LA VALUTAZIONE

DELLA SICUREZZA

NOTE SUL RELATORE :

Ing. Marcello Mistre (marcello.mistre@sistinf.it)

Membro del comitato direttivo di Isaca Roma, è certificato CISA, CISM, Lead auditor BS7799/ISO27001

E' responsabile dell'offering "audit e sicurezza informatica" di Sistemi Informativi S.p.A., società di IBM.

INDICE DELLA PRESENTAZIONE :

1. Il piano di sicurezza
2. Il piano di business continuity
3. Valutazione economica della sicurezza

IL PIANO DI SICUREZZA

CONCETTI GENERALI

PROCESSI

Si definiscono come “l’insieme delle sequenze di decisioni, di operazioni e attività spesso formalizzate (procedure), che l’Azienda nel suo complesso svolge per gestire il ciclo di vita di una risorsa o di un gruppo di risorse, per il proseguimento della missione”

Il riferimento alle risorse sta a sottolineare l’importanza dell’associazione tra processi e risorse al fine del conseguimento degli obbiettivi aziendali

Più semplicemente i processi indicano, in modo più o meno formalizzato, le regole per utilizzare le risorse nel modo migliore ai fini del conseguimento degli obbiettivi aziendali

DATI

I dati costituiscono il patrimonio informativo dell'Azienda

Il dato, a differenza dell'informazione, è caratterizzato da una rappresentazione formale specifica

Un insieme di data-set omogeneo per funzionalità aziendale costituisce una entità di dati. La relativa denominazione segue l'organizzazione della struttura tecnica, organizzativa e contabile dell'Azienda

Quanto sopra descritto si può riassumere nella correlazione:
DATI => DATA SET => ENTITA' DI DATI

MINACCE

Eventi (azioni o “non azioni”) non desiderati, sia deliberati che accidentali, in grado di arrecare un danno

AGENTI

Potenziali portatori di una minaccia

Agenti non umani:

- eventi naturali (uragani, terremoti, inondazioni, ecc.)
- eventi accidentali (allagamenti, incendi, ecc.)

Agenti umani (danni volontari o involontari):

- programmatori
- hackers
- vandali
- personale interno ostile
- spie, ecc.

FUNZIONI DI SICUREZZA

Elementi di base con cui si realizzano le contromisure necessarie per soddisfare gli obiettivi di sicurezza del sistema

Si distinguono in:

- fisiche
- procedurali
- tecnico-informatiche

MECCANISMI DI SICUREZZA

Costituiscono i mezzi con cui realizzare le funzioni di sicurezza

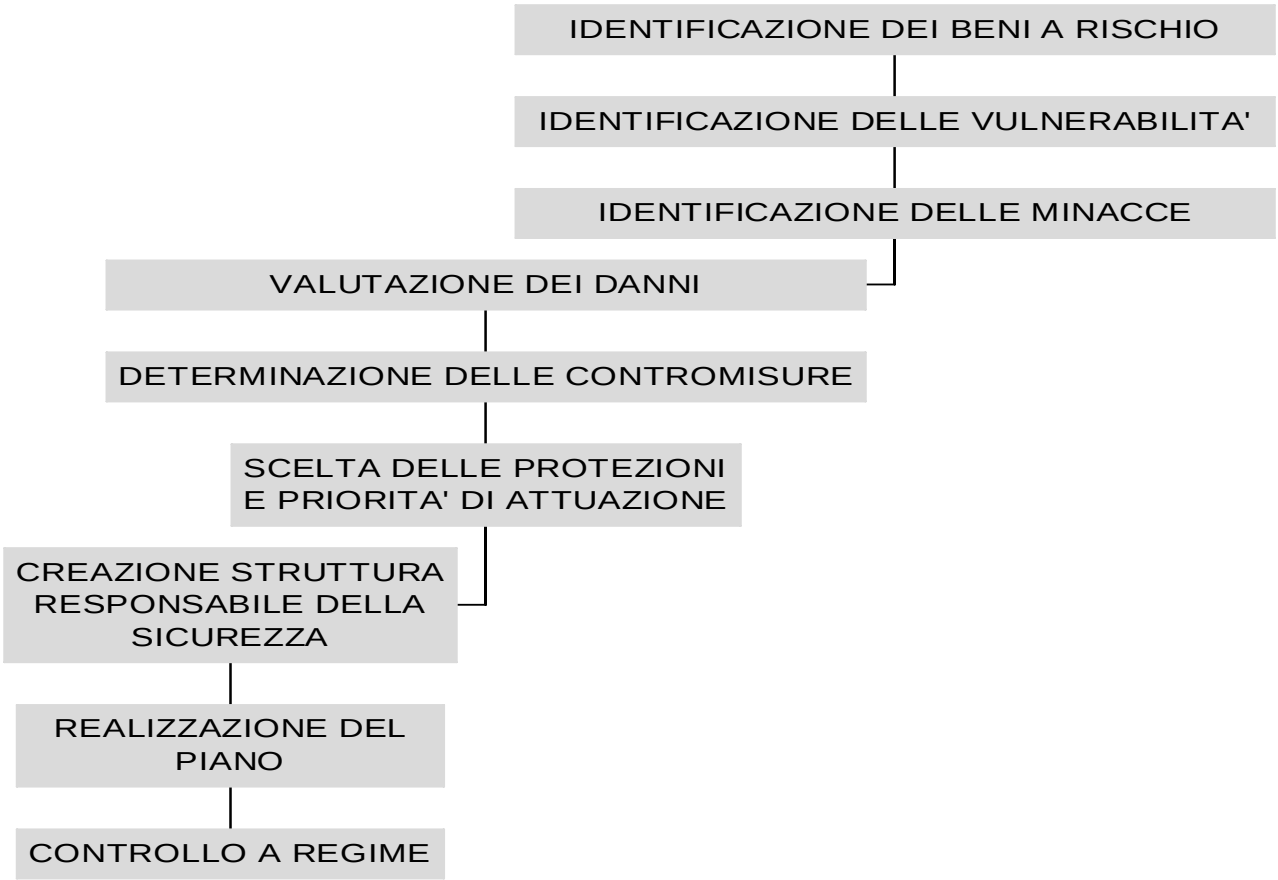
L'analisi dei meccanismi deve tener conto di quelli già presenti nel sistema

E' necessario analizzare le interconnessioni tra i vari meccanismi, al fine di garantire la loro corretta integrazione

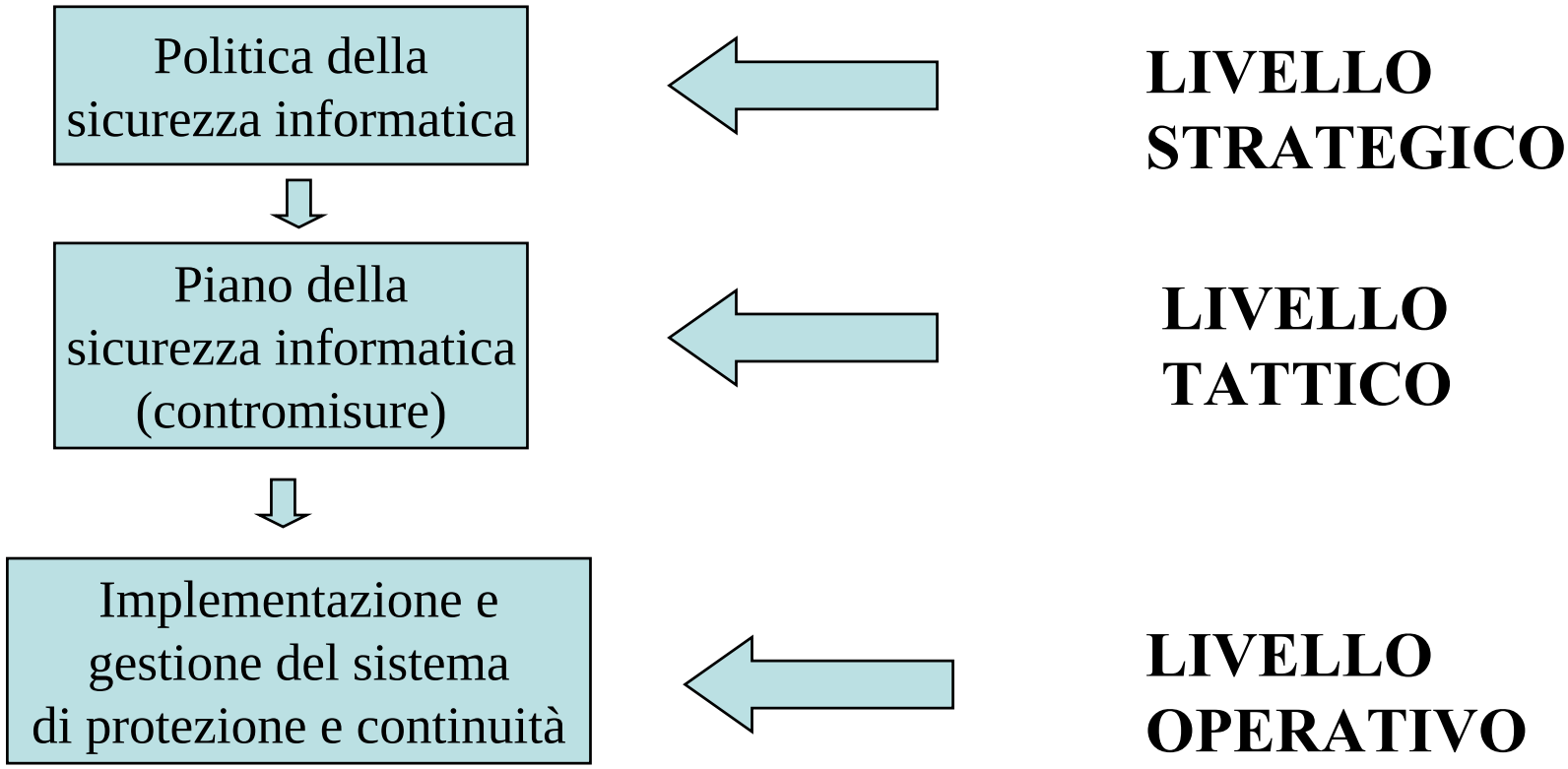
Un Security Target (Piano di Sicurezza) può prescrivere l'utilizzo di determinati meccanismi di sicurezza, ma ciò, pur se consigliato, è facoltativo

Nel caso non vengano specificati meccanismi, si intende che è lasciata libertà di azione a chi realizza le funzioni di sicurezza

Piano aziendale per la sicurezza

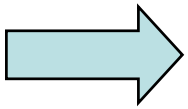


Livelli di attuazione del piano



RACCOLTA DEI DATI

IL PIANO DI SICUREZZA



ESAME DELLA POLITICA DI SICUREZZA

CLASSIFICAZIONE DEI DATI

RILEVAZIONE DELLA STRUTTURA INFORMATICA

DISTRIBUZIONE DEI DATI NEI SISTEMI

ANALISI DELLE MINACCE E DEGLI ATTACCHI

POLITICA DI SICUREZZA AZIENDALE

E' l'insieme di norme, regole, consuetudini che regolano come i beni aziendali vengono gestiti, protetti e gestiti all'interno dell'organizzazione. Tali norme sono spesso sintetizzate in un documento aziendale

POLITICA DI SICUREZZA DI SISTEMA

E' un documento, facente degli obiettivi di sicurezza se il TOE è costituito da un sistema, che illustra l'insieme di norme, regole, consuetudini che regolano come le informazioni rilevanti per la sicurezza (sensitive) ed altre risorse sono gestite, protette e distribuite all'interno dello specifico sistema. Il documento fa riferimento agli eventuali documenti di *politica di sicurezza aziendale e tecnologica*. Il documento dovrebbe identificare gli obiettivi di sicurezza del sistema e le relative minacce e dovrebbe coprire tutti gli aspetti di sicurezza relativi al sistema, inclusi quelli associati alle misure di sicurezza fisica, procedurale e del personale.

POLITICA DI SICUREZZA TECNOLOGICA

E' l'insieme di norme, regole, consuetudini che regolano l'elaborazione delle informazioni rilevanti per la sicurezza (sensitive) e l'uso di altre risorse da parte dell'hardware e software di un sistema informativo. Tali norme possono essere suddivise in più documenti dedicati a specifiche tecnologie per esempio reti locali, trasmissione dati, stazioni di lavoro personali ecc..
Il documento fa riferimento alla politica di sicurezza aziendale e dovrebbe essere aggiornato quando si introducono nuove tecnologie.

PRODUCT RATIONALE

Documento, facente parte degli obiettivi di sicurezza se il TOE è costituito da un prodotto, che dovrebbe fornire all'eventuale acquirente le informazioni necessarie a valutare se il prodotto può soddisfare gli obiettivi di sicurezza e a definire cosa altro deve essere fatto affinché tali obiettivi possano essere raggiunti completamente. Pertanto il documento dovrebbe identificare le modalità d'uso del prodotto, l'ambiente a cui è indirizzato e le minacce previste in tale ambiente.

IL PIANO DI SICUREZZA

ESAME DELLA POLITICA DI SICUREZZA

CLASSIFICAZIONE DEI DATI

RILEVAZIONE DELLA STRUTTURA INFORMATICA

DISTRIBUZIONE DEI DATI NEI SISTEMI

ANALISI DELLE MINACCE E DEGLI ATTACCHI

I dati devono essere disponibili in una forma strutturata, come i report prodotti dai vari strumenti di Data Dictionary

DATA SET	LABEL	DESCRIPTION	COMMENT
Data set #1			
Data set #2			
……..			
……..			
……..			
……..			
Data set #n			

IL PIANO DI SICUREZZA

Ai responsabili dei dati e manager aziendali viene chiesto di riempire degli opportuni questionari in cui si richiede di valutare la sensibilità dei dati gestiti o utilizzati rispetto ai parametri canonici di integrità, riservatezza e disponibilità con un valore 1, 2 o 3.
Il questionario che ogni soggetto intervistato riceve contiene solo i data set di propria competenza

DATA SET	RELEVANCE		
	Integrity	Confidentiality	Availability
Data set #1	3	3	3
Data set #2	1	1	2
Data set #3	1	2	2
Data set #4	2	2	1

IL PIANO DI SICUREZZA

I valori attribuiti ai data set vengono sommati in modo ponderato (∑/n) e scalati per evitare numeri decimali (x10, x100, ecc..)

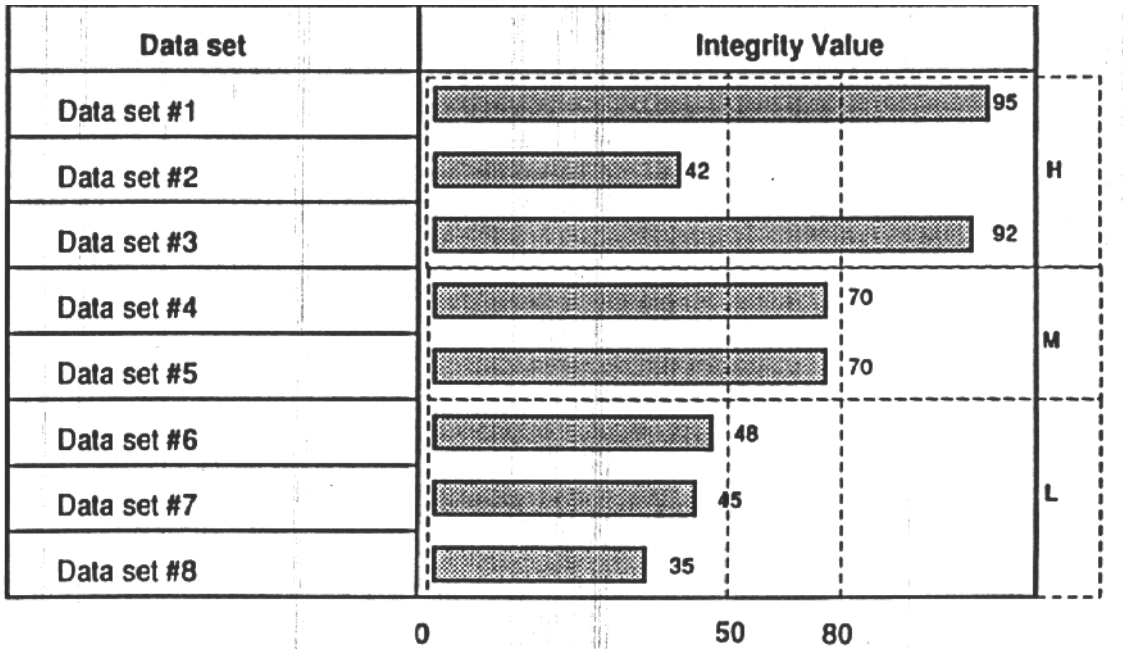
L'obiettivo è di dividerli in tre macro-classi (High, Medium, Low) per ogni parametro di sensibilità.

V1	Integrity
High	H
Medium	M
Low	L

V2	Confidentiality
High	H
Medium	M
Low	L

V3	Availability
High	H
Medium	M
Low	L

Alla fine si ottiene la figura seguente:



IL PIANO DI SICUREZZA

Successive analisi ed interviste eliminano le eventuali situazioni di incongruenza (i manager desiderano che un certo data-set sia posizionato, ad esempio per ragioni strategiche aziendali, in una classe diversa da quella spettante per l'elaborazione

Il risultato finale è un report di questo tipo:

DATA SET	Integrity	Confidentiality	Availability
Data set #1	H	M	M
Data set #2	L	M	L
…….	….	….	….
…….	….	….	….
…….	….	….	….
…….	….	….	….
Data set #n	M	L	L

IL PIANO DI SICUREZZA

ESAME DELLA POLITICA DI SICUREZZA

CLASSIFICAZIONE DEI DATI

RILEVAZIONE DELLA STRUTTURA INFORMATICA

DISTRIBUZIONE DEI DATI NEI SISTEMI

ANALISI DELLE MINACCE E DEGLI ATTACCHI

IL PIANO DI SICUREZZA

Attraverso interviste e questionari si ottiene una rappresentazione del sistema informativo, distinguendo tra livelli omogenei e sistemi che rivestono particolare importanza.

Ad esempio:

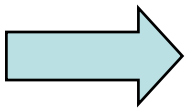
- **HOST** (Mainframe)
- **RETE** (Rete Geografica Aziendale)
- **MINICOMPUTER** (Sistemi Dipartimentali)
- **LAN** (Local Area Network)
- **WORKSTATION** (Personal Computer)
- **NASTROTECHE**

IL PIANO DI SICUREZZA

ESAME DELLA POLITICA DI SICUREZZA

CLASSIFICAZIONE DEI DATI

RILEVAZIONE DELLA STRUTTURA INFORMATICA



DISTRIBUZIONE DEI DATI NEI SISTEMI

ANALISI DELLE MINACCE E DEGLI ATTACCHI

IL PIANO DI SICUREZZA

La sensibilità di ogni data-set è la stessa per ogni sistema in cui è presente o elaborato ed è pari al valore precedentemente determinato

INTEGRITY						
Data set	Architectural levels					
	Host	WAN	Mini	LAN	WS	Tape room
Data set #1	H	H	H			H
Data set #2	L			L		
….	….	….	….	….	….	….
….	….	….	….	….	….	….
Data set #n	M	M		M		

Analoghe tabelle vengono costruite per i restanti parametri di sensibilità (riservatezza e disponibilità)

IL PIANO DI SICUREZZA

La sensibilità di ogni sistema informatico viene definita pari a quella del data-set presente o elaborato di valore più elevato

Integrity						
Data set	Architectural levels					
	Host	WAN	Mini	LAN	WS	Tape room
Data set #1	(H)	(H)	(H)			(H)
Data set #2	L			L		
...	...	...	...	...	...	...
...	...	...	...	...	...	...
Data set n	M	M		(M)		

IL PIANO DI SICUREZZA

La sensibilità del sistema informatico può essere diversa rispetto ai tre parametri di sicurezza

Confidentiality

Data set	Architectural levels					
	Host	WAN	Mini	LAN	WS	Tape room
Data set #1	(M)	(M)	(M)			(M)
Data set #2	M			(M)		
...	...	...	...	...	...	...
...	...	...	...	...	...	...
Data set #5	L			L		

Availability

Data set	Architectural levels					
	Host	WAN	Mini	LAN	WS	Tape room
Data set #1	(M)	(M)	(M)			(M)
Data set #2	L				(L)	
...	...	...	...	...	...	...
...	...	...	...	...	...	...
Data set #5	L			(L)		

IL PIANO DI SICUREZZA

Se un sistema non contiene o non elabora data-set sensibili, il suo valore è “non classificato” e viene ignorato

In base ai risultati conseguiti nei passi precedenti, è possibile costruire la tavola riepilogativa finale

Arch. level	Integrity	Confidentiality	Availability
Host	H	M	M
WAN	H	M	M
Mini	H	M	M
LAN	M	M	L
WS	…	…	…
Tape room	H	M	M

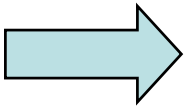
IL PIANO DI SICUREZZA

ESAME DELLA POLITICA DI SICUREZZA

CLASSIFICAZIONE DEI DATI

RILEVAZIONE DELLA STRUTTURA INFORMATICA

DISTRIBUZIONE DEI DATI NEI SISTEMI



ANALISI DELLE MINACCE E DEGLI ATTACCHI

MINACCIA: evento non desiderato, sia deliberato che accidentale, che potrebbe in qualsiasi modo arrecare danno direttamente o indirettamente

Sono possibili molte classificazioni delle minacce in grado di agire su un sistema. Una è la seguente:

FURTI
Azioni di appropriazione di apparati, impianti, tabulati, supporti magnetici o copie di dati e/o programmi, sottratti all'azienda con finalità diverse. Per ciò che concerne i dati ed i programmi non necessariamente finalizzati alla divulgazione all'esterno

FRODI O MALVERSAZIONI (COMPUTER CRIME)
Azioni finalizzate ad arrecare un danno all'azienda sia per ricavarne profitti personali illeciti, o per terzi, sia per attivare missioni di ritorsione, intimidazione o comunque compromissori per la missione o l'immagine dell'azienda stessa

DANNEGGIAMENTO
Eventi di tipo fisico o logico che comportano danni tali da provocare la perdita di affidabilità, fino all'interruzione del servizio

MANIPOLAZIONE DI DATI E/O PROGRAMMI
Azioni vandaliche in grado di arrecare danno all'azienda senza finalità conclamate (altrimenti rientrerebbero nelle frodi)

PERDITA DI PRIVACY
Azioni, sia accidentali che procurate, che possono condurre all'accesso ad informazioni riservate o che se non utilizzate dai diretti interessati possono essere suscettibili di erronee o fuorvianti interpretazioni

ERRORI SUI DATI E PROGRAMMI
Errori derivanti sia dalla mancanza di adeguati test e collaudi al software prima della messa in esercizio, sia derivanti da mancanza di controlli adeguati sui dati immessi nel sistema

UTILIZZO ILLEGALE DI SOFTWARE

Azioni di inserimento di software non legale e comunque, anche se legale, non autorizzato dalla struttura responsabile del S.I.

DIVULGAZIONE DI DATI E PROGRAMMI

Minaccia particolare posta in una posizione intermedia tra la frode e il furto: può avere conseguenze sull'immagine dell'azienda, ma non sono presenti elementi tali per cui si configurino reati penali

UTILIZZO ILLEGALE DI RISORSE

Utilizzo illecito delle risorse aziendali, costituente di fatto un abuso nei confronti dell'azienda stessa o una appropriazione indebita di beni immateriali

AVARIE AI SISTEMI

Malfunzionamenti del sistema, sia dell'hardware che del software, in grado di compromettere l'affidabilità del sistema stesso

INAGIBILITA' DEI LOCALI

Condizioni di impraticabilità, temporanea o definitiva, dei locali dove operano i sistemi o dove sono depositati gli archivi off-line necessari ad un esercizio affidabile del sistema. L'inagibilità cui si fa riferimento è quella relativa alle infrastrutture ausiliarie e logistiche di supporto ove i sistemi sono collocati

Le minacce in grado di agire sui sistemi si attuano mediante diverse tipologie di attacchi, come ad esempio:

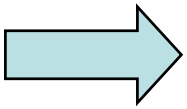
- **Accesso non autorizzato a dati e programmi**
- **Intercettazione delle informazioni in transito sulle linee di comunicazione**
- **Analisi del traffico sulla rete locale**
- **Abuso di privilegi**
- **Furto di supporti o documenti**
- **Modifica di dati e programmi**
- **Inserimento di virus**
- **Ecc**

L'ANALISI CONDOTTA IN AZIENDA CONSENTE DI DETERMINARE QUALI SONO GLI ATTACCHI POSSIBILI E LE MODALITA' DI ATTUAZIONE

ELABORAZIONE DEI DATI

ITSEC PREVEDE DI DEFINIRE GLI OBIETTIVI DI SICUREZZA COME INSIEME DELLE FUNZIONI DI SICUREZZA (SECURITY FUNCTIONS) ATTE A CONTRASTARE GLI ATTACCHI

IL PIANO DI SICUREZZA



ANALISI DEGLI OBIETTIVI SULLE CLASSI DI SENSIBILITA' DEI DATI

DETEMINAZIONE DELLE FUNZIONI DI SICUREZZA

DETERMINAZIONE DEI MECCANISMI

GRADO DI ROBUSTEZZA DEI MECCANISMI

GRADO DI CONFIDENZA (ASSURANCE) RICHIESTO

Gli obiettivi (reazione agli attacchi) vengono precisati per le tre classi di sensibilità dei dati

Obiettivi di sicurezza	H	M	L
Accesso non autorizzato a dati e programmi	X	X	X
Intercettazione delle informazioni in transito sulle linee di comunicazione	X		
Analisi del traffico sulla rete locale	X	X	
Abuso di privilegi	X		
Furto di supporti o documenti	X	X	X
Modifica di dati e programmi	X		
Inserimento di virus	X	X	

IL PIANO DI SICUREZZA

ANALISI DEGLI OBIETTIVI SULLE CLASSI DI SENSIBILITA' DEI DATI

DETEMINAZIONE DELLE FUNZIONI DI SICUREZZA

DETERMINAZIONE DEI MECCANISMI

GRADO DI ROBUSTEZZA DEI MECCANISMI

GRADO DI CONFIDENZA (ASSURANCE) RICHIESTO

IL PIANO DI SICUREZZA

I criteri ITSEC, pur lasciando libertà di scelta delle funzioni di sicurezza, ne suggeriscono l'ordinamento in gruppi. A tal fine raccomandano (ma non impongono) l'uso dei seguenti gruppi generici (generic headings)
identification and authentication

- **access control**
- **accountability**
- **audit**
- **object reuse**
- **accuracy**
- **reliability of service**
- **data exchange**

A queste si aggiungono un gruppo di funzioni di tipo **organizzativo** e un altro gruppo di tipo **logistico**

IL PIANO DI SICUREZZA

Gli obiettivi di sicurezza vengono tradotti nelle funzioni di sicurezza necessarie ad attuarli (ciascuna per ogni parametro di sicurezza: integrità riservatezza, disponibilità)

Obiettivi di sicurezza	Funzioni di sicurezza
Accesso non autorizzato a dati e programmi	Access control
Intercettazione delle informazioni in transito sulle linee di comunicazione	Access control Identification and authentication Organizzazione
Analisi del traffico sulla rete locale	Accountability Access control Funzioni logistiche
Abuso di privilegi	Access control Organizzazione
Furto di supporti o documenti	Organizzazione Funzioni logistiche
Modifica di dati e programmi	Access control Reliability of service
Inserimento di virus	Organizzazione Accountability

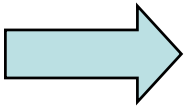
IL PIANO DI SICUREZZA

	Sensitivity classes / Security parameters / Security functions	HIGH			MEDIUM			LOW		
		I	C	A	I	C	A	I	C	A
GEN./HEAD.	Identification and Authentication	X	X		X	X		X	X	
	Access control	X	X		X	X		X	X	
	Data access control	X	X		X	X		X	X	
	Accountability	X	X	X	X	X	X			
	Audit	X	X	X	X	X	X			
	Object reuse		X							
	Accuracy	X			X			X		
	Reliability of service	X		X	X		X	X		X
	Data exchange	X	X							
ORG	Rules and responsibilities definition	X	X	X	X	X	X			
	Procedures for system utilization	X	X	X	X	X	X			
	Procedures for system management	X	X	X	X	X	X	X	X	X
	Training	X	X	X						
	Communication activity to make users aware of security needs	X	X	X	X	X	X	X	X	X
LOG	Passive detection systems			X			X			
	Active detection systems			X			X			
	Physical access control systems	X	X	X	X	X	X			
	UPS	X		X	X		X			
	General building structures			X			X			

IL PIANO DI SICUREZZA

ANALISI DEGLI OBIETTIVI SULLE CLASSI DI SENSIBILITA' DEI DATI

DETEMINAZIONE DELLE FUNZIONI DI SICUREZZA



DETERMINAZIONE DEI MECCANISMI

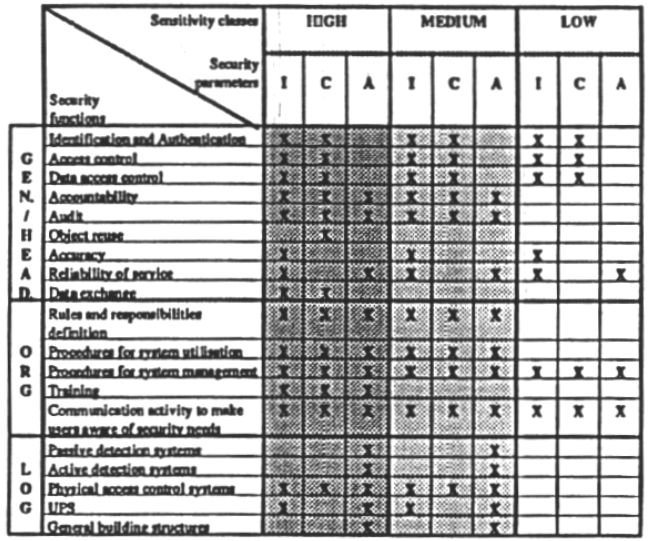
GRADO DI ROBUSTEZZA DEI MECCANISMI

GRADO DI CONFIDENZA (ASSURANCE) RICHIESTO

IL PIANO DI SICUREZZA

Dal confronto tra la tabella relativa alle sensibilità dei sistemi informatici e quella delle funzioni

Arch. level	Integrity	Confidentiality	Availability
Host	H	M	M
WAN	H	M	M
Mini	H	M	M
LAN	M	M	L
WS	…	…	…
Tape room	H	M	M



	Sensitivity classes	HIGH			MEDIUM			LOW		
	Security parameters / Security functions	I	C	A	I	C	A	I	C	A
GEN./HEAD.	Identification and Authentication	X	X		X	X		X	X	
	Access control	X	X		X	X		X	X	
	Data access control	X	X		X	X		X	X	
	Accountability	X	X	X	X	X	X			
	Audit	X	X	X	X	X	X			
	Object reuse		X							
	Accuracy	X			X			X		
	Reliability of service	X		X	X		X	X		X
	Data exchange	X	X							
ORG	Rules and responsibilities definition	X	X	X	X	X	X			
	Procedures for system utilization	X	X	X	X	X	X			
	Procedures for system management	X	X	X	X	X	X	X	X	X
	Training	X	X	X						
	Communication activity to make users aware of security needs	X	X	X	X	X	X	X	X	X
LOG	Passive detection systems			X			X			
	Active detection systems			X			X			
	Physical access control systems	X	X	X	X	X	X			
	UPS	X		X	X		X			
	General building structures			X			X			

si determina quali funzioni di sicurezza e con quale efficacia (H, M, L, pari alla sensibilità dei dati da proteggere) devono essere adottate per ogni sistema e per ogni parametro

IL PIANO DI SICUREZZA

I meccanismi di sicurezza attuano le funzioni previste

Si cerca di utilizzare meccanismi certificati

Vengono scelti sulla base di considerazioni economiche, a parità di grado di robustezza offerta

Non esiste un metodo preciso per la loro adozione: è compito dell'esperto di sicurezza in base alla propria esperienza

IL PIANO DI SICUREZZA

ANALISI DEGLI OBIETTIVI SULLE CLASSI DI SENSIBILITA' DEI DATI

DETEMINAZIONE DELLE FUNZIONI DI SICUREZZA

DETERMINAZIONE DEI MECCANISMI

GRADO DI ROBUSTEZZA DEI MECCANISMI

GRADO DI CONFIDENZA (ASSURANCE) RICHIESTO

La robustezza dei meccanismi è definita con precisione in ITSEC

Può essere Alta, Media o Bassa, che rappresentano crescenti livelli di resistenza ad un attacco diretto

ITSEM definisce le modalità di determinazione del grado di robustezza per i *generic headings* validi anche per quelli riferiti alle funzioni logistiche, basate su

- tempo a disposizione per effettuare l'attacco
- complicità necessaria
- esperienza tecnica posseduta
- attrezzatura utilizzata

IL PIANO DI SICUREZZA

Per i meccanismi di tipo organizzativo si può usare la seguente tabella

Funzioni organizzative **Grado di robustezza**	Ruoli e responsablità	Norme di utilizzo	Procedure di gestione	Formazione	Sensibilizzazione e comunicazione
BASE	Definiti				Generale
MEDIA	Definiti	Descrizione generale	Descrizione generale		Generale
ALTA	Definiti	Descrizione dettagliata con formalizzazio-ne	Descrizione dettagliata	Specifica per la sicurezza	Generale

BASE: definiti ruoli e responsabilità

MEDIO: definiti ruoli e responsabilità. Descritto utilizzo e gestione delle funzioni di sicurezza

ALTO: definiti ruoli e responsabilità. Descritto in dettaglio utilizzo e gestione delle funzioni di sicurezza. Addestramento alla sicurezza

IL PIANO DI SICUREZZA

ANALISI DEGLI OBIETTIVI SULLE CLASSI DI SENSIBILITA' DEI DATI

DETEMINAZIONE DELLE FUNZIONI DI SICUREZZA

DETERMINAZIONE DEI MECCANISMI

GRADO DI ROBUSTEZZA DEI MECCANISMI

GRADO DI CONFIDENZA (ASSURANCE) RICHIESTO

IL PIANO DI SICUREZZA

ITSEC definisce sette livelli (E0...E6) di confidenza (assurance) del sistema di sicurezza rispetto alla sua capacità di attuare le funzioni previste

Ogni livello rappresenta crescenti livelli di confidenza

Il livello di confidenza è influenzato da diversi fattori, tra cui la completezza e approfondimento della documentazione

IL PIANO DI BUSINESS CONTINUITY

IL PIANO DI BUSINESS CONTINUITY

Contiene l'evidenziazione di tutte le attività da svolgere per garantire la continuità della missione d'impresa e, quanto più possibile, la redditività nelle condizioni di crisi

Parte dall'analisi dei processi aziendali, finalizzati alla gestione delle risorse su cui opera l'azienda e delle risorse necessarie al loro svolgimento

Agisce sulle risorse avendo il compito di pianificare e rendere disponibili, in caso di disastro, quelle essenziali per garantire la continuità dei processi vitali

IL PIANO DI BUSINESS CONTINUITY

- CLASSIFICAZIONE DEI PROCESSI AZIENDALI

- DETERMINAZIONE DEL LIVELLO DI CRITICITA' DELLE APPLICAZIONI

- DETERMINAZIONE DEL PESO DELLE APPLICAZIONI

- ANALISI DELLA CORRELAZIONE PROCESSI/APPLICAZIONI

- VALUTAZIONE DELLE APPLICAZIONI RISPETTO AI PROCESSI AZIENDALI

- CALCOLO FINALE DELLA CRITICITA' DELLE APPLICAZIONI

IL PIANO DI BUSINESS CONTINUITY

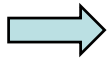
L'obiettivo di questa fase è di valutare la criticità di ogni processo riguardo il suo contributo al successo dell'azienda e al raggiungimento della missione
Viene realizzata una tabella dove nelle ascisse è riportata una scala che esprime il posizionamento dei processi in relazione della prossimità alla missione aziendale:
Struttura generale: processi aziendali improduttivi che sono comunque necessari in quanto legati all'esistenza dell'azienda
Struttura di controllo: processi aziendali, anch'essi improduttivi, finalizzati ad esercitare il controllo della gestione per il rispetto dei risultati d'esercizio previsti
Supporto alla gestione: processi che concorrono in maniera determinante alla gestione efficiente ed economica dell'azienda
Supporto alla missione: processi che, pur non sviluppando direttamente reddito, ne concorrono comunque alla produzione
Missione di impresa: tutte le attività finalizzate alla produzione del reddito

Nelle ordinate invece è espresso il livello di contribuzione dei processi al successo e alla competitività dell'azienda sul mercato

IL PIANO DI BUSINESS CONTINUITY

Contribution to the company success/competitiveness

Determinant	5	10	15	20	25
Relevant	4	8	12	16	20
Influent	3	6	9	12	15
Little influent	2	4	6	8	10
Marginal	1	2	3	4	5
	General structure	**Control structure**	**support to management**	**Support to mission**	**Company mission**

Company mission 

Ad ogni processo viene attribuito un valore pari al prodotto riga x colonna

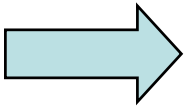
$$V_p = P_m \; X \; C_S$$

Dove:
- **Vp** è il valore del processo
- **Pm** è la posizione del processo rispetto alla missione aziendale (colonna)
- **Cs** è il contributo al successo/competitività dell'azienda

Una volta riempita la tabella, i processi vengono ordinati in base al loro valore, che rappresenta la loro importanza e contributo al successo e competitività dell'azienda

IL PIANO DI BUSINESS CONTINUITY

CLASSIFICAZIONE DEI PROCESSI AZIENDALI



DETERMINAZIONE DEL LIVELLO DI CRITICITA' DELLE APPLICAZIONI

DETERMINAZIONE DEL PESO DELLE APPLICAZIONI

ANALISI DELLA CORRELAZIONE PROCESSI/APPLICAZIONI

VALUTAZIONE DELLE APPLICAZIONI RISPETTO AI PROCESSI AZIENDALI

CALCOLO FINALE DELLA CRITICITA' DELLE APPLICAZIONI

IL PIANO DI BUSINESS CONTINUITY

Il ruolo fondamentale è svolto dagli utenti responsabili dell'utilizzo delle applicazioni

L'obiettivo è di riempire una tabella come la seguente:

Applications	Block 1		Block 2 Lc					Block 3						Block 4 Pe					Notes
	%1	%2	HH	H	M	L	N	1	3	5	10	15	over	N	R	A	S	C	

Blocco 1: percentuale stimata di contribuzione dell'applicazione e dei relativi archivi alla struttura generale (%1) e alla missione aziendale (%2)

Blocco 2: un segno deve essere posto nella colonna corrispondente alla criticità stimata dell'applicazione riguardo il raggiungimento della missione aziendale

HH	Vitale/critica (i dati gestiti dall'applicazione e il suo funzionamento sono essenziali per il mantenimento delle posizioni di mercato
H	Importante
M	Molto utile
L	Utile
N	Non importante

Blocco 3: stima del periodo di tempo massimo in giorni (o secondo altra misura di tempo adatta alla situazione) che l'azienda può tollerare senza iniziare a perdere posizioni di mercato o soffrire di perdite economiche rilevanti

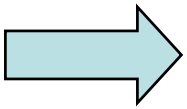
Blocco 4: valutazione approssimata delle perdite economiche che l'azienda soffrirà trascorso il periodo di tempo indicato nel blocco 3

- N Nulla
- R Recuperabile (il danno verrà recuperato senza particolari problemi)
- A Assorbibile (il danno non è recuperabile, ma implica perdite economiche non rilevanti per l'azienda)
- S Significativo (la perdita economica è di grande importanza per il business aziendale)
- C Compromissiva (il danno produce perdite gravi che possono compromettere il futuro aziendale)

IL PIANO DI BUSINESS CONTINUITY

CLASSIFICAZIONE DEI PROCESSI AZIENDALI

DETERMINAZIONE DEL LIVELLO DI CRITICITA' DELLE APPLICAZIONI



DETERMINAZIONE DEL PESO DELLE APPLICAZIONI

ANALISI DELLA CORRELAZIONE PROCESSI/APPLICAZIONI

VALUTAZIONE DELLE APPLICAZIONI RISPETTO AI PROCESSI AZIENDALI

CALCOLO FINALE DELLA CRITICITA' DELLE APPLICAZIONI

Il peso aziendale di ogni applicazione è determinato moltiplicando il valore delle risposte fornite nel Blocco 2 (Lc: Vitale [HH]=5 ... Non importante [N] = 1) per quello del Blocco 4 (Pe: Compromissiva = 5 ... Nulla = 1

$$P_a = L_c \times P_e$$

Il risultato è una misura delle perdite stimate causate all'azienda dall'indisponibilità di un'applicazione

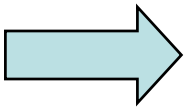
I valori del Blocco 1 hanno lo scopo di verificare e validare le risposte fornite negli altri blocchi

IL PIANO DI BUSINESS CONTINUITY

CLASSIFICAZIONE DEI PROCESSI AZIENDALI

DETERMINAZIONE DEL LIVELLO DI CRITICITA' DELLE APPLICAZIONI

DETERMINAZIONE DEL PESO DELLE APPLICAZIONI



ANALISI DELLA CORRELAZIONE PROCESSI/APPLICAZIONI

VALUTAZIONE DELLE APPLICAZIONI RISPETTO AI PROCESSI AZIENDALI

CALCOLO FINALE DELLA CRITICITA' DELLE APPLICAZIONI

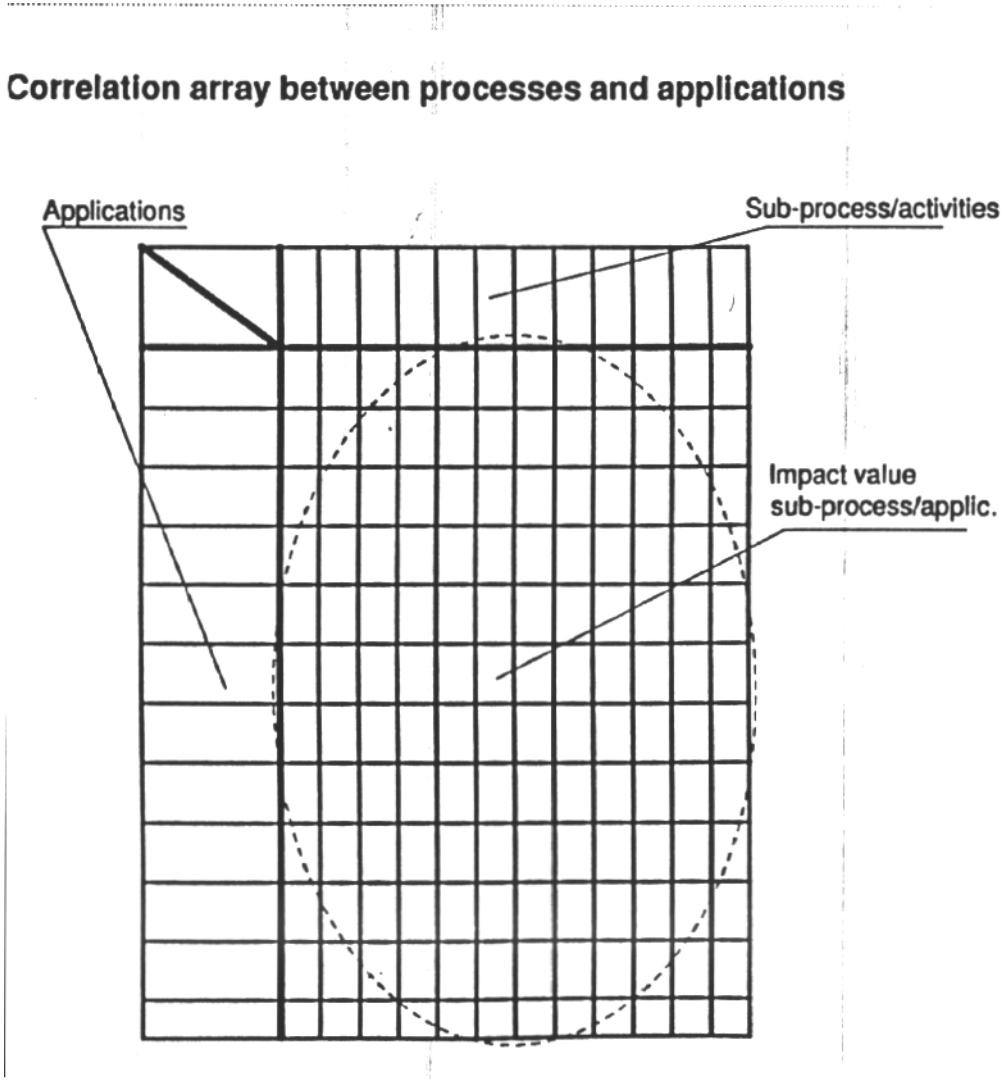
L'obiettivo è di valutare l'impatto di ogni applicazione sui processi aziendali

I processi più importanti possono essere suddivisi nei sottoprocessi o attività che li compongono

Con l'aiuto di persone esperte che l'azienda indicherà, verrà riempita la tavola che segue. In corrispondenza di ogni applicazione e processo o sottoprocesso si inserirà un valore *Vi*, chiamato **valore dell'impatto**

Vi = 3 diretta correlazione tra l'applicazione e il processo
Vi = 2 correlazione indiretta e quindi non determinante
Vi = 1 correlazione marginale
Vi = nulla l'applicazione è completamente estranea al processo (lasciare vuota la casella)

IL PIANO DI BUSINESS CONTINUITY



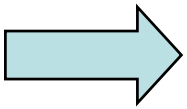
IL PIANO DI BUSINESS CONTINUITY

CLASSIFICAZIONE DEI PROCESSI AZIENDALI

DETERMINAZIONE DEL LIVELLO DI CRITICITA' DELLE APPLICAZIONI

DETERMINAZIONE DEL PESO DELLE APPLICAZIONI

ANALISI DELLA CORRELAZIONE PROCESSI/APPLICAZIONI



VALUTAZIONE DELLE APPLICAZIONI RISPETTO AI PROCESSI AZIENDALI

CALCOLO FINALE DELLA CRITICITA' DELLE APPLICAZIONI

Nella fase precedente ogni applicazione è stata posta in relazione ai processi (o sottoprocessi) per ottenere un valore Vi variabile da 1 a 3 in corrispondenza di ogni correlazione esistente
Il valore totale di ogni applicazione è dato dalla somma dei valori Vi.
Tale somma è ponderata: ogni valore viene moltiplicato per il peso del processo stesso al fine di tenere in conto l'importanza del processo stesso

$$V_a = \Sigma(V_i \, X \, V_p)$$

Va è il valore dell'applicazione relativo a tutti i processi
Vi è il valore dell'impatto
Vp è il peso del processo

IL PIANO DI BUSINESS CONTINUITY

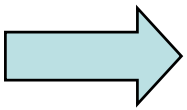
CLASSIFICAZIONE DEI PROCESSI AZIENDALI

DETERMINAZIONE DEL LIVELLO DI CRITICITA' DELLE APPLICAZIONI

DETERMINAZIONE DEL PESO DELLE APPLICAZIONI

ANALISI DELLA CORRELAZIONE PROCESSI/APPLICAZIONI

VALUTAZIONE DELLE APPLICAZIONI RISPETTO AI PROCESSI AZIENDALI



CALCOLO FINALE DELLA CRITICITA' DELLE APPLICAZIONI

I dati ottenuti nel passo precedente (Va) vengono infine moltiplicati per il peso delle applicazioni (Pa) calcolato inizialmente, per determinare la criticità di ogni singola applicazione

$$C_a = V_a \; X \; P_a$$

Va è il valore dell'applicazione
Pa è il peso dell'applicazione
Ca è la criticità dell'applicazione

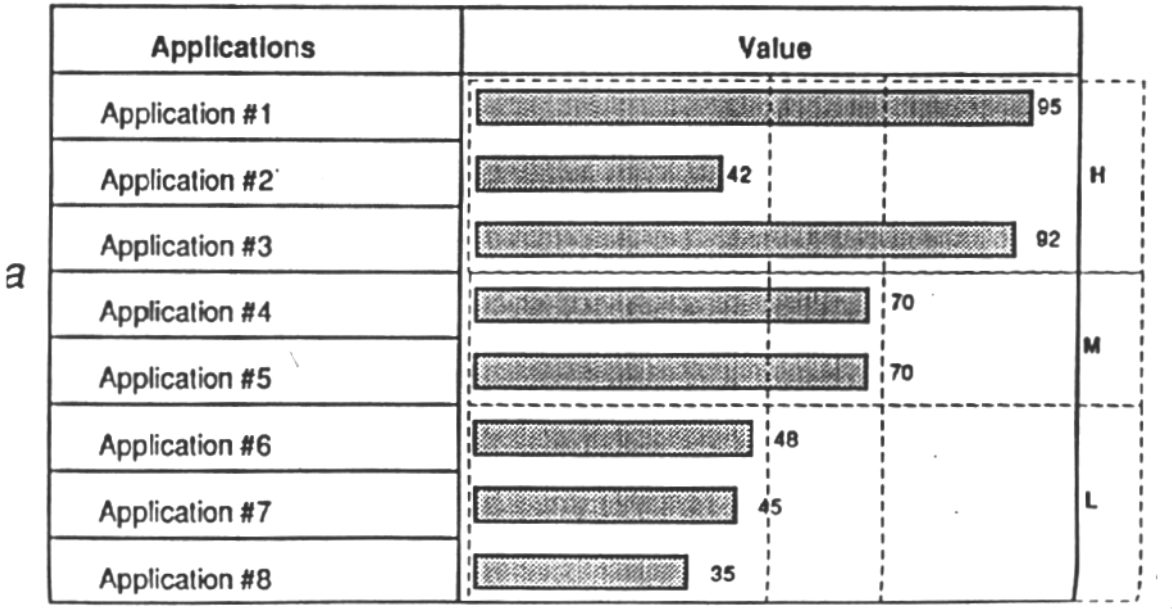
IL PIANO DI BUSINESS CONTINUITY

I risultati ottenuti, poiché dipendono da stime fornite dai vari responsabili aziendali, devono essere analizzati con cura e discussi

Le applicazioni vengono divise in tre grandi classi (H = Alta importanza aziendale, M = media, L = bassa).

Punti di discontinuità nella distribuzione che il metodo adottato facilmente produce, aiutano a determinare i confini fra le classi

IL PIANO DI BUSINESS CONTINUITY



In questo esempio l'azienda, dopo gli approfondimenti, ha espressamente richiesto di includere tra le applicazioni critiche una (#2) che nell'analisi effettuata apparteneva ad una classe inferiore

VALUTAZIONE ECONOMICA DELLA SICUREZZA

ASPETTI GENERALI

VALUTAZIONE ECONOMICA DELLA SICUREZZA

Le contromisure (meccanismi) di sicurezza determinate dall'applicazione della metodologia devono essere scelte in base a:

- una valutazione economica e quantitativa dei costi connessi al rischio residuo
- al costo delle contromisure stesse

avendo per obiettivo quello di raggiungere la soluzione che presenta il costo minore

In realtà è molto difficile adottare un tale approccio perché se da un lato è possibile determinare con esattezza il costo dei sistemi di protezione, dall'altro è estremamente difficile calcolare il costo della loro efficacia, cioè del rischio evitato

Si tratta di un costo previsto, che dipende dalla volontà di qualcuno di causare un danno (o dalla probabilità di accadimento di un evento naturale) e dal fallimento del sistema di contromisure

VALUTAZIONE DEL COSTO DEL RISCHIO

VALUTAZIONE ECONOMICA DELLA SICUREZZA

Il calcolo del costo del rischio è effettuato tramite l'analisi del valore economico e del grado di sensibilità dei dati, come determinato dalla applicazione della metodologia

In precedenza i data-set sono stati classificati secondo la loro sensibilità

Ora ai responsabili aziendali si chiede di indicare (ponendo un segno sulla colonna opportuna) se il data-set è **importante** o **essenziale** per l'organizzazione dal punto di vista del **costo**

SECURITY QUESTIONNAIRE DATA CLASSIFICATION ACCORDING TO THEIR VALUE AND SENSITIVITY					
Information system: ……					
Relevant data list	**VALUE**		**SENSITIVITY**		
	Important	**Essential**	**Sensivity class**	**Risk class**	**Coverage grade**

VALUTAZIONE ECONOMICA DELLA SICUREZZA

DATA-SET: .....

Stimare il valore del data set per l'azienda, l'individuo e il danneggiatore, utilizzando i seguenti parametri

0 = trascurabile
1 = circa 10.000 lire
2 = circa 100.000 lire
3 = circa 1 milione di lire
4 = circa 10 milioni di lire
5 = circa 100 milioni di lire
6 = circa 1 miliardo di lire
7 = circa 10 miliardi di lire

A. Valore per l'azienda	**Parametro V**
Costo di ricostruzione	.....
Costo di penalizzazione	.....
Opportunità perdute	.....
Impossibilità a prendere decisioni	.....
Altro	.....
B. Valore per l'individuo	
Reputazione	.....
Libertà civili	.....
Credito	.....
Altro	.....
C. Valore per il danneggiatore	
Risorsa da vendere	.....
Appropriazione	.....
Vendetta	.....
Miglioramento del credito, stipendio, posizione	.....
Competitività	.....
Vantaggio politico	.....
Altro	.....

VALUTAZIONE ECONOMICA DELLA SICUREZZA

DATA-SET: .....

Valutare le probabilità di ciascuno degli eventi sotto indicati, utilizzando i seguenti parametri

0 = impossibile
1 = 1 volta ogni 100 anni
2 = 1 volta ogni 10 anni
3 = 1 volta all'anno
4 = 1 volta ogni 30 giorni
5 = 1 volta ogni 3 giorni
6 =3 volte al giorno
7 = 30 volte al giorno

A. Disastri	**Parametro R**
Naturali	.....
Danni all'hardware e al software	.....
Incuria umana	.....
Altro	.....

B. Violazione della riservatezza	
Curiosità	.....
Ottenimento di informazioni per ragioni politiche o legali	.....
Rivelazione involontaria di informazioni riservate	.....
Altro	.....

C. Dolo	
Saccheggio e sabotaggio	.....
Utente malintenzionato	.....
Appropriazione indebita	.....
Miglioramento del credito, stipendio, posizione	.....
Spionaggio industriale	.....
Altro	.....

ESPOSIZIONE ANNUA

Dalla somministrazione dei questionari precedenti si può determinare quello riassuntivo, dove in ogni riga si può indicare la media dei risultati ottenuti o il caso peggiore tra essi (per effettuare, ad esempio, delle simulazioni

SECURITY QUESTIONNAIRE						
INFORMATION SYSTEM VALUES AND PROBABILITY OF HAPPENING OF A DAMAGING EVENT						
Information system	**VALUE (V)**			**RISK (R)**		
	Company (A)	**Person** (B)	**Saboteur** (C)	**Integrity** (1)	**Confidentiality** (2)	**Availability** (3)

Dal significato attribuito ai parametri V ed R si ha:

Valore del flusso di dati considerato = $10^{(v+3)}$ **[lire]**

Probabilità annua = $10^{(R-3)}$

Il valore dell'intero sistema informativo sarà: $\sum_{i=1}^{n} 10^{(Vi+3)}$

L'esposizione annua (in lire) è il prodotto del valore del sistema informativo (in lire) e della probabilità annua di accadimento dell'evento dannoso

$$E = 10^{(V+R)}$$

Dove:
E = "esposizione annua" in lire
V = valore del sistema informativo
R = probabilità di accadimento dell'evento dannoso

VALUTAZIONE ECONOMICA DELLA SICUREZZA

Con tale procedimento si perviene a un prospetto riassuntivo, in cui l'esposizione annua è suddivisa, per comodità di analisi, nelle categorie: disastro (colonne 1 e A del prospetto precedente), violazione di riservatezza (colonne 2 e B) e dolo (colonne 3 e C)

ESPOSIZIONE ANNUA				
AMMONTARE DELL'ESPOSIZIONE ANNUA RELATIVA AL LIVELLO DI SICUREZZA DI OGNI SISTEMA INFORMATIVO				
Sistema informativo	**ESPOSIZIONE ANNUA (LIRE)**			
	Disastro	**Violazione riservatezza**	**Dolo**	**TOTALE**

ESEMPI DI CALCOLO

La perdita di un file comporta un costo di L 1.000.000 per ricostruirlo (V = 3) e accade una volta ogni 30 giorni (R = 4)

$$E = 10^{(4+3)} = 10.000.000 \text{ lire/anno}$$

Un incendio comporta una perdita di 1 miliardo di lire (V = 6) e la sua probabilità di accadimento è una volta ogni 100 anni (R = 1)

$$E = 10^{(1+6)} = 10.000.000 \text{ lire/anno}$$

La ripartenza di un elaboratore fallita per un errore di un operatore comporta un costo di lire 19.000 (V = 1); se ciò accade 30 volte al giorno (R = 7) la corrispondente esposizione é:

$$E = 10^{(7+1)} = 100.000.000 \text{ lire/anno}$$

SCELTA DEL GRADO DI SICUREZZA

VALUTAZIONE ECONOMICA DELLA SICUREZZA

Il problema della scelta del grado consiste nell'individuare, tra le possibili combinazioni di sistemi di salvaguardia, l'alternativa ritenuta "migliore" in base al criterio dei costi e benefici.
A tale scopo può essere utilizzato il metodo che comporta la determinazione del **costo totale atteso** per ogni alternativa

$$T(K) = X_i(K) + X_g(K) + Y(K)$$

Dove:

Xi(K)	è la quota di ammortamento annua relativa al costo dell'installazione del generico sistema di sicurezza K
Xg(K)	è il costo annuale di gestione dello stesso
Y(K)	è l'esposizione annuale dovuta al costo del rischio residuo connesso con l'adozione di tale sistema di sicurezza
T(K)	è il suo costo totale annuo

VALUTAZIONE ECONOMICA DELLA SICUREZZA

A causa degli alti costi di realizzazione, la determinazione del "miglior" sistema di sicurezza sarà generalmente basata sul confronto dei costi totali dei sistemi alternativi relativi ad un periodo di circa 5 anni.
La relazione precedente può essere quindi espressa come:

$$T(K) = X_i(K) + \sum_{n=1}^{5} F_n^t \left(X_{gn}(K) + Y_n(K)\right)$$

dove **F** è il fattore attuale relativo all'anno n-esimo, cioè il valore attuale di una lira dell'anno n-esimo, al tasso di interesse t.

La relazione separa i costi di installazione da quelli ricorrenti.

Il fattore **F** riporta i costi futuri al valore attuale consentendone il confronto

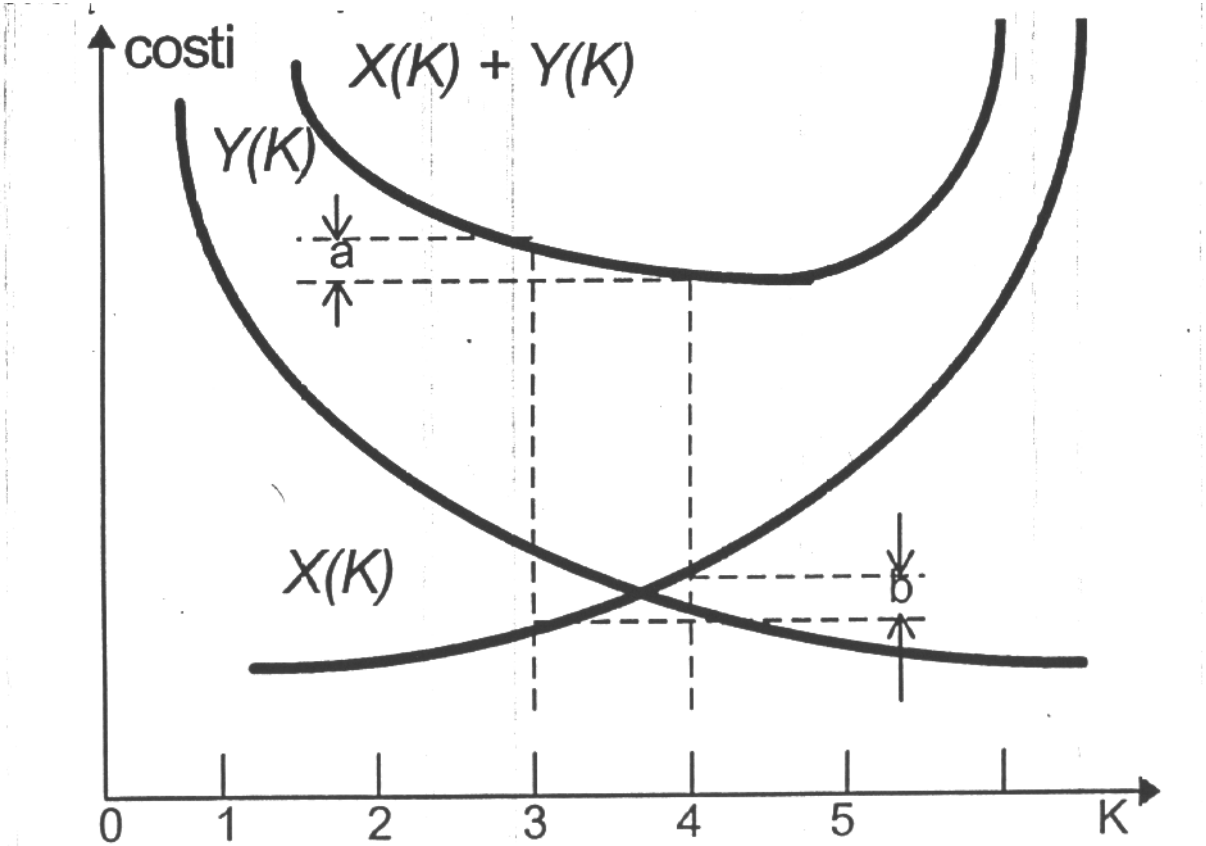
Si possono quindi prendere in esame un certo numero di sistemi di sicurezza determinandone le componenti di costo.
Se si contraddistingue con un indice **K** più elevato i sistemi più sofisticati, è evidente che al crescere di **K** aumenteranno i costi di installazione e gestione **X(K)** con:

$$X(K) = X_i(K) + \sum_{n=1}^{5} F_n^t \; X_{gn}(K)$$

mentre si ridurrà il costo del rischio **Y(K)** con:

$$Y(K) = \sum_{n=1}^{5} F_n^t \; Y_n(K)$$

I risultati potranno quindi essere riportati in un grafico



Dall'esame del caso ipotizzato nella figura, il sistema di sicurezza che comporta il minimo costo totale atteso risulterebbe quello numero 4.

Tuttavia, in considerazione dell'aleatorietà della determinazione del costo del rischio, è consigliabile interpretare il risultato di una analisi del tipo proposto.

In particolare, se l'adozione di un sistema di sicurezza più sofisticato (n. 4 anziché n. 3) comporta una riduzione del costo totale (a) modesta rispetto all'incremento del costo del sistema di sicurezza (b), potrebbe risultare opportuno dare la preferenza al sistema di sicurezza di grado inferiore.

VALUTAZIONE ECONOMICA DELLA SICUREZZA

Il procedimento di ottimizzazione presentato può apparire eccessivamente teorico.

In effetti non sempre l'analisi dei costi e benefici può essere applicata in modo quantitativamente rigoroso al problema di scelta del miglior livello di sicurezza nell'EDP.

Vi sono tuttavia numerosi problemi, anche di portata più limitata, che possono essere affrontati con tale metodologia, ottenendo ottimi risultati concreti