



Analisi del Rischio

Approccio alla valutazione del rischio
Informatico

Contromisure

Cosa è l'Analisi del Rischio

- ◆ Un metodo per quantificare l'impatto di un potenziale attacco ad un sistema
- ◆ Il risultato finale dell'analisi del rischio:
 - Aiuta a bilanciare rischi e costi
 - Aiuta il management nella decisione di quali rischi prevenire, limitare o accettare

Metodologia

- ◆ **Analisi Qualitativa**
 - Si basa su una valutazione intuitiva
 - I risultati si esprimono con parole
- ◆ **Analisi Quantitativa**
 - Si basa su dati statistici e di probabilità
 - I risultati si esprimono con numeri

Approccio qualitativo

		VALORE		
		BASSO	MEDIO	ALTO
RISCHIO	BASSO	Yellow	Orange	Red
	MEDIO	Orange	Red	Dark Orange
	ALTO	Red	Dark Orange	Dark Red

Approccio quantitativo

- ◆ $\text{Rischio annuo} = \text{Valore del bene} \times \text{Fattore di Esposizione} \times \text{Frequenza di Accadimento}$
- ◆ Esempio di un rischio Incendio:
Valore = 1M €
Esposizione = 50%
Frequenza = 1/10 (ogni 10 anni)
 $\text{Rischio annuo} = 1\text{M €} \times 50\% \times 1/10 = 50\text{K €}$

Elementi della valutazione del Rischio:

- ◆ Beni e Dati da proteggere
- ◆ Minacce
- ◆ Vulnerabilità
- ◆ Perdite
- ◆ Contromisure



Una corretta valutazione dei rischi permette di scegliere tra una delle seguenti decisioni:

- ◆ Accettare il Rischio
- ◆ Ridurre il Rischio adottando contromisure
- ◆ Trasferire il Rischio (a una Compagnia Assicuratrice)

Dominio del rischio

Rischio

RISK MANAGEMENT

CONTROMISURE

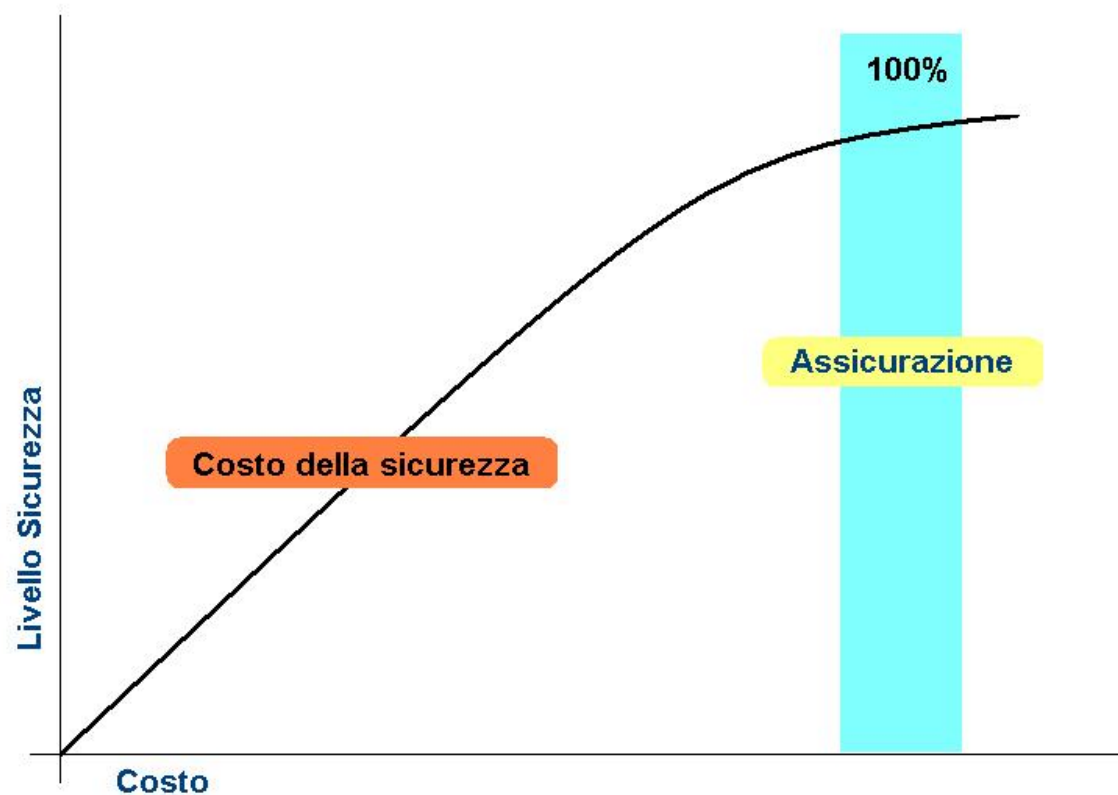
COPERTURA
ASSICURATIVA

PREVEDIBILE

DIFFICILMENTE PREVEDIBILE

IMPONDERABILE

Copertura Assicurativa del Rischio Residuo



Quanto investire in sicurezza?

- ◆ E' difficile valutare quanto investire in Sicurezza Informatica, se non si conosce il valore dell'esposizione del rischio.
- ◆ Uno degli obiettivi di una valutazione del rischio è quantificare il costo dei danni provocati da violazioni al sistema informatico.
- ◆ Questa informazione permette di sapere il **ritorno dell'investimento in Sicurezza** (ROI) e stabilire un budget adeguato.

Come misurare i costi

Nel mondo commerciale bisogna tenere in considerazione:

- ◆ **Costi tangibili**
- ◆ **Costi intangibili**

Costi tangibili:

- Perdite di materiale (danno fisico)
- Perdite dovute alla non disponibilità delle informazioni
- Perdite dovute a clientela che nel frattempo si rivolge ai ns.concorrenti
- Perdita di produttività del personale (non IT) che si trova a lavorare in condizioni degradate (o non lavora del tutto) durante le operazioni di ripristino.
- Costi di lavoro e materiali per il rilevamento, il contenimento, la riparazione e la ricostruzione dei danni ai dati.
- Costi di lavoro per la corretta raccolta dei dati e il mantenimento delle prove, necessari per le indagini e le eventuali denunce ai responsabili.
- Costo per la preparazione delle comunicazioni in relazione all'accaduto (comunicati stampa, posizione nei confronti della clientela, ecc.)
- Costi di difesa legale qualora possa essere ravvisata una qualsiasi responsabilità dell'Azienda relativa alle conseguenze di quanto accaduto.
- Eventuali aumenti del premio assicurativo.

Costi intangibili:

Identificabili come perdite per “**svantaggio competitivo**”

- Perdita di fiducia dei clienti
- Rallentamento, se non arretramento, della propria posizione di mercato, in seguito a cattiva pubblicità.
- Accesso dei concorrenti a informazioni confidenziali o riservate.

Quanto spendere in un anno per la sicurezza ?

Una ipotesi azzardata.

- ◆ Valore dell'esposizione **100**
- ◆ Investimento in contromisure di sicurezza: **4%**
- ◆ Costo della copertura assicurativa: **1%**

Esempio di copertura assicurativa Rischio Informatico

Rischio coperto	Somma assicurata	Premio
HD Rischio Hardware (ripristino materiali danneggiati)	L. 200.000.000	600.000
SW Rischio Software/dati (ricostruzione dati/archivi, indagini)	L. 300.000.000	4.500.000
SW rischio software/dati presso clienti*	L. 500.000.000	7.500.000
EE Extra Expenses (spese extra conseguenti e per limitare i danni)	L. 500.000.000	2.500.000
BI Business Interruption (Perdite profitto lordo)	L. 500.000.000	3.000.000
RI Ricostruzione Immagine	L. 50.000.000	1.500.000
Totale	L. 2.050.000.000	19.600.000

Esempi di sinistri

Cliente: Impresa di produzione
Sistema: AS/400
Causa: inondazione dei locali
Danno: guasto del sistema di backup e ripristino dati
Indennizzo: 115.000 €

Cliente: Impresa metallurgica
Sistema: 10 PC in rete
Causa: Virus
Danno: Antivirus inefficiente e non correttamente impiegato
Indennizzo: 16.000 €

Cliente: Impresa servizi di borsa
Sistema: 8 PC in rete
Causa: Guasto nel server durante il backup, ritardato avvio del sistema di riserva
Indennizzo: 12.000 €