Troppe Informazioni

=

Poca Sicurezza ?

Andrea Pasquinucci
Comitato Direttivo AIPSI

Informazioni...

- La Sicurezza non si basa solamente sul nascondere le informazioni
- Ma quello che vogliamo proteggere sono le Informazioni
- Molte informazioni di poca importanza singola, insieme possono dare una informazione importante

Indice:

- Informazioni utili ad un attaccante
- Informazioni utili a chi deve proteggere un sistema informatico
- Come gestire la sicurezza dei sistemi informatici
- Conclusione:

Non c'è Speranza ?

Un attacco dall'esterno

- Come fare ad entrare?
- Per prima cosa bisogna sapere cosa c'è:
  - **Lista dei sistemi**
  - **Lista delle applicazioni**
  - **Lista degli utenti**
- Informazioni di solito facili da reperire

Repository Pubblici

- Dal **NIC**:
  - Nomi a dominio
  - Cognome, Nome, indirizzo, numero di telefono, fax, email del responsabile
- Dal **RIPE**:
  - Indirizzi IP
  - Routing
  - Cognome, Nome, indirizzo, numero di telefono, fax, email del responsabile

Repository Pubblici - 2

- Dal **DNS**:
  - Nome ed indirizzo server di posta
  - Indirizzi IP di server noti
  - Se è presente la risoluzione inversa dei nomi (da numero a nome), nome di tutte le macchine connesse ad internet
- Da **Google** ... *di tutto e di più:*
  - Indirizzi email
  - Pagine web con nome e versione dell'applicazione che le ha generate
  - ecc...

Un attacco dall'esterno - 2

- **Tutto questo senza connettersi alla rete da attaccare !**
- Connettendosi alle macchine in internet
  - Versioni sistemi operativi ed applicativi
  - Informazioni specifiche da
    - Server web
    - Proxy web
    - Server di posta elettronica
    - Server DNS
    - Domain controller MS
    - ecc...

Un attacco dall'esterno - 3

- Molto (troppo) spesso da questa analisi si è in grado di ottenere:
  - **Lista delle vulnerabilità dei sistemi in Internet**
  - **Lista dei possibili vettori di attacco dall'esterno**
  - **Lista delle reti private interne**
  - **Lista dei domini MS interni**
  - **Lista dei sistemi interni**
  - **Lista (parziale) di utenti interni**
  - **Ecc...**

Un attacco dall'interno

- Una volta che l'attaccante è riuscito ad entrare, *la guerra è praticamente persa*
- L'attaccante può connettersi via **WiFi** direttamente dall'esterno all'interno?
- L'attaccante può **entrare di persona** e connettere il proprio portatile?
- L'attaccante è un **dipendente**?

Un attacco dall'interno - 2

- Con le liste
  - **Delle reti**
  - **Dei sistemi**
  - **Delle applicazioni**
  - **Dei domini e degli utenti**
  - **Delle vulnerabilità**
  - **Dei vettori di attacco**
- È un gioco da ragazzi riuscire ad entrare dove non si dovrebbe

Un attacco dall'interno - 3

- Ad esempio
  - Sfruttare una vulnerabilità nota
  - Sfruttare un servizio aperto per test ma mai spento
  - Sfruttare un servizio attivato inavvertitamente
  - Sfruttare password deboli o di default
  - Ecc.
- Per diventare **amministratore** di una macchina qualsiasi e da li controllare tutta la rete

Difendersi oggi

- *Non è possibile eliminare del tutto le informazioni pubbliche*
- E' possibile ridurre le informazioni pubbliche
- E' possibile ridurre le vulnerabilità esposte
- E' possibile ridurre i vettori di attacco dall'esterno e dall'interno
- **Bisognerebbe poter controllare i sistemi per rendersi conto se un attacco è in corso** (od è avvenuto recentemente, i.e. nelle ultime 24 ore)

Controllo ed informazioni

- Per essere informati se un attacco è in corso, i sistemi devono inviare informazioni agli amministratori quali
  - **Chi** si è connesso ai sistemi (**dove** e **quando**)
  - **Cosa** sta facendo, ovvero quali
    - Applicazioni
    - Dati
    - Risorse

  sta utilizzando, leggendo, creando, modificando ecc.

Controllo ed informazioni - 2

- Queste informazioni dovrebbero essere presenti nei **log** dei
  - **Sistemi Operativi**
  - **Database**
  - **Applicazioni**
- Ma ... molto (troppo) spesso **non ci sono**!
- E nel caso in cui ci fossero,
  - *Non si è in grado di estrarle*
  - *Nessuno le legge*!

Il problema Log

- I sistemi informatici registrano informazioni sul proprio funzionamento in archivi chiamati **Log** (file, tabelle di database ecc.)
- Di norma le informazioni registrate sono per il **Debugging** del sistema (spesso interpretabili solo da chi lo ha sviluppato) e **non per il controllo delle attività** (**Audit**)
- Ogni sistema registra informazioni di tipo diverso in formato diverso

Il problema Log - 2

- Di solito sono usati protocolli (syslog, snmp ecc.) che **non garantiscono** l'origine, l'integrità e la consegna dei messaggi
- Anche se le informazioni fossero presenti nei log:
  - Sono troppe
  - Non complete
  - In formati diversi non facilmente incrociabili

Il problema Log - 3

- Chi oggi prova a raccogliere i log per controllare le attività dei propri sistemi informatici, si trova
  - Una quantità enorme di informazioni
  - Dalle quali è difficile estrarre quelle utili
  - Che non si riesce a confrontare fra fonti diverse
  - Che non si sa dove archiviare
  - Che non si riesce ad analizzare in tempo
- **Troppe informazioni => Meno sicurezza !**

Il problema log - 4

- Questo problema sta diventando attuale
  - Sicurezza
  - Normative (i.e. Privacy)
- Stanno nascendo le prime soluzioni
- Molto da fare, poiché bisogna partire da come sono scritti tutti i programmi e **modificarli** per fare in modo che registrino le informazioni utili all'**Audit** e non solo al *Debugging*
- Mancano ancora **Standard** che aiutino a formalizzare il *cosa* e il *come*

Gestire la Sicurezza IT

- ***Non*** è solo una questione di **HW** (firewall ecc.)
- ***Non*** è solo una questione di **Politiche di Sicurezza**
- ***Non*** è solo una questione di **Personale**
- ***Non*** è solo una questione di **controlli periodici, certificazioni ecc.**
- ***E'*** anche una questione di **controllo e monitoraggio costante delle attività dei sistemi**

Conclusioni

C'è molto ancora da fare, ma se ci rimbocchiamo le maniche ...

c'è speranza

Copyright e Licenza

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

a.pasquinucci-At-integra-group.it www.integra-group.it