Ciberseguridad para que IoT se afiance en la red

Cada momento crecen vertiginosamente las posibilidades que ofrece internet de las cosas (IoT), en casas, edificios, ciudades, redes, autos inteligentes o el IIoT (industrial). Esta perspectiva que exige mayores esquemas de seguridad fue tratada en el foro organizado por el Departamento de Ingeniería de Sistemas y Computación (DISC), con el apoyo de la empresa francesa Airbus Defense and Space (DS) Cibersecurity.

Imagen: Jeferrb en www.pixabay.com. Licencia CCO Creative Commons

Un ataque cibernético a una central eléctrica para dejar a oscuras varias ciudades, asesinar a alguien a través de un dispositivo cardiaco o escuchar las conversaciones de un salón mediante de un televisor apagado eran asuntos de películas de ciencia ficción hace una década.

Sin embargo, ahora estos hechos son una realidad. Con el advenimiento, la rápida expansión y la consolidación del internet de las cosas (IoT) aumentó el confort de los usuarios al contar con nuevos dispositivos en la red, pero también crecieron las vulnerabilidades en la seguridad cibernética de la cotidianidad familiar, industrial y empresarial.

Este panorama con sus problemáticas fue tratado en el "3.er Foro en Seguridad de la Información: Seguridad en IoT, una tecnología emergente en la era de la economía digital" que se llevó a cabo el 15 de marzo del 2017, con el apoyo de Airbus, como parte de la promoción del año Francia-Colombia. Participaron representantes del Gobierno, la industria y la academia quienes recalcaron sobre la necesidad de construir dispositivos IoT seguros, educar a los usuarios y diseñar ensambles protegidos en todas sus aplicaciones. También se habló de los peligros de pérdida de privacidad.

La conferencia central en el contexto industrial "*Security challenges in Industrial Environments: the conflict between operations and security*" la pronunció Fayçal Daira, de Stormshield (AirBus Defence & Space, Estados Unidos) (ver págs. 12-14). Y sobre "Ciberseguridad en la era digital: más allá de la Información, de la To al IoT" habló Diego Zuluaga, especialista senior de Seguridad en Isagen, Colombia (ver págs. 14-15).

Generar datos como infraestructura

La visión del Gobierno fue presentada por Iván Castaño, encargado de Investigación-Desarrollo-Innovación (I + D + I) de MinTIC, quien recalcó la necesidad de generar datos como infraestructura y de ofrecerle seguridad al usuario *end-to-end*, una protección completa que incluye la red, la persona y los dispositivos.

Hoy se dice que los datos son el nuevo petróleo. Porque conoce ese valor, MinTIC está tratando de hacer que los datos se entiendan como infraestructura, es decir que se conviertan en materia prima de la producción y el conocimiento.

Foto: jeshoots.com en http://bit.ly/2hc0v9E Licencia CCO Creative Commons

Semáforo inteligente.

Foto: David Berkowitz en www.pixabay.com, IoT, Connection, Cloud. CCO Creative Commons

Nevera inteligente. Con la tecnología de internet de las cosas se interconectan artefactos de nuestro entorno para ser controlados de forma remota.

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