La VeuIp està cada vegada més de moda. Hi ha més servidors, més usuaris, més centraletes i, evidentment, més gent que intenta aprofitar-se d'algún servidor mal configurat per intentar fer diners.

Hi ha serveis en el que algú pot fer alguns diners però que a nosaltres no ens en fa perdre. Per exemple si algú que envia spam ens troba un servidor de correu obert. L'spamer pot fer servir el nostre servidor per enviar mails a tothom però nosaltre no perdrem diners (o no molts). El que ens pot passar son "inconvenients" (que depen de l'empresa són més greus o menys) com que ens posin a una blacklist de correu.

En la telefonia això no és així. En la telefonia si algú aconsegueix entrar al nostre servidor i cursar trucades, aquestes trucades no son gratis com els correus. Cada trucada que fagi una trucada és un cost econòmic per nosaltres i, evidentment, no en farà una, sinó que en farà tantes com pugui. Posarem un petit exemple.

Tenim un servidor que està conectat amb un trunk a un proveidor sip. Posem que podem arribar a fer 5 trucades simultàneas i que no tenim cap tipus de restricció ni de destí ni de durada de la trucada. En un escenari com aquest si algú aconseguís la contrasenya de una de les extensions d'aquesta centraleta i es posés a trucar a un destí de posem 3 euro per minut, cada minut consumiria 15 euros, en 20 minuts hauria consumit 300 euros, en 2 hores 1800 euros, que està aviat dit.

La gent que es dedica a buscar centraletes mal configurades no és per trucar a la seva família o a la seva parella sinó que és per fer diners. I com els fan? doncs són gent que tenen contractats números premium.

Els números premium són números al que és molt car trucar ja que ofereixen un servei i part de la facturació de la trucada va a parar al que ha contestat la trucada. Per tant si algú pogués trucar al seu número premiun a través de la vostre centraleta el que estaria fent, més o menys, és una transferència de diners de la teva butxaca a la seva. Si mai algú entra a la vostre centraleta podeu està segurs que us pasarà algo com el que li ha passat, malauradament, a molta gent que us robaran un bon grapat de diners aprofitant-se de la mala configuració, mal manteniment, contrasenyes febles.

Per evitar-ho hem de tenir la nostra centraleta ben protegida i només obrir accés a el que realment necessitem. I en aquestes coses que necessitem que estiguin obertes tenir-les molt controlades:

- La primera mesura és no obrir rés a l'exterior. Al montar una centraleta que no tindrà extensions externes no ens cal obrir cap port, o redirigir cap port del router a la centraleta. Les centraletes tenen maquenismes per mantenir el nat obert (nat keep alive) i no tenir problemes al rebre trucades entrants.
- Si s'ha d'obrir la centraleta a l'exterior:

1. Posar contrasenyes bones. La majoria dels atacs son a força bruta i amb diccionaris contra la centraleta. Per tant tenir contrasenyes aleatories amb números, lletres (majúscules i minúscules) i algún simbol ajuda a que tardin molt més, i fins i tot els sigui impossible de trobar-la.
2. Canviar el port SIP. Per trobar centraletes obertes els atacants escanegen la xarxa buscant ports SIP oberts. El port SIP per defecte és el 5060 però es poden configurar les centraletes per utilitzar-ne un altre. Si es canvia el port SIP la majoria d'escanejos no detectaran que tenim una centraleta en aquell ordinador i per tant no ens atacaran. Per altre banda això vol dir que cada vegada que configurem un terminal SIP haurem de dir-li que fagi servir el port que hem posat, ja que tots van configurats per fer servir el port 5060.
3. També podem posar un analitzador que prengui accions quan detecti que ens estan atacant. Com hem dit els atacs els fan a força bruta i una de les característiques d'aquests atacs és que no son gens dissimulats, son molt fàcils de detectar. El que fem és posar un programa que detecti quan ens estan fent un atac i banajem la ip des d'on prové durant 3 o 4 hores.

Un exemple és el fail2ban. El sistema és molt senzill. El fail2ban va mirant els logs de la nostra centraleta i quan veu que algú està intentant registrar-se moltes vegades des d'una mateixa ip i sense èxit, baneja aquella ip durant un cert temps.

4. Limitar la capacitat de fer trucades de la centraleta no farà que no ens entrin però si que es redueixi el cost de l'atac. Algunes de les coses que es poden limitar son:

- Número de trucades concurrents que pot fer una extensió.
- Número de trucades concurrents que es poden fer en un trunk.
- Limitar i controlar el crèdit gastat durant periodes de temps fixes. Per exemple controlar que en una hora el crèdit gastat no sigui més gran que un valor.

Amb això ens evitarem sorpreses de trucades que no hem fet però que hem de pagar i amb les quals podem predre tranquilament 100 euros amb 15 minuts.

Totes aquestes pràctiques les recomano tant a gent que es monta un petit servidor per fer probes a casa seva com a empreses que monten la seva centraleta. Si el que teniu entre mans són coses més grans s'haurien d'implementar altres sistemes, però d'això en parlarem un altre dia.

{jcomments off}