IoT: interconexión digital, un reto mayor de seguridad

Los cambios en los diferentes estilos de vida que conllevan los avances tecnológicos son abrumadores y las generaciones llegan a verlos reflejados en su diario vivir.

Joshsua J. González Díaz, MSc.

Introducción

En tiempos de cambio, quienes estén abiertos al aprendizaje se adueñarán del futuro, mientras que aquellos que creen saberlo todo estarán bien equipados para un mundo que ya no existe. Eric Hoffer.

La próxima era de Internet de las Cosas (IoT) borrará la línea entre nuestras vidas, en cuanto a la perspectiva del mundo físico y aquel al cual estamos conectados “en línea”. Los ataques dirigidos a nuestros espacios en la red, donde somos moradores ciberpespaciales, pondrán en peligro nuestra seguridad física, cosa que puede llegar a sonar como historia de ciencia ficción. Tradicionalmente, los vectores de ataque a nuestros lujos fundamentales tecnológicos han requerido manipulación física, sobre todo porque el acceso a la infraestructura se ha llega-

do a limitar desde Internet. Esto está a punto de cambiar con la participación causada por un futuro con miles de millones de "cosas" conectadas a Internet, y de cómo un ataque simple puede causar un apagón perpetuo de bombillas LED en una autopista, o de cómo las decisiones de seguridad mal tomadas pueden llegar a violar groseramente la seguridad física y la privacidad de las familias, o cómo la inseguridad de los vehículos eléctricos poderosos pueden poner su vida en riesgo y la sustracción de información mediante electrodomésticos altera su privacidad.

Existe un riesgo tangible en los dispositivos IoT y, cada vez, vamos a depender en mayor grado de la tecnología, a medida que avanza el tiempo. Una vez que comencemos a comprender la causa de las actuales vulnerabilidades de seguridad en los dispositivos de hoy, comenzaremos a establecer el camino para un futuro que nos ayudará a habilitar estos dispositivos para mejorar y aumentar de forma segura nuestras vidas.

Los atacantes maliciosos ya están trabajando en ello, descubriendo y explotando estos defectos de seguridad y seguirán encontrando formas astutas e inimaginables de abusar de sus conocimientos de todas las maneras posibles. Estos atacantes contemplan desde estudiantes universitarios curiosos a grupos delictivos y patrocinados por gobiernos u organizaciones al margen de la ley –y no propiamente nos referimos a grupos de *hacktivismo*–, interesados en aterrorizar a los individuos y/o poblaciones. El impacto de las vulnerabilidades de seguridad en los dispositivos IoT puede conducir a un compromiso masivo de privacidad y causar daño físico. Las apuestas son altas.

IoT es el futuro, el futuro de la industria, el futuro de las organizaciones y pro-

Ilustración 1. Se descubre un envío de electrodomésticos espía procedente de China. Disponible en: https://es.rbth.com/cultura/technologias/2013/10/30/se_descubre_un_envio_de_electrodomesticos_espia_proceden_33821

bablemente su futuro personal. Bienvenido al futuro. Se deletrea I-o-T. Todo esto puede parecer un 'bombo' ahora, pero al final resultará ser bastante discreto; IoT es muy, muy real.

Dispositivos *Wearables y Healthcare,* es más que estar a la moda

En muchos casos de historias de ciencia ficción, donde Hollywood mostraba cosas que llegaban a considerarse fantasiosas, como el hecho de que por medio de un reloj se pudiese uno comunicar, como era el caso de Dick Tracy, o la posibilidad que en este mismo dispositivo un agente espía extrajera herramientas para la consulta y robo de información, como era el caso del agente 007. Los dispositivos *wearables* (aquellos dispositivos electrónicos que pueden ser usados como parte de su vestimenta) es un tema que ha recibido la atención de muchos pioneros en tecnología, tal como lo llega a mostrar el nuevo desafío de "Make it Wearable"[1] de $ 5,000 publicado por Intel. Este desafío recompensa tanto a visionarios como a los constructores que conciben o construyen aplicaciones portátiles que pueden cambiar la computación personal en nuevas direcciones innovadoras. Los dispositivos *wearables* ahora están en el centro de casi todas las discusiones relacionadas con Internet de las cosas (IoT), y la gama completa de nuevas capacidades que la conectividad generalizada puede traer.

A menudo, algunas de estas discusiones crean más preguntas que respuestas. Tal vez eso es algo común, dado que todavía estamos en las primeras etapas de su ciclo de vida, pero algunas preguntas tienen que ser respondidas antes de un verdadero "despliegue" de dichos dispositivos. Por ejemplo, "¿Estos dispositivos van a ser sólo periféricos para un teléfono inteligente, o hay un papel más importante para ellos como parte de la Internet de las cosas?"

Una de las primeras funciones de los dispositivos, ya están relacionadas con la identificación y aún más sorprendente, con la seguridad. Quizás no considere que usted use en el trabajo un dispositivo *wearable*, pero estos pueden llegar a proporcionar características para su identificación y manejo de la seguridad dentro del ambiente laboral. Algunas configuraciones avanzadas incluyen algunas capacidades biométricas (como la activación mediante huellas dactilares, por lo que sólo el propietario del dispositivo pueden realizar acciones sobre este).

Existen implementaciones de estos dispositivos orientados a la salud y muchas veces a la actividad física, y ofrecen mediciones biométricas tales como frecuencia cardíaca, niveles de transpiración e incluso mediciones complejas como los niveles de oxígeno en el torrente sanguíneo. Los avances tecnológicos pueden permitir que los niveles de alcohol u otras similares se realicen a través de un dispositivo *wearable*. La capacidad de detectar, almacenar y rastrear mediciones biométricas a lo largo del tiempo y luego analizar los resultados, es sólo una posibilidad interesante. Y, más allá de un tipo de entretenimiento en actividad física, se encuentra esa línea

[1] Iniciativa dada por Intel, concurso que entregaba US$5.000ºº. Extraído de: https://newsroom.intel.com/chip-shots/chip-shot-nixie-wins-500000-grand-prize-in-intel-make-it-wearable-challenge/

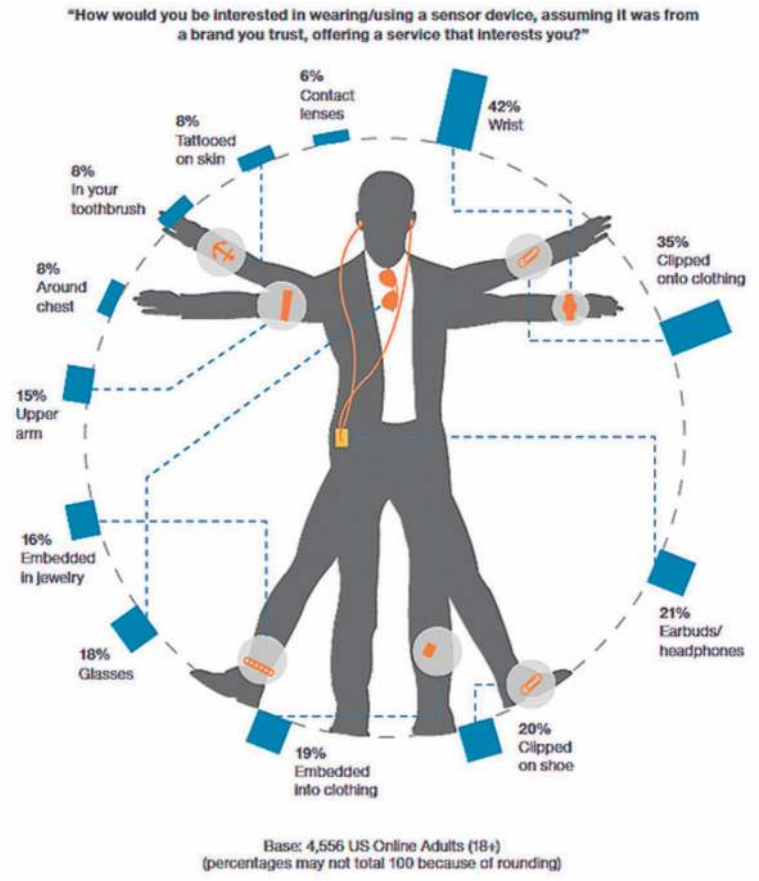

Ilustración 2. Extraído de North American Consumer Technographics Consumer Technology Survey 2014

de los dispositivos de *health-care* que llegan a basarse en un mismo principio de un dispositivo *wearable*, pero con fines de cuidado de la salud. Claro ejemplo de ello podría ser el seguimiento de la temperatura corporal, que al ser analizada podría proporcionar una indicación temprana de un resfriado.

Otras capacidades adicionales de los dispositivos usables son más mundanas, pero también pueden proporcionar información que podría ser útil para ajustar los controles ambientales. Los ejemplos anteriores podrían contemplar un teléfono inteligente como el control central para la entrega de estas capacidades, pero ¿es realmente el enfoque más eficiente? ¿Sería mejor si los dispositivos de Internet de Cosas (IoT) pudieran comunicarse directamente? Ciertamente, nadie quiere ser obligado a usar su teléfono inteligente para cada transferencia de información de sus dispositivos *wearable*. Tal vez un modelo mejor es que el teléfono inteligente puede ayudar a configurar los modos de operación, así como el nivel de privacidad que desea aplicar. Una vez que la comunicación "estratégica" está en su lugar, todos los dis-

positivos pueden comunicarse de la manera que se les ha permitido.

Veamos un ejemplo sencillo. Digamos que el reloj inteligente está captando sus lecturas biométricas para que pueda obtener una alerta temprana de una posible enfermedad (tal vez porque estaba en un avión). Supongamos además, que tomó el viaje de avión para una entrevista de trabajo y que está en su camino hacia su primera reunión. ¿Desea que sus lecturas biométricas estén disponibles para la persona que realiza la entrevista? Probablemente no. ¿Sería posible utilizar el teléfono inteligente para proteger las lecturas biométricas en tiempo real (y cualquier historial de lecturas) del acceso del entrevistador? Alternativamente, si su reunión no fue para una entrevista de trabajo, sino un chequeo anual de su médico, usted querrá permitir el acceso a todos sus datos biométricos.

Los dispositivos *wearables* le podrían permitir conectarse automáticamente a dispositivos alrededor de la casa también. Un posible escenario sería la preferencia de iluminación preferida cuando se use la televisión según la ubicación dentro de la sala. Usted podría encender el televisor y su dispositivo portátil podría ayudar a ajustar el nivel de iluminación de las luces LED conectadas dentro de la habitación. Una casa inteligente podría incluso soportar el bloqueo automático de la luz de las ventanas que creaban reflejos en el televisor. Incluso la retroiluminación en la pantalla del televisor LCD se puede ajustar y todos los ajustes optimizados para ahorrar energía, así como la creación de la experiencia de visualización más favorable. Todas estas interacciones podrían hacerse de forma automática, directamente entre dispositivos, una vez que la estrategia global se ha establecido a través de una interfaz de teléfono inteligente.

Una tecnología que abusa de su iniciativa

El apagón del año 2003 fue generalizado y afectó a las personas a lo largo de partes del noreste y medio oeste de los Estados Unidos y Ontario. Aproximadamente, 45 millones de personas fueron afectadas durante dos días. Sólo en Nueva York, fueron reportadas 3.000 llamadas de incendios, debido a incidentes relacionados con individuos que usaban velas. Hubo 60 casos de incendios de alarma que fueron causados por el uso de velas y dos casos de muerte. En Michigan, las velas encendidas que fueron olvidadas causaron un fuego fatal que destruyó una casa.

La cuestión sorprendente no es que se produjera el apagón del noreste, sino cómo el mundo desarrollado depende de la electricidad. De la misma manera, giramos un interruptor y esperamos el resplandor instantáneo de la 'llama eléctrica'. Abrimos la nevera y esperamos que nuestra comida y bebidas nos esperen a la temperatura adecuada. Caminar hacia nuestras casas y esperar que el aire acondicionado mantenga de forma continua y automática un equilibrio cómodo entre las temperaturas fría y caliente. Han pasado aproximadamente 100 años desde que descubrimos cómo generar electricidad. Antes de eso, las casas estaban encendidas con lámparas de queroseno y calentadas con estufas. Nuestro nivel actual de dependencia de la electricidad es fenomenal; las ciudades y negocios se detienen en segundos por un apagón.

Ahora con el uso de tecnologías de IoT para la automatización de este tipo de servicio, los dispositivos IoT que controlan la iluminación deben incluir la seguridad como parte de su arquitectura y diseño. El sistema de iluminación de tonos de Philips es uno de los dispositivos IoT más populares del mercado actual y ha presentado varios problemas de seguridad, incluyendo cuestiones fundamentales como la seguridad con contraseña y la posibilidad de que el *malware* abuse de los mecanismos de autorización débiles para causar apagones sostenidos. Por otro lado, la complejidad de interconexión con nuestro espacio ciberespacial (Facebook) con dispositivos IoT que utilizan servicios como IFTTT son servicios útiles y permitirán nuestro futuro automatizado, pero es necesario pensar en las implicaciones de las cuestiones de seguridad y privacidad.

Se ha descubierto que una partida de aparatos eléctricos enviados a San Petersburgo desde China servían también como terminales de espionaje. Se colocaron chips especiales en planchas y hervidores de agua, que se pueden conectar a la red y son capaces de expandir virus y spam. Los equipamientos se conectan vía wifi a cualquier ordenador no protegido en un radio de 200 metros[2].

Los empresarios recibieron ayuda de miembros de la aduana para descubrir los productos “espía”. Antes de ser enviados desde China a los rusos les extrañó el peso de los aparatos, que difería ligeramente con lo apuntado en los documentos. La partida se detuvo en la frontera y fue examinada por expertos en electrónica. Se descubrió que tenían incorporados chips diseñados para distribuir spam y virus informáticos.

Sin embargo, alrededor de 30 planchas, hervidores de agua, teléfonos y cámaras de vídeo del lote inspeccionado han sido distribuidas en tiendas de San Petersburgo. No está claro si esta tecnología ha llegado también a otras regiones de Rusia[3].

[2] Jamy Tostadora: N Brunstein diseñó un concepto de tostadora llamada "Jamy Toaster", que utiliza el Wi-Fi al centro meteorológico para averiguar el pronóstico del tiempo. Y cuando tuesta un pedazo de pan para el desayuno 'imprime' el pronóstico del día sobre el mismo.

[3] Extraído de: https://es.rbth.com/cultura/technologias/2013/10/30/se_descubre_un_envio_de_electrodomesticos_espia_proceden_33821

Ilustración 3. JAMY TOASTER, Tostador inteligente predicción estado del tiempo.

El poder de IoT radica en parte, en su capacidad de operar no sólo en el mundo físico de las cosas reales, sino también en el mundo virtual, donde las cosas se digitalizan y sólo existen como información digital. Debido a que atraviesa ambos mundos, IoT puede enviar datos digitales a través de la red a un controlador distante conectado a un dispositivo físico, por ejemplo una máquina de producción importante.

Dichos datos entonces indican a la máquina que se apague o encienda, dependiendo de lo que usted quiera que haga.

Pensemos un momento en esto: se tiene un sistema virtual que controla remotamente una máquina física. ¿Puede ver por qué la seguridad es tan importante para IoT? Sin un enfoque de seguridad eficaz, un *hacker* podría apagar una pieza importante de un equipo de producción y mantenerlo apagado, tal vez en algún momento crítico de producción.

Es posible que ni siquiera sepa que el problema existe e intente volver a conectar la máquina hasta que descubra que la producción se ha detenido y envía físicamente a alguien a la máquina para reiniciarla en forma manual.

El ataque de Stuxnet, donde el gusano penetró inicialmente en una instalación nuclear iraní, llevó a las máquinas a un sobrecalentamiento más allá del punto de ruptura, cerrando la producción durante meses. Se extendió a través de las operaciones industriales en muchos países, lo que llevó a las personas de sistemas a implementar medidas para prevenir incidentes de tipo Stuxnet.

A falta de detalles sobre cómo el ataque realmente funcionó, se apresuraron a soluciones rápidas como el despliegue de *Firewalls* frente a los equipos en el taller. Desde entonces, la industria ha aprendido que los *Firewalls* tradicionales son un sobrante de la era de la defensa perimetral de TI, que nunca detendría un ataque de este tipo.

La seguridad como un desafío más para la gestión de riesgos

El proceso para gestionar los riesgos de seguridad de IoT es el mismo que para cualquier otro riesgo:

- Identificar las posibles amenazas individuales.
- Evaluar cada amenaza en términos de su probabilidad de ocurrir y el daño que puede causar.
- Identificar y desplegar medidas defensivas adecuadas a la probabilidad de cada riesgo y posibles daños.

Diferentes tipos de vulnerabilidad producen diferentes amenazas con el potencial de diferentes daños. Una amenaza que potencialmente puede apagar una línea de montaje de fábrica o una plataforma petrolera es de una magnitud diferente a la de una amenaza que puede interferir con un proceso de almacenamiento del inventario. Mediante la evaluación del valor en riesgo, es posible tomar decisiones informadas sobre cuánto invertir en medidas defensivas. De esta manera, invertir en seguridad IoT no es diferente de comprar cualquiera de los diferentes tipos de seguros que la organización necesita. En todos los casos, la inversión debe ser proporcional a la probabilidad del riesgo y al valor potencial de la pérdida o daño.

Las compañías han estado desplegando con éxito IoT bajo diversos nombres por años. Sí, hay riesgos serios, sin embargo la industria ha estado ocupada desarrollando estrategias defensivas y participando en esfuerzos colaborativos para contrarrestar varios riesgos con métodos defensivos, productos y mejores prácticas. Todo comienza con una sólida identificación, evaluación y gestión del riesgo.

Sin embargo, es importante entender que IoT no tiene una estrategia mágica de seguridad. El alcance y la variedad de soluciones IoT evitan eficazmente la aparición de una defensa de seguridad sin fallos. La tecnología IoT está cambiando en forma constante, las soluciones están evolucionando continuamente, y también las amenazas y los vectores de ataque. Usted está tratando con adversarios activos que trabajan en forma permanente para ser más astutos que usted y sus defensas. No es una solución única, y tampoco es su defensa. La gestión de riesgos, como he dicho, es un proceso continuo que debe revisarse al menos una vez al año –quizás con mayor frecuencia–, a medida que cambian las soluciones y surgen nuevas amenazas. La clave para todos nosotros es ser inteligentes y conscientes de los riesgos de TI, y no tener miedo.

Hay muchas razones por las que alguien 'hackearía' una solución IoT. Para algunos, es un acto de exploración de nuevas tecnologías y para unos pocos un acto de guerra o terror. La mayoría –sospecho–, está esperando ganancias financieras al robar datos o secretos comerciales para obtener ventaja competitiva, las razones son tan numerosas y variadas como las tramas de la televisión de muchos programas policiales y del crimen. Una conclusión particular de años de estudios de seguridad es clara: la mayoría de las brechas de seguridad se aprovechan de vulnerabilidades bien conocidas que no se han resuelto a pesar de las amplias alertas, y la mayoría de los atacantes son conocidos por usted, empleados, contratistas o socios de un tipo u otro. En general, los ataques no son ni esotéricos ni exóticos.

La seguridad se ha convertido en uno de los principales inhibidores de la adopción de IoT [4]. Un modelo de separación física de dispositivos es algo inaudito de aplicar, todo debe estar conectado. ¿Cuánto tiempo podría funcionar una organización si el correo electrónico e Internet no estuvieran disponibles? Todo, prácticamente todos los procesos de negocio, dependen de la capacidad de conectarse. Hoy en día, la idea de desconectar una organización de la red global es simplemente absurda.

La verdad es que no todas las amenazas son las mismas y no todas las amenazas tienen el mismo valor para una organización. Su respuesta a diferentes tipos de amenazas y objetivos de amenazas diferentes debe ser medida y proporcional. Por eso –aunque suene a algo que muchas personas en seguridad llegan a predicar y no aplicar– esto requiere la gestión de riesgos.

Desafíos de la seguridad de IoT

El desafío número uno en la gestión de riesgos y la evaluación de amenazas es la gran escala esperada de IoT. Hablamos de los miles de millones de dispositivos conectados. Por supues-

to, muchas organizaciones no tendrán miles de millones de dispositivos conectados. Sin embargo, no tiene que ser un negocio muy grande para encontrarse con un millón de dispositivos conectados, especialmente si se incluyen todos los de sus empleados y otros. Incluso si usted tiene sólo unos miles de dispositivos conectados, representa mucho más, para tratar de manejar el desafío de seguridad sin herramientas automatizadas de análisis, monitoreo y mucho más. Sólo un millar de dispositivos conectados pueden generar corrientes masivas de datos de 24 × 7, así como un gran número de alertas que afectarán cualquier cosa, excepto herramientas automatizadas e inteligentes (basadas en reglas o basadas en políticas) y tecnología [3].

Además, la seguridad encuentra la amplia variedad de dispositivos, incluyendo diferentes tipos de controladores, monitores, medidores y aparatos. Muchos de estos dispositivos pertenecerán a sus empleados, por lo que probablemente tendrán un conocimiento limitado de lo que son y lo que hacen, sin mencionar cómo entender y comunicarse entre ellos.

Mejores prácticas de seguridad

Las prácticas de seguridad de IoT siguen evolucionando. El diseño (arquitectura) y la construcción de una estrategia integrada (holística), debe incluir seguridad desde el principio. No deje la seguridad como un cerrojo al final. Debe ser inherente en su proceso de IoT desde el principio.

Adopte estándares apoyados por la industria, los enfoques patentados minimizaran sus esfuerzos de seguridad en el futuro. Consultar cuando sea necesario los organismos de normalización, así sean asociaciones comerciales, para obtener orientación.

Implemente la seguridad en todas partes: desde el centro de datos central detrás y fuera del *firewall* corporativo y hasta los dispositivos de borde, que en este caso serían aquellos que hemos discutido. Esto significa insistir en que sus empleados y proveedores participen y colaboren en su estrategia de seguridad.

Automatice y monitoree la seguridad de IoT de extremo a extremo. Construir modelos que incluyan análisis predictivo, especialmente analítica basada en la nube. Alertar a la gente para que tome medidas, tan pronto como los problemas se vuelvan evidentes. Los esfuerzos manuales serán rápidamente inundados y rebasados por el volumen de la actividad de IoT, incluso en una pequeña organización.

Segmente el tráfico IoT y el tráfico regular de la red de TI y utilice una infraestructura de red *multitenant* para aislar los problemas. Use segmentación y otros procesos bien conocidos, pero al mismo tiempo trabaje con los proveedores de TI para expandir su *software* y herramientas existentes para manejar vulnerabilidades de seguridad IoT. No se trata de difamar a los diferentes fabricantes y proveedores, pero resista la tentación de implementar herramientas específicas de IoT.

Para finalizar quisiera proponer como un primer paso para afrontar el tema de seguridad frente a IoT: evaluación y monitoreo de riesgos informados, acompañado de una respuesta de seguridad apropiada y proporcional, que

explique el nivel de amenaza específico y la cantidad de valor en riesgo. Los riesgos tenderán a ser similares, solo que utilizan un tipo de tecnología diferente.

Una vez que determine esto, puede elegir la mejor opción de proveedor entre las soluciones de seguridad IoT más apropiadas y construirlo en su ecosistema de IoT desde el principio de manera segura. Otra opción emergente que vale la pena considerar es una póliza de seguro cibernético que algunas compañías de seguros están comenzando a ofrecer. Después de eso, sólo hay un paso final, pero importante: involucrar a sus altos ejecutivos y obtener su apoyo, porque ninguno de ellos querría que su empresa aparezca como una víctima de ciberataque de IoT en la portada de un periódico.

Referencias

[1] Irvine, Cynthia (2014) *Security Education and Critical Infrastructures*.

[2] Ventre, Daniel (2015) *Chinese Cybersecurity and Defense*. Wiley 1st Edition,

[3] Maciej, Kranz (2017) *Building the Internet of Things*. Wiley 1st Edition,

[4] Dhanjani, Nitesh (Early Release – 2017) *Abusing the Internet of Things*. O'Reilly 1st Edition

[5] Pfister, Cuno (2011) *Getting Started with the Internet of Things* O'Reilly

[6] Gragido, Will & Pirc, John (2011) *Cybercrime and Espionage*. Syngress

[7] Andress, Jason & Winterfeld Steve (2011) *Cyber Warfare*. Syngress

Joshsua J. González Díaz, MSc. *Ingeniero de Sistemas de la Pontificia Universidad Javeriana, especialista en seguridad de la información de la Universidad de los Andes, Especialista en Derecho Informático de la Universidad Externado de Colombia y Magíster en Seguridad de la Información de la Universidad de los Andes. Actualmente, se desempeña como profesor instructor de la maestría en Seguridad de la Información en la Universidad de Los Andes y CEO de la empresa de consultoría Stark Industries SAS.*