INFOSECURITY 2006 – 9 febbraio 2006

La difficile arte del compromesso fra semplicità e sicurezza in architetture complesse

ing. Andrea Gelpi
security @ gelpi.it
www.gelpi.it

La difficile arte del compromesso fra semplicità e sicurezza in architetture complesse

ing. Andrea Gelpi

- I computer sono al servizio dell'uomo e non l'uomo al servizio dei computer.
- Negli anni si è cercato di rendere questi strumenti sempre più semplici da usare
  - Si è passati dalla linea di comando dove si dovevano ricordare tutti i comandi e i loro parametri
  - al sistema a finestre dove basta un clic per lanciare comandi anche complessi e lunghi.
  - Si è passati da sistemi singoli non collegati ad altri dove i dati si trasportavano con le schede perforate, nastri magnetici, dischi magnetici o altri supporti
  - A sistemi sempre collegati ad una qualche rete sia essa locale e/o Internet

La difficile arte del compromesso fra semplicità e sicurezza in architetture complesse

ing. Andrea Gelpi

- La sicurezza era nulla nei primi computer (non serviva)
  - I computer erano isolati e stavano in locali chiusi
  - I dati non rimanevano dentro i computer, ma stavano su supporti esterni.
  - I dati erano pochi e relativamente importanti
  - ***Erano quindi sufficienti misure fisiche***

La difficile arte del compromesso fra semplicità e sicurezza in architetture complesse

ing. Andrea Gelpi

- La sicurezza è divenuta un elemento importante, vitale
  - I sistemi sono interconnessi a volte con più realtà differenti
  - I dati sono “in linea”
  - I dati sono quantitativamente più numerosi e più importanti dal punto di vista qualitativo.
  - Sempre più dati sono accessibili da terzi
  - Sempre più spesso non conosco chi accede ai dati
  - I supporti contenenti dati sono usati 24 ore al giorno
  - Oltre a problemi di sicurezza ho anche problemi di disponibilità dei dati

La difficile arte del compromesso fra semplicità e sicurezza in architetture complesse

ing. Andrea Gelpi

- La sicurezza delle informazioni pone limiti e restrizioni, rende più complesse le cose.
- Il modello usato è di origine militare ed è vecchio di centinaia di anni.
- Lo potremmo definire il **modello del castello**

La difficile arte del compromesso fra semplicità e sicurezza in architetture complesse

ing. Andrea Gelpi

- In un castello ci sono più forme di sicurezza (fossato, ponte levatoio, cinta muraria, porte, ecc...) a volte ripetute (più cinte murarie una dentro l'altra)
- Se un livello di sicurezza veniva compromesso, restavano gli altri a garantire la sicurezza degli abitanti.

- La sicurezza delle informazioni si realizza con sistemi simili ai castelli, cioè si realizzano più livelli di sicurezza
- Se un livello viene compromesso gli altri reggono e le informazioni restano al sicuro.

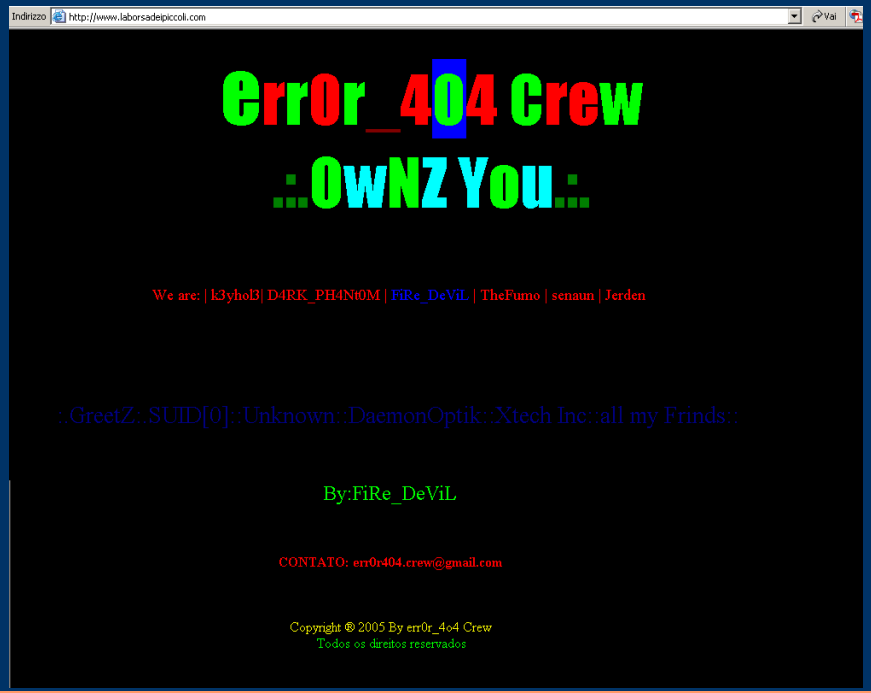
MA ...

- E' necessario che ci sia chi controlla le misure di sicurezza implementate, come nei castelli c'erano le guardie sulle mura.

La difficile arte del compromesso fra semplicità e sicurezza in architetture complesse

ing. Andrea Gelpi

- **Un castello senza guardie viene conquistato in poco tempo.**
- **Un sistema informatico senza controlli può essere compromesso in tempi brevi.**



La difficile arte del compromesso fra semplicità e sicurezza in architetture complesse

ing. Andrea Gelpi

- Sicurezza è sinonimo di complessità?
- Ogni componente aggiunto ad un sistema informatico lo rende più complesso e più vulnerabile
  - Un solo server che fa tutto può sembrare la soluzione migliore (bassa complessità), ma a fronte di un problema hardware ho tutto fermo.
  - Due server che si spartiscono le attività aumentano la complessità, ma diminuiscono la probabilità di restare completamente fermi in caso di guasti.
  - Un server per ogni servizio sembra essere la soluzione migliore. In caso di guasto ad un server si ferma un solo servizio.

- Esiste il rovescio della medaglia.
  - Quanto mi costa tenere in piedi tanti server (costo dell'hardware, della corrente elettrica, licenze sistema operativo, personale da dedicare alla manutenzione ordinaria e straordinaria, controlli di sicurezza, ecc...)
  - Ne vale la pena?
- La soluzione migliore è spesso un compromesso fra le risorse che ho a disposizione e che posso impegnare e un rischio più alto di andare incontro a qualche problema.

- Esempio
  - Firewall
    - Firewall con 2 interfacce (WAN e LAN) è poco flessibile e mi costringe a rischiare molto sul lato LAN
    - Firewall con molte interfacce è molto complesso e difficile da gestire. La complessità cresce al ritmo di Num. Int. * (Num. Int.+1)
    - La soluzione con 3 interfacce è forse la migliore nella stragrande maggioranza dei casi

- Errori nelle implementazioni
  - Ridondanza nelle alimentazioni, ma utilizzo unica presa di corrente.
  - Ridondanza di server alimentati tutti con lo stesso UPS
  - Ridondanza delle interfacce di rete, ma utilizzo di unico switch o router
  - Errori nelle configurazioni dei servizi

- Alcune regole valide sempre
  - Togliere tutto quello che non serve – o installare solo ciò che serve
  - Abilitare i servizi che servono solo sulle interfacce che servono
  - Usare firewall per permettere l'accesso solo da reti o postazioni note, evitare di lasciare servizi aperti al mondo
  - Servizi aperti al mondo valutare di cambiare la porta standard (esempio SSH su porta maggiore di 1024)
  - Ove possibile usare canali cifrati (SSL è sufficiente)

- Esempio
  - Posta elettronica con server interno
    - Server di posta messo in DMZ
    - Accesso al server di posta dall'esterno solo alla posta
    - Dall'esterno lettura della posta solo su canali cifrati e invio solo dopo autenticazione sempre su canale cifrato
    - Dall'interno posta inviata solo al server in DMZ
    - No posta che va diretta su Internet
    - Invio di posta autenticato anche sulla LAN
    - Valutare webmail mediante http proxy

- In realtà piccole il numero di server è un problema
- Viene in aiuto la virtualizzazione dei sistemi
- Xen è un sistema di virtualizzazione GPL
  - Creo un sistema minimale vuoto (dom0)
  - Dentro questo creo più server virtuali (domU)
    - Server di lan, server in dmz, web proxy, ecc...
    - Limite è dato dalla RAM disponibile
    - Limite dato dallo spazio disco disponibile
    - Limite dato dal numero di interfacce di rete (?)
    - La CPU di solito non è un problema

- Xen è un sistema di virtualizzazione GPL
  - Vantaggi di tale soluzione
    - I server non hanno accesso a dispositivi fisici
    - Comunicano tra loro solo tramite rete
    - Le connessioni di rete sono tutte controllate dal Dom0
  - Possibili punti di rischio per la sicurezza
    - La memoria
    - Le interfacce di rete

- Xen è un sistema di virtualizzazione GPL
  - Possibili soluzioni
    - Utilizzo più schede di rete (separo il traffico fisicamente)
    - Le schede di rete aggiuntive sono prive di IP a livello dom0
    - Proteggo le varie schede di rete con regole di firewall

- La soluzione appena vista è elegante, ma mi riporta al problema iniziale.
- **Ho un unico server fisico**
- Soluzione
  - Ridondare l'intero server con tutti i suoi sistemi.
  - Utilizzo quindi sistemi in alta disponibilità (High avalibility)
  - Esiste la possibilità di realizzare l'alta disponibilità con software Open Source sotto licenza GPL

- Utilizzo DRBD ==> mirror di partizioni fra sistemi
  - Due sistemi con installati gli stessi servizi
  - Utilizzo una scheda di rete dedicata per collegare fra loro i sistemi
  - Via DRBD tengo aggiornate una o più partizioni dati dei due sistemi
  - Vantaggi
    - Ho i dati in mirror su un altro sistema
  - Svantaggi
    - Se un sistema è non raggiungibile (problemi di rete, servizi down, sistema down) devo cambiare la configurazione a mano per raggiungere l'altro sistema

- Utilizzo Heartbeat ==> gestore alta disponibilità
  - Assegno un indirizzo virtuale ai due sistemi
  - Se un sistema è non raggiungibile, heartbeat cambia la configurazione e fa lo switch da un sistema all'altro
    - Tira giù i servizi sul server che non risponde
    - Dice a DRBD che non è più master
    - Spegne l'interfaccia di rete virtuale
    - Attiva l'interfaccia virtuale sul secondo server
    - Dice a DRBD sul secondo server che ora lui è master
    - Attiva i servizi sul secondo server
  - Interruzione del servizio può essere inferiore al minuto.
  - L'utente non si accorge di nulla.
  - Utile anche nei sistemi in round robin

- Importanza dei monitoraggi
  - Se i sistemi complessi non sono monitorati a seguito di due guasti ho l'interruzione del servizio.
  - Che cosa monitorare
    - Utilizzo CPU
    - Utilizzo Memoria e swap
    - Temperatura CPU e sistema
    - Monitorare i dischi per i guasti (SMART)
    - Monitorare i dischi per lo spazio libero
    - Utilizzo interfacce di rete (lo compresa)
    - Utilizzare software di analisi dei log
    - Se disponibili attivare le statistiche dei vari servizi

- Importanza dei salvataggi (BKUP)
  - Salvare non solo i dati, ma anche le configurazioni
  - Tenere i salvataggi in luoghi sicuri
  - Attenzione ai salvataggi su dischi rimovibili
  - Verificare che nei salvataggi ci sia tutto

GRAZIE
:-)

ing. Andrea Gelpi
security @ gelpi.it
www.gelpi.it
ICQ 275243598
Skype gelpi_andrea