BACSIRT
Vamos Buenos Aires | Centro de Ciberseguridad
LA AGENCIA DE SISTEMAS
www.ba-csirt.gob.ar
BOLETÍN N°13
FECHA DE PUBLICACIÓN
28 04 17

INTERNET DE LAS COSAS: QUÉ ES Y COMO INFLUYE EN NUESTRA VIDA COTIDIANA

En este boletín decidimos abordar un tema que actualmente es vox pópuli en todos los sitios en los que se juntan personas y dispositivos tecnológicos; a saber, IoT. Seguramente escuchaste o leíste la expresión muchas veces y posiblemente no tengas muy claro qué significa ni, mucho menos, seas del todo consciente de que seguro disponés de algún dispositivo IoT.

Pues bien, **dicha sigla proviene de la frase en inglés "Internet of things", que significa "Internet de cosas" y se usa para referirse a todos los objetos que emplean para su funcionamiento, aunque sólo sea para algunas funciones específicas, conexión a Internet**.

Puede que, en principio, nos parezca poco intuitivo o no nos hagamos rápidamente a la idea de que en la actualidad muchos de los objetos con los que interactuamos en nuestro día a día se conecten efectivamente a Internet, por más de que los nombremos como "Smart" o "inteligentes", pero la realidad es que así es. Desde los teléfonos móviles hasta las tostadoras, aires acondicionados o lavarropas que podemos programar a través del celular o nos envían un informe de estado de la tarea para la cual son usados cada vez que se ponen en marcha, todos ellos pueden funcionar como lo hacen gracias a que se conectan a Internet. Esa es la premisa fundamental.

A pesar de que la mayoría de los objetos que utilizamos a diario tienen funciones inteligentes y los podemos programar a distancia, muchas veces nos olvidamos de que eso es así porque los mismos funcionan conectados a internet.

Es decir, la gran red de Internet, además de funcionar como una inmensa fuente de información e intercambio, sirve en este caso como canal de transmisión de datos, los cuales permiten, a su vez, que determinados objetos puedan funcionar de forma remota y admitan instrucciones enviadas por medios digitales. La "magia" que implica el hecho de poder

poner en marcha la cafetera sin siquiera salir de la cama, por ejemplo, no es más que un caso concreto de Internet aplicado a las cosas.

Ahora bien, son obvias las ventajas que esta innovación tecnológica ofrece (comodidad, agilidad, rapidez, eficiencia y confort) pero lo que tal vez no es tan evidente y sí bastante problemático son los riegos, en materia de seguridad, que la aplicación de IoT conlleva. **Por el simple hecho de conectar un dispositivo a Internet, sea cual sea, este se vuelve plausible de ser interceptado y manipulado por terceros**. Es decir, en caso de no estar lo suficientemente protegido o correctamente configurado, los datos que el dispositivo transmite se tornan vulnerables; si alguna persona quisiera podría cambiar o eliminar las instrucciones que el usuario hubiera establecido o generar otras diferentes.

Esto que acabamos de describir, que parece exagerado o sobredimensionado si se considera un dispositivo como una tostadora inteligente, en realidad no lo es. Por ejemplo: si una persona tiene en su cocina una tostadora con tecnología IoT y la deja programada desde la noche anterior para que a la mañana siguiente tueste el pan durante un minuto y alguien, habiendo interceptado la misma, modificara el tiempo de funcionamiento de la tostadora, podría tranquilamente provocar un incendio. El ejemplo es extremo y afortunadamente no es algo que suceda a diario, sirve simplemente para ilustrar la magnitud del alcance que tiene el hecho de disponer de dispositivos IoT no asegurados.

Debemos tener presente que todo dispositivo que funcione conectado a internet se vuelve vulnerable a ciberataques.

Lo que sí pasa muy a menudo y es posible gracias a la poca seguridad con la que se manejan estos objetos, es la creación de botnets, las cuales se usan, a su vez, para llevar adelante ciberataques más complejos y ambiciosos. Un caso concreto de ello que podemos usar como ejemplo es el mega ataque DDoS ocurrido a fines del año pasado, que ocasionó la caída de múltiples sitios web altamente populares (como Twitter, Spotify, Netflix, etc.) durante todo un día.

La mayoría de los objetos con los que interactuamos a diario funcionan con tecnología IoT.

Pero... en concreto, ¿de qué hablamos cuando decimos botnets?

Ese término hace referencia a las redes compuestas por dispositivos que funcionan como bots (robots). Es decir, objetos con tecnología IoT que, habiendo sido infectados previamente por un virus, quedaron a merced de las ordenes e instrucciones del administrador de dichas redes quien, valiéndose de ellas, tiene la capacidad de lanzar ataques masivos con el mínimo de esfuerzo e implicando a terceros (los dueños de los dispositivos infectados) que no tienen conocimiento alguno acerca de que forman parte de un ataque informático.

Dicho esto, es muy importante entender que debemos, por nuestro

Considerando el gran avance tecnológico de los últimos tiempos, no es descabellado pensar que en un futuro no muy lejano viviremos en casas y ciudades totalmente inteligente.

propio bien, estar muy atentos a la utilización que le damos a nuestros dispositivos IoT y, sobre todo, configurarlos y resguardarlos correctamente. Para ello, a continuación, te dejamos algunos tips de seguridad para que puedas aplicarlos de inmediato.

1. Instalá y mantené siempre actualizado algún programa antivirus en TODOS los dispositivos que uses conectados a Internet y admitan la instalación del mismo.
2. Mantené actualizado el software de los dispositivos, prestando atención a los avisos de nuevas versiones.
3. Descargá programas, aplicaciones y juegos sólo de sitios oficiales.
4. No descargues adjuntos ni elementos que te envíen por correo electrónico si provienen de un remitente desconocido y procurá tener activada la función de escaneo previo a las descargas en tu programa antivirus, para los casos en los que sí quieras o necesites descargar algo que te hayan enviado o hayas buscado en la web.
5. Cambiá SIEMPRE las contraseñas que vienen por defecto en los routes, cámaras IP, webcams, impresoras y demás electrodomésticos “Smart”. Si no sabés como hacerlo, consultalo con el soporte técnico del fabricante.
6. No accedas a redes wifi abiertas o públicas a menos que sepas que las mismas son seguras.
7. Implementá algún método de bloqueo en todos los dispositivos con los que ingreses a tus cuentas online (Smartphones, tablets, PC, etc). ▪