa-italia.org) in linea con gli standard internazionali di valutazione in psicologia clinica e del lavoro.		
<u>Approccio alla misurazione dei rischi:</u>		
<input checked="" type="checkbox"/> qualitativo	<input checked="" type="checkbox"/> quantitativo	<input type="checkbox"/> semi-quantitativo
L'attività di misurazione è finalizzata ad interventi diretti e mirati di prevenzione del crime e di comportamenti pericolosi che possono favorire il verificarsi di incidenti a danno dell'organizzazione nel suo complesso.		
<input checked="" type="checkbox"/> misurazione sia del rischio potenziale o intrinseco (cioè a prescindere dalle contromisure) sia del rischio effettivo o residuo (cioè tenendo conto delle contromisure poste in essere)		
<input type="checkbox"/> misurazione del rischio effettivo o residuo (cioè il rischio relativo alla situazione in essere, comprese le contromisure implementate)		
<input type="checkbox"/> misurazione del rischio potenziale o intrinseco (cioè a prescindere dalle contromisure adottate)		
<u>Concetti e definizioni chiave:</u>		
<input checked="" type="checkbox"/> RISCHIO: la concezione del rischio nel PRA dell'ICAA è l'ipotesi che appartenenti ad un'organizzazione possano intraprendere azioni illegali ai danni della stessa o favorire incidenti attraverso il non rispetto delle <i>policy</i> di sicurezza.		
<input checked="" type="checkbox"/> MINACCIA: [<i>Threat</i>] Una minaccia è rappresentata dalla carenza di <i>security awareness</i> in un ambito specifico che possa favorire un attacco o un incidente.		
<input type="checkbox"/> VULNERABILITA': Non utilizzato.		
<input type="checkbox"/> DANNO: Non utilizzato.		
<input type="checkbox"/> IMPATTO: Non utilizzato.		
<input type="checkbox"/> CONSEGUENZE: Non utilizzato.		
<u>Elementi della Metodologia di misurazione dei rischi:</u>		
Misurazione di dimensioni qualitative di percezione del crimine e <i>security awareness</i> attraverso scale per la misurazione della conoscenza e degli atteggiamenti di tipo <i>Lickert</i> e basate sul differenziale semantico di Osgood.		
Numerizzazione delle variabili qualitative con punteggi numerici bilanciati dagli autori del test (Strano M., Bruzzone R., 2003).		

VALUTAZIONE DELLE RISORSE:

La metodologia consente di valutare le risorse umane poste in diversi livelli gerarchici dell'organizzazione e con diverso livello di competenza informatica.

- | | | |
|--|--|---------------------------------------|
| <input type="checkbox"/> Dati | <input type="checkbox"/> Tecnologia | <input type="checkbox"/> Applicazioni |
| <input type="checkbox"/> <i>Facilities</i> | <input type="checkbox"/> Risorse umane | |

VALUTAZIONE DELL'IMPATTO:

Non applicabile.

- | | | |
|---------------------------------------|---|--|
| <input type="checkbox"/> Riservatezza | <input type="checkbox"/> Integrità | <input type="checkbox"/> Disponibilità |
| <input type="checkbox"/> Conformità | <input type="checkbox"/> Efficienza operativa | <input type="checkbox"/> Efficacia operativa |

VALUTAZIONE DELLA PROBABILITA':

Non applicabile

VALUTAZIONE DELLE CONTROMISURE:

La metodologia prevede sia il suggerimento sia la valutazione delle contromisure da adottare, sulla base degli effettivi elementi di criticità emersi attraverso l'impiego dello strumento.

- | | | |
|--|-------------------------------------|--|
| <input type="checkbox"/> riduzione probabilità | <input type="checkbox"/> preventive | <input type="checkbox"/> disegno della contromisura |
| <input type="checkbox"/> riduzione conseguenze | <input type="checkbox"/> reattive | <input type="checkbox"/> applicazione della contromisura |
| <input type="checkbox"/> evitare il rischio | | |
| <input type="checkbox"/> trasferire il rischio | | |
| <input type="checkbox"/> accettare il rischio | | |

Approccio:

La metodologia prevede l'applicazione dell'analisi dei rischi su:

- | | | |
|-----------------------------------|--|---|
| <input type="checkbox"/> processi | <input type="checkbox"/> risorse di business | <input type="checkbox"/> risorse tecnologiche |
|-----------------------------------|--|---|

Non applicabile.

Passi metodologici:

1 Ricerca di sfondo e analisi dell'organizzazione:

- Analisi architetturale del sistema informativo dell'organizzazione.
- Analisi dell'infrastruttura di sicurezza e delle procedure di sicurezza.
- Rilevazione delle piattaforme tecnologiche di rete.

Questa fase permette di rilevare l'ambiente tecnologico e organizzativo di riferimento.

2 Analisi dei rischi e delle vulnerabilità specifici dell'organizzazione

- Mappatura delle criticità connesse al fattore umano.
- Definizione dello scenario di intervento.
- Messa a punto degli strumenti calibrati sulla base dello scenario di riferimento.
- Determinazione del campione di risorse da coinvolgere nell'analisi.
- Somministrazione degli strumenti.
- Analisi dei dati raccolti attraverso gli strumenti che compongono l'*assessment* PRA.
- Definizione delle aree critiche.
- Redazione del report finale e definizione della *roadmap* di intervento.

Tool a supporto:

software

questionari/ *check-list*, ecc.

Questionario per l'analisi della percezione del crimine e della percezione del rischio di attacco sia interno che esterno.

manuali e linee guida

disponibilità training

Sono disponibili sia corsi di formazione sia seminari/convegni sul tema.

disponibilità aggiornamenti periodici

possibilità di personalizzazioni

Sono possibili personalizzazioni della metodologia in base alle eventuali specifiche esigenze.

Risultati ottenibili:

Il processo di analisi del rischio ha come output una lista di aree critiche in base a scale predefinite su cui orientare un possibile intervento, con l'obiettivo di ottenere una riduzione tangibile degli attacchi inside e dei comportamenti pericolosi che possono favorire gli attacchi (sia interni che esterni) boicottando la sicurezza dell'organizzazione nel suo complesso.

Lingua

Italiano

Inglese

Altro _____

RAF - Risk Analysis Facility

Informazioni fornite da Roberto Margherita di Banksiel

Ambito d'applicazione:

Aziende/Istituzioni di ogni dimensione, per diversi settori di business. Impiegato con successo in attività di certificazioni BS7799 in ambito di servizi bancari e di hosting/housing di Centri Elaborazione Dati (CED) di grandi aziende.

Standard di riferimento

Metodologia sviluppata da Deveco Informatica s.r.l. (www.deveco.it) a supporto delle attività di analisi del rischio nei moderni sistemi di gestione della sicurezza delle informazioni aderenti allo standard ISO27001.

Approccio alla misurazione dei rischi:

- qualitativo quantitativo semi-quantitativo
- misurazione sia del rischio potenziale o intrinseco (a prescindere dalle contromisure, e nello specifico definito "rischio calcolato") sia del rischio effettivo o residuo (tenendo conto delle contromisure poste in essere)
- misurazione del rischio effettivo o residuo (cioè il rischio relativo alla situazione in essere, comprese le contromisure implementate)
- misurazione del rischio potenziale o intrinseco (cioè a prescindere dalle contromisure adottate)

Concetti e definizioni chiave:

- RISCHIO:** Misura dell'esposizione del sistema alla terna impatti, minacce e vulnerabilità, senza (rischio calcolato) e con le contromisure (rischio residuo).
- MINACCIA:** Evento indesiderato in grado di provocare un malfunzionamento o un danno al sistema.
- VULNERABILITA':** Caratteristica intrinseca del sistema che può condurre, anche accidentalmente, a danni e/o perdite per l'azienda.
- DANNO:** Non utilizzato.
- IMPATTO:** Conseguenza che si scatena al verificarsi di un dato evento.
- CONSEGUENZE:** Non utilizzato.

Elementi della Metodologia di misurazione dei rischi:

La metodologia si fonda su:

- un censimento degli asset;
- una valutazione degli asset in termini di valore intrinseco, se conosciuto;
- una valutazione degli impatti in termini di RID (riservatezza, integrità, disponibilità), con attribuzione di un peso relativo;
- una valutazione delle minacce e delle vulnerabilità;
- un calcolo del rischio assoluto in funzione del valore attribuito a impatti, minacce e vulnerabilità;
- una selezione delle contromisure con il loro stato, la determinazione del grado di abbattimento e la generazione del calcolo del rischio residuo.

La metodologia non è strettamente data-centrica: i tipi di asset sono paritetici e non viene pre-constituita una gerarchia governata dal dato. Questo consente una maggiore libertà di scelta per quelle analisi che richiedono di indagare più puntualmente alcuni aspetti che devono prescindere necessariamente dal valore dei dati.

Gli asset sono raggruppabili per tipi omogenei al fine di velocizzare le attività di valutazione. Si può ricorrere ad un'ulteriore entità di aggregato (Procedura), che consente il raggruppamento di asset eterogenei ma afferenti ad uno stesso "processo", permettendo una rappresentazione dei rischi per "processo" di business. In ogni generazione degli insiemi il valore di rischio dell'insieme coincide con quello tra i suoi elementi che presenta il valore di rischio più elevato.

L'analista può liberamente determinare le voci di impatto, di minacce e contromisure, agendo in amministrazione sulle opportune tabelle, attraverso le quali può altresì personalizzare le relazioni tra minacce e contromisure, ricorrendo a tabelle intermedie, denominate "aree di controllo".

Questo disaccoppiamento delle relazioni che possono essere costruite tra tipo di asset-minaccia, minaccia-area di controllo, contromisura-area di controllo, rende lo strumento particolarmente adatto a mappare qualunque dizionario di minacce e contromisure impiegati da standard (es. ISO27001) o best practice.

Il rischio assoluto (o "calcolato") è generato come risultante della matrice che associa impatti (pesati con il proprio coefficiente), minacce e vulnerabilità.

Il rischio residuo è ricavato valutando ciascuna contromisura concernente la stessa area di controllo interessata dalle minacce per il singolo asset. Il coefficiente di abbattimento è funzione dello stato (da operativa a non operativa, con altri diversi stati intermedi) e di un peso intrinseco funzione del numero di minacce contrastate dalla stessa contromisura (si assume avente peso maggiore la contromisura che, tra quelle in essere, sia priva di alternative per quella minaccia applicata a quell'asset).

VALUTAZIONE DELLE RISORSE:

- | | | |
|--|---|--|
| <input checked="" type="checkbox"/> Dati | <input checked="" type="checkbox"/> Tecnologia | <input checked="" type="checkbox"/> Applicazioni |
| <input checked="" type="checkbox"/> Facilities | <input checked="" type="checkbox"/> Risorse umane | |

VALUTAZIONE DELL'IMPATTO:

- | | | |
|--|---|---|
| <input checked="" type="checkbox"/> Riservatezza | <input checked="" type="checkbox"/> Integrità | <input checked="" type="checkbox"/> Disponibilità |
| <input type="checkbox"/> Conformità | <input type="checkbox"/> Efficienza operativa | <input type="checkbox"/> Efficacia operativa |

Lo strumento è inizialmente impostato per fornire voci di impatto afferenti la riservatezza l'integrità e la disponibilità e valorizzabili qualitativamente in scala 1-10.

VALUTAZIONE DELLA PROBABILITA':

La probabilità è di fatto indagata attraverso la valutazione qualitativa delle minacce e delle vulnerabilità sugli asset. Le minacce sono espresse in scala 5 (molto alta-alta-media-bassa-molto bassa), le vulnerabilità in scala 3 (alta-medio-bassa).

VALUTAZIONE DELLE CONTROMISURE:

- | | | |
|--|-------------------------------------|--|
| <input type="checkbox"/> riduzione probabilità | <input type="checkbox"/> preventive | <input type="checkbox"/> disegno della contromisura |
| <input type="checkbox"/> riduzione conseguenze | <input type="checkbox"/> reattive | <input type="checkbox"/> applicazione della contromisura |
| <input type="checkbox"/> evitare il rischio | | |
| <input type="checkbox"/> trasferire il rischio | | |
| <input type="checkbox"/> accettare il rischio | | |

Sono previsti i seguenti stati delle contromisure, che contribuiscono in maniera positiva o negativa nel calcolo dell'abbattimento dal rischio assoluto a quello residuo:

- operativa;
- già coperta;
- coperta con trasferimento del rischio;
- in corso di sviluppo;
- sviluppata;
- sotto esame;
- non implementata per accettazione del rischio;
- attualmente non applicata;
- non applicabile.

Approccio:

La metodologia prevede l'applicazione dell'analisi dei rischi su:

processi risorse di business risorse tecnologiche

L'approccio metodologico può consentire all'analista di focalizzarsi sulle sole risorse tecnologiche, piuttosto che prevedere un ampio ricorso ai dati, le une e gli altri liberamente riferibili come asset appartenenti ad un processo oppure no.

Passi metodologici:

- 1 Individuazione dello scenario di riferimento da analizzare
- 2 Individuazione degli asset pertinenti l'ambito
- 3 Valutazione degli asset e/o dei loro impatti
- 4 Stima dei livelli di minacce e vulnerabilità
- 5 Calcolo del livello di rischio assoluto.
- 6 Scelta delle contromisure con il loro stato di implementazione
- 7 Calcolo del corrispondente livello residuo di rischio

Tool a supporto:

software

La metodologia è istanziata per mezzo del tool omonimo, con architettura web a tre livelli con ampio ricorso a componenti open source.

questionari/ check-list, ecc.

manuali e linee guida

Manuale d'uso per l'utente.

disponibilità training

Liberamente determinabile con l'azienda in funzione anche del grado di preparazione dell'utente finale.

disponibilità aggiornamenti periodici

Sono inviate via mail gli upgrade o le patch. L'utente può segnalare interventi correttivi via web accedendo al portale allestito ad hoc dalla casa produttrice.

possibilità di personalizzazioni

Si, per tutte le tabelle più importanti.

Risultati ottenibili:

Calcolo del rischio assoluto e residuo per asset, gruppi di asset e ottima personalizzazione delle voci di impatto, minacce e contromisure. Molto precisa la funzionalità di export dei dati in excel per la reportistica, che consente ampie libertà di rappresentazione.

Lingua

Italiano

Inglese

Altro _____

Concetti e definizioni chiave:

- ☑ **RISCHIO:** Il rischio è la possibilità di subire perdite o danni derivante dal concretizzarsi di minacce che colpiscono i beni e le risorse costituenti il patrimonio aziendale.
- ☑ **MINACCIA:** Qualunque evento, potenzialmente pericoloso, che, sfruttando una vulnerabilità può arrecare danno.
- ☑ **VULNERABILITA':** Inadeguatezza delle misure di sicurezza esistenti nel sistema di protezione adottato.
- ☑ **DANNO:** Qualunque conseguenza o effetto negativo di qualunque natura (monetaria, ambientale, ecc.).
- ☑ **IMPATTO:** Misura della perdita in seguito al verificarsi di una minaccia.
- ☐ **CONSEGUENZE:** Non utilizzato

Altre definizioni:

TRACCIABILITA' A RITROSO: [*Backward Traceability*] Possibilità, una volta valutato il valore di rischio, di conoscere la percentuale di tale rischio dovuta alle aree di vulnerabilità rilevanti per una data minaccia e da tale informazione poter risalire alle vulnerabilità elementari che hanno causato il rischio in oggetto.

INDICE DI IMPATTO RELATIVO: [*Impact Relative Index – IRI*] Indice di misura del rischio relativo, espresso con la metrica 0 - 100 che rappresenta il rapporto tra il rischio effettivo ed il rischio massimo (0 rischio nullo, protezione ottimale e 100 rischio massimo, nessuna protezione) per una determinata minaccia. Esso esprime anche la mancanza di protezione che si ha per tale minaccia.

Elementi della Metodologia di misurazione dei rischi:

Vengono identificati due tipi di valutazioni sostanzialmente indipendenti di cui è costituito il processo di analisi del rischio.

La prima valutazione è quella relativa al valore esposto al rischio (Rischio Potenziale), in altre parole il valore di rischio che si avrebbe se non vi fosse nessuna protezione in essere, corrispondente al valore di rischio massimo.

La seconda valutazione è quella relativa al livello di protezione, la cui determinazione può essere identificata tramite un confronto ottimale per le conoscenze tecniche attuali, corrispondente al livello di protezione definito.

Dalle valutazioni precedenti si ottiene il livello di rischio effettivo (RLE- Risk Level Estimated) espresso con una metrica da 0 a 10 (metodologia TLQE).

Da tale valore, una volta definita una soglia di accettabilità, è possibile decidere se intervenire e, utilizzando la tracciabilità a ritroso, dove intervenire. Vengono forniti grafici di priorità di intervento in base ai criteri di accettabilità e indicatori per le aree rilevanti per la sicurezza.

La metodologia SQRM (Standard Quantitative RiskWatch Methodology) è conforme agli standard internazionali di valutazione del rischio quantitativo. Dai dati sui beni (Asset) dell'organizzazione, dalla valutazione del livello di protezione fornisce: la conformità ai controlli dell'ISO17799 e al D.lgs 196/03, la vulnerabilità nelle varie aree di rilevanza per la sicurezza, il valore di rischio quantitativo relativo alle minacce possibili per i beni inseriti nel modello, il ROI per l'introduzione delle salvaguardie, le riduzioni di rischio ottenibili con l'introduzione sia di singole minacce che la riduzione cumulativa ottenibile con la progressiva introduzione delle 10 minacce con il maggiore ritorno dell'investimento.

Le varie metodologie di RiskWatch sono state pensate in modo integrato, cioè è possibile iniziare a lavorare con la TLQ QUAL e poi passare alla TLQE e alla SQRM, salvaguardando l'investimento fatto e graduando i tempi e le risorse impiegate e disponibili.

Gli elementi che vengono utilizzati nelle metodologie di RiskWatch per la misurazione del rischio sono:

- conformità e attuazione dei "controlli" relativi al Modello di riferimento di sicurezza basato su standard, normative vigenti e best practices;
- dati sui beni dell'organizzazione, in particolare le informazioni, in forma quantitativa o qualitativa a secondo della metodologia usata;
- indicazioni sulle salvaguardie in essere e, se desiderata l'analisi costi/benefici quantitativa, i prezzi richiesti dai fornitori per le possibili salvaguardie da introdurre.

VALUTAZIONE DELLE RISORSE:

RiskWatch richiede di identificare le informazioni circa le principali categorie di beni e risorse da proteggere. Deve essere effettuata un'identificazione dei beni da proteggere, associandoli ad una "categoria" di appartenenza in funzione dell'entità delle conseguenze economiche, derivanti dal concretarsi di una specifica minaccia contro di essi.

- Beni Critici;
- Beni Finanziari, Controllati, Economici;
- Beni Sensitivi;
- Beni di Supporto.

I dati richiesti sui beni sono meno stringenti come dettaglio a seconda della impostazione metodologica scelta: SQRM, TLQE, TLQ QUAL. Uno strumento di preprocessing sui dati dei beni dell'organizzazione facilita e guida la costruzione del modello quantitativo in SQRM.

- | | | |
|--|---|--|
| <input checked="" type="checkbox"/> Dati | <input checked="" type="checkbox"/> Tecnologia | <input checked="" type="checkbox"/> Applicazioni |
| <input checked="" type="checkbox"/> Facilities | <input checked="" type="checkbox"/> Risorse umane | |
- VALUTAZIONE DELL'IMPATTO:**
- | | | |
|--|---|---|
| <input checked="" type="checkbox"/> Riservatezza | <input checked="" type="checkbox"/> Integrità | <input checked="" type="checkbox"/> Disponibilità |
| <input checked="" type="checkbox"/> Conformità | <input type="checkbox"/> Efficienza operativa | <input checked="" type="checkbox"/> Efficacia operativa |

VALUTAZIONE DELLA PROBABILITA':

La quantificazione del rischio è in grado di tener conto sia dell'impatto, conseguente alle carenze rilevate ("severità"), che della probabilità di accadimento di tali conseguenze ("frequenza").

VALUTAZIONE DELLE CONTROMISURE:

RiskWatch esegue un'analisi costi/benefici che permetterà di rendere note le contromisure più efficaci, in termini di riduzione di rischio, ed anche quelle economicamente più convenienti.

Segue l'analisi di riduzione del rischio, in cui, attraverso un confronto diretto tra la situazione esistente "di rischio" e quella ideale operata dal sistema RiskWatch, sulla base di una simulazione dell'impiego delle contromisure indicate, è evidenziata la riduzione delle diverse categorie di rischio distinte per tipologia di perdita.

- | | | |
|---|--|--|
| <input checked="" type="checkbox"/> riduzione probabilità | <input checked="" type="checkbox"/> preventive | <input checked="" type="checkbox"/> disegno della contromisura |
| | <input checked="" type="checkbox"/> reattive | <input type="checkbox"/> applicazione della contromisura |
| <input checked="" type="checkbox"/> riduzione conseguenze | | |
| <input checked="" type="checkbox"/> evitare il rischio | | |
| <input checked="" type="checkbox"/> trasferire il rischio | | |
| <input checked="" type="checkbox"/> accettare il rischio | | |

Approccio:

La metodologia prevede l'applicazione dell'analisi dei rischi su:

- | | | |
|--|---|--|
| <input checked="" type="checkbox"/> processi | <input checked="" type="checkbox"/> risorse di business | <input checked="" type="checkbox"/> risorse tecnologiche |
|--|---|--|

Passi metodologici:

In primo luogo, dovranno essere fornite al sistema RiskWatch le informazioni circa le principali categorie di beni e risorse da proteggere.

E' opportuno, infatti, che per un'efficace protezione delle risorse dell'ambito sotto analisi, ognuna sia opportunamente identificata, qualificata e valutata, in una o più categorie separate indicate: (vedi "Valutazione delle risorse")

L'individuazione e la valorizzazione economica dei beni dell'azienda, consente al sistema RiskWatch di individuare, da subito, le risorse che necessitano di un maggior livello protettivo in funzione degli aspetti di disponibilità, integrità e confidenzialità che le stesse presentano.

A questo punto, il sistema RiskWatch procede all'inserimento delle varie tipologie di beni "da proteggere" in un'apposita Tabella Sommario Beni che conterrà informazioni dettagliate riguardo ogni bene giudicato tale.

Viene indetta, in seguito, una riunione del gruppo di lavoro che ha come oggetto l'identificazione e la selezione delle minacce da prendere in considerazione per lo specifico ambito sotto analisi, scartando quelle che non possono interessare l'area in esame

Segue, la fase fondamentale e più critica dell'intero processo di Risk Analysis, relativa all'analisi ed alla valutazione delle vulnerabilità.

L'acquisizione delle informazioni, da parte del sistema RiskWatch, sulle vulnerabilità presenti nel sistema di protezione dell'ambito sotto analisi, sono acquisite mediante l'introduzione delle risposte ad appositi questionari (check list) proposti dal sistema ai diretti interessati. Nelle domande si richiede un giudizio di conformità o meno ai controlli delle vulnerabilità analizzate dallo standard di riferimento contenuto in RiskWatch. Tale indicazione di conformità è data servendosi di una scala di riferimento, sotto riportata. Essa costituisce una sorta di giudizio complessivo capace di poter esprimere, con un numero che va da 0 a 100 (o nella forma da 0 a 10), la percentuale di non conformità delle vulnerabilità analizzate, tra il valore che esse presentano nel sistema di sicurezza analizzato e quello ideale di riferimento conforme alle normative contenuto in RiskWatch.

Tramite un'apposita elaborazione delle risposte ai questionari, segue l'indicazione, da parte del sistema RiskWatch, delle vulnerabilità, corredate, anche, da un insieme di grafici. Tali grafici forniscono indicatori di vulnerabilità (in percentuale) e di conformità agli standard di riferimento, sia totali sia per ogni singola categoria di vulnerabilità considerata.

Successivamente, il sistema RiskWatch, elaborando le informazioni ottenute sui beni da proteggere ed utilizzando, anche, i dati sulle vulnerabilità riscontrate, sarà in grado di offrire una valutazione quantitativa dei rischi presenti, espressa per ciascuna minaccia in percentuale di Perdita Annuale Attesa (Annual.Loss.Expected - ALE.), connessi alle rispettive vulnerabilità (metodologia SQRM).

I rischi saranno distinti per tipologia di perdite cui può dar luogo una specifica minaccia (classificabili in : Perdite Dirette; Perdite Indirette; Ritardi o Mancanza di servizio; Diffusione di informazioni sensibili; Alterazioni di programmi e di database; Perdite Immateriali), in modo tale da valutare, anche, l'impatto economico-finanziario ad essi conseguente. Il sistema RiskWatch permetterà, peraltro, di identificare, per ognuna di esse, le principali categorie di minacce che hanno contribuito a determinare le perdite.

Giunti a questo punto, il sistema RiskWatch possiede gli elementi per operare, in base alle informazioni ottenute sulle variabili indicate, l'analisi e la valutazione delle relative salvaguardie. Esso eseguirà un'analisi costi/benefici che permetterà di rendere note le contromisure più efficaci, in termini di riduzione di rischio, ed anche quelle economicamente più convenienti.

Segue, l'analisi di riduzione del rischio, in cui, attraverso un confronto diretto tra la situazione esistente "di rischiosità" e quella ideale operata dal sistema RiskWatch, sulla base di una simulazione dell'impiego delle contromisure indicate, viene evidenziata la riduzione delle diverse categorie di rischio distinte per tipologia di perdita.

Tool a supporto:

software

Lo strumento RiskWatch usato nell'analisi e tecnicamente realizzato attraverso un "pacchetto" di software applicativo che utilizza come piattaforma hardware un P.C. di fascia medio/alta, può definirsi una vera e propria metodologia di "Risk Management System".

questionari/check-list, ecc.

manuali e linee guida

Elettronici in pdf su CD e come parte dell'aggiornamento e manutenzione

disponibilità training

Nella versione internazionale fruibile dal sito www.riskwatch.com

disponibilità aggiornamenti periodici

annuali, aggiornamenti già compresi nel costo di acquisto per il primo anno

Lo standard SQRM viene aggiornato conformemente alle indicazioni metodologiche del SAI (Supreme Auditor Institutions), secondo esigenze (non periodicamente). La versione disponibile è stata aggiornata nel 2004.

La versione italiana viene aggiornata annualmente e in alcuni casi, per specifiche esigenze, anche ad intervalli più brevi.

possibilità di personalizzazioni

RiskWatch consente di personalizzare i questionari modificando o aggiungendo domande relative a nuovi "controlli" di sicurezza. Inoltre è possibile scegliere le minacce, le tipologie di impatto da valutare, le categorie di beni e le salvaguardie che si vuole facciano parte del modello di sicurezza utilizzato. Si possono ad esempio preparare dei modelli standard da utilizzare per le analisi da effettuare nella propria organizzazione.

E' possibile anche ampliare la lista delle minacce con tipologie proprie specifiche valutate inserendo nella base di conoscenza dello strumento gli elementi necessari alla valutazione, i quali dipendono anche dalla metodologia scelta tra quelle disponibili.

Risultati ottenibili:

La metodologia automatizzata legata allo strumento RiskWatch porta con sé una serie di vantaggi (oggettività dei risultati, strumento di supporto all'auditors, rilevazione di informazioni da fonti multiple, possibilità di ottenere raccomandazioni su possibili interventi, personalizzazione dello strumento, standardizzazione dell'analisi), sia in fase di progettazione del sistema di sicurezza, poiché permette la simulazione dello scenario di rischio, sia prima dello svolgimento della fase di implementazione, sia successivamente nella fase operativa. In quest'ultima fase, utilizzato ad intervalli regolari, consente infatti, agli esperti responsabili dell'azienda esaminata, la realizzazione di specifiche operazioni di valutazione e monitoraggio sul livello di rischio esistente ed il conseguente costante adeguamento delle misure di sicurezza ai cambiamenti del settore Edp sottoposto a controllo.

Lingua

Italiano

Inglese (SQRM)

Altro _____

SARA - Simple to Apply Risk Analysis

Informazioni fornite da Luca Corciulo di PricewaterhouseCoopers

Ambito di applicazione:

SARA è una metodologia associata a SPRINT (vedere relativa scheda) ed orientata a sistemi “*altamente critici*”. In sostanza, utilizza i risultati conseguiti in SPRINT, nella fase di “Business Impact Assessment”, per poi consentire di effettuare un Risk Assessment sui *sistemi critici* identificando più nei dettagli l’esatta natura dei rischi e calcolandone più accuratamente il livello in base alla quale si determinano le contromisure (security controls).

Standard di riferimento

E’ una metodologia standard definita dall’Information Security Forum.

Approccio alla misurazione dei rischi:

- qualitativo quantitativo semi-quantitativo
- misurazione sia del rischio potenziale o intrinseco (cioè a prescindere dalle contromisure) sia del rischio effettivo o residuo (cioè tenendo conto delle contromisure poste in essere)
- misurazione del rischio effettivo o residuo (cioè il rischio relativo alla situazione in essere, comprese le contromisure implementate)
- misurazione del rischio potenziale o intrinseco (cioè a prescindere dalle contromisure adottate)

Concetti e definizioni chiave:

- RISCHIO:** L’eventualità di ottenere perdite o danneggiamenti a seguito di problemi legati alla sicurezza informatica (security breach).
- Il rischio associato a un sistema informativo (information system) è una funzione del grado di possibile perdita o danneggiamento che si potrebbe ottenere a seguito di un problema di sicurezza informatica (i.e. business impact) e della probabilità che questo problema si manifesti.
- Il rischio inerente associato ad un sistema informativo tiene conto della probabilità che il problema legato alla sicurezza venga sfruttato e che si trasformi in minaccia concreta assumendo che non ci siano controlli di nessun tipo su quel determinato problema.
- Il rischio residuo è il rischio che rimane una volta che il controllo, volto a risolvere quel determinato problema, è stato applicato.
- Nella metodologia SARA, come del resto anche nella metodologia SPRINT, il “business risk” associato ad un sistema informativo è determinato sulla base del danno che un problema di sicurezza potrebbe causare. Un sistema ad alto rischio è un sistema in cui un problema di sicurezza potrebbe causare un elevato danno.
- Il rischio può essere ridotto grazie all’applicazione di appropriati controlli ma rimane dove i controlli sono deboli o non applicati (controls weaknesses). Di conseguenza, il business risk è più elevato nei sistemi classificati ad alto rischio che presentano debolezze nei controlli.

- ☑ **MINACCIA:** Il mezzo grazie al quale può aver luogo un incidente informatico (security incident), i.e. le minacce si materializzano in forma di incidenti informatici (security incidents).
- ☑ **VULNERABILITA':** La probabilità che si verifichi un problema di sicurezza informatica considerando la probabilità inerente che la minaccia correlata (threat) si manifesti; le condizioni ambientali particolari (es. sala macchine situata in locali facilmente allagabili); i punti di forza e le debolezze dei controlli di una organizzazione (es. accesso a centri di calcolo alternativi situati in locali "safe").
- ☑ **DANNO:** Il concetto di danno è collegabile ai seguenti concetti definiti dalla metodologia:
- conseguenza per il business;
 - falla nella sicurezza.
- Vedi definizioni nel seguito.
- ☑ **IMPATTO:** [*Business impact*] L'entità del danno sofferto dal business a seguito di un incidente informatico (valutazione della conseguenza sul business a seguito di una falla nella sicurezza).
- ☑ **CONSEGUENZE:** [*Business consequence*] un effetto negativo sul business derivante da un problema di sicurezza informatica (es. una frode andata a buon fine);

Altre definizioni:

APPLICAZIONE: [*Application*] Il termine applicazione è sinonimo di sistema informativo (information system).

SISTEMA INFORMATIVO: [*Information System*] Un insieme di computer, reti e componenti ausiliari, software, dati, documenti e procedure, utili a identificare e processare informazioni e a fornire risultati in grado di supportare le attività di una organizzazione.

FALLA NELLA SICUREZZA: [*Security Breach*] Una perdita di confidenzialità, integrità, e/o disponibilità di informazioni processate da un sistema informativo o appartenenti al sistema informativo stesso, derivante da un incidente informatico, es. un data center fuori servizio per 10 ore, data files corrotti, ecc..

CONTROLLO: Una politica, metodologia, procedura, dispositivo o meccanismo programmato atto a proteggere la confidenzialità, integrità o disponibilità del sistema informativo, o delle informazioni processate dallo stesso, da una o più minacce (threats).

I controlli possono essere progettati per:

- prevenire l'insorgere di problemi di sicurezza informatica;
- identificare problemi di sicurezza informatica quando questi si verificano;
- cercare di minimizzare l'effetto delle minacce quando queste si manifestano.

Lo scopo dell'information security è quello di definire un insieme di controlli operazionali in grado di mantenere il rischio all'interno di limiti accettabili

INCIDENTE: [*Security Incident*] Un evento che potrebbe compromettere la confidenzialità, integrità e/o la disponibilità di un sistema informativo o delle informazioni processate dallo stesso (es. malfunzionamento o sovraccarico del sistema, errori nell'inserimento di dati, attacco da parte di virus, attacchi informatici o disastri naturali).

Elementi della Metodologia di misurazione dei rischi:

Gli elementi, fattori che vengono utilizzati per la misurazione del rischio sono gli stessi utilizzati per la metodologia SPRINT .

A tal proposito si rimanda alla scheda relativa a quest'ultima metodologia, in quanto SARA viene eventualmente utilizzata in base ai risultati raggiunti da SPRINT (nella fase iniziale di Business Impact Assessment).

VALUTAZIONE DELLE RISORSE:

- | | | |
|-------------------------------------|--|--|
| <input type="checkbox"/> Dati | <input type="checkbox"/> Tecnologia | <input checked="" type="checkbox"/> Applicazioni |
| <input type="checkbox"/> Facilities | <input type="checkbox"/> Risorse umane | |

VALUTAZIONE DELL'IMPATTO:

Viene utilizzata la seguente scala di valori qualitativi:

- A – Sopravvivenza del Business a rischio;
- B – Danno Serio;
- C – Danno Significativo;
- D – Impatto Minore;
- E – Trascurabile.

- | | | |
|--|---|---|
| <input checked="" type="checkbox"/> Riservatezza | <input checked="" type="checkbox"/> Integrità | <input checked="" type="checkbox"/> Disponibilità |
| <input type="checkbox"/> Conformità | <input type="checkbox"/> Efficienza operativa | <input type="checkbox"/> Efficacia operativa |

VALUTAZIONE DELLA PROBABILITA':

Viene utilizzata la seguente scala di valori qualitativi:

- A – Probabile;
- B – Altamente Possibile;
- C – Possibile;
- D – Non verosimile;
- E – Impossibile.

VALUTAZIONE DELLE CONTROMISURE:

- | | | |
|---|--|--|
| <input checked="" type="checkbox"/> riduzione probabilità | <input checked="" type="checkbox"/> preventive | <input type="checkbox"/> disegno della contromisura |
| <input checked="" type="checkbox"/> riduzione conseguenze | <input checked="" type="checkbox"/> reattive | <input type="checkbox"/> applicazione della contromisura |
| <input type="checkbox"/> evitare il rischio | | |
| <input type="checkbox"/> trasferire il rischio | | |
| <input type="checkbox"/> accettare il rischio | | |

Approccio:

La metodologia prevede l'applicazione dell'analisi dei rischi su:

- | | | |
|--|---|--|
| <input checked="" type="checkbox"/> processi | <input checked="" type="checkbox"/> risorse di business | <input checked="" type="checkbox"/> risorse tecnologiche |
|--|---|--|

L'analisi dei rischi viene applicata sui processi di Business, per la fase di "Business Impact Assessment"- BIA, secondo la metodologia SPRINT (vedere relativa scheda); successivamente, sulla base dell'individuazione delle applicazioni che supportano i processi aziendali analizzati nella fase di BIA, l'analisi dei rischi, nelle due fasi successive si applica su risorse di business e risorse tecnologiche (vedere concetto di "Information resource") definite "critiche".

Passi metodologici:

Vedere scheda della metodologia SPRINT, in quanto SARA viene adottata eventualmente in base ai risultati conseguiti con la prima metodologia (nella fase iniziale di Business Impact Assessment); SARA presenta quindi gli stessi passi metodologici di SPRINT previsti per le altre due fasi di "Threats, Vulnerabilities and Control Assessment" e di "Action Plan"

Tool a supporto:

software

questionari/ check-list, ecc.

Forms di Business Impact Assessment utilizzati nella metodologia di SPRINT e forms per “Threat, Vulnerability and Controls Assessment” e “definizione di un Action Plan”.

manuali e linee guida

“SARA Methodology - User guide” costituisce il manuale descrittivo della metodologia e riporta linee guida per la conduzione dell’attività di risk analysis.

disponibilità training

I membri e gli agenti di ISF erogano corsi di formazione ed organizzare seminari /convegni sul tema

disponibilità aggiornamenti periodici

ISF (Information Security Forum) predispone aggiornamenti della metodologia , mettendoli a disposizione dei suoi membri.

possibilità di personalizzazioni

Possono essere predisposte personalizzazioni della metodologia in base a specifiche esigenze.

Risultati ottenibili:

Vedere sezione “Passi metodologici”

Lingua

Italiano

Inglese

Altro _____

SPRINT Simplified Process for Risk Identification*Informazioni fornite da Luca Corciulo di PricewaterhouseCoopers***Ambito di applicazione:**

Si tratta di una metodologia relativamente veloce e facile da utilizzare per la valutazione degli impatti sul business e per l'analisi dei rischi informatici relativi a sistemi informativi (information systems) classificati come "importanti, ma non critici".

Standard di riferimento

E' una metodologia standard definita dall'Information Security Forum.

Approccio alla misurazione dei rischi:

- qualitativo quantitativo semi-quantitativo
- misurazione sia del rischio potenziale o intrinseco (cioè a prescindere dalle contromisure) sia del rischio effettivo o residuo (cioè tenendo conto delle contromisure poste in essere)
- misurazione del rischio effettivo o residuo (cioè il rischio relativo alla situazione in essere, comprese le contromisure implementate)
- misurazione del rischio potenziale o intrinseco (cioè a prescindere dalle contromisure adottate)

Concetti e definizioni chiave:

- RISCHIO:** L'eventualità di ottenere perdite o danneggiamenti a seguito di problemi legati alla sicurezza informatica (security breach).
- Il rischio associato a un sistema informativo è una funzione del grado di possibile perdita o danneggiamento che si potrebbe ottenere a seguito di un problema di sicurezza informatica (i.e. business impact) e della probabilità che questo problema si manifesti.
- Il rischio inerente associato ad un sistema informativo tiene conto della probabilità che il problema legato alla sicurezza venga sfruttato e che si trasformi in minaccia concreta assumendo che non ci siano controlli di nessun tipo su quel determinato problema.
- Il rischio residuo è il rischio che rimane una volta che il controllo, volto a risolvere quel determinato problema, è stato applicato.
- Nella metodologia SPRINT, il rischio per il business (business risk) associato ad un sistema informativo è determinato sulla base del danno che un problema di sicurezza potrebbe causare. Un sistema ad alto rischio è un sistema in cui un problema di sicurezza potrebbe causare un elevato danno.
- Il rischio può essere ridotto grazie all'applicazione di appropriati controlli ma rimane dove i controlli sono deboli o non applicati (controls weaknesses). Di conseguenza, il business risk è più elevato nei sistemi classificati ad alto rischio che presentano debolezze nei controlli.

- ☑ **MINACCIA:** [*Threat*] Il mezzo grazie al quale può aver luogo un incidente (security incident; le minacce si materializzano in forma di incidenti (security incidents).
- ☑ **VULNERABILITA':** La probabilità che si verifichi un problema di sicurezza informatica considerando la probabilità inerente che la minaccia correlata (threat) si manifesti; le condizioni ambientali particolari (es. sala macchine situata in locali facilmente allagabili); i punti di forza e le debolezze dei controlli di una organizzazione (es. accesso a centri di calcolo alternativi situati in locali "safe").
- ☑ **DANNO:** Il concetto di danno è collegabile ai seguenti concetti definiti dalla metodologia:
 - conseguenza per il business;
 - falla nella sicurezza.
 Vedi definizioni nel seguito.
- ☑ **IMPATTO:** [*Business impact*] L'entità del danno sofferto dal business a seguito di un incidente informatico (valutazione della conseguenza sul business a seguito di una falla nella sicurezza).
- ☑ **CONSEGUENZE:** [*Business consequence*] un effetto negativo sul business derivante da un problema di sicurezza informatica (es. una frode andata a buon fine);

Altre definizioni:

APPLICAZIONE: [*Application*] Il termine applicazione è sinonimo di sistema informativo (information system).

SISTEMA INFORMATIVO: [*Information System*] Un insieme di computer, reti e componenti ausiliari, software, dati, documenti e procedure, utili a identificare e processare informazioni e a fornire risultati in grado di supportare le attività di una organizzazione.

FALLA NELLA SICUREZZA: [*Security Breach*] Una perdita di confidenzialità, integrità e/o disponibilità di informazioni processate da un sistema informativo o appartenenti al sistema informativo stesso, derivante da un incidente informatico, es. un data center fuori servizio per 10 ore, data files corrotti, ecc..

CONTROLLO: Una politica, metodologia, procedura, dispositivo o meccanismo programmato atto a proteggere la confidenzialità, integrità o disponibilità del sistema informativo, o delle informazioni processate dallo stesso, da una o più minacce (threats).

I controlli possono essere progettati per:

- prevenire l'insorgere di problemi di sicurezza informatica;
- identificare problemi di sicurezza informatica quando questi si verificano;
- cercare di minimizzare l'effetto delle minacce quando queste si manifestano.

Lo scopo dell'information security è quello di definire un insieme di controlli operazionali in grado di mantenere il rischio all'interno di limiti accettabili

INCIDENTE: [*Security Incident*] Un evento che potrebbe compromettere la confidenzialità, integrità e/o la disponibilità di un sistema informativo o delle informazioni processate dallo stesso (es. malfunzionamento o sovraccarico del sistema, errori nell'inserimento di dati, attacco da parte di virus, attacchi informatici o disastri naturali).

Elementi della Metodologia di misurazione dei rischi:

Gli elementi, fattori che vengono utilizzati per la misurazione del rischio sono:

- conseguenze sul business derivanti dalla perdita di riservatezza, integrità e disponibilità delle informazioni correlate ai processi, valutate su una scala di cinque valori, consentono di classificare i sistemi e le applicazioni oggetto di analisi su una scala di valori rappresentanti il diverso livello di criticità (“regolari”, “importanti ma non critici”, “critici”);
- fattori di minaccia e di vulnerabilità (Threat and Vulnerability Factors), valutati su una scala di cinque valori, con l'obiettivo di:
 - stimare le vulnerabilità e le minacce chiave del sistema in relazione a confidenzialità (riservatezza) dell'informazione, integrità dell'informazione, disponibilità dell'informazione;
 - identificare i controlli richiesti per mantenere il rischio entro livelli accettabili.

VALUTAZIONE DELLE RISORSE:

- | | | |
|-------------------------------------|--|--|
| <input type="checkbox"/> Dati | <input type="checkbox"/> Tecnologia | <input checked="" type="checkbox"/> Applicazioni |
| <input type="checkbox"/> Facilities | <input type="checkbox"/> Risorse umane | |

VALUTAZIONE DELL'IMPATTO:

Viene utilizzata la seguente scala di valori qualitativi:

- A – Sopravvivenza del Business a rischio;
- B – Danno Serio;
- C – Danno Significativo;
- D – Impatto Minore;
- E – Trascurabile.

- | | | |
|--|---|---|
| <input checked="" type="checkbox"/> Riservatezza | <input checked="" type="checkbox"/> Integrità | <input checked="" type="checkbox"/> Disponibilità |
| <input type="checkbox"/> Conformità | <input type="checkbox"/> Efficienza operativa | <input type="checkbox"/> Efficacia operativa |

VALUTAZIONE DELLA PROBABILITA':

Viene utilizzata la seguente scala di valori qualitativi:

- A – Probabile;
- B – Altamente Possibile;
- C – Possibile;
- D – Non verosimile;
- E – Impossibile.

VALUTAZIONE DELLE CONTROMISURE:

- | | | |
|---|--|--|
| <input checked="" type="checkbox"/> riduzione probabilità | <input checked="" type="checkbox"/> preventive | <input type="checkbox"/> disegno della contromisura |
| <input checked="" type="checkbox"/> riduzione conseguenze | <input checked="" type="checkbox"/> reattive | <input type="checkbox"/> applicazione della contromisura |
| <input type="checkbox"/> evitare il rischio | | |
| <input type="checkbox"/> trasferire il rischio | | |
| <input type="checkbox"/> accettare il rischio | | |

Approccio:

La metodologia prevede l'applicazione dell'analisi dei rischi su:

- | | | |
|--|---|--|
| <input checked="" type="checkbox"/> processi | <input checked="" type="checkbox"/> risorse di business | <input checked="" type="checkbox"/> risorse tecnologiche |
|--|---|--|

L'analisi dei rischi viene applicata sui processi di Business, per la fase di BIA; successivamente, sulla base dell'individuazione delle applicazioni che supportano i processi aziendali analizzati nella fase di BIA, l'analisi dei rischi si applica su risorse di business e risorse tecnologiche (vedere concetto di "Fonte di informazione" (Information resource), nelle due ultime fasi di "Threat, Vulnerability and Controls Assessment" e di "definizione dell'Action Plan",

Passi metodologici:

1 Valutazione dell'impatto sul business (BIA) & Classificazione Generale (*Overall classification*):

Consente di calcolare le conseguenze sul business derivanti dalla perdita di riservatezza, integrità e disponibilità delle informazioni correlate ai processi, utilizzando la scala di valori qualitativi del business impact rating.

In base ai risultati conseguiti dalla compilazione degli appositi questionari (3 form di BIA, 1 per la riservatezza, 1 per l'integrità e 1 per la disponibilità), si classificano i sistemi e le applicazioni oggetto di analisi su una scala di valori rappresentanti il diverso livello di criticità ("regolari", "importanti ma non critici", "critici").

Termina il processo di SPRINT, nel caso di sistema "regolare", ossia non critico (livello di rischio basso); in tale caso si ritiene sufficiente controllare solamente l'effettiva presenza dei controlli di base necessari a mantenere l'ottimale livello di protezione del sistema;

Si procede con le restanti fasi della metodologia SPRINT, nel caso di sistema ritenuto "importante ma non critico" (livello di rischio medio);

Si continua con l'approccio previsto da SARA (vedere relativa scheda descrittiva), metodologia complementare a SPRINT, nel caso di sistema "critico" (livello di rischio alto), in quanto in tal caso necessita un approccio più analitico condotto da personale specializzato.

2 Valutazione di Minacce, Vulnerabilità e Controlli:

Prevede, utilizzando il relativo questionario, di:

- valutare e correlare minacce e vulnerabilità, in relazione ai parametri della sicurezza (riservatezza, integrità e disponibilità), sulla base della scala di Vulnerability rating;
- calcolare il livello di esposizione ai rischi;
- identificare i controlli (requisiti di sicurezza) necessari per contrastare i rischi calcolati.

3 Piano d'azione:

Consente di definire un piano d'interventi per l'implementazione dei controlli individuati nella fase precedente.

Tool a supporto:

- software
 questionari/ check-list, ecc.

Business Impact Assessment form (Form BIA – 4 pagine), che include:

- sommario (1 pagina);
- sezione relativa a Riservatezza (1 pagina);
- sezione relativa a Integrità (1 pagina);
- sezione relativa a Disponibilità (1 pagina).

Threats, Vulnerabilities And Controls Assessment form (Form TVCA – 8 pagine), che copre le seguenti aree:

- riservatezza (3 pagine);
- integrità (3 pagine);
- disponibilità (2 pagine).

Action Plan form (Form AP – 1 pagina)

- manuali e linee guida

“Sprint Methodology - User guide” costituisce il manuale descrittivo della metodologia e riporta linee guida per la conduzione dell’attività di risk analysis.

- disponibilità training

I membri e gli agenti di ISF erogano corsi di formazione ed organizzare seminari /convegni sul tema

- disponibilità aggiornamenti periodici

ISF (Information Security Forum) predisporre aggiornamenti della metodologia, mettendoli a disposizione dei suoi membri.

- possibilità di personalizzazioni

E’ possibile predisporre personalizzazioni della metodologia in base a specifiche esigenze.

Risultati ottenibili:

- Registrare il risultato generale della revisione (review).
- Definire un action plan per i controlli, progettato per mantenere il rischio di business all’interno di limiti accettabili:
 - priorità di intervento, in base alla combinazione dei due suddetti valori;
 - controlli richiesti in base ai livelli di rischi individuati;
 - assegnazione delle responsabilità nell’implementazione delle misure individuate richieste
 - data o scadenza per l’implementazione delle misure individuate.

Lingua

- Italiano Inglese Altro _____

SSM - Scalable Security Model

Informazioni fornite da Alberto Piamonte di Wise Map (Gruppo Adfor S.p.A.)

<p><u>Ambito di applicazione:</u></p> <ul style="list-style-type: none"> • Sicurezza informatica in sistemi complessi ed in evoluzione • Sicurezza e gestione del rischio in generale • Validazione sistematica di sistemi di Continuità Operativa (Business Continuity Plan – BCP)
<p><u>Standard di riferimento</u></p> <p>Attualmente sono disponibili schemi di controllo per:</p> <ul style="list-style-type: none"> • BS7799; • BSI (Bundesamt fuer Sicherheit und Informationstechnik); • Dlgs 196/03 (All. B Misure Minime di Sicurezza). <p>Sono in fase di completamento o allo studio schemi per:</p> <ul style="list-style-type: none"> • Dlgs 626/94; • CobiT; • Basilea II
<p><u>Approccio alla misurazione dei rischi:</u></p> <p><input checked="" type="checkbox"/> qualitativo <input checked="" type="checkbox"/> quantitativo <input type="checkbox"/> semi-quantitativo</p> <p><input checked="" type="checkbox"/> misurazione sia del rischio potenziale o intrinseco (cioè a prescindere dalle contromisure) sia del rischio effettivo o residuo (cioè tenendo conto delle contromisure poste in essere)</p> <p><input type="checkbox"/> misurazione del rischio effettivo o residuo (cioè il rischio relativo alla situazione in essere, comprese le contromisure implementate)</p> <p><input type="checkbox"/> misurazione del rischio potenziale o intrinseco (cioè a prescindere dalle contromisure adottate)</p>
<p><u>Concetti e definizioni chiave:</u></p> <p><input checked="" type="checkbox"/> RISCHIO: Per rischio si intende la misura dell'effetto (impatto) su un processo Aziendale considerando :</p> <ul style="list-style-type: none"> • La probabilità che una minaccia (threat-source) sfrutti (accidentalmente o intenzionalmente) una particolare vulnerabilità; • l'effetto del conseguente evento. <p>Il rischio può riguardare aspetti di riservatezza, integrità, disponibilità (breve, media, lungo termine) , conformità, efficienza ed efficacia.</p> <p>L'unità di misura di un'analisi quantitativa dei rischi è il prodotto della probabilità di accadimento (frequenza) per il danno potenziale, ad esempio €/anno potenziali.</p>

- MINACCIA:** La possibilità per una fonte di minacce di venir applicata ad una determinata vulnerabilità.
La fonte della minaccia è costituita (1) dall'intento o metodo mirato ad un utilizzo intenzionale della vulnerabilità o (2) una situazione che trasformi accidentalmente la vulnerabilità in evento dannoso.
- VULNERABILITA':** Un difetto o un punto di debolezza in procedure, nel progetto, nella realizzazione (implementazione) o nei controlli interni che utilizzata (accidentalmente od intenzionalmente) comporti conseguenze dannose o comunque negative.
- DANNO:** La conseguenza negativa di un evento accidentale o intenzionale.
- IMPATTO:** È la valutazione/misura delle conseguenze dell'evento negativo a livello di processo aziendale. Il riferimento non è la risorsa od il complesso di risorse dove si è verificato l'evento quanto i danni ad esso conseguenti.
- CONSEGUENZE:** Le aree impattate in termini di riservatezza, integrità, disponibilità (breve, media, lungo termine), conformità, efficienza ed efficacia.

Altre definizioni:

SOGLIA DI SENSIBILITA' E DEL DOLORE: Rispettivamente, danno minimo percepito e danno massimo considerato (catastrofe)

PROBABILITA' DI ACCADIMENTO MINIMA E MASSIMA:
Frequenze associate convenzionalmente ai concetti di mai e di sempre

Elementi della Metodologia di misurazione dei rischi:

I rischi e la loro riduzione vengono misurati in perdite potenziali di €/anno.

VALUTAZIONE DELLE RISORSE:

- | | | |
|--|---|--|
| <input checked="" type="checkbox"/> Dati | <input checked="" type="checkbox"/> Tecnologia | <input checked="" type="checkbox"/> Applicazioni |
| <input checked="" type="checkbox"/> Facilities | <input checked="" type="checkbox"/> Risorse umane | |

È possibile definire nuovi classi di risorse

VALUTAZIONE DELL'IMPATTO:

Valore (logaritmico) della perdita associabile ad un incidente relativo ad uno dei rischi considerato (riservatezza, integrità, ecc). La base viene scelta in modo che alla soglia minima percepita corrisponda il valore 0 e alla "soglia del dolore" corrisponda il rischio massimo.

- | | | |
|--|--|---|
| <input checked="" type="checkbox"/> Riservatezza | <input checked="" type="checkbox"/> Integrità | <input checked="" type="checkbox"/> Disponibilità |
| <input checked="" type="checkbox"/> Conformità | <input checked="" type="checkbox"/> Efficienza operativa | <input checked="" type="checkbox"/> Efficacia operativa |

VALUTAZIONE DELLA PROBABILITA':

Logaritmo della frequenza dell'evento. La base viene definita in modo tale che la probabilità la corrispondente alla percezione di "mai" abbia valore 0. e quella corrispondente alla percezione di "sempre" abbia il valore massimo

VALUTAZIONE DELLE CONTROMISURE:

- | | | |
|---|--|---|
| <input checked="" type="checkbox"/> riduzione probabilità | <input checked="" type="checkbox"/> preventive | <input type="checkbox"/> disegno della contromisura |
| <input checked="" type="checkbox"/> riduzione conseguenze | <input checked="" type="checkbox"/> reattive | <input checked="" type="checkbox"/> applicazione della contromisura |
| <input checked="" type="checkbox"/> evitare il rischio | | |
| <input checked="" type="checkbox"/> trasferire il rischio | | |
| <input checked="" type="checkbox"/> accettare il rischio | | |

L'implementazione di ogni contromisura (o gruppo di) può venir associata ad un progetto di costo determinato per il calcolo del Return On Security Investment.

ALTRI ELEMENTI:

- Aggiornamento dinamico del livello di implementazione (o del venir meno) delle contromisure per un monitoraggio continuo dei livelli di rischio cui sono soggetti i processi aziendali.
- È possibile in tempi successivi aumentare il livello di dettaglio di analisi.

Approccio:

La metodologia prevede l'applicazione dell'analisi dei rischi su:

- | | | |
|--|---|--|
| <input checked="" type="checkbox"/> processi | <input checked="" type="checkbox"/> risorse di business | <input checked="" type="checkbox"/> risorse tecnologiche |
|--|---|--|

Passi metodologici:

- 1 Definizione del Modello di Business (Servizi/Processi/...)
Viene costruito in modello dei processi/servizi di business erogati per poter condurre sistematicamente e con il dettaglio desiderato (scalabilità) una valutazione quantitativa dell'impatto di eventi negativi.
- 2 Valutazione dell'impatto (Business Impact Analysis o BIA), estesa oltre che agli aspetti di non disponibilità, anche a quelli di violazione di riservatezza, integrità, ecc. che si intendono misurare/monitorare, su ogni elemento del modello di business da parte dei responsabili (Business Owners).
- 3 Viene costruito il modello delle risorse utilizzate, indicandone i gruppi omogenei e dipendenze.
Viene costruito un modello e con il dettaglio desiderato (scalabilità) delle risorse utilizzate nell'erogazione dei servizi (applicazione -> elaboratore -> Sala Server -> Edificio.....).
Le risorse vengono associate ai processi che le utilizzano.

- 4 Per ogni risorsa vengono valutate minacce incombenti, contromisure adottate o da adottare (pianificare).
Per ogni risorsa (o gruppo di risorse) vengono associate minacce/probabilità di accadimento/effetto delle contromisure (mantenendo distinto il calcolo dell'efficacia della contromisura nella riduzione della probabilità di accadimento e la riduzione delle conseguenze).
- 5 Vengono calcolati i rischi (per ogni aspetto considerato), riferendoli a processi di business considerati.
E' possibile ottenere *report* di insieme e *reports* interattivi (*Drill down*) per risalire alle cause di determinate situazioni di rischio.

Tool a supporto:

software

Piattaforma Microsoft – Interfaccia tipo Explorer

Il *tool* supporta tutti i passi della metodologia descritta tramite un'interfaccia intuitiva per:

- definire la struttura (ad albero) dei processi e delle loro caratteristiche
- definire la struttura (ad albero) delle risorse e delle loro caratteristiche
- associare Processi-Risorse e Risorse-Risorse

questionari/ *check-list*, ecc.

Possibilità di produrre questionari personalizzati (utilizzabili soprattutto in fase di manutenzione/aggiornamento)

manuali e linee guida

disponibilità training

disponibilità aggiornamenti periodici

possibilità di personalizzazioni

Risultati ottenibili:

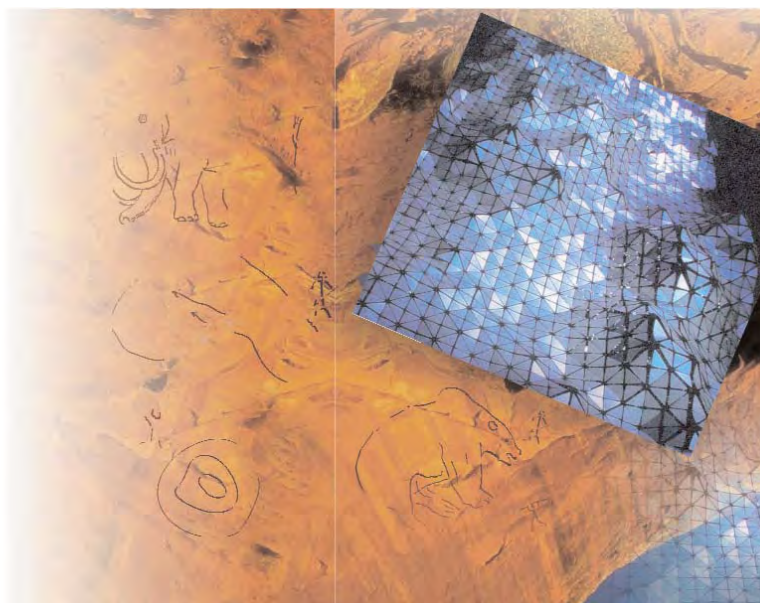
Report html, SVG, Word, scarico dei dati elaborati su fogli Excel per consentire analisi interattive, grafica personalizzate, Moduli PDF , ecc.

Lingua

Italiano

Inglese

Altro: Tedesco



Tutte le Linee Guida Iscom sono scaricabili dal sito
www.iscom.gov.it

realizzazione GRAPHICLAB
SETTORE DIVULGAZIONE E COMUNICAZIONE ESTERNA ISCOM



Ministero delle Comunicazioni



**DIVULGAZIONE E
COMUNICAZIONE ESTERNA**

**LINEE GUIDA ISCOM
PUBBLICATE**

**SICUREZZA DELLE RETI
DALL'ANALISI DEL
RISCHIO ALLE STRATEGIE
DI PROTEZIONE**

**SICUREZZA DELLE RETI
NELLE INFRASTRUTTURE
CRITICHE**

**LA QUALITÀ DEI SERVIZI
NELLE RETI ICT**

**GESTIONE DELLE
EMERGENZE LOCALI**

**RISK ANALYSIS
APPROFONDIMENTI**

**QUALITÀ DEL SERVIZIO
SU UMTS**

**QUALITÀ DEL SERVIZIO
SU BANDA LARGA**

**CERTIFICAZIONE DELLA
SICUREZZA ICT**

**OUTSOURCING E
SICUREZZA**

