



Proposte per attività in tema di analisi delle contromisure informatiche

Orsenigo

Hacking Team S.r.l.	http://www.hackingteam.it
<i>Via della Moscova, 13 20121 MILANO (MI) - Italy</i>	info@hackingteam.it
<i>Tel. +39.02.29060603</i>	<i>Fax +39.02.63118946</i>

STORIA DEL DOCUMENTO

Versione	Data	Modifiche Effettuate
1.0	Maggio 2008	Prima emissione

INFORMAZIONI

Data di Emissione	Maggio 2008	
Versione	1.0	
Tipologia Documento	Allegato tecnico ad offerta	
Numero di Protocollo		
Numero Pagine	5	
Numero Allegati		
Descrizione Allegati	1	
	2	
Redatto da	Costantino Imbrauglio	
Approvato da	Gianluca Vadruccio	

INDICE

1	Introduzione	4
2	Attività di analisi del sistema informativo	5

1 Introduzione

Il Gruppo ELDOR ha ravvisato la necessità di introdurre un insieme di contromisure volte a ridurre il rischio informatico. Parte delle contromisure sono di natura tecnologica e parte di natura organizzativa.

Oggetto del presente allegato tecnico è la formulazione di un insieme di proposte mirate all'analisi dello stato delle infrastrutture tecnologiche che costituiscono il sistema informativo del Gruppo ELDOR dal punto di vista della sicurezza informatica.

2 Attività di analisi del sistema informativo

Obiettivo dell'attività di analisi è verificare lo stato del sistema informativo aziendale del Gruppo ELDOR dal punto di vista della sicurezza. In particolare si tratta di un'attività di analisi dei meccanismi di controllo (contromisure) in essere.

Ad oggi il Gruppo ELDOR non ha inteso adottare un modello standard per il governo del rischio informatico (Es. ISO 27001). Ciononostante ha comunque provveduto a implementare un certo insieme di contromisure a tutela del proprio sistema informativo.

L'analisi dei meccanismi di controllo in essere dovrebbe essere condotta facendo riferimento a un qualche modello di categorizzazione. Ciascuno standard orientato al governo del rischio informatico propone una sua categorizzazione dei meccanismi di controllo (contromisure).

La mancata adozione di un modello standard per il governo del rischio informatico da parte del Gruppo ELDOR non permette di analizzarne le contromisure in termini di uno specifico criterio di categorizzazione. Procederemo pertanto ad analizzare l'efficacia e lo stato dell'insieme dei seguenti meccanismi di controllo:

- Contromisure a protezione delle infrastrutture di comunicazione geografica
- Contromisure a protezione dell'infrastruttura SAP
- Contromisure a protezione degli ambienti di ricerca e sviluppo
- Data backup
- Contromisure a protezione di altri servizi
- Contromisure fisiche

L'attività è quantificata in 8/10 gg./uomo.

La tabella seguente dettaglia analiticamente la stima dell'effort per ciascuna fase con riferimento all'impegno di affiancamento del personale interno del Gruppo ELDOR.

Tabella di stima dell'effort		
Attività	Stima effort	Stima affiancamento
Raccolta informazioni	da 3 a 5 giorni	da 3 a 5 giorni
Analisi e stesura documentazione	5	non prevista

Tabella 1 - Tabella di stima dell'effort