Un metodo di Risk Assessment semplice

Cesare Gallotti

Roma, 3 marzo 2010

Introduzione

- Questa presentazione si basa su osservazioni fatte:
  - in più di 50 aziende (medie, grandi, piccole)
  - in quasi 11 anni di audit e consulenza
  - in diversi Paesi del Mondo (Europa e Africa)
- Le osservazioni fatte non sono state solo negative!
- Non si vuole proporre "il metodo giusto": si vuole aprire una discussione sui metodi più diffusi.

Sommario

- Qualche domanda
- Alcuni limiti delle metodologie più diffuse
- Un Very Easy Risk Assessment (VERA)
- Conclusioni

Qualche domanda (1/2)

- Quante risorse spendete ogni anno per la valutazione dei rischi (Risk Assessment) di sicurezza delle informazioni?
- Il Risk Assessment fornisce risultati realmente utili? (da E&Y Global Security Survey 2010, per l'84% la disponibilità di risorse è una sfida significativa e il 44% non ha una strategia di sicurezza per il prossimo anno; eppure, il 42% intende avere un sistema di gestione per la sicurezza delle informazioni conforme alla ISO/IEC 27001)
- Tutti i progetti di sicurezza sono collegati ai rischi evidenziati dal Risk Assessment?

Qualche domanda (2/2)

- Il personale operativo segue le procedure di sicurezza? E' veramente sensibilizzato sulla loro utilità e necessità? (da E&Y Global Security Survey 2010, il 74% delle imprese ha erogato corsi di sensibilizzazione sulla sicurezza generali, solo il 35% ne ha erogati di specifici).
- Nel corso degli audit e Risk Assessment avete mai evidenziato carenze in termini di inefficienza?

Alcuni limiti delle metodologie più diffuse

Citazione

"Il risk assessment è un metodo complicato per fornire risposte già note"

Anonimizzato, maggio 2001

Uso di questionari

- Spesso sono utilizzati questionari per intervistare i "process owner" su minacce, vulnerabilità, impatti degli incidenti
- I questionari fanno perdere informazioni utili, ma come raccoglierle se il metodo è chiuso e le interviste sono condotte in sale riunioni da persone junior?
- I questionari portano a raccogliere molti dati con:
  - tempi troppo lunghi
  - risultati sui livelli di rischio non intuitivi
  - perdita di informazioni a causa della loro aggregazione (un rischio 10 si perde nella media)
- I questionari non garantiscono l'oggettività dei dati
- L'uso di questionari ha dei limiti, perché non usare altri metodi con altri limiti?

Piani di trattamento del rischio

- A fronte di risultati complessi e non intuitivi, spesso le azioni riguardano:
  - modifica di procedure documentate
  - sensibilizzazione del personale
- I "veri" progetti seguono altre strade:
  - modifica dei tornelli all'ingresso
  - riesame delle utenze dei sistemi IT
  - introduzione di strumenti di IAM
  - modifica dei sistemi di monitoraggio
  - modifica di processi
- I controlli di sicurezza spesso non sono collegati alle minacce che intendono contrastare:
  - sono adeguati?
  - sono troppo robusti?
  - sono troppo deboli?

Perché focalizzarsi sugli asset?

- Si intervistano gli "asset owner", i "process owner" (spesso dirigenti e quadri) sugli asset:
  - il loro livello di competenza sui singoli asset non può essere ottimale
  - si perdono informazioni dei tecnici
  - l'interesse è sui servizi
  - gli asset sono spesso gestiti con processi spesso simili, anche se gli asset sono diversi tra loro
- Spesso sono ripetute le stesse domande per ogni asset
- Si raccolgono troppi dati per risk assessment "di alto livello"
- L'asset inventory è necessario per le attività di gestione dei sistemi: perché utilizzarlo anche per un risk assessment?
  - Ogni tanto si trovano doppioni: il CMDB e l'asset inventory
- E se un servizio è ancora in fase di progettazione, con l'architettura da definire?

C’è solo un tipo di risk assessment?

- Si perdono le differenze tra:
  - risk assessment “generale” a livello alto
  - risk assessment sul singolo servizio (o sistema)
  - vulnerability assessment
  - audit tecnici
  - audit di processo
  - analisi degli incidenti e dei problemi
- E spesso non sono collegati tra loro.

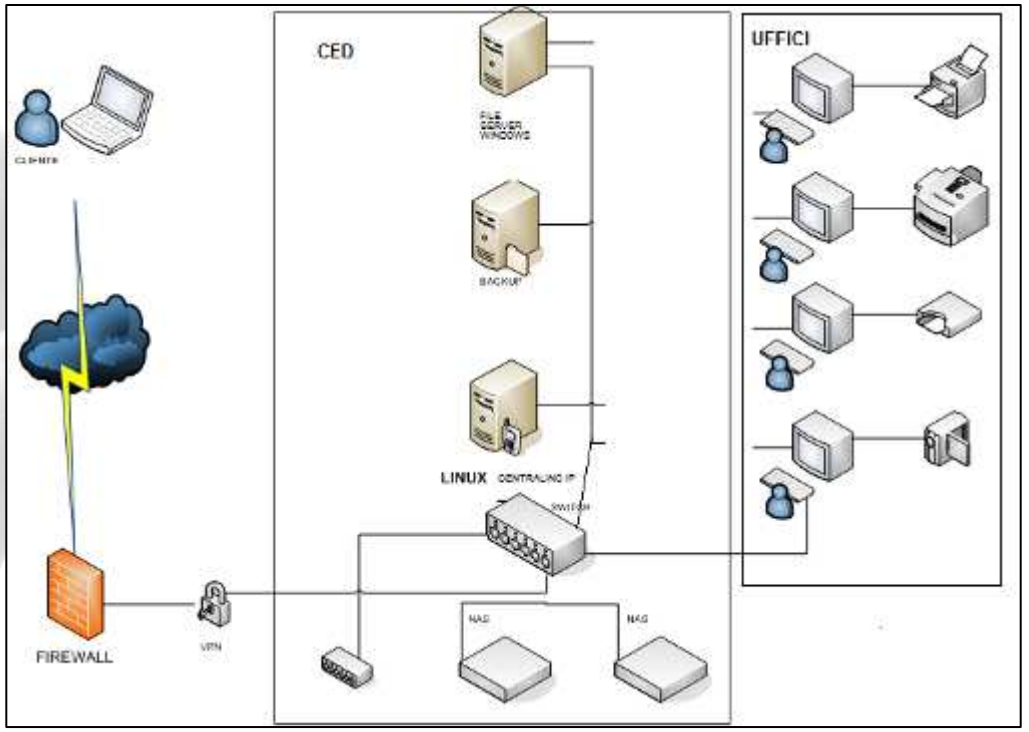
Tool e “fogli di calcolo”

- Spesso sono usati tool per il risk assessment. Devono essere facilmente da modificare se:
  - si considera una nuova minaccia (es. phishing, diffusione dei PDA, gestione dei fornitori, passaggio al cloud)
  - si individuano nuove vulnerabilità
  - si scelgono diversi metodi per rappresentare le misure di sicurezza
  - si vogliono prendere note per il passaggio di informazioni tra un risk assessment e il successivo
- E’ veramente così sconveniente usare gli strumenti di office automation?
- I tool in commercio non permettono analisi quantitative (né sono possibili, nella sicurezza delle informazioni)

Un Very Easy Risk Assessment

Prima fase – Individuazione dei servizi

- La prima fase è 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.



Seconda fase: 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

Terza fase: Identificazione e valutazione delle minacce

- Dovranno essere identificate e valutate le minacce che potrebbero avere impatti sul servizio 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 (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”.

Terza fase: minacce (esempio)

Minaccia	**Prob.**	**RID**	**Note**
Incendio	1	ID	Vigili del Fuoco hanno concordato su rischio basso
Allagamento	1	D	Data Center è al 2° piano
Inquinamento - Polvere - Corrosione – Gelo	1	D	Umidità max 100%, temperatura max 40℃. Usati apparecchi standard. MTBF di 10 anni.
Distruzione non aut. di apparecchi o media	3	D	Pochi incidenti registrati negli ultimi 2 anni, non deliberati
Bombe o attacchi armati	1	D	

Quarta fase: 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 e vulnerabilità compreso da 1 a 3.
- 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 dei valori.

Control	Value	Description	Vulnerability	Documentation
A.9.1.1 Physical security perimeter	1	• Telecamere esterne • Accessi all'edificio con guardia • CED, sala energia e sala rete isolate	• Accesso alla sala riunioni non controllato • Porte e finestre non allarmate • No allarmi volumetrici	• Procedura xy sulla gestione dei badges • Istruzioni alle guardie

Quarta fase: Analisi dei controlli (ulteriori esempi)

- Bisogna sempre considerare l'ambito in cui si lavora ed eventualmente separare le considerazioni.
- Prima dell'analisi bisogna comunque ragionare sugli aspetti da valutare.

Control	Value	Description	Vulnerability
A.10.3.1 Capacity management	2	• Server: monitorata capacità disco, CPU, RAM • Firewall: monitorata capacità CPU e RAM	• Router: non monitorati • Firewall: monitorati ma non impostate soglie
A.7.2.2 Information labeling and handling	1	• Ufficio commerciale: ok informazioni negli armadi con chiave	• Ufficio HR: armadi senza chiave

Quinta fase: calcolare il livello di rischio

- Il rischio è calcolato per ciascuna minaccia e ciascun controllo
  - > rischio (attuale) = (VR+VI+VD)*PM/(ER+EI+ED)
    - VR, VI, VD = valore R, I, D per il servizio
    - PM = probabilità minaccia
    - ER, EI, ED = 1 se la minaccia impatta su R, I o D; 0 viceversa
- Se il controllo che la contrasta ha robustezza minore del rischio, allora la casella diventa rossa
- Non si ha una "media" del rischio anche per non correre il rischio di non considerare le "code"

		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

Sesta fase: trattare il rischio

- Per le caselle rosse, deve essere deciso se il rischio deve essere trattato, trasferito o accettato.
- Un apposito foglio permette di documentare le opzioni fatte e le azioni conseguenti

Threat	Inherent risk	Control	Strength/ Vulnerability	Treatment		
				Action	End date	Responsible
Software Malfunction	3	A.10.1.4 Separation of development, test and operational facilities	2	A project of separation of facilities will be started in october. The feasibility study has been done and a draft project plan has been issued.	January	Cesare

Threat	Inherent risk	Control	Strength/ Vulnerability	Reason for acceptance
Unauthorised use of equipment	2	A.11.2.2 Privilege management	1	The number of system administrator is too low for having a proper privilege management policy

Considerazioni

- I dati possono essere raccolti nel modo preferito
  - in realtà, si fa affidamento sulle competenze di chi guida l'analisi
  - bisogna lasciar liberi gli intervistati di dire quello che vogliono, consapevoli di avere di fronte persone preparate che capiscono il loro punto di vista
- Focus sui servizi e sui processi
- Si possono aggiungere e togliere facilmente minacce e controlli
- Permette di documentare facilmente le osservazioni e le scelte fatte
- Non si perdono le code

Conclusioni

- Il risk assessment fornisce (forse) risposte già note, ma deve essere un metodo semplice per sistematizzare e consolidare e categorizzare le idee e le esperienze in modo da fornire un quadro utile per il processo decisionale.
- Metodi molto strutturati sono stati (forse) utili per la crescita della consapevolezza dei risk manager, ma:
  - si utilizzano ancora strumenti troppo complessi
  - "semplicità" non vuol dire "incompletezza", così come "complesso" non vuol dire "efficace" (anche perché uno strumento inefficiente diventa inesorabilmente inefficace)
- Un metodo di risk assessment semplice e completo, permette di dedicare le energie nel seguire le fasi di implementazione della sicurezza: aiutare gli utenti a seguire le procedure, migliorare le procedure, scegliere i tool più adeguati.

Riflessione finale

- La fase di educazione del personale è troppo spesso sottovalutata, ma è la più difficile e critica e dove dovrebbe essere più importante la presenza dei consulenti.

Cartello: "Tenere sempre la porta chiusa"

Grazie

Cesare Gallotti
cesaregallotti@cesaregallotti.it
http://www.cesaregallotti.it
Newsletter ICT Management News: www.cesaregallotti.it/newsletter.htm