

La Gestione della Sicurezza Informatica nelle Aziende

**L'importanza di una corretta impostazione
delle politiche di sicurezza**

Paolo Da Ros

Membro del Direttivo CLUSIT



**Associazione Italiana per la
Sicurezza Informatica**

**Firenze
29 gennaio 2003**

L' importanza della information security policy

1. Cio' che la policy *non deve* essere:
 - Una serie di ovvietà
 - Un bel binder dietro la poltrona del security manager
2. Cio' che la policy *puo'* essere (*low-level policy*):
 - Linee guida sull' uso dell' e-mail
 - Regole tecniche per l' uso di un sistema particolare
3. Cio' che *qui* intendiamo per security policy
 - La documentazione delle decisioni relative alla information security

La security Policy di alto livello (un esempio)

Lo scopo delle politiche per la sicurezza delle informazioni della Società XYZ e' di proteggere risorse vitali quali le informazioni e le risorse informatiche aziendali consentendo simultaneamente:

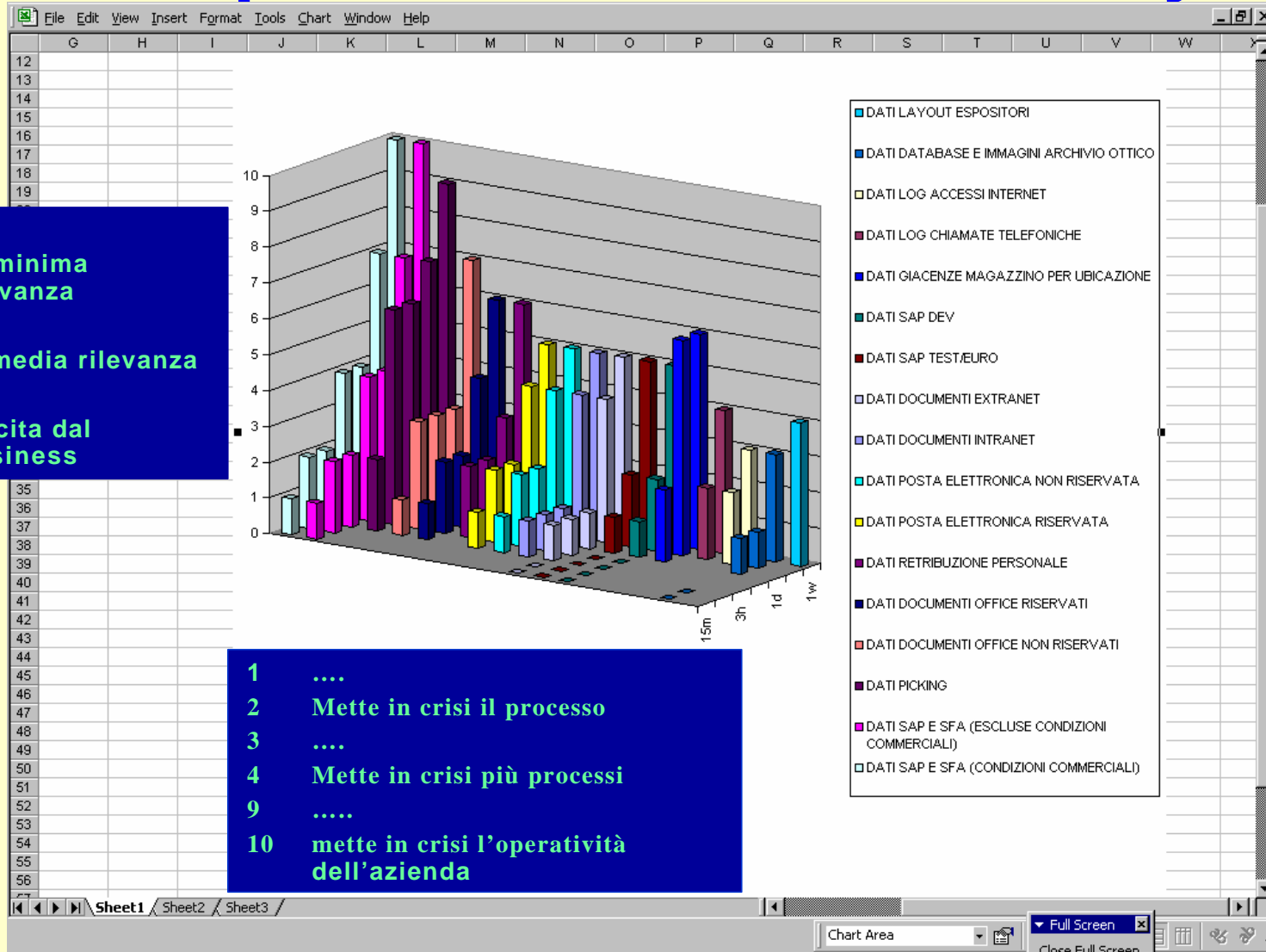
- 1) Comunicazioni via e-mail sia all' interno che all' esterno della Società';
- 2) Trasferimento di informazioni all' interno ed all' esterno della Società' e
- 3) Accesso al portale ed ai server aziendali ai Clienti, Partners e utenti interni secondo I criteri dettagliati nel seguito.

Inoltre essa definisce le politiche per la protezione dei dati all' interno della Società', il rispetto delle Leggi vigenti, e risponde alle esigenze di Confidenzialita', Integrita e disponibilita' dei dati, di Responsabilita' e di verificabilita' di cui ogni Collaboratore della Società' deve essere consapevole e che chiunque, all' interno della Società', deve rispettare e far rispettare.

Dalla policy di alto livello alle politiche operative:

L' output della Risk Analysis

- 1
- 2 Di minima rilevanza
- 3
- 4 di media rilevanza
- 9
- 10 uscita dal business



- 1
- 2 Mette in crisi il processo
- 3
- 4 Mette in crisi più processi
- 9
- 10 mette in crisi l'operatività dell'azienda

Come e' fatta una Security Policy, e cosa Contiene (di solito)? (1)

1. Obiettivo.

Descrive l'importanza che l'Organizzazione attribuisce alle informazioni e la volonta' dell'organizzazione di difenderne confidenzialita', integrita', disponibilita'.

2. Applicabilita'.

Definisce i beni aziendali regolati ed i soggetti tenuti al rispetto della Policy (dipendenti, consulenti, partner commerciali...)

3. Responsabilita'.

Definisce quanto gli utenti (dipendenti, dirigenti, addetti alla sicurezza) sono tenuti a fare per ottemperare alla SP. Puo' contenere indicazioni relative alle responsabilita' di un reparto particolare dell'Azienda, o di un Dirigente

Come e' fatta una Security Policy, e cosa Contiene (di solito)? (2)

4. Sicurezza fisica.

Definisce il modo in cui l' Azienda protegge i propri beni materiali. Potrebbe contenere la descrizione delle modalita' e dei criteri di accesso alle aree riservate; potrebbe descrivere i doveri del responsabile della sicurezza

5. Sicurezza della rete.

Definisce le modalita' di protezione degli assets accessibili via rete. Puo' descrivere

6. Sicurezza del software.

Definisce le modalita' di utilizzo di software commerciale e non commerciale, responsabilita' di installazione e manutenzione su PC, server e sulla rete; potrebbe contenere le regole che stabiliscono modalita' di download da Internet

Come e' fatta una Security Policy, e cosa Contiene (di solito)? (3)

7. Business Continuity / Disaster Recovery.

Definisce il modo in cui l' Azienda garantisce la continuita' delle proprie attivita' legate al trattamento delle informazioni.

Puo' contenere la lista delle persone che costituiscono l' Emergency Response Team, il cui intervento e' previsto in caso di disastri o di attacchi

8. Uso accettabile.

Definisce gli utilizzi accettabili delle risorse aziendali; potrebbe contenere una descrizione dei contenuti inviabili via e-mail al di fuori dell' azienda, o la liceita' di utilizzare il PC aziendale a scopo ludico.

Come e' fatta una Security Policy, e cosa Contiene (di solito)? (4)

9. Consapevolezza degli utenti.

Descrive le modalita' di istruzione degli utenti sulla security policy, e le modalita' di verifica della conoscenza della SP.

10. Rispetto della policy.

Descrive le modalita' adottate dall' Azienda per fare rispettare la SP. Potrebbe specificare le sanzioni per coloro che non ottemperano alla SP

6. Alcuni esempi(1):

Gestione dei virus (Basso livello di rischio) :

Gli utenti saranno informati sulle attività che comportano il rischio di importare *malicious code*;

Gli utenti devono riferire agli amministratori di rete di ogni virus rilevato, di cambiamenti avvertiti nel comportamento del computer; in caso di rilevamento di un virus, tutti gli utenti che hanno accesso allo stesso programma o agli stessi dati verranno informati del rischio che corrono e delle azioni da intraprendere per verificare la presenza di un virus sulla loro macchina e nel caso, rimuoverlo; gli utenti informeranno gli amministratori dell'esito dei test effettuati;

Ogni macchina sospettata di essere infettata da un virus va immediatamente sconnessa dalla rete; la macchina non potrà essere connessa alla rete finché il virus non sia stato rimosso;

Se non sarà stato possibile rimuovere il virus, tutto il software necessario all'uso della macchina andrà reinstallato da media sicure.

6. Alcuni esempi (2):

Gestione dei virus (Medio livello di rischio) :

L' addestramento degli utenti dei sistemi a medio livello di rischio includerà l' approfondimento delle problematiche legate ai virus;

Per contenere il rischio di diffusione dei virus il software antivirus andrà installato sui file server; l' esecuzione dell' antivirus verrà effettuata giornalmente; le postazioni di lavoro disporranno di sw antivirus che controllerà tutti i files mano a mano che arrivano sul PC; verranno controllate tutti i messaggi e-mail; i programmi non potranno essere eseguiti, ed i files suscettibili di includere macro virus non potranno essere aperti senza essere preventivamente controllati.

I log prodotti dagli antivirus verranno memorizzati ed esaminati dagli amministratori di rete;

Un computer su cui venga rilevata la presenza di virus dovrà essere immediatamente sconnesso da tutte le reti cui sia collegato

Conclusioni

- E' importante documentare le politiche sia di alto livello che di livello operativo
- La politica deve rispondere alle domande "Cosa devo proteggere, e da cosa"?
- Non esiste security policy senza assegnare responsabilita' (e budget)
- E' importante formalizzare gli usi accettabili
- Formazione e verifica della conoscenza della SP
- Sanzioni per chi non ottempera

Grazie!!