

# Network Security Service Solution



<http://www.infosec.it>

[info@infosec.it](mailto:info@infosec.it)

**Internet e Security Conference**  
**4 aprile 2001 – Guttadauro Sistemi srl**

*Relatore : Stefano Venturoli*

---

*Internet e security conference - Presentazione - Pagina 1*

© 2001 Infosec srl - E' vietata la riproduzione di questo documento o sue parti in qualsiasi forma e su qualsiasi supporto.



# Introduzione

- Internet rappresenta un bacino d'utenza stimato sopra i 300 milioni di utenti (dati del 2000)
- 1^ PROBLEMA: Il mondo digitale (Internet) si rispecchia nel mondo reale e viceversa.
- Anche i delinquenti usano Internet
- 2^ PROBLEMA: Attraverso Internet non vi sono confini territoriali
- Nel mondo reale, lascereste la vostra azienda con porte e finestre socchiuse? Senza vigilanza? Senza un sistema d'allarme?
- Se la risposta e' NO, “forse” avete un problema.

# Le soluzioni software e hardware esistenti

- Le soluzioni software e hardware esistenti sul mercato sono indispensabili
- Tali soluzioni vanno integrate in maniera adeguata per coprire eventuali fattori di rischio umano/organizzativo
- Oggi le aziende ricorrono all'outsourcing per la risoluzione dei loro problemi
- Ricorrono a società' specializzate nelle quali ripongono i propri problemi con grossa serenita'

# Le esperienze maturate nell'analisi al problema e nella sua risoluzione

- NetProbing (Scan e penetration testing)
- Secure Planning (Progettazioni e Riprogettazioni)
- Secure System (Hardening e configurazioni particolari)

# NetProbing

- L'amministratore di sistema mi ha garantito che i nostri sistemi informatici sono sicuri. Perche' dovrei fare una verifica?
- Perche' un test di sicurezza?
- Perche' in outsourcing?
  
- Potremmo rispondere con: *Chi controlla il controllore?*
- Non sempre l'amministratore ci rende partecipi dello stato di fatto.

# Responsabilita'

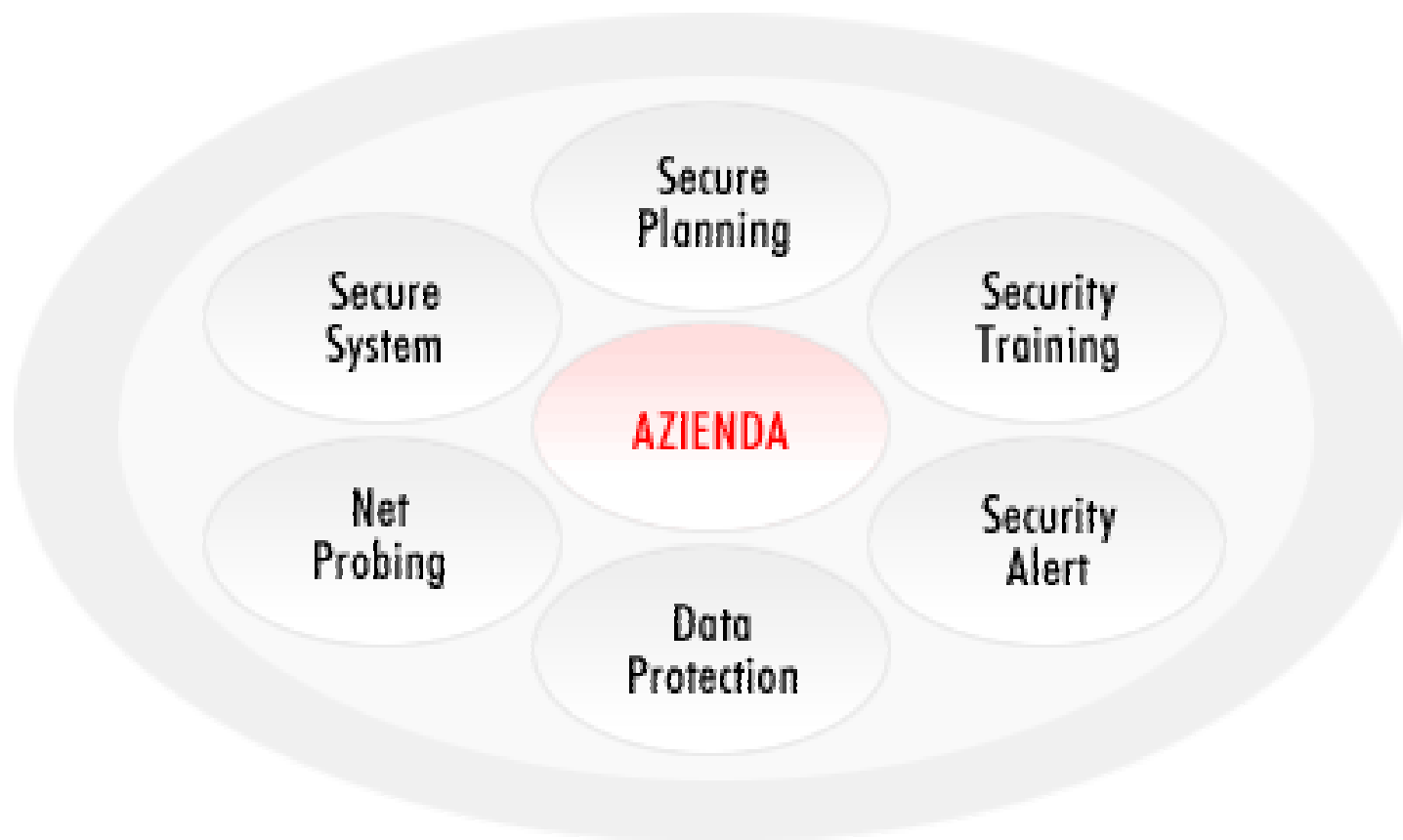
Il responsabile della sicurezza ed il responsabile del trattamento dei dati personali sono i principali soggetti ad essere direttamente coinvolti; a loro vengono **DELEGATE** queste funzioni, a loro ci si rivolge quando sorgono i problemi.

- Il Test di Sicurezza permette a tutti i soggetti di accertare e documentare la corrispondenza tra lo stato di fatto e lo stato dell'arte richiesto dalla Legge (L.675/96 e DPR318/99).
- Permette di assumere le proprie responsabilita' in modo chiaro, senza essere soggetti a rischi di cui non si è a conoscenza e individuare le aree di scarsa protezione.
- Fornisce informazioni preziose per la predisposizione di un solido piano di sicurezza.

# NetProbing Infosec VS Scan generici

- L'analisi di un computer o di una struttura di rete complessa richiede un'approccio particolare e personalizzato che un programma OpenSource o Commerciale non sara' MAI in grado di fornire
- I programmi non bastano, serve un tecnico che a mano vada a vedere la realta' dei fatti
- Il problema dei falsi positivi

# Secure Planning



# Secure Planning

- Installare una struttura di networking senza essere a conoscenza dei rischi e delle problematiche di sicurezza e' un azzardo che nessuno oggi puo' piu' permettersi.
- Una rete mal progettata aumenta esponenzialmente i rischi e presenta spesso problemi di difficile soluzione, anche nel tempo.
- Il miglior sistema di sicurezza per la Vostra rete, e' la corretta progettazione ed installazione di ogni sua componente.

# Secure System

- Hardening (rendere sicuro il software o il sistema operativo in uso)
- Configurazioni particolari
- Eliminazione delle configurazioni inadeguate
- Certificazioni dei maggior produttori software e hardware

# Metodologia e Know-how specifico

- Policy Planning (organizzazione e tutela)
- Check up (controllo dello stato di fatto)
- Security Assessment Planning (un supporto specifico entro 24 ore dalla chiamata)

# Policy Planning

- Un documento basato sui “Common criteria” che guida in una analisi del sistema azienda o ente pubblico per definire una corretta politica di sicurezza con lo scopo di evitare l’errore umano nelle operazioni, di “difendere” i dati da utilizzi non consentiti o da accessi non autorizzati, e quindi portare il valore aggiunto di una guida pratica di compilazione a una stesura di un documento completo ed efficace.

# Policy Planning = Valore aggiunto

## A cosa serve?

- A tutelarsi legalmente dal DPR 318/99
- A tutelarsi legalmente dai propri dipendenti per un'uso scorretto delle risorse che l'azienda mette a disposizione
- Come integrazione al proprio regolamento aziendale (ISO, etc.)
- A organizzare nel dettaglio le procedure

# Check-UP

## Per chi ha o puo' avere un problema

- Individua i problemi di sicurezza
- Ne valuta il rischio
- Viene riprogettata la realta' sulla valutazione dei punti precedenti
- Viene rilasciata una certificazione

# Security Assessment Planning

## Cos'è?

- Nello sforzo di aiutare le aziende quando effettivamente ne hanno bisogno e poterle soccorrere in un tempo massimo di 24 ore lavorative dalla chiamata, Infosec confeziona il suo know-how e lancia un nuovo servizio online

# Security Assessment Planning

## A cosa serve?

- A chi vuole un'esperto per la risoluzione di un problema specifico
- Quando le proprie risorse non sono disponibili e non si puo' rimandare
- Quando il problema e' critico e serve la tempestivita'
- Quando il konw-how non basta

# La consapevolezza = Fattore rischio!!

- Privacy Service (Misure minime di sicurezza previste per legge)
- Security Training (corsi per amministratori, CED, e responsabili di networking)

# Privacy Service

- Misure minime di sicurezza previste per legge dal DPR 318/99 (trattamento dati sensibili)
- Documento Programmatico ai fini del DPR 318/99
- ES. Pubblica amministrazione, Ospedali, realta' aziendali con collegi sindacali, chiunque tratti dati sensibili
- Infosec e' in grado di fornire il supporto tecnologico, organizzativo e legale per la corretta adozione delle misure minime previste dal DPR.318/99.

# Security Training

- Per ridurre al minimo le vulnerabilità connesse al fattore umano, una politica di sicurezza adeguata deve prevedere un piano di formazione del personale, in relazione alle funzioni svolte ed al livello di esposizione al rischio.
- La formazione deve ottenere obiettivi concreti di sensibilizzazione sulle problematiche e sulla loro importanza e permettere la conoscenza delle misure di sicurezza da adottare e da gestire ai diversi livelli di responsabilità

# Security Training

- Infosec propone i seguenti corsi di base e avanzati:
- Norme di sicurezza per l'utenza
- Network security base (generale)
- Security vulnerabilities per amministratori (debolezze della rete)
- Computer security per amministratori (debolezze dei sistemi)
- Realizza corsi su richiesta per esigenze specifiche.

# Non e' un Costo, e' un Investimento!!!

- Quanto vale il patrimonio aziendale?
- Che valore ha il nostro database?
- Possiamo permetterci una perdita o una compromissione dei nostri dati aziendali?
- La ns. vetrina sul Web rispecchia l'immagine aziendale, e se domani contenesse pubblicita' negativa verso i nostri servizi e prodotti?

# Esempio a scopo didattico

- <http://www.attrition.org/mirror/attrition/months.html>

# I costi

- Per le diverse tipologie di soluzioni previste, si può immaginare di fare una proporzione tra il costo di un'automobile con il costo del suo antifurto e i costi che un'azienda sostiene tra software, hardware, impianti, cablaggi, utenti, manutenzione, etc. e la sua messa in sicurezza
- Il rapporto è identico

# Conclusioni

- Come in tutte le cose fatte a regola d'arte, serve un'approccio globale e complessivo
- Si deve capire il problema nella sua forma “astratta”
- **L'unica soluzione possibile e' la riduzione dei rischi**

# Your Business is Internet exposed?

→ <http://www.infosec.it> ←

*Noi possiamo aiutarvi*

Product&Service Reseller:

<http://www.guttadauro.com>