smau MILANO 22-23-24 OTTOBRE 2014
FIERAMILANOCITY

Firewall (in)Security

Smau Milano - 22 ottobre 2014

Giuseppe Augiero

aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

Agenda

- Introduzione - Sicurezza Informatica.
- Firewall.
- Casi in cui il firewall crea una breccia alla sicurezza.
- Conclusioni.

La Sicurezza Informatica

- Per sicurezza informatica si intende quel ramo dell'informatica che si occupa dell'analisi delle vulnerabilità, del rischio, delle minacce o attacchi e quindi della protezione dell'integrità fisica (hardware) e logico-funzionale (software) di un sistema informatico e dei dati in esso contenuti o scambiati in una comunicazione con un utente.
- Deve garantire:
  - la correttezza dei dati (integrità);
  - la confidenzialità dei dati (cifratura);
  - l'accesso fisico e/o logico solo ad utenti autorizzati (autenticazione);
  - la fruizione di tutti e soli i servizi previsti per quell'utente nei tempi e nelle modalità previste dal sistema (disponibilità);
  - la protezione del sistema da attacchi di software malevoli per garantire i precedenti requisiti.

La Sicurezza Informatica (II)

- La sicurezza dell'informazione definisce:
  - **Le regole per il controllo dell'accesso all'informazione e alle risorse.**

La Sicurezza Informatica (III)

- Possiamo affermare:
  - la sicurezza totale (100%) non esiste.
  - il concetto di sicurezza è prettamente soggettivo.
  - la sicurezza è un processo iterativo.

La Sicurezza come processo

- La sicurezza non ha uno sviluppo statico ma è un processo iterativo.

Il valore della Sicurezza

- Quando si parla di sicurezza spesso non si comprende il valore dei dati da proteggere.
- Esiste un conflitto tra sicurezza e facilità di utilizzo di un computer.
- La sicurezza è considerata un costo e non un beneficio.
- Quanto costa non adottare la sicurezza?
- I benefici della sicurezza non sono sempre quantificabili.

Beneficio della Sicurezza

- *I costi da sostenere sono inferiori al costo che l'organizzazione sosterrebbe in caso di compromissione del sistema.*

Firewall

Firewall

- E' un sistema di protezione perimetrale tra due reti.
- Connette una rete fidata "trusted" (presumibilmente sicura) con una rete non fidata "untrusted" (potenzialmente insicura).
- Tutto il traffico da e verso Internet deve passare da un unico nodo (il firewall).
- Il firewall non deve essere visibile.

Firewall = Full Security?

- La semplice installazione e messa in produzione di un firewall non è sinonimo di sicurezza informatica.
- Il Firewall non può essere la panacea a tutti i mali.
- Permette la mitigazione o il blocco di traffico "malevole".
- Non basta "installarlo".

Insicurezza

- *Un firewall "mal configurato" o il cui design è errato porta ad abbassare il livello di sicurezza dell'interno sistema.*

Design

- Il design del proprio network è stato realizzato in maniera corretta?
- Siamo sicuri che il firewall rappresenti l'unico punto di ingresso e uscita verso il "resto del mondo"?
- Potremmo non essere a conoscenza di ulteriori punti di contatto con altre reti.
- Es. Chiavette, routing errato, Wifi.

Da dove arrivano gli attacchi?

- Outsider attack.
- Insider attack.

- Occorre non sottovalutare gli attacchi dall'interno della rete da proteggere.

- Meglio posizionare un secondo firewall prima del datacenter.

Bastionizzare

- Se il firewall utilizzato è una soluzione software occorre rendere sicura la macchina che lo ospita.
- Il server che fa girare il firewall non dovrebbe ospitare altri servizi.
- Il non corretto irrobustimento della macchina porta inevitabilmente a una possibile falla di sicurazza.
- Implicitamente la sicurezza dipende anche dal sistema operativo (patch, servizio ecc).

Personal Firewall

- Molto popolari e grande parco di software installato.
  - Sono sempre efficaci?
  - Ci proteggono sempre?

- Problema del Windows Network Architecture e del relativo LSP.
  - Bypass.
  - Analisi del traffico.

Packet Filter

- Un packet filtering firewall semplicemente esamina l'intestazione di ciascun pacchetto (IP) e decide se lasciarlo transitare o di bloccarlo in funzione delle regole definite dall'amministratore del firewall.
- Per definire una singola policy di sicurezza occorre definire una ennupla per "matchare" il traffico desiderato:
    - Source Ip
    - Destination IP
    - Protocol
    - source / destination port

Packet Filter Insecurity

- I firewall basati su packet filter nascono oltre 20 anni fa e ormai non rappresentano una scelta sufficiente per filtrare il traffico di rete.
- Riconoscere e filtrare il traffico lavorando solo sui livelli sottostanti a quello applicativo non permette di avere la giusta granularità.
- Soluzione molto economica usata soprattutto in ambito soho.

Statefull inspection

- Passare allo statefull inspection, mantenendo informazioni sullo stato delle connessioni, è utile ma non ci garantisce, sino in fondo, quello che vorremmo.
- Il grado di sicurezza non aumenta in maniera decisiva.
- E' sicuramente da preferire al semplice packet filter.

Nat

- *Il Nat non è sinonimo di sicurezza!!!*

Le policy di sicurezza

- Definire policy di sicurezza potrebbe non essere facile e può indurre ad errori.

- Security breach potrebbero derivare da:
  - policy scritte in modo errato.
  - policy temporanee dimenticate.
  - errato ordine delle regole.
  - deroghe mal definite.
  - policy inesistenti.

Falsi positivi

- Attenzione nel rimuovere regole che sembrano generare solo falsi positivi.
- E' possibile creare un attacco ad hoc con fine di far eliminare o modificare una buona policy presente nel firewall.
- Tre step:
  - Continui falsi positivi.
  - Rimozione policy.
  - Attacco vero e proprio.
- Occorre concatenare gli eventi.

Application Layer

- Ormai buona parte del traffico verso Internet è uno stream http.

- Una semplice regola di un packet filter che permette il passaggio del traffico verso la porta 80 di un nostro webserver potrebbe permettere un sql-injection.
- E' impossibile discriminare il traffico in uscita.
- Content Delivery Network.

Application Layer (II)

- Occorre necessariamente fare analisi a livello applicativo.
- E' possibile, in questo modo, discriminare per singolo stream http e quindi per singola applicazione (Gmail, Facebook, Skype, DropBox).
- Può essere utile usare anche tecniche statistiche.

- In alcuni casi è l'unico modo per filtrare o bloccare alcune applicazioni (ad es.TeamViewer).

Deep Inspection

- Un pacchetto che venga riconosciuto aderente ai criteri prestabiliti può essere gestito dai dispositivi DPI in varie forme, tra cui scartato, rediretto, variata la sua priorità, ne puo' essere limitato il bit rate (la "velocità" massima di questo flusso di pacchetti e anche notificato a un sistema di monitoraggio).

- La Deep Inspection va usata cum grano salis.

Firewall Evasion - AET

- Tecniche più o meno avanzate per bypassare il firewall.
- Comune denominatore:
  - spezzettamento del payload malevole in pezzettini più piccoli.
  - camuffamento.
  - trasporto del payload frazionato con più protocolli.
  - riassemblaggio.

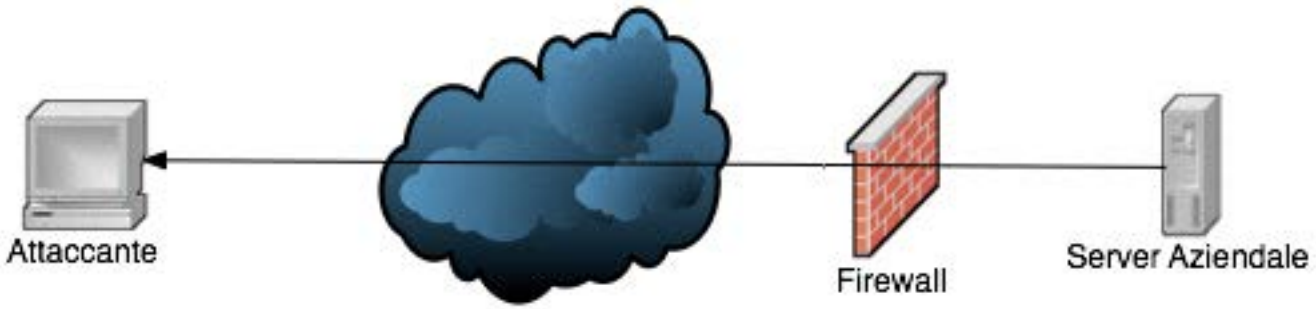
Filtraggio in un solo senso

- Molti firewall vengono configurati in modo da filtrare in maniera puntuale il traffico dall'esterno verso l'interno mentre lasciano passare tutto o quasi tutto nel senso opposto.

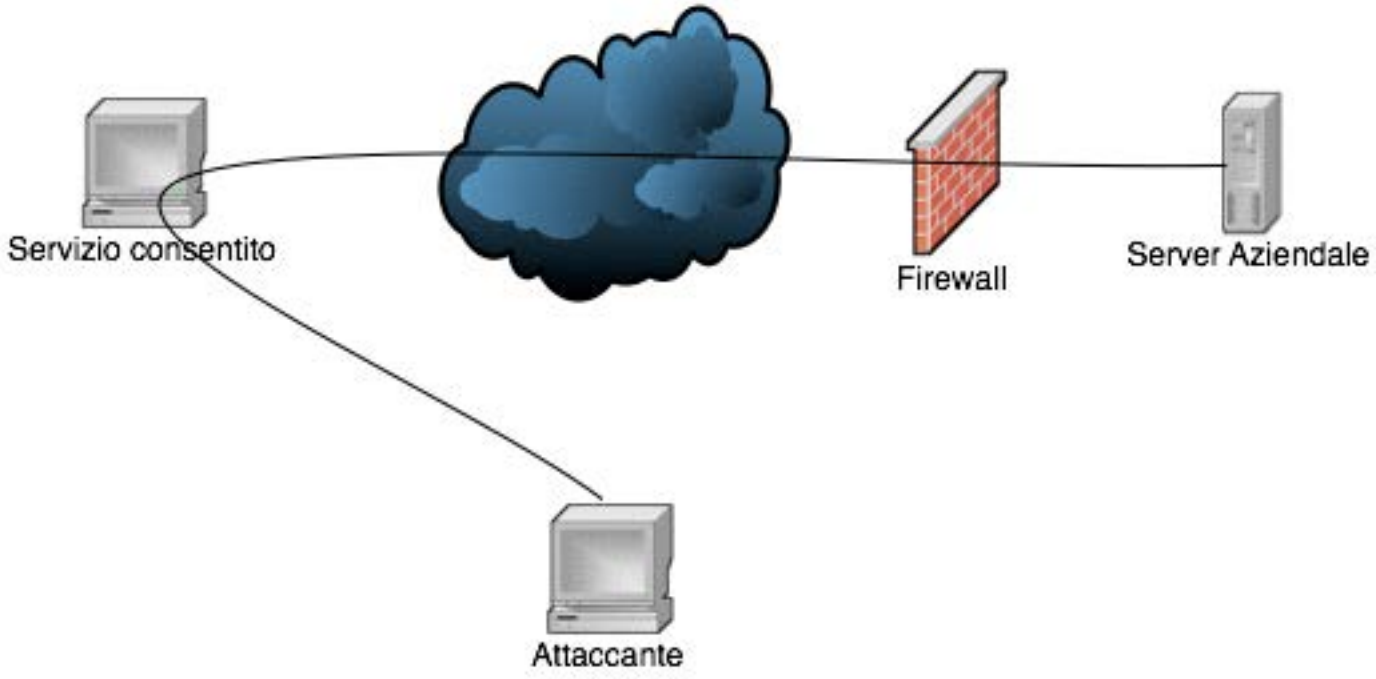
- Cosa succede se l'attaccante esterno riesce ad aprire una connessione verso di lui che nasce dall'interno?

- Macchine infette e Zombie.

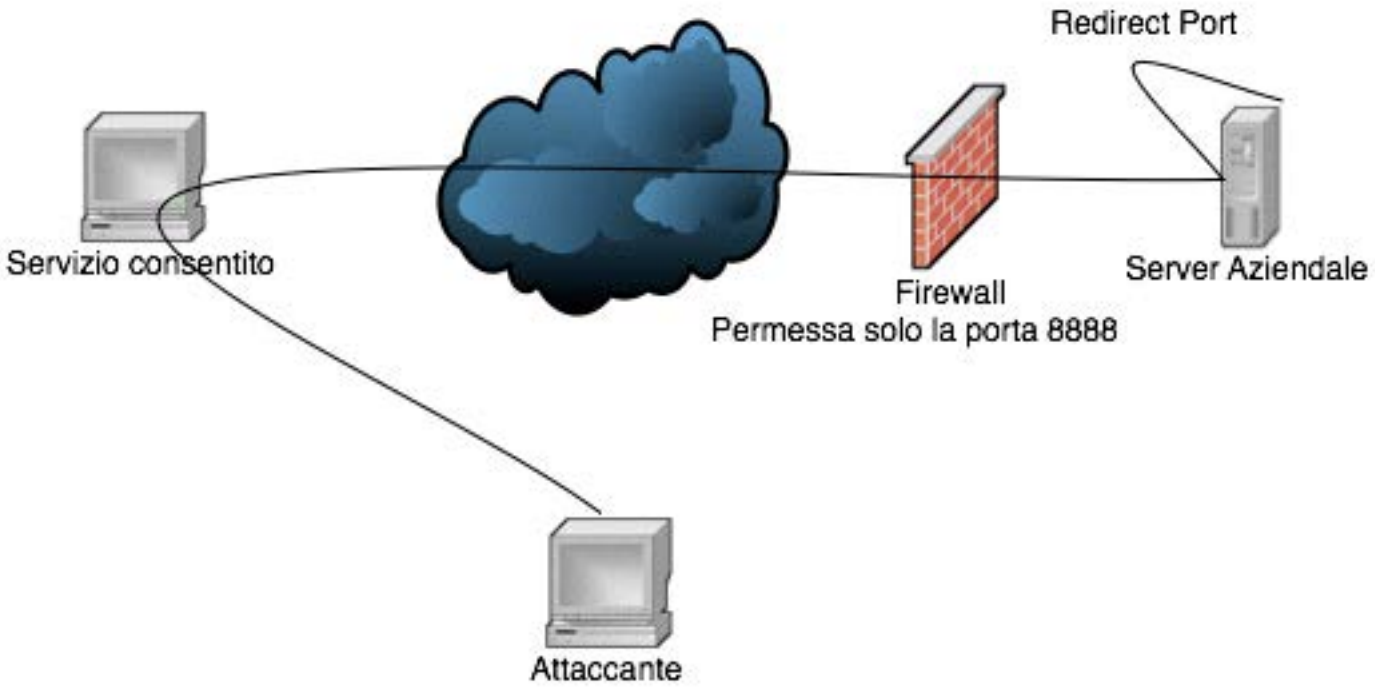
Filtraggio in un solo senso (II)



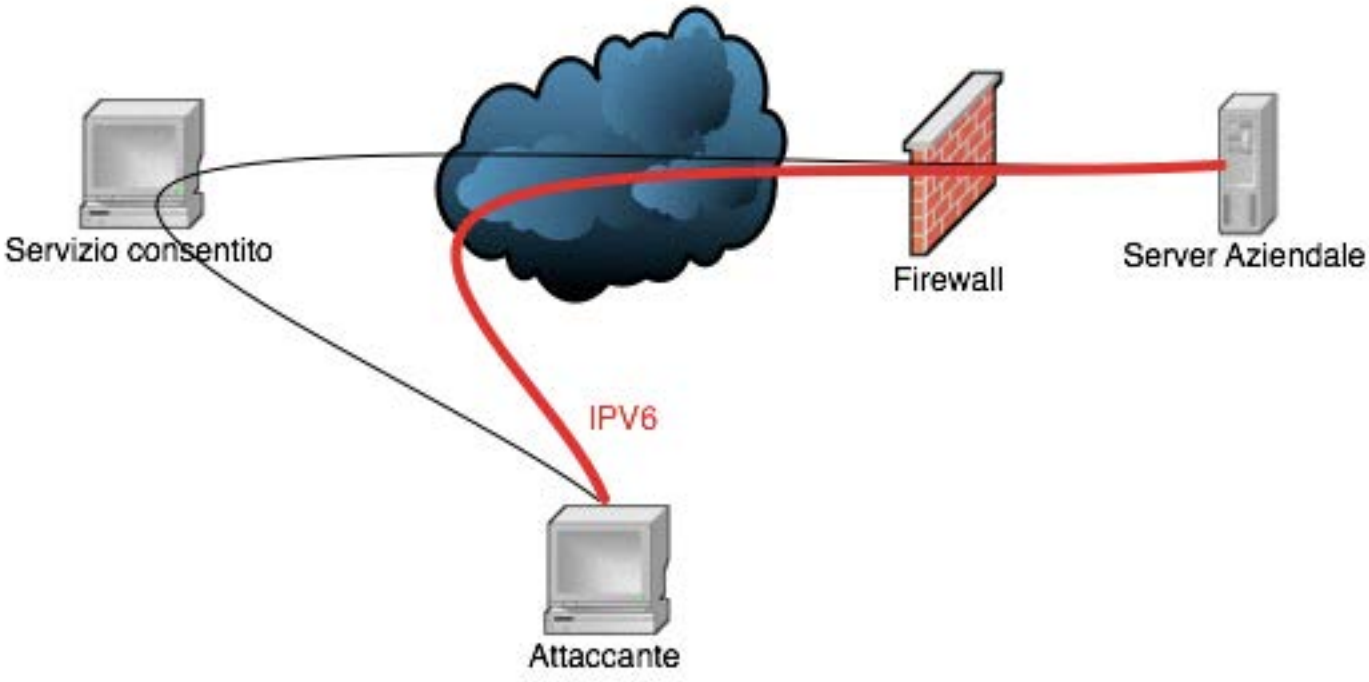
Perfezioniamo l'ipotetica minaccia (I)



Perfezioniamo l'ipotetica minaccia (II)



Perfezioniamo l'ipotetica minaccia (III)



Conclusioni

Quale strada intraprendere?

- Occorre cambiare radicalmente l'approccio nella definizione delle policy di sicurezza.
- Necessità di continui audit e tunning al proprio sistema di sicurezza.
- Cooperazione tra più soluzioni eterogenee.
- Analisi delle anomalie attraverso l'analisi dei flussi di rete.
- Concatenazione degli eventi (firewall, ids, …).

smau MILANO 22-23-24 OTTOBRE 2014
FIERAMILANOCITY

Firewall (in)Security

- Email: talk@augiero.it
- Web: augiero.it
- Twitter: @GiuseppeAugiero

aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA