UN METODO DI RISK ASSESSMENT SEMPLICE

In uno dei primi numeri di ICT Security, nel 2002, Giulio Carducci lanciava un appello perché si discutesse di metodologie di Risk Assessment. Io risposi a suo tempo con alcune considerazioni in *Sicurezza delle informazioni. Analisi e gestione del rischio*. Dopo altri 6 anni di esperienza come consulente e Lead Auditor ISO/IEC 27001 in aziende di ogni dimensione e di diverse tipologie, ho avuto modo di sviluppare un metodo di risk assessment semplice. Questa esperienza mi permette di aggiungere e, in parte, modificare, alcune idee espresse a suo tempo.

Questo articolo presenta la metodologia di Risk Assessment denominata VERA (Very Easy Risk Assessment), che permette analisi rapide e ben documentate, in modo da garantire l'efficacia di successivi riesami e da fornire gli elementi per pianificare il trattamento del rischio.

La metodologia si basa sull'analisi dei servizi offerti dall'ente che intende condurre il Risk Assessment.

E' possibile scaricare il foglio di calcolo con cui condurre il risk assessment da http://www.cesaregallotti.it/art_pres/2009-Vera.xls [4].

Come si vedrà, il metodo di calcolo del rischio non presenta nulla di innovativo. Quello che si propone questo articolo, come verrà meglio spiegato nella seconda parte, è illustrare come sia possibile condurre analisi veloci ma non superficiali, in modo da concentrarsi sulla realizzazione e sul miglioramento dei controlli di sicurezza, anziché sull'analisi.

1 LA METODOLOGIA IN BREVE

La metodologia richiede come prima fase l'individuazione dei servizi su cui svolgere l'analisi.

Ciascun servizio dovrà essere descritto indicandone sommariamente le specificità, l'organizzazione coinvolta nella sua gestione e utilizzo, incluse le terze parti, i confini fisici e la tecnologia coinvolta.

1.1 Valutazione degli impatti

Per ciascun servizio dovranno essere valutati i danni per l'azienda in caso di perdita di Riservatezza, Integrità e Disponibilità delle informazioni gestite dal servizio.

Service		**Confidentiality**	**Integrity**	**Availability**
Servizio 1		1	2	3

Per i criteri di valutazione, da 1 a 3, si può far riferimento alla SP 800-30 del NIST [13].

1.2 Identificazione e valutazione delle minacce

Per il servizio, dovranno essere identificate e valutate le minacce che potrebbero avere impatti su di esso, inclusi i parametri di Riservatezza, Integrità e Disponibilità su cui possono incidere.

VERA presenta un elenco di 41 minacce, derivate dalla ISO/IEC 27005, a cui attribuire un valore di probabilità compreso tra 1 e 3. Per i criteri di valutazione, si può far riferimento alla SP 800-30 del NIST .

Vista la semplicità del foglio di calcolo, potranno essere aggiunte ulteriori minacce, oltre a quelle già previste.

Per ogni minaccia, devono essere documentate le motivazioni che hanno portato alla decisione del valore attribuito.

Il valore attribuito a ciascuna minaccia, pesato con gli impatti calcolati per il servizio e definiti nel primo passo, viene denominato "Rischio inerente".

1.3 Analisi dei controlli di sicurezza

Dovranno essere analizzati i controlli di sicurezza che operano sul servizio. Per ciascuno di essi potrà essere attribuito un valore di robustezza/vulnerabilità compreso da 1 a 3, facendo riferimento ai criteri descritti dalla SP 800-30 del NIST.

La metodologia propone i 133 controlli della ISO/IEC 27001:2005 e per ciascuno di essi devono essere documentate le motivazioni che hanno condotto all'attribuzione del valore di robustezza/vulnerabilità, una descrizione delle modalità con cui il controllo è implementato e l'eventuale documentazione a supporto.

1.4 Calcolo del livello di rischio

Il foglio di calcolo confronta il valore del rischio inerente per ciascuna minaccia con quello attribuito a ciascun controllo che la contrasta. Se il valore del controllo di sicurezza è più basso di quello del rischio, allora si ha una casella rossa, viceversa si ha una casella verde.

Se il controllo di sicurezza non contribuisce al trattamento del rischio, si ha una casella bianca.

		Treath	Business data alteration by malicious user	Malicious software	Bomb attack and use of arms
		Probability	3	3	1
		Parameters	CIA	CIA	A
		Inherent Risk	2,00	2,00	1,00
A.6.2.1 Identification of risks related to external parties	3		X	X	
A.6.2.2 Addressing security when dealing with customers	2		X	X	X
A.7.2.2 Information labelling and handling	1		X		X

Figura 1 - Esempio di calcolo dei rischi

Il metodo di calcolo è ispirato a quello presentato dallo stesso Carducci in *La tutela dei dati aziendali. Come integrare gli aspetti giuridici, organizzativi e tecnici per proteggere i dati* ed è facilmente deducibile dalle formule del foglio di calcolo.

1.5 Trattamento del rischio

Per i rischi accettati, bisogna sostituire la “X” di ciascuna casella con una “A” e la cella diventa gialla. Devono essere quindi documentate le motivazioni che hanno condotto all’accettazione.

Per i rischi “rossi” che si intende trattare, deve essere lasciata la “X”. Per questi, il foglio di calcolo propone una sezione in cui documentare le azioni, i tempi e le responsabilità.

2 ALCUNE CONSIDERAZIONI

2.1 Come raccogliere i dati

VERA presenta solo un algoritmo di calcolo, lasciando libertà sulle modalità di raccolta dei dati. Il metodo consigliato è quello "collaborativo" di Octave [1] o FRAP [12] con la guida di personale esperto (facilitatori), accompagnato da un assessment, sempre condotto da personale esperto del business e dei sistemi informatici coinvolti nell'erogazione dei servizi.

E' anche possibile elaborare dei questionari, eventualmente seguendo le indicazioni di Mehari [3].

Il problema riscontrabile nell'uso dei questionari è che di solito le interviste sono condotte in sale riunioni da persone junior, con poche competenze in merito al business, alla tecnologia e agli asset coinvolti. In queste situazioni, spesso, gli intervistati non sono spinti a condividere le proprie riflessioni in merito alla sicurezza e ai possibili miglioramenti da apportare ai processi e alla tecnologia in uso. In altre parole, non trovano l'occasione per discutere delle vulnerabilità.

L'uso dei questionari, inoltre, porta alla raccolta di molti dati in tempi molto lunghi, con il risultato che il calcolo del livello di rischio è molto complesso, non intuitivo, non utile per una sua valutazione e, nei casi peggiori, senza avere conseguenze sulle scelte di trattamento del rischio. Sono innumerevoli gli esempi in cui l'analisi del rischio è seguita da azioni di trattamento molto semplici (spesso formazione e riscrittura di procedure) slegate dai progetti effettivamente messi a budget dall'azienda (come per esempio il completo rifacimento dei tornelli di controllo degli accessi fisici, riesame delle utenze registrate sui sistemi, introduzione di una soluzione di IAM, modifica dei sistemi di monitoraggio dei sistemi informatici, eccetera).

La semplicità dello strumento di calcolo dei livelli di rischio, il metodo "collaborativo" suggerito per la raccolta dei dati e il coinvolgimento di facilitatori competenti permettono di mettere in relazione servizi, minacce, contromisure e progetti di miglioramento.

2.2 Focus sui servizi e sui processi

VERA fu sviluppata nell'ambito di un progetto di sicurezza informatica. Oggi, anche con la diffusione di ITIL, è diffusa l'opinione che per gestire al meglio l'informatica è opportuno centrare la visione sui servizi.

Questo punto di vista può essere convenientemente abbracciato anche quando si parla di sicurezza delle informazioni. Infatti, gli utenti e il business non hanno familiarità con banche dati, macrodati e information asset, ma con i servizi

utilizzati per il proprio processo di business. Risulterà quindi più significativo per loro assegnare un "valore" a Riservatezza, Integrità e Disponibilità per i servizi.

Per quanto riguarda la documentazione su supporto diverso da quello dei servizi IT (carta, inclusi fax e fotocopie, fotografie, dischi rimovibili) è invece conveniente fare riferimento ai processi di business che fanno uso di quelle informazioni. Se l'impresa ha già un Sistema di Gestione per la Qualità in conformità alla norma ISO 9001, tale approccio risulterà molto efficiente (considerazione apparentemente scontata, ma sono molto frequenti i casi in cui Qualità e Sicurezza lavorano a compartimenti stagni).

L'approccio per servizi e per processi è anche conveniente in termini di efficienza: l'approccio per asset si è sempre dimostrato molto dispendioso in termini di tempo e non sempre efficace in termini di risultati. Infatti, la valutazione di ogni singolo asset e la conseguente analisi di minacce e contromisure porta velocemente ad accumulare un'enorme quantità di dati, in cui è difficile orientarsi e che, a seguito delle necessarie operazioni di consolidamento, forniscono risultati di sintesi che nascondono le vulnerabilità specifiche di ciascuno di essi. Il perdere, per effetto del consolidamento, alcuni riscontri sulle vulnerabilità è estremamente pericoloso, lasciando non rilevate alcune falle di sicurezza.

In alcuni casi, le metodologie di Risk Assessment richiedono la costituzione di un vero e proprio CMDB o CMS, ossia di un database di tutti i componenti del sistema informativo. Questo richiede sforzi notevoli e un processo di aggiornamento continuo, raramente messo in opera nel contesto specifico della Gestione della Sicurezza, con il risultato che i risultati del lavoro non sono più adeguati dopo poco tempo e l'anno successivo, in occasione del riesame del Risk Assessment, è necessario riprodurre la medesima mole di lavoro.

Il CMDB è fondamentale per l'operatività e l'esercizio dei sistemi informativi, ma deve essere visto come controllo di sicurezza (di cui valutarne robustezza ed efficacia), non come strumento necessario per il risk assessment. Un approccio basato sul censimento completo degli asset è sconsigliabile anche perché il risk assessment deve essere condotto sui servizi in fase di progettazione o riprogettazione, per i quali un iniziale censimento degli asset non è possibile con il grado di accuratezza richiesto dal tool per fornire risultati affidabili.

VERA, anche in linea con la ISO/IEC 27001, richiede che vengano "identificati" gli asset, ossia che venga fornita una descrizione ad alto livello e molto sintetica degli asset utilizzati per la gestione dei servizi. Tale descrizione sarà sufficientemente accurata per fornire risultati affidabili e non troppo dettagliata per poter essere utile in fase di progettazione e riprogettazione dei servizi e per non necessitare una manutenzione comparabile a quella richiesta dal CMDB.

2.3 Per necessità di maggior dettaglio

In alcuni casi è rilevante condurre delle analisi dei rischi a livello di asset. Per esempio, nel caso di sistemi informatici particolarmente critici.

VERA è un metodo utilizzabile per analisi di tipo "gestionale", ossia per la messa in opera di Sistemi di Gestione per la Sicurezza delle Informazioni secondo i requisiti della ISO/IEC 27001.

Per analisi di tipo tecnico, componente per componente, allora è consigliabile utilizzare metodologie tradizionalmente utilizzate con successo nella costruzione di macchine o di impianti, come la FMEA/FMECA o la FTA, che non si basano più sul valore di ogni singolo asset (già determinato, visto che si applica a sistemi "particolarmente critici"), ma sugli effetti che un incidente può avere su altri asset, sulle informazioni e quindi sul business.

Altre tipologie di analisi di dettaglio possono essere quelle tipiche di processi più operativi come l'Incident Management e il Problem Management. Per questo si rimanda a ITIL.

2.4 Relazione controlli minacce

Come si vede anche da Figura 1, con VERA è semplice correlare le minacce con i controlli che le contrastano.

Questo aspetto è troppe volte sottovalutato e sono presentati "livelli di rischio" senza specificare quali siano le minacce meno contrastate o i controlli più vulnerabili o meno robusti. Alcuni tool di risk assessment permettono addirittura di specificare un piano di trattamento dei rischi e di condurre delle analisi di tipo *What If* senza mostrare esattamente quali controlli (e quindi quali progetti e quali soldi investiti) sono di prioritaria importanza per contrastare quali minacce di maggior rischio.

E' invece importante essere consapevoli del rapporto tra controlli di sicurezza e minacce, per non correre il rischio di implementare o modificare controlli con effetti positivi di poco conto e per impiegare tempo ed energie in attività con migliori risultati e, forse, minor impatto economico.

La stessa ISO/IEC 27001 richiede esplicitamente di correlare da una parte le minacce ai controlli di sicurezza e dall'altra (indicazione non sempre seguita) di indicare, per ciascun controllo di sicurezza, le minacce che intende contrastare.

2.5 Semplice da modificare

VERA è molto semplice da modificare e aggiornare con nuove minacce e controlli di sicurezza. Anche in implementazioni più complesse, per aggiungere una minaccia è necessario solo considerare se ha impatti su Riservatezza, Integrità e Disponibilità e quali controlli di sicurezza la contrastano. Una persona con esperienza nei controlli della ISO/IEC 27001:2005 può svolgere questo compito in non più di 20 minuti.

La rigidità di altre metodologie non permette di inserire nuove minacce. Per questo motivo, a titolo di esempio, è comune vedere come le banche, quando utilizzano certi tool di risk assessment, abbiano difficoltà ad evidenziare la minaccia di phishing e le conseguenti azioni di trattamento.

Il processo di risk assessment e tutta la gestione della sicurezza delle informazioni prevedono invece che si svolga un riesame periodico dei risultati delle analisi e che siano valutate minacce e controlli eventualmente non precedentemente considerati. Se però il tool utilizzato non permette l'inserimento di nuove voci, allora il processo risulterà mancante di due sue componenti essenziali: il miglioramento continuo e il costante adattamento alla realtà in cui opera.

2.6 Documentare

La semplicità d'uso di VERA permette di documentare ogni valutazione fatta. Per ogni servizio e processo, minaccia e controllo di sicurezza è possibile e doveroso specificare le considerazioni fatte per attribuire i diversi valori.

Questo servirà per giustificare le scelte fatte e per condurre i successivi riesami senza dover reinventare nulla o cercare di ricordare cose ormai dimenticate.

2.7 Un metodo qualitativo

VERA è una metodologia puramente qualitativa. Anche metodologie che si dichiarano semi-quantitative, come il CRAMM, sono in realtà puramente qualitative.

Ad oggi, come già detto in altra sede, non è possibile fare analisi di tipo quantitativo, se non in casi molto particolari e rilevanti per il solo parametro di disponibilità.

2.8 Un metodo veloce

VERA è un metodo che permette un veloce Risk Assessment. In realtà di medie dimensioni e con un sistema gestionale abbastanza maturo, è possibile condurre analisi un report di trattamento del rischio in non più di 4-5 giornate. Per un numero maggiore di servizi, è possibile ridurre le analisi per ogni singolo servizio, visto che molti controlli di sicurezza e molte minacce saranno comuni. Ovviamente, la presenza di più servizi introduce altre complicazioni non trattate in questa sede.

VERA, ad oggi, è basata su fogli di calcolo che permettono una sua semplice manutenzione. Nulla impedisce di replicarne le logiche in applicazioni distribuite.

La velocità di VERA dipende anche dalle competenze degli analisti che la utilizzano, come accennato prima.

Il minor tempo speso in raccolta dati e in analisi permetterà di dedicare maggiori energie nella progettazione e realizzazione dei controlli di sicurezza di tipo tecnico e nella realizzazione di procedure e processi veramente aderenti alle necessità e alla cultura della realtà in cui si andranno ad applicare. Troppe volte si vedono progetti di sicurezza in cui quasi tutto il tempo è speso nell'analisi del rischio e nel voler imporre processi e procedure ben fatte ma inefficienti e inefficaci per la realtà a cui sono destinati.

BIBLIOGRAFIA

[1] Alberts Christopher J., Dorofee Audrey J., *OCTAVE Criteria, Version 2.0*, Carnegie Mellon University, USA, 2001, http://www.cert.org/octave

[2] Carducci Giulio, *La tutela dei dati aziendali. Come integrare gli aspetti giuridici, organizzativi e tecnici per proteggere i dati*, Franco Angeli, Milano, 1999

[3] CLUSIF, *Mehari 2007*, CLUSIF, Francia, 2007

[4] Gallotti Cesare, *Foglio di calcolo VERA*, ver 2.0, 2009, http://www.cesaregallotti.it/art_pres/2009-Vera.xls

[5] Gallotti Cesare, *Sicurezza delle informazioni. Analisi e gestione del rischio*, FrancoAngeli Editore, Milano, 2003

[6] International Electrotechnical Commission TC/SC 56, *IEC 60812 Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)*, Edition 2.0, IEC, Svizzera, 2006

[7] International Electrotechnical Commission TC/SC 56, *IEC 61025 Fault tree analysis (FTA)*, Edition 2.0, IEC, Svizzera, 2006

[8] ISO/IEC JTC 1/SC 27, *ISO/IEC 27005:2008 Information technology -- Security techniques -- Information security risk management*, ISO/IEC, Svizzera, 2008

[9] ISO/IEC JTC 1/SC 27, *ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems -- Requirements*, ISO/IEC, Svizzera, 2005
[10] Office of Government Commerce, *ITIL Service Transition*, TSO (The Stationery Office), United Kingdom, 2007
[11] Office of Government Commerce, *ITIL Service Operation*, TSO (The Stationery Office), United Kingdom, 2007
[12] Peltier Thomas R., Information Security Risk Analysis, Auerbach, USA, 2001
[13] Stoneburner Gary, Goguen Alice, Feringa Alexis, *SP-800-30 Risk Management Guide for Information Technology Systems*, National Institute of Standards and Technology, USA, 2002

Ringraziamenti
Ringrazio Massimo Cottafavi di Spike Reply e Franco Ferrari di DNV Italia per il lavoro di editor.

Cesare Gallotti ha lavorato come consulente sulla sicurezza delle informazioni e Lead Auditor ISO/IEC 27001 in Securteam, Intesis, DNV Italia e Quint Wellington Redwood. Ha pubblicato nel 2003, per i tipi della FrancoAngeli, *Sicurezza delle informazioni. Analisi e gestione del rischio*. Curatore della newsletter IT Service Management. Dal 2008 lavora come libero professionista. Il suo sito web è http://www.cesaregallotti.it