Internet of Things (IoT)

El concepto de internet de las cosas se refiere a la tecnología por medio de la cual se interconectan artefactos, así es posible controlarlos de forma remota o recibir mensaje de alerta de los mismos. Por ejemplo, una nevera puede avisar al propietario que un alimento caducará pronto. IoT puede ser usada en diferentes contextos, como el hogar y las industrias. Este último, IoT industrial, se usa en las fábricas para mejorar la eficacia en el uso de la maquinaria y tener una óptima producción.

La interconexión digital de dispositivos o los artículos conectados a la red –que se relacionan entre sí y con las personas– se ha extendido más allá de la vivienda y ha dado lugar a objetos inteligentes como *smart things* (cosas inteligentes), *smart homes* (casas inteligentes), *smart cars* (vehículos inteligentes), *smart cities* (ciudades inteligentes) o *smart grids* (redes de distribución eléctrica inteligentes), las cuales pueden ser monitoreadas en tiempo real.

Foto: Geralt, en http://bit.ly/2yTm74l. Licencia CC0 Creative Commons

La interconexión digital de dispositivos o artículos vinculados a la red se ha extendido más allá de la vivienda y ha dado lugar a objetos inteligentes.

Iván Castaño, ingeniero electrónico de la Universidad Nacional, magíster en Ingeniería de la Comunicación de la Universidad de Toronto, explicó que desde el punto de vista teórico, los datos pueden considerarse infraestructura si cumplen con tres criterios: ser un bien no rival (no excluyente), ser un bien-capital (utilizado para otro producto) y tener un propósito general.

Pero no basta con tener la tecnología para recogerlos (en este caso IoT), también hay que analizarlos como parte de un ecosistema y esta es una tarea pendiente en Colombia. En ese ecosistema no todo es tecnología: existe una correlación entre la ciencia aplicada y otros componentes del sector TIC, que se conectan con tres aspectos: la regulación (que las leyes avancen al mismo paso), habilidades (no solo conocer los programas sino, por ejemplo, hablar un segundo idioma, tener formación en gerencia o inteligencia emocional) e instituciones (lo cual va de la mano de la regulación).

Por otro lado, el representante del Ministerio señaló que si se quiere entrar a la revolución tecnológica, también hay que superar barreras como el temor de las personas a usar servicios en línea. Y es preocupante que (según cifras del 2015 del Grupo de Respuesta a Emergencias Cibernéticas-Colcert), el 42,4 % de las vulnerabilidades digitales corresponde a los ciudadanos, lo que les genera mayor desconfianza al hacer trámites por la web.

Resaltó la importancia del ciudadano dentro del proceso y dijo que la visión del Ministerio sobre internet de las cosas se identifica con la de IBM, la cual se centra en el usuario, con una protección *end-to-end* para generar confianza y que ese sea un entorno seguro. Una apreciación que compartieron los demás participantes en el foro.

Seguridad cibernética, prioridad en políticas industriales

Sobre dos grandes ciberataques, uno contra una fábrica de papel en Estados Unidos que costó más de un millón de dólares y otro contra la central eléctrica que dejó a oscuras a Ucrania, habló Fayçal Daira. Además trató sobre el conflicto entre las operaciones y la seguridad, cómo mejorar y las soluciones de protección en la industria.

Los ciberataques a procesos industriales son una realidad. Sin embargo, su prevención no está en la cultura de la mayoría de las industrias, pues conservan la idea de enfocar el manejo de riesgos en daños en máquinas o accidentes de empleados. Algunos artefactos con más de 20 años son muy vulnerables y a pesar de tener un funcionamiento planificado, el 90 % operan sin antivirus.

De ahí el conflicto entre las operaciones de una compañía y su seguridad. Así, si alguien se conecta, accede

a todo el proceso y puede causar un daño. "No hay una cultura de decir: 'Voy a controlar, voy a investigar qué pasa', porque se carece de monitoreo y de auditorías", explicó el ingeniero Fayçal Daira, con amplia experiencia en empresas de producción de cemento y de agua.

El conferencista ilustró el alcance de la problemática con el ataque a la fábrica de papel Georgia Pacific (Port Hudson, Luisiana, Estados Unidos) y el apagón en Ucrania. La primera ocurrió cuando un exgerente de sistemas, que había sido despedido, se conectó con su contraseña a la red de la empresa y causó un daño de más de un millón de dólares en la producción. "Esa entidad no contaba con auditoría, el acceso VPN (*Virtual Private Network*) no había sido revocado y faltaba monitoreo de ICS (*Integrated Computer Solutions)*", señaló y agregó que encontraron al responsable 15 días después del suceso cuando al conectarse a la VPN vieron que allí estaba.

Ciberataque a red eléctrica en Ucrania

El 23 de diciembre del 2015, la mayor parte de Ucrania quedó a oscuras. Era el resultado de un ataque que había comenzado a planearse ocho meses antes e incluyó dos ofensivas: una que comprometió algunas partes del sistema de distribución y otra que bloqueó las llamadas de aviso de los usuarios sobre la falta de luz.

Fue un hecho perfectamente manejado por los atacantes, explicó Fayçal Daira; inicialmente investigaron a la organización, el funcionamiento de la red operacional y la red interna. La ofensiva tuvo muchas etapas y los delincuentes identificaron las características de seguridad de las dos redes.

Al analizar los hechos después del ataque se encontró que no había auditorías y la información forense era limitada porque el *malware* tenía funciones de borrado, por lo cual desaparecieron las trazas. Además, la compañía no contaban con un procedimiento para seguir en caso de un siniestro de este tipo.

Fuentes de ataques

Fayçal Daira enumeró algunos de los más frecuentes en industrias:

- *Correos Spearphishing*. Mensajes que son enviados a un conjunto seleccionado de empleados de la compañía. Estos incluyen un mecanismo escondido para activar una función maliciosa y desde allí tratar de llegar al servidor central de la empresa. "Una vez el servidor está infectado, tienen acceso a este y a las claves de la compañía", explicó.
- *Watering Hole*. Los atacantes comprometen un sitio web que muchos trabajadores visiten, por ejemplo un periódico. Y esperan a que uno se conecte desde su computador en la empresa, para así ingresar al sistema.
- *USB Key*. Se infecta la memoria USB, probablemente de alguien que no es empleado directo de la compañía, pero que eventualmente tendrá acceso a los computadores y conectará la USB en el transcurso de sus labores.

Fuentes de ataques

Spearphising
Es una forma sencilla con la que todavía operan los ataques. Envían e-mail efectivos porque desencadenan una emoción de urgencia o de manejo directivo.

Watering Hole + Vulnerability
Uso de una página web común para iniciar un ataque por una vulnerabilidad.

USB Key
La herramienta perfecta para infectar varias máquinas.

Exempleados
La forma de ataque más peligrosa.

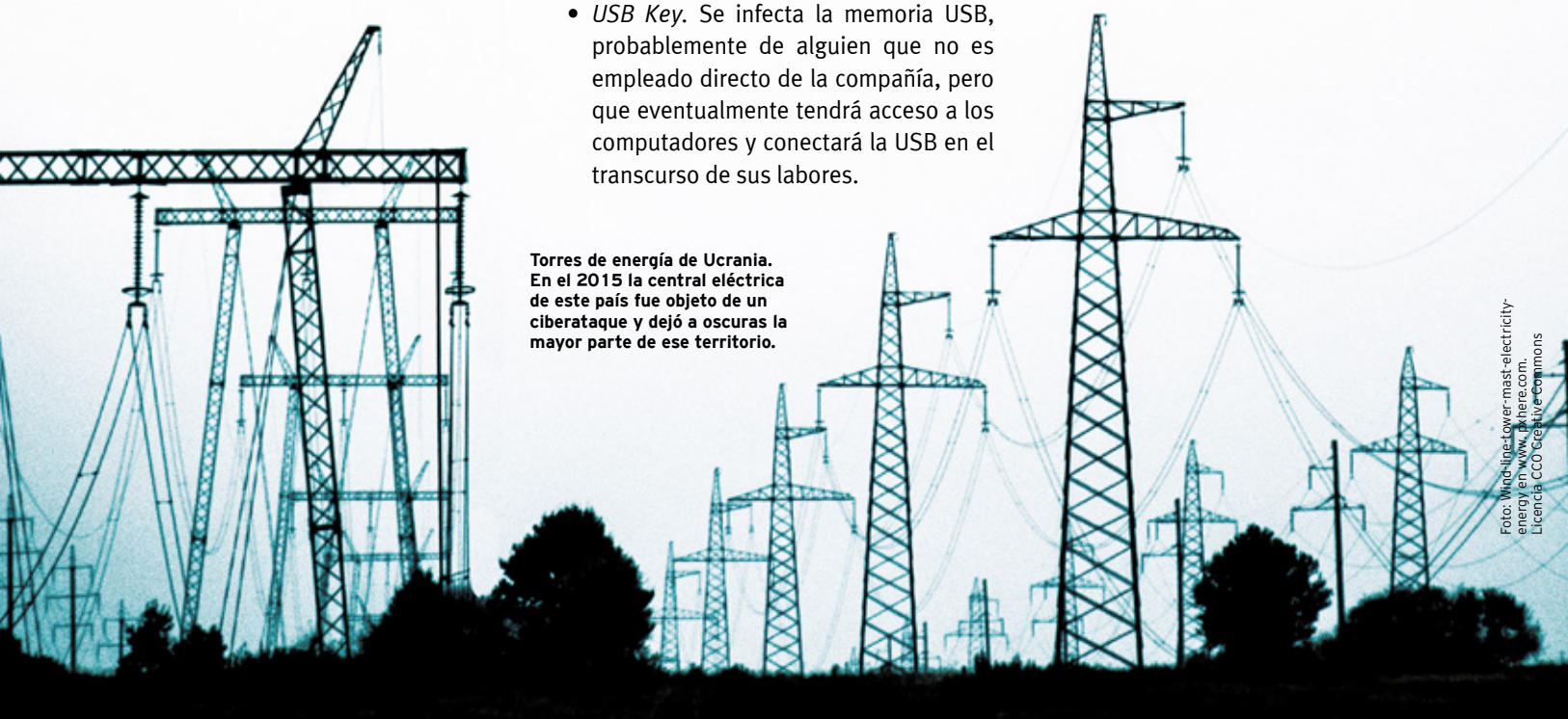
Cuadro presentado por Fayçal Daira.

Seguridad de las redes

Algunos puntos, expuestos por el conferencista, para mejorar la seguridad de una red son:

Antes de poner más capas de seguridad en el sistema, es importante mejorar lo que se tiene.

- Dispositivos y personas seguros. Se debe incluir la seguridad cibernética en



Torres de energía de Ucrania. En el 2015 la central eléctrica de este país fue objeto de un ciberataque y dejó a oscuras la mayor parte de ese territorio.

Foto: Wind-line-tower-mast-electricity-energy en www.pxhere.com. Licencia CCO Creative commons

la política de procesos industriales. La estrategia de alta tecnología alemana se basa en el documento Industry 4.0, que promueve el uso de tecnología para la revolución de la industria.

- Usar protocolos estándares. OPC UA (*OLE for Process Control Unified Architecture*) puede mejorar las prácticas de seguridad. Es conveniente auditar todos los accesos a la red operacional considerando cuándo, quién y qué hizo, e invertir en ciberseguridad.
- Usar autenticación de dos factores. El ataque en Ucrania se habría evitado si fuera necesario autenticarse con dos factores; un atacante necesitaría conocer los dos para lograr acceso al sistema.
- *OT Security*. Proteger y monitorear la red OT (*Operational Technology*), durante y fuera de un horario laboral. Esto incluye usar productos de seguridad en la red OT.
- Políticas de administración. Algunos ejemplos de este tipo de políticas son: Definir procesos para remover los permisos de los usuarios que ya no trabajan con una compañía y restringir el empleo de USB para evitar la ejecución automática de *scripts*/ejecutables.
- *Enable Auditing*. Programas de *software* como Windows y otras aplicaciones tienen incluidos sistemas de auditorías y estos deberían habilitarse y configurarse.

Foto: Óscar Aldair Morales

Fayçal Daira, gerente de Preventa y Operación en Stormshield, AirBus Defence & Space, Estados Unidos.

Defensas activas y pasivas para arquitecturas seguras

Con el advenimiento del IoT es necesario establecer la ciberseguridad desde el diseño de los dispositivos y las redes. Así, se reducirá el riesgo frente a los peligros y las vulnerabilidades dentro de la red, cada vez más amplia y variada.

En la era digital, los riesgos de ataques se incrementan y son más complejos: no solo hay más amenazas y espionaje, sino que han aparecido programas *malware* como Stuxnet, Duqu y Flame, al tiempo que las ofensivas pueden estar en manos de grandes mafias terroristas, gobiernos o bandidos que simplemente contratan los servicios de un *hacker* en la web.

Este es el panorama de la nueva generación de cambios que se están dando con internet descrito por Diego Zuluaga*, encargado senior de la seguridad de Isagen, quien habló de la relación de IoT con la Tecnología de Operación (TO).

El conferencista precisó que hay nuevas dimensiones en el internet de las cosas, por la interacción de las máquinas y la gran variedad de dispositivos, que implican retos de seguridad y privacidad. Con IoT las cifras de aparatos conectados hoy alcanzan billones, lo que provee una superficie más grande para los ataques. Antes se podía atentar a través del computador en la casa o la oficina, ahora es posible hacerlo desde los teléfonos móviles, es decir, desde cualquier lugar por donde nos movamos. Además la información no está solo en el disco duro de un computador local, también se replica a la nube y cualquiera de esos puntos puede ser atacado. "Estamos involucrando el cuerpo físico, hay dispositivos que pueden causar la muerte. Los que venimos del mundo de seguridad en operación sabíamos que podíamos tener dificultades importantes que podrían afectar las vidas de las personas".

Después de Stuxnet (que atacó sistemas de control en una planta nuclear en el 2010), explicó el conferencista Zuluaga, comenzaron a aparecer otros programas maliciosos cada vez más avanzados; por ejemplo, algunos permiten abrir la cámara y el micrófono de un teléfono y buscar dispositivos *bluetooth* alrededor. "Vemos que Duqu 2.0, en junio del 2015, ni siquiera debe estar en disco duro, es un *malware* que funciona en la memoria, no se va a encontrar rastro, él simplemente confía en que hay vulnerabilidades en el entorno con las cuales se va a replicar en todas las máquinas que pueda". Agregó que hay otros como *Ramsonware* que seguirán popularizándose porque son una forma fácil de obtener beneficios económicos.

El sector energético, en riesgo

En la anatomía de un ataque, este no va directo al objetivo: es planeado y coordinado con tiempo; primero pasan por la red