Gestire L'Insicurezza Quotidiana dei Sistemi Informativi

Andrea Pasquinucci
Comitato Direttivo AIPSI

Ieri ... Oggi ... Domani ...

- Cosa ci dobbiamo aspettare ?
- Considerazioni basate sulla mia esperienza personale
- Qualche provocazione a fin di bene

Domanda:

- Nel 1985 comprai il mio primo PC per sostituire la macchina da scrivere
- Quanti **OGGI** pensano che il PC usato quotidianamente non sia altro che la **versione moderna della macchina da scrivere**?
- Quanti hanno coscienza della **differenza** tra un PC in rete ed una macchina da scrivere + fax ?

Anni '80

- Elaboratori ==> Camici Bianchi

Anni '90

- PC
- Reti (locali [dialup] e lunga distanza)
- Applicazioni
- Web

==> **Diffusione su larga scala**

Oggi

- Diffusione di massa di una tecnologia

  ==> **Trasformazione in Commodity** !!

- Primi segnali già presenti:
  - Non è più necessario essere dei tecnici per configurare, gestire e usare strumenti informatici
  - “Scatole” sempre più “nere”
  - “Scatole” sempre più simili ed inter-operanti

Esempio Firewall

Ieri:

- Pila ISO/OSI
- protocolli/porte
- Stateful Inspection
- Proxy
- Antivirus
- Filtri
- ...

Oggi:

- Bottone: permetti traffico web da LAN => Internet
- Bottone: permetti traffico web da Internet => server in DMZ

Possibile Scenario

3 tipi di attori:

- **Produttori** => tutti i problemi tecnici, di sicurezza e di integrazione (scatola nera)
- **Gestori** => combinano gli strumenti (senza conoscerne i dettagli) per realizzare e gestire i servizi
- **Utenti** => totale ignoranza della tecnologia, pigiano bottone per ottenere risultato

I Problemi di Chi Gestisce

- Non c'è bisogno di essere dei tecnici
- **Non si può** essere dei tecnici
- Deve scegliere, integrare, configurare e gestire correttamente gli strumenti per:
  - Offrire i servizi
  - Garantirne prestazioni, continuità, qualità, sicurezza (nel senso più lato del termine) ecc.

Attacchi

- Prestazioni, continuità, qualità: a carico del produttore
- Difese del sistema informativo sono un problema anche, o meglio principalmente di chi gestisce!

- Breve storia dei tipi di attacchi:

Attacchi nel tempo

- Anni '80: ambienti universitari per scopi dimostrativi
- Anni '90: hackeraggio, a volte goliardico/competitivo, aumento dei danni
- 2000: Script-Kiddies, riduzione competenze tecniche, aumento diffusione e dei danni

Attacchi Oggi

Malavita organizzata

- Sistemi informatici non più scopo dell'attacco ma mezzo
  - **Scopo** è: rapina, furto, estorsione, truffa, terrorismo, lotta politica ...
  - **Mezzo** è: pistola, bomba, coltello, virus, DoS, worm, trojan, rootkit ...

Esempio di attacchi

- Virus/worm/Trojan mirati, distribuiti via email, CD dimostrativi, ecc.
- Spionaggio industriale (costi per aziende stimati in USA 2005 in $200 Billion)
- *Target Eye* di Michael & Ruth Haephrati (Israele/UK 2005/2006)
- Aumento: da 1/week in 2005, 1/day in 2006 (MessageLabs)

Difesa dagli attacchi

- Per difenderci non bastano le misure tecnologiche, perché la tecnologia non è lo scopo dell'attacco
- L'attaccante usa la tecnica che ritiene più efficace
- Difesa deve basarsi sull'oggetto dell'attacco, il possibile attaccante ed i possibili mezzi di attacco

Vulnerabilità

- Produttori hanno preso a cuore la sicurezza
  - Vulnerabilità minori meno frequenti
- Vulnerabilità ci sono ancora
  - Spesso sono **gravi** => crollo totale del sistema

Esempi Vulnerabilità

- Ben note:
  - Browser (Internet Explorer, Firefox ...)
  - Media Player
  - ...
- Meno nota: Firme Digitali RSA con esponente 3 (standard imprecisi [ASN.1, PKCS#1] con implementazioni imprecise)

Rischi

- Aumento gravità vulnerabilità anche se ridotte in numero
- Aumento numero utenti, sistemi e connessioni
- Aumento velocità di connessione
- Aumento importanza e numero applicazioni
- Aumento numero di transazioni

==> **Aumento dei rischi**

Fattore Umano

- Molte vulnerabilità sono sfruttabili solo tramite un'azione dell'utente (inconsapevole)
  - Cliccare il bottone è pericoloso!
  - Perché la tecnologia sottostante non è matura
- Necessità di gestire il **Fattore Umano**
- **L'Uomo è oggi il punto più debole**

Gestire l'Uomo

- Soluzioni tecniche a problemi tecnici sono indipendenti dal contesto
- Soluzioni ai problemi di gestione, in particolare del fattore umano, dipendono crucialmente dal contesto
  - **Metodi** per affrontare i problemi
  - **Non tecniche** per risolvere i problemi

Storiella...

Anni '80 Yosemite National Park:

- Gli orsi svuotano i cestini dei rifiuti, avvicinandosi ai visitatori => pericolo per l'uomo
- Soluzione: Cestini con chiusura di sicurezza
- Ma ... Said one park ranger:
  There is considerable overlap between the intelligence of the smartest bears and the dumbest tourists.

Esempi

- Perdita device mobili: PC portatili, smart phone ecc.
- Phishing (ultima moda con notizie ANSA, Reuters in Italiano ecc.)
- Download da siti web
- Social Engineering
- Perdita nastri di backup...

Gestione e Controllo

- Cambiano i problemi:
  - Non più conoscere ed implementare la tecnologia
    - Ridotte esigenze di verifica delle configurazioni e delle implementazioni tecniche
  - Piuttosto gestire i sistemi e le persone dal punto di vista delle informazioni
    - Capire i problemi dal punto di vista del business e verificare che le soluzioni adottate siano coerenti

Approccio

- Dall'alto
- A 360 gradi
- A partire dal business
- Capire cosa si deve proteggere, cioè a cosa un attaccante può essere interessato
- Indipendentemente dalla tecnologia

Approccio - 2

- Concentrandosi sui processi e flussi di informazioni
- Partendo dalle politiche aziendali e di sicurezza allineate al business
- Tenendo conto di come un *uomo può utilizzare una tecnologia che non conosce/capisce*
- (Vedi ad esempio Cobit 3 vs. Cobit 4, ISO27001/BS7799, ITIL ...)

In pratica

- Firewall ed Antivirus sono questioni tecniche, se ne occupa il produttore
- Le politiche aziendali sulla gestione delle informazioni sono la base su cui si fonda la sicurezza dell'azienda, non il firewall + antivirus!
- **Addio all'approccio tecnologico!**

Analisi dei rischi - 1

- Elenco servizi, elaboratori e disegno rete
  - *Lista e flusso delle informazioni*
- Sistemi critici
  - *Personale/funzioni critiche*
- Vulnerabilità dei sistemi/OS/applicazioni
  - *Vulnerabilità dei processi/flussi informazioni*

Analisi dei rischi - 2

- Attacchi via rete/DoS/worm/virus
  - *frodi/impersonificazioni/social engineering/ errori di gestione/implementazione...*
- Misura dei rischi: quali oggetti e quali metriche?
  - Misura dell'oggetto sbagliato
  - Uso della metrica sbagliata

Analisi dei rischi - 3

- Approcci dall'alto semplificati:
  - **Due Diligence**: omogeneità delle misure
  - **Compliance**: adozione misure obbligatorie
  - **Enablement**: Best-Practice ecc.
- *Capability Maturity Model* per valutare lo stato di applicazione delle misure e dei controlli e quindi gestire i rischi

La Sfida

- Far scendere in pratica gli *Information Security Management System* sino ad incontrare la tecnica
- Salire dall'approccio puramente tecnico ad uno che coinvolga anche la gestione delle informazioni e delle persone
- E' un problema di Uomini! Ci manca il

Man-in-the-Middle

Riferimenti

- A.P., *Il CISO: un ruolo tra mito e realtà*, Chief Security Officer, 24-7-2006, http://www.nwi.it/
- A.P., *Gestire la (in-) Sicurezza Informatica,* ICTSecurity, Ottobre 2006
- A.P., *Abbandonare la Sicurezza Basata sull'Analisi dei Rischi ?*, ICTSecurity, Novembre 2006

Grazie

Andrea Pasquinucci

a.pasquinucci-At-aipsi.org

Socio Fondatore e membro Comitato Direttivo

AIPSI (Associazione Italiana Professionisti Sicurezza Informatica) - Capitolo Italiano ISSA

www.aipsi.org www.issa-italy.org

pasquinucci-At-ucci.it www.ucci.it

Copyright e Licenza