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

Foto: Óscar Aldair Morales

Diego Zuluaga, de Isagen.

corporativa, buscan la red industrial y luego van al objetivo real.

Una evidencia de lo anterior se da en el sector energético que, por interesar a muchos públicos, fue uno de los objetivos principales de las ofensivas. Havex, por ejemplo, fue un *malware* usado en Tecnología de Operación (TO). no directamente contra las empresas sino contra la cadena de suministro, pues atacó a un proveedor de los sistemas SCADA al incluir un troyano en los sitios web disponibles para actualizar el *software* de estos sistemas, de tal forma que cuando se descargaban actualizaciones se afectaban los equipos.

Zuluaga recordó que el apagón en Ucrania (ver "Seguridad cibernética, prioridad en políticas industriales", pág. 12) fue planeado contra 186 ciudades de las cuales 103 quedaron completamente oscuras y cerca de 80 fueron afectadas parcialmente. "Lo que previene un ataque de estos es una arquitectura organizada y establecida con anterioridad. Y que tenga defensas pasivas y activas, que haya inteligencia para saber qué pasa en el entorno", explicó.

El primero, en el 2015, se orientó contra la compañía de distribución de energía. En el 2016, el 6 de diciembre, el blanco fueron las empresas de trasmisión y también generó apagones en todo ese territorio. "Por eso algunos dicen que pueden estar usando al país como laboratorio de ataques a la infraestructura crítica", dijo.

Por otro lado, se refirió a las redes inteligentes de energía y a los millones de medidores que se instalarían en las casas o edificios. Y señaló que se pueden presentar diferentes peligros: de privacidad, de acceso, de borrado, de negación del servicio o de ataque desde el centro de operaciones al cortar la señal a todos y generar un apagón.

Por todos esos riesgos, agregó, hay que trabajar en un ecosistema en donde intervengan las industrias, los operadores, las fábricas, los que saben de seguridad, los consultores, para solucionar los problemas que surgen en este entorno y hacerlo de manera segura.

Y reiteró que la ciberseguridad debe establecerse desde el diseño para evitar incidentes que no solo afectan al mundo virtual, sino al real, puesto que estamos entrando a un entorno donde se tocan IoT y TO con el ámbito físico.

* Diego Zuluaga precisó que las opiniones emitidas en el foro no representan a la compañía donde trabaja.

Foto: U.S. Navy photo by Mass Communication Specialist 2nd Class J.T. Bolestridge [Public domain], via Wikimedia Commons

Un especialista en operación evalúa imágenes tácticas en un centro de combate de la US Navy.

Operational Technology (OT)

Los sistemas informáticos empleados en el manejo de las operaciones industriales, diferentes a las operaciones administrativas, se conocen como Tecnología de Operación (OT, por sus siglas en inglés). Los sistemas operacionales incluyen la gestión de la producción, control de operaciones mineras o hidroeléctricas, monitoreo de petróleo y gas, entre otros.

Industrial Control Systems (ICS) o Sistema de Control Industrial es una parte importante dentro de la OT e incluye sistemas para supervisar y controlar procesos industriales. Pueden ser el consumo de energía en las redes eléctricas o las alarmas de los sistemas de información de la construcción.

La mayoría de los ICS se ubican en un sistema de control de proceso continuo, gestionado a través de controladores lógicos programables (PLC), o sistemas discretos de control de procesos (DPC).

Los ICS suelen administrarse a través de sistemas de supervisión y adquisición de datos (SCADA) que proveen una interfaz gráfica de usuario para que los operadores puedan observar fácilmente el estado de un sistema o recibir alarmas.

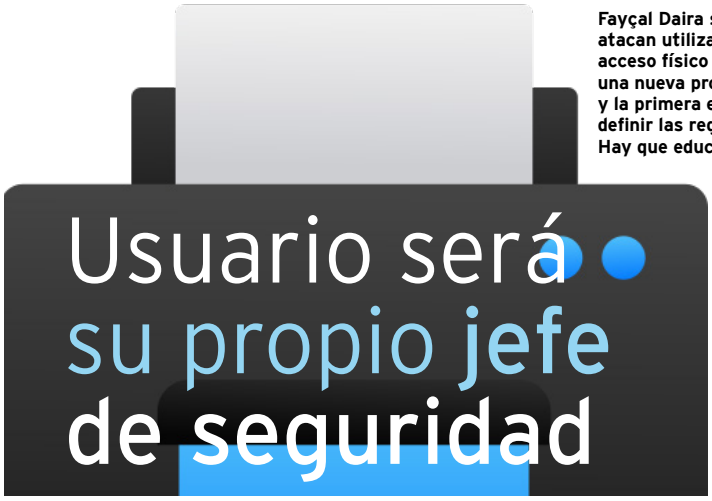

Imagen: Fabián Alexis en github.com/ Licencia Creative Commons

Fayçal Daira señaló que algunas personas atacan utilizando una impresora o por un acceso físico que está conectado a una red. Es una nueva problemática que debemos incluir y la primera etapa es tener los procesos, definir las reglas y los modelos de seguridad. Hay que educarse sobre los temas.

Usuario será su propio jefe de seguridad

Apartes del panel "Visión y elementos técnicos en la seguridad en IoT e industrial IoT".

Oportunidades y ventajas con el IoT industrial

Mayor Milena Realpe

Esta tecnología se está extendiendo y el Gobierno no es ajeno a ello. En el sector militar se trabaja en sistemas de comando y control terrestres, marítimos y aéreos. Y en defensa se componen de vehículos y medios no tripulados.

En el área corporativa ha servido para el control de activos, inventarios y sensores conectados a redes de internet, de seguimiento y control, los cuales han ayudado a tener información en tiempo real. Y a los funcionarios, en los celulares, las oficinas y las instalaciones, les ha permitido aumentar la seguridad y automatizar procesos.

Luis Javier Parra

Como cofundador de Info Projects veo en IoT la base para desarrollar requerimientos de conocimiento y consultoría. Como empresario advierto la posibilidad de generar una cantidad de servicios novedosos para que empresas, desde las más pequeñas hasta las más grandes, puedan utilizar estas tecnologías de TI con una aplicación segura y que afecte de buena manera el sistema central de sus negocios.

Sandra Rueda

La academia da la posibilidad a los estudiantes de empezar a trabajar con estas tecnologías e integrarlas, pero el gran desafío es hacerlo de forma responsable.

Retos respecto a la seguridad

Fayçal Daira

En IoT hay diseños que nunca tomaron en cuenta la seguridad. El caso Samsung, con el teléfono celular Galaxy Note 7, fue un desastre. La seguridad debe estar desde el inicio del diseño, pero cada vez hay personas que encuentran más tecnología. Es un partido entre proteger y arrancar. Hay que mejorar el proceso para que sea más ágil y para que en la industria sea posible fabricar partes que se puedan remplazar fácilmente.

Mayor Milena Realpe

Un reto importante es cómo vamos a gestionar estos dispositivos, si no hay estándares en el tema de IoT, ni protocolos que se puedan aplicar, pese a que cada vez están más conectados a nuestras redes. Otro desafío es en las infraestructuras críticas digitales o en la parte cibernética, porque cuantos más dispositivos están conectados a la red, hay más riesgos y vulnerabilidades.

Riesgos en la industria y los usuarios

Mayor Milena Realpe

Hay que mantener actualizados los sistemas de defensa, buscar alternativas; el análisis de vulnerabilidades se hizo más complejo porque tenemos un nuevo punto desde donde se pueden meter diferentes tipos de infección o de ataques.

Luis Javier Parra

Los responsables de seguridad van a requerir una cantidad de herramientas que no se han construido o que pueden ser mejor construidas.

Sandra Rueda

El usuario común y corriente tendrá que asumir los roles de administrador y jefe de seguridad en su oficina y en su hogar.

Foto: Óscar Aldair Morales

El panel moderado por Tito Neira, de Scotiabank, contó con la participación de Diego Zuluaga, de Isagen. Mayor Milena Realpe, jefe de Prospectiva del Comando Conjunto Cibernético; Fayçal Daira, de Stormshield; Sandra Rueda, profesora asistente del DISC, y Luis Javier Parra, cofundador de Info Projects.