Prevenzione ON/IN-line

Questo mese, invece di concentrarci su come adoperare qualche particolare strumento informatico per rendere un po' più sicuri i nostri elaboratori, ci proponiamo di fare una breve riflessione sulle direzioni che alcune aree della sicurezza informatica stanno prendendo ed i problemi di base che si cerca di risolvere, aggirare o ignorare. E' una riflessione molto limitata (anche dallo spazio) e se vogliamo personale, basata sull'esperienza maturata negli ultimi anni ed ovviamente, trattandosi di opinioni, suscettibile di contraddittorio.

La situazione

E' un dato di fatto abbastanza noto che l'attenzione della grande maggioranza degli addetti e non addetti all'informatica è alle problematiche della sicurezza della *rete:* firewall, antivirus, antispam, Intrusion Detection/Prevention System e così via. A nostro personale parere le ragioni di ciò sono varie, e tra queste riteniamo importanti citare le seguenti:

- la diffusione del networking, in particolare quello su scala mondiale tramite *internet*, è una tecnologia che a buon vedere si può dire *nuova,* ancora nella propria infanzia; non solo, i protocolli e le tecniche sono nate inizialmente non con l'idea di fornire un sistema di comunicazione globale, e quindi a posteriori soffrono di importanti problemi anche di sicurezza che ora non è semplice risolvere;
- è abbastanza naturale e corretto, e lo facciamo tutti normalmente, pensare di risolvere i propri problemi di sicurezza non rendendo più intrinsecamente sicuro ciò che deve essere protetto ma prevenendo i possibili attacchi; ora è sicuramente fondamentale prevenire l'attacco, ma al contempo è altrettanto fondamentale rendere l'oggetto del potenziale attacco intrinsecamente più sicuro.

L'ultimo punto ci sembra importante. A nostro parere la situazione generale[1] oggi ci sembra basarsi su due fenomeni: la presenza di sistemi informatici progettati e realizzati con insufficiente logica di sicurezza, sia a livello di protocolli che di realizzazione di software, dalla progettazione alla scrittura del codice sorgente spesso di dimensioni immani, ma anche di piattaforme hardware pensate quasi esclusivamente per le prestazioni e non per la sicurezza, e la enorme diffusione ed adozione degli stessi. Ne consegue direttamente che è molto difficile rendere intrinsecamente più sicuri questi sistemi in breve tempo. Per fare ciò sarebbe necessario ripensare e riprogettare dall'inizio le piattaforme hardware e tutti i software, operazione che nessuno immagina neanche di fare. Bisogna perciò che l'intero sistema evolva lentamente verso una nuova generazione ove il tutto, hardware,

1 Ci sono ovviamente eccezioni.

software, protocolli, avranno una maggiore sicurezza intrinseca.

Il secondo punto è che inserendo una tale sistema in una rete di comunicazione globale che praticamente non offre alcun sistema di sicurezza, si giunge facilmente ad una situazione di quasi totale disfatta.

Cosa si può fare

Per il domani la soluzione è unica ed è quella già indicata: evolvere lentamente verso sistemi più sicuri.

Per l' oggi possiamo cercare di difenderci per lo più prevenendo gli attacchi ed ovviamente cercando di scegliere per quanto possibile piattaforme ed applicazioni meno suscettibili a problemi.

Vogliamo però ora discutere un attimo dei vettori di attacco, limitandoci alla rete globale, cioè internet. Bisognerebbe ovviamente considerare anche tutti gli attacchi interni ad una organizzazione, di solito i più pericolosi, più frequenti e più facili al successo, ma ne discuteremo casomai in un'altra occasione. I vettori di attacco più frequenti in internet sono:

- la posta elettronica
- i siti web
- le chat ed i canali peer-to-peer
- gli attacchi diretti ai server ed alle macchine *on-line*
- gli attacchi all'infrastruttura, ovvero i Denial-of-Service.

In questo breve spazio non possiamo addentrarci in un commento di tutti i possibili aspetti di questi argomenti, ne citiamo solo alcuni che forse non sono molto apprezzati.

Uno dei principali problemi della posta elettronica è il fatto che il protocollo attuale non permette l'identificazione sicura del mittente dei messaggi. Inoltre chiunque può spedire messaggi direttamente a chiunque altro, i canali e le procedure ufficiali di trasmissione sono molteplici. In altre parole, per ricevere un messaggio di posta è sufficiente avere un server con un processo smtp attivo ed un nome di dominio ufficiale; per spedire un messaggio basta avere un client ed un server di posta per la spedizione, il quale server si collega direttamente al server destinatario. In quest'ultimo caso, se il server destinatario implementa dei filtri anti-spam e quello di spedizione non è un server *ufficiale*, ad esempio con un record MX nelle tavole DNS ecc., è molto probabile che il server destinatario non accetti il messaggio, ma questo è lasciato alla configurazione fatta dall'amministratore del server destinatario.

Supponiamo invece che esista una lista mondiale dei server di posta elettronica autorizzati ad inviare messaggi,[2] questi server sarebbero ad esempio presso gli Internet Provider. Un server che

2 Questo esempio vuole solo essere indicativo di quali possono essere i problemi reali, ma non vuole essere e non è

riceve la posta potrebbe decidere quindi di accettare messaggi solo dai server elencati in questa lista. In questo modo l'identità del mittente verrebbe garantita dal ISP a cui appartiene il server mittente ed i problemi di spamming e attacchi via posta elettronica si potrebbero ridurre di molto. Questo però introdurrebbe una gerarchia molto rigida all'interno di internet, non solo, gli ISP potrebbero utilizzare questo per controllare o anche solo tassare chi invia messaggi, il che è contrario alla *filosofia* che ha fatto il successo, anche commerciale, di internet. Infine, se una procedura del genere fosse introdotta oggi, ci troveremmo a poter comunicare solo con pochi corrispondenti, probabilmente solo quelli che usano lo stesso ISP!

Il DNS ed il routing BGP sono le due infrastrutture, *critiche,* che supportano il funzionamento di internet. Entrambi hanno il serio rischio di cadere sotto attacchi di Denial-of-Service e di sovversione. Per sovversione DNS si intende la possibilità di far risolvere un nome di dominio in un numero IP di un attaccante invece che del legittimo proprietario, oppure per il routing BGP di indirizzare il traffico per una certa rete verso la rete dell'attaccante. Gli attacchi di sovversione sono possibili immettendo informazioni false nei protocolli di DNS e BGP. Questo è possibile per la debolezza dei protocolli dovuta anche alla loro semplicità e duttilità, che d'altra parte ne fanno una delle ragioni principali del loro successo. Gli attacchi di DoS, ed in particolar modo quelli di Distributed DoS, sono ancora più difficili da contrastare, ma una cosa che potrebbe renderli meno efficaci sarebbe la possibilità di identificare esattamente il mittente di ogni pacchetto IP. Modificare i protocolli DNS e BGP senza ridurre le caratteristiche che li hanno resi così efficaci ma al tempo stesso inserendo funzionalità di sicurezza avanzate non è cosa per nulla facile, oltre tutto andrebbe fatta senza interferire con il normale funzionamento della rete, neanche per pochi secondi.[3]

Cosa possiamo fare in pratica? Localmente le solite cose ben note: avere molta cura nella progettazione della rete, soprattutto se vi sono anche punti di accesso WiFi ecc., utilizzare la segmentazione, le VLAN, gli opportuni firewall, IDS e IPS, avere anti-virus centrali e locali per la posta elettronica, ALG o proxy per i principali protocolli che si vogliono far passare tra internet e la propria rete interna.

Un nuovo punto di vista che sta emergendo è di portare la prevenzione anche sulle reti di Internet Provider e Carrier. Sino ad ora il concetto è stato che un ISP o carrier protegge le proprie macchine, router ecc. ma lascia passare tutto il traffico destinato a o dai propri clienti finali senza alcun filtro.[4] Con il livello di attacchi presenti oggi in rete, dagli scanning ai worm, allo spam, ai virus di posta elettronica ecc., se gli ISP ed i carrier filtrassero almeno parte del traffico diretto ai, e

---

un esempio realistico.

3 Per avere un'idea di quanto questo sia difficile in pratica, basti pensare alla transizione da IPv4 a IPv6, ormai annunciata da anni ma ancora lontana nel futuro.

4 Vi sono eccezioni a questa politica soprattutto da parte degli ISP i cui clienti sono su di una rete con IP privati, ve ne sono alcuni noti esempi anche in Italia.

possibilmente anche proveniente dai, propri clienti potrebbero ottenere una riduzione del traffico sulla propria dorsale oltre ad offrire un servizio a valore aggiunto ai propri clienti. Tecnicamente però questo non è semplice per la quantità di traffico e la richiesta di non interferire con il flusso dello stesso, in altre parole senza introdurre ulteriori ritardi. Ultimamente però gli sviluppi della tecnologia IDS/IPS fanno pensare che nel prossimo futuro ci possa essere una tecnologia adatta. L'idea è di sviluppare delle piattaforme hardware in grado di esaminare il traffico anche a velocità di Gbps con funzionalità di IDS/IPS e firewall. In altre parole, tutto il traffico verrebbe esaminato e confrontato con una, ragionevolmente piccola, lista di firme di attacchi noti. Questa analisi, se fatta solo su di una piccola parte di ogni pacchetto potrebbe introdurre ritardi molto ridotti. Nel caso in cui venga trovato un pacchetto contenente una attacco noto, la funzionalità di IPS/firewall verrebbe automaticamente attivata bloccando selettivamente quel flusso di pacchetti. Anche se l'idea sembrerebbe semplice, l'implementazione non lo è, e sulla soluzione dei molti dettagli tecnici si gioca la possibilità che una tale soluzione possa essere implementata. Inoltre bisogna sottolineare che si tratterebbe solo di una protezione che adotta la politica di *Almost Open*, ovvero solo alcuni ben noti e comuni attacchi verrebbero filtrati, come potrebbero essere i famosi *nimda* o *code-red,* il che vuol dire che la necessità di adottare tutte le difese a livello individuale di azienda e di macchina non cambierebbero.

Andrea Pasquinucci
Libero Professionista in Sicurezza Informatica
pasquinucci@ucci.it