LA SEGURIDAD DE LA INFORMACIÓN EN LA ERA DEL INTERNET DE LAS COSAS (IOT)

Ada P. Salazar

El 21 de Octubre del 2016, se suscitó la caída de servicios de internet de uno de los mayores proveedores de la infraestructura clave para la red, que soporta algunas de las aplicaciones y páginas más populares como: Twitter, Netflix, Spotify, Airbnb, Paypal, etcétera.

Según los análisis posteriores esta caída de los servicios, se identificó que se debió a un ataque a los servidores de *Domain Name System* (DNS) del tipo *Distributed Denial of Service* (DDOS) coordinado, a través de millones de diferentes direcciones de IP. Los 18 *data centers de Dyn* (que están en todo el mundo) fueron atacados de forma coordinada, a diferentes horas y desde diferentes locaciones.

¿Como fue posible coordinar un ataque de esta magnitud?

Para llevar a cabo una intervención de este tipo, se utilizó la vulnerabilidad de millones de dispositivos conectados, al que ahora se llama internet de las cosas (IOT), como por ejemplo: impresoras, cámaras de seguridad, *webcams*, *routers caseros*, monitores de bebé y otros.

Hemos incorporado de forma paulatina en nuestras vidas este tipo de dispositivos que nos hacen la vida más fácil, pero pocas veces nos preocupamos por el tema de su seguridad. Parecería que no es necesario atender este rubro, pues aparentemente son inofensivos; sin embargo, si juntamos todos estos aparatos y hacemos que trabajen en conjunto, pueden lograr un gran daño.

Para el caso que abordamos, los *hackers* desarrollaron un malware, al que nombraron MIRAI (en japonés significa "el futuro"), este *malware* convirtió en "bots" a los sistemas operativos basados en Linux, los cuales fueron controlados de manera remota y se utilizaron en conjunto en este ataque de escala mayor.[1]

La empresa *XiongMai Technologies*, fabricante de dispositivos conectados a internet y vulnerables en temas de seguridad (cuyo principal problema de seguridad fue que los usuarios, por omisión, no cambian la contraseña de sus equipos)[2], aceptó la responsabilidad por sus equipos usados en estos ataques, y puso en marcha una campaña para retirar los productos identificados con vulnerabilidades (los elaborados y vendidos antes de septiembre de 2015).[3]

Esta acción, aunque mitigará próximos ataques, ciertamente no los detendrá, ya que muchas personas, dueñas de equipos infectados con el *malware*, no están conscientes de que estos dispositivos tienen vulnerabilidades y deben ser retirados y/o actualizados.

Teniendo en cuenta que internet es la plataforma de comunicación y negocios en la época actual, que crece continuamente la forma en la que lo usamos para ofrecer nuevos servicios y formas de interacción, y el hecho de que la información es considerada el activo más importante de cualquier organización, cobra mayor relevancia tomar las acciones necesarias para proteger la seguridad de la información y las plataformas en las que ésta se encuentra almacenada. Ante esto, es de vital importancia que las compañías implementen procesos que les permitan atender los riesgos asociados a la información.

El estándar de ISO 27000 ofrece una guía para identificar, evaluar y atender los riesgos a la seguridad de la información. Es muy importante aprender la lección de este ataque y no minimizar elementos que parecen inofensivos, pero que ocultan un gran riesgo para la información de las compañías.

[1] "MIRAI (MALWARE)" [en línea], en Wikipedia, México, [fecha de consulta: 31 de octubre de 2016], disponible en: <https://en.wikipedia.org/wiki/Mirai_(malware)>.

[2] KAN, MICHEL. "CHINESE FIRM RECALLS CAMERA PRODUCTS LINKED TO MASSIVE DDOS ATTACK" [en línea], en PCWorld, IDG, Estados Unidos, [fecha de consulta: octubre de 2016], pág. 1/1, disponible en: <http://www.pcworld.com/article/3133962/chinese-firm-recalls-camera-products-linked-to-massive-ddos-attack.html>.

[3] ENRIQUE, DANS. "LA RED DISTRIBUIDA YA NO ES INVULNERABLE" [en línea], en Enrique Dans, España, octubre 2016, [fecha de consulta: 31 de octubre de 2016], disponible en: <https://www.enriquedans.com/2016/10/la-red-distribuida-ya-no-es-invulnerable.html>.