PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 18 - numero 3760 di giovedì 14 aprile 2016

Come migliorare la protezione dagli attacchi informatici

Uno studio ha preso in esame il livello di protezioni esistenti contro gli attacchi informatici. I punti deboli finora individuati. A cura di Adalberto Biasiotti.

Negli Stati Uniti è stato recentemente pubblicato uno studio, che ha preso in esame il livello di protezioni esistenti, nelle infrastrutture federali, contro gli attacchi informatici.
In particolare, lo studio ha preso in esame il livello di protezione delle infrastrutture informatiche critiche, con particolare riferimento alla protezione dei dati personali. Quest'ultimo studio è stato condotto nel 2015.
I risultati non sono particolarmente soddisfacenti, a riprova del fatto che, ancora ad oggi, gli specialisti di attacchi informatici trovano delle strutture che non sono così resistenti all'attacco, come si potrebbe sperare.
Ecco, in particolare quali sono stati i **punti deboli** finora individuati.

Tanto per cominciare, le **strutture in grado di rivelare un tentativo di intrusione** non sembrano sufficientemente evolute. La tecnica normalmente utilizzata è quella di fare un confronto fra l'andamento del traffico in rete rispetto a modelli, costruiti su base statistica, che potrebbero lasciar pensare che un attacco possa essere in corso. Purtroppo questi schemi sono molto rigidi e non hanno un livello di flessibilità sufficiente per contrastare tecniche di attacco facilmente modificabili dagli attaccanti stessi, rendendo quindi l'applicativo non particolarmente efficace.
Altre strutture di sicurezza fanno riferimento alla **prevenzione delle intrusioni**, ad esempio bloccando un messaggio di posta elettronica che si ritiene possa essere utilizzato per trasportare applicativi fraudolenti. Anche in questo caso, la funzione utilizzata non sembra essere sufficientemente evoluta e non riesce, ad esempio, ad individuare applicativi fraudolenti che possano arrivare attraverso pagine Web.

Un altro elemento negativo, che è caratteristico di altre strutture pubbliche, non solo negli Stati Uniti, discende dal fatto che le varie agenzie ed enti coinvolti non hanno un programma sistematico di scambio di informazioni, diminuendo in maniera significativa la possibilità di fare fronte unito contro particolari tipi di attacchi.

Anche se il dipartimento della sicurezza interna ha sviluppato degli applicativi, che sono in grado di misurare le prestazioni dei sistemi di individuazione e prevenzione di intrusione, i risultati sembrano essere poco affidabili e difficilmente comparabili, rispetto a quelli che si ottengono presso diverse agenzie ed enti federali.

Un'altra area che lascia ancora perplessi gli ispettori del *General accountability Office* è legata all'**utilizzo delle risorse residenti in un cloud**.
Ancora oggi i gestori del cloud non sono in grado di garantire livelli di sicurezza accettabili. Tale fatto discende dai requisiti posti dal responsabile dei sistemi informativi, che sembra si preoccupi molto di più della rapidità di risposta, nello spazio di memoria e della potenza di calcolo nel cloud, piuttosto che dei livelli di sicurezza disponibili.

Sono convinto che molti lettori, che operano in questo settore, potrebbero trasferire queste considerazioni, cambiando soltanto il testo inglese in testo italiano, nell'ambito dei sistemi informativi affidati alle loro cure.

Adalberto Biasiotti

Leggi gli altri articoli di PuntoSicuro sulla sicurezza informatica

---

www.puntosicuro.it