Gestire la (in-) Sicurezza Informatica

In questa rubrica abbiamo quasi sempre trattato argomenti per lo più tecnici illustrando con esempi presi, per ovvi motivi, spesso dal mondo dell'open-source. L'intento iniziale era quello di illustrare alcune problematiche e le associate tecnologie di sicurezza portate alla ribalta dall'arrivo della rivoluzione *Internet*. Negli ultimi 10 anni infatti il modo di utilizzare gli strumenti informatici è cambiato radicalmente, come sono cambiati gli utilizzatori e chi gestisce i sistemi sia a livello tecnico che manageriale. E' quindi parso utile concentrarsi sulle novità introdotte da questa rivoluzione, ed in primo piano il concetto della *rete* e delle comunicazioni. In questa rubrica abbiamo perciò cercato di descrivere tecnologie e problematiche di sicurezza relative alla *messa in rete* dei sistemi informatici.

La tecnologia

A nostro parere ora siamo però di fronte ad un mutamento dello scenario. Ormai questa tecnologia, anche se non conosciuta come dovrebbe, almeno è stata provata ed accettata dai più. La diffusione dell'informatica è di massa, ed i concetti di rete, networking eccetera sono ormai familiari agli addetti ed agli utilizzatori, che in pratica vuol dire tutti quanti. Storicamente quando si sono verificate queste condizioni per altre tecnologie, il passo successivo è stato la trasformazione in *Commodity* o Servizio. In altre parole, la tecnologia non è più per pochi (cosa ovvia già da qualche anno nel nostro caso) ma soprattutto non richiederà la partecipazione attiva e cosciente dell'utilizzatore, che dovrà avere solo alcune limitate conoscenze sul come usare l'oggetto ma non preoccuparsi di null'altro.

Nel nostro caso possiamo pensare ad uno scenario con tre tipi di attori:

1. i produttori, che si dovranno fare carico di tutte le problematiche tecniche, di gestione eccetera
2. i gestori dei servizi, che dovranno utilizzare nella maniera corretta i prodotti acquistati dai

produttori

3. gli utilizzatori finali, che non si dovranno preoccupare per nulla della tecnologia, ma dovranno solamente 'pigiare il bottone'.

Se pensiamo allo sviluppo delle tecnologie a cui stiamo tutti assistendo, ci rendiamo conto che da un periodo ove gli strumenti erano pochi e richiedevano molto lavoro per poter essere messi in opera e connessi tra di loro, stiamo passando a prodotti che non necessitano di particolari configurazioni, in grado di interagire autonomamente ed automaticamente con gli altri già presenti o che aggiungiamo al nostro sistema, e che spesso gestiscono da soli aggiornamenti e quant'altro.

In questo panorama diventa quasi inutile e spesso difficile scegliere dei temi puramente tecnici di interesse per questa rubrica: la spiegazione di come funziona la scatola 'dentro' sta diventando sempre più di interesse ristretto ai soli sviluppatori della scatola stessa. Se vogliamo, anche giustamente, chi li deve gestire ed utilizzare non è più tenuto a sapere come funziona 'dentro' ma solo il comportamento esterno.

Per fare un esempio specifico nel nostro campo, per configurare un firewall un gestore di servizi non deve più avere alcuna idea di come funziona dentro, di cosa è la pila tcp/ip e così via, ma solo cliccare sul bottone 'permetti il traffico da internet verso il server web in DMZ' oppure 'permetti il traffico dei client in LAN verso i server web in internet'. Che poi questi bottoni si traducano in molteplici regole a vari livelli della pila, dai filtri sugli indirizzi IP e le porte TCP al filtraggio anti-virus del traffico in tempo reale, alle limitazioni sui possibili attacchi di denial-of-service, al filtraggio di siti indesiderati eccetera, realizzati con firewall stateful, proxy, anti-virus ..., tutto ciò sarà del tutto ignoto all'utilizzatore ed anche al gestore, che si aspettano che solo il traffico permesso e non nocivo possa passare.

Quello che oggi invece diventa sempre più importante è capire **come** gestire i sistemi di sicurezza

informatica. Infatti, se chi gestisce i sistemi non è più tenuto a sapere come funzionano 'dentro' gli apparati e soluzioni che utilizza, diventa più critica la corretta gestione degli stessi.

Il fattore Uomo

Parallelamente a questi sviluppi, anche la forma degli attacchi e soprattutto l'identità degli attaccanti è cambiata molto negli ultimi anni. Come tutti ben sappiamo, i primi virus, worm eccetera sono stati scritti per ragione di studio, ovvero per dimostrare l'esistenza di gravi problemi di sicurezza. Lo spirito iniziale era scientifico (ed un po' goliardico), anche se i danni erano tangibili. Si è passati poi ad un periodo in cui riuscire a violare un sistema era quasi qualche cosa di cui vantarsi, almeno tra i compagni di avventura, al punto che vi furono vere 'competizioni'. Ed ovviamente i danni continuarono ad aumentare. Arrivarono poi gli Script-Kiddies, che pur non avendo le competenze tecniche, erano comunque in grado di usare un programma scritto da altri per sfruttare una vulnerabilità a loro ignota. I danni aumentarono ulteriormente, ma lo spirito degli attaccanti era ancora spesso più ludico che altro.

Oggi non più. Attacchi, virus, worm e quant'altro sono sviluppati da bande di malviventi con scopi economici ed in alcuni casi politici o di terrorismo. Internet, i siti web ecc. non sono più lo scopo dell'attacco ma il mezzo dell'attacco. Il fine dell'attacco non è più informatico ma economico o politico, e può essere realizzato in via informatica come con altri mezzi. L'attaccante sceglie il mezzo che ritiene più consono a conseguire i propri (loschi) fini e questo mezzo può anche essere un virus piuttosto che un attacco di denial-of-service, come potrebbe essere una rapina a mano armata. Oggi infatti parliamo più di truffe realizzate su canali informatici (phishing) che dell'ultimo virus o worm in circolazione.

Ne consegue un fatto molto importate: le difese puramente tecnologiche non sono più sufficienti, è necessario gestire la sicurezza a partire da chi deve utilizzare gli strumenti informatici, ovvero

gestire il *Fattore Uomo*.

Le vulnerabilità

Se il fronte degli attacchi e degli attaccanti è mutato radicalmente negli ultimi anni, non lo stesso è successo sul fronte delle vulnerabilità. Non vogliamo essere pessimisti, dobbiamo infatti notare che negli ultimi anni il problema sicurezza è balzato ai primi posti nell'attenzione dei produttori, e questo è già un grande risultato. Molti tipi di attacchi, ovviamente i più semplici, oggi non sono più possibili perché quasi la totalità dei sistemi non ha più le relative vulnerabilità da sfruttare. D'altra parte, la interconnessione, la banda larga, gli Zero-Day-Exploit e così via, hanno aumentato i rischi invece di ridurli. In pratica oggi non esistono quasi più vulnerabilità che se sfruttate porterebbero a piccoli inconvenienti, invece rimangono e purtroppo aumentano le vulnerabilità che se sfruttate portano al crollo completo del sistema. Abbiamo quindi vulnerabilità molto più gravi, che fortunatamente sono più difficili da sfruttare, ma rispetto alle quali è anche più difficile adottare misure di protezione alternative soprattutto perché molto spesso le vulnerabilità possono essere sfruttate solo con la collaborazione (ignara) dell'utente. In altre parole, è l'utilizzatore stesso del sistema che viene spinto a sfruttare la vulnerabilità a favore dell'attaccante. Un tipico esempio molto attuale sono programmi a prima vista *innocui* che permettono di *condividere* file o informazioni con altri e che al contempo però permettono ad altri di utilizzare a loro piacimento il nostro PC.

Gestire l'insicurezza quotidiana

Nella scala Uomo-Macchina, le problematiche associate alla sicurezza informatica si stanno spostando sicuramente verso il fattore Uomo visto che la parte tecnica sarà sempre più solo appannaggio dei produttori. Come utilizzatori dei prodotti diventa sempre più importante *gestire* le problematiche di sicurezza rispetto ai propri rischi. Questo però richiede un cambio completo di approccio: se la soluzione tecnica ad un problema tecnico è indipendente dal contesto in cui il

prodotto è utilizzato, la soluzione ad un problema di gestione dei sistemi dipende crucialmente da chi li utilizza ed in quale modo.

Dobbiamo partire dalla convinzione che nessun sistema è assolutamente sicuro e che quindi dobbiamo gestire l'insicurezza quotidiana cercando di minimizzarne i rischi. Per fare questo dobbiamo:

1. sapere cosa la tecnologia offre ed essere in grado di valutarne non solo le caratteristiche e le prestazioni ma anche i limiti
2. avere chiara la situazione organizzativa, gestionale e produttiva della propria azienda, ente, amministrazione eccetera
3. valutare i punti di maggior rischio sia economico che di immagine, legale ...
4. creare, gestire ed evolvere dei sistemi di sicurezza delle informazioni che includano tutti gli elementi: dall'uomo, ai processi, ai sistemi elaborativi.

Per questi motivi prossimamente in questa rubrica cominceremo a discutere di aspetti meno tecnici e più di gestione dei sistemi di sicurezza delle informazioni (con ciò avvicinandosi di più alla vera attività di chi scrive) pur sempre riportandovi, quando ne troveremo l'occasione, argomenti tecnici come fatto sinora. Visto che il nome di questa rubrica è Hands-On, l'approccio alle problematiche di sicurezza che prenderemo sarà il più pratico possibile, cercando di discutere sia concetti che metodologie, ma anche per quanto possibile casi pratici.

Andrea Pasquinucci

pasquinucci@ucci.it