

La sicurezza su Internet



<http://www.infosec.it>

info@infosec.it

Relatore : Stefano Venturoli

Sommario

- 1) L' obiettivo di questa presentazione è cercare di capire di cosa stiamo parlando in termini di sicurezza e di Internet
- 2) Di analizzare i rischi e le problematiche annesse
- 3) Gli approcci al problema

La sicurezza in generale come concetto oggettivo o soggettivo

- a. Siamo abituati a comprare un antifurto per le nostre automobili (oggi è di serie, 10 anni fa, no)
 - ✓ Con il problema in crescita, si ricorre a una soluzione "standard" o di serie (Firewall, IDS, VPN, etc.)
- b. Dotiamo le finestre di casa al piano terra di inferriate, oppure usiamo sistemi d'allarme e porte blindate (nelle grandi città si, nei paesi, no)
 - ✓ Diventa una necessità nel contesto operativo nel quale si opera (sicurezza azienda, sicurezza clienti, DPR318/99, etc.)
- c. Nella Formula 1, i collegamenti radio tra le macchine in gara, i box e i pit-stop sono crittografati
 - ✓ Diventa un fattore soggettivo a seconda del contesto nel quale si opera (HomeBanking, B2B, B2C, etc.)

"Il problema Internet" 1/2

Dove nascono i problemi

- Internet rappresenta un bacino d'utenza stimato sopra i 400 milioni di utenti (dati del 2001)
- ✓ 1° PROBLEMA: il mondo digitale (Internet) si rispecchia nel mondo reale e viceversa.
 - Anche i delinquenti usano Internet
- ✓ 2 ° PROBLEMA: su Internet non vi sono confini territoriali
- ✓ 3 ° PROBLEMA: Stiamo utilizzando una tecnologia vecchia di 30anni che non e' nata per applicazioni di E-Commerce o per garantire sicurezza

“ Il problema Internet” 2/2

Dove nascono i problemi

- Per far fronte ai problemi legati alla tecnologia in uso, possiamo parlare di fw, di ids, di vpn ma la struttura di base per la comunicazione rimane sempre la stessa
- Si possono costruire sw migliori, quindi fw più efficienti, ma non risolviamo il problema alla radice
- Di fatto, nelle comunicazioni digitali esistono problematiche tecniche “non risolvibili” (protocolli di comunicazione e applicativi, standard, etc.)
- E' una necessita' affrontare la sicurezza come progetto complessivo, e non affidarsi unicamente a dei prodotti

Non esiste la sicurezza assoluta

- Esistono soluzioni Hardware e Software ma, per la natura intrinseca di questi prodotti, non saranno mai sufficienti al problema: Comprare un Firewall non vuol dire essere sicuri, vuol dire aumentare le proprie difese
- Non esiste e non esisterà mai una soluzione definitiva o standard per tutti: E' un processo sempre in divenire

Analizzare il proprio status

- Così come non esiste un modello di Business standard per ogni campo commerciale, così non esiste una soluzione standard di security per i propri problemi
- Non si può ricorrere a soluzioni “magiche”
- La soluzione ai propri problemi deve essere studiata e analizzata punto per punto

Domande da porsi:

- Mi serve? (Cosa facciamo? In che ambito operiamo? E' un problema reale?)
 - Cosa vogliamo proteggere? (dati, computer, flussi di informazioni, etc.)
 - Cosa possiamo fare a riguardo? Quali tra tutte le soluzioni proposte dal mercato possono interessarmi?
 - A chi mi rivolgo?
-
- SOLUZIONE: Dipende **sempre** da cosa si deve fare
 - LA SOLUZIONE: Deve conformarsi alle esigenze aziendali

Il “mito” Firewall

- Prima di comprare un firewall a volte è meglio eseguire un servizio di assessment o Risk Analysis
- Con un'analisi dei rischi, è possibile identificare a monte:
 - 1) A che tipo di rischi si va incontro
 - 2) Cosa proteggere, come, dove e perché
 - 3) Se è necessario munirsi di Firewall o di altre tecnologie
 - 4) Identificare le giuste soluzioni a fronte di un'investimento migliore

Problemi interni e/o esterni

- Da cosa proteggersi? Da Internet?, dai dipendenti?, Da entrambi?
 - Furto, modifica, cancellazione di informazioni e dati
 - ✓ Sono il patrimonio aziendale!!!
 - Server e servizi compromessi
 - ✓ Sono gli strumenti aziendali!!!
 - Problemi legali
 - ✓ Responsabilita' penali e D.P.R. 318/99

La "sicurezza" non esiste

- Di sicuro (quindi perfetto) non esiste nulla
- La sicurezza informatica è uno status da raggiungere:
 - ✓ Aggiungere sempre livelli di security
 - ✓ Tenere aggiornate le proprie soluzioni (applicativi, server, etc.)

Sono le soluzioni che garantiscono maggiore sicurezza

Outsourcing? O gestione interna?

- ASP (Application Service Provider) ci risolve il problema?
 - Vantaggi:
 - ✓ Costi minori, licenze, supporto IT interno, etc.
 - Svantaggi:
 - ✓ Non è detto che un ASP sia in grado di gestire la sicurezza, e quindi di tutelare i Vs. dati
 - ✓ Clausole contrattuali

Conclusioni 1/2

- E' da capire se ci serve, in che contesti e con che modalità
- Dobbiamo individuare a chi rivolgerci e per cosa:
 - ✓ In qualsiasi contesto operativo esistono le specializzazioni:
Nella costruzione di un ponte o una diga, ci si avvale di Ingegneri specializzati in materia, non di Ingegneri generici
- Per la sicurezza informatica, ci si deve rivolgere a tecnici specializzati in sicurezza informatica

Conclusioni 2/2

Dobbiamo ridurre gli attacchi

- Esistono i mezzi per ridurre drasticamente i rischi
- Esistono esperienze consolidate nel tempo
- Esistono metodologie, know-how specifici, soluzioni dedicate
- Avere uno staff preparato e sensibile alla sicurezza
- Utilizzare una varietà di strumenti coordinati (Policy, Antivirus, Firewall, IDS, VPN, etc.)
- Venire costantemente verificato ed aggiornato
- Non affidarsi unicamente alla tecnologia

Your Business is Internet exposed?



<http://www.infosec.it>

info@infosec.it

Noi possiamo aiutarvi