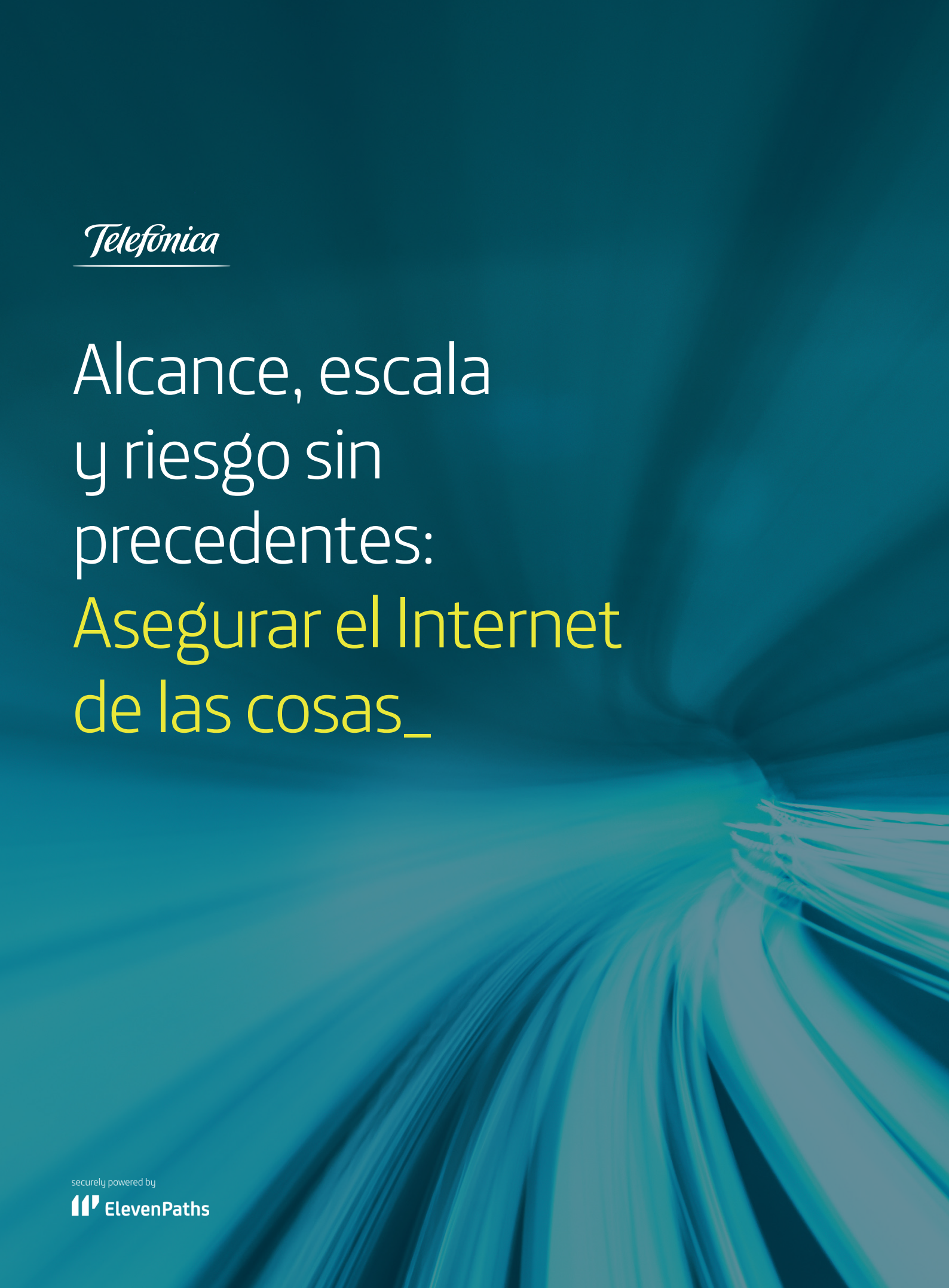
Telefónica

Alcance, escala y riesgo sin precedentes: Asegurar el Internet de las cosas_



securely powered by ElevenPaths

Prólogo de Telefónica_

Aunque el Internet de las cosas (IoT) puede verse como una novedad, no es más que la evolución natural de algo que ha recibido finalmente un nombre con gancho, una marca que integra las consecuencias en un término único y atractivo. Desde su nacimiento, los dispositivos se han conectado a Internet. Solo que ahora los dispositivos son más pequeños, más atractivos, más móviles y están mejor conectados. El Internet de las cosas ofrece ventajas casi infinitas, pero la sociedad necesita reaccionar con rapidez.

No es tanto que la tecnología o el concepto hayan cambiado. Han cambiado las personas que implementan, desarrollan y utilizan estos dispositivos así como cómo y dónde los utilizan. La primera alusión a la privacidad y la seguridad debe hacerse en el momento en que exista un consumo masivo y normalizado. No cometamos los mismos errores del pasado, no esperemos hasta el último momento para establecer las prioridades en materia de seguridad para después lamentar que es demasiado tarde para modificar ciertos «hábitos adquiridos».

Las amenazas para la seguridad del IoT no son tan diferentes de las de otros entornos. No se han creado nuevos problemas de seguridad, solo han evolucionado desde áreas como la seguridad industrial, las redes de distribución y la seguridad de la información. Las amenazas con respecto al robo de identidad siguen estando vigentes, si bien ahora se extienden también a la identificación de uno mismo entre dispositivos.

Las amenazas de denegación de servicio (DoS), se plantean desde el punto de vista de la informática en la nube y se ha desarrollado `malware' que infecta toda clase de sistemas. Las motivaciones de estas amenazas no han variado demasiado, sino que más bien se han intensificado y diversificado. Los piratas informáticos continuarán estando motivados por razones económicas e ideológicas, y la ciberguerra seguirá afectando a los dispositivos presentes en nuestras vidas. Y por si esto no fuera suficiente, los piratas informáticos ven un abanico de nuevas posibilidades en el IoT,

con objetivos estratégicos para poner en peligro la seguridad de infraestructuras críticas y, consecuentemente, la seguridad de todos los ciudadanos.
Es cierto que la tecnología en la que se basa IoT ha evolucionado para abordar la escala y la diversidad de dispositivos (con nombres nuevos en escena como Zigbee o 6LoWPan), pero estamos seguros de que es solo cuestión de tiempo para que se descubran nuevas vulnerabilidades en torno a estas tecnologías recientes. Por definición, los dispositivos IoT tienen recursos limitados, pero sin embargo no debería ponerse en juego la seguridad. Se trata de un reto pendiente de resolver.
Por tanto, es fundamental actuar desde el primer instante, implementando dispositivos en los que la seguridad sea de suma importancia. Aquí es donde el IoT desempeñará un papel fundamental. No se trata únicamente de la privacidad de nuestros propios datos ni de la seguridad de nuestras identidades digitales. En los próximos años viviremos rodeados de dispositivos conectados a Internet que digitalizarán cada paso que demos, convertirán nuestra actividad diaria en información, distribuirán cualquier interacción por la red e interactuarán con nosotros en función de esta información. Nunca antes nuestro día a día había estado tan cerca del mundo digital. La difusa línea entre el mundo digital y el mundo real es precisamente el espacio donde se materializan los cambios introducidos por el IoT.
Entendamos el problema antes de que sea demasiado tarde y garanticemos que somos capaces de ofrecer un plan de protección total, aprovechando todos los conocimientos que se han desarrollado en otros ámbitos. Gartner situa el Internet de las cosas en el “Peak of inflated expectations” de su “Hype Cycle” de tecnologías emergentes[1], y señala que aún nos encontramos a cierta distancia de comportamientos estables y productivos. A todos nos queda mucho por hacer. Dado que el IoT formará parte de nuestra vida diaria, no podemos permitirnos cometer los errores del pasado y que una avalancha de nueva tecnología nos sobrepase. Aceptemos el reto.

Chema Alonso, consejero delegado de ElevenPaths, empresa filial de Telefónica

> Entendamos el problema antes de que sea demasiado tarde y garanticemos que somos capaces de ofrecer un plan de protección total, aprovechando todos los conocimientos que se han desarrollado en otros ámbitos.

Contenido del informe_

Biografías de los colaboradores_

Chema Alonso, CEO de ElevenPaths, empresa filial de Telefónica

Chema está centrado en la innovación en productos de seguridad mediante desarrollos patentados y alianzas con los principales fabricantes y organizaciones del sector. Anteriormente dirigió durante 14 años Informática 64, empresa dedicada a la seguridad informática y la formación. Es doctor en Seguridad Informática por la Universidad Rey Juan Carlos de Madrid.

Antonio Guzmán, Director científico de ElevenPaths, empresa filial de Telefónica

Antonio ha registrado casi una decena de patentes relacionadas con la seguridad, identidad y privacidad. Autor de numerosos artículos, ahora está centrado en la investigación financiada con fondos privados. En 2005 fue cofundador y director de un grupo de investigación sobre seguridad y privacidad. También cuenta con un doctorado en Ingeniería Informática por la Universidad Rey Juan Carlos.

Belisario Contreras, Gerente del Programa de Seguridad Cibernética de la Secretaría del CICTE

Belisario presta apoyo a la Secretaría del Comité Interamericano contra el Terrorismo (CICTE) en la Organización de los Estados Americanos (OEA). Participa en iniciativas de seguridad cibernética como la creación y el desarrollo de Equipos de Respuesta para Emergencias Informáticas (CERT). Asimismo, coordina la participación y colaboración con otras organizaciones internacionales y regionales dedicadas a cuestiones cibernéticas.

John Moor, Vicepresidente de Desarrollo de Segmentos de NMI

John cuenta con más de 30 años de experiencia en los sectores de la electrónica y la microelectrónica. En 1997 fue uno de los fundadores de ClearSpeed Technology y se incorporó a NMI en 2004, donde lidera el desarrollo de numerosas iniciativas como establecer las redes técnicas de NMI y la UK Electronics Skills Foundation. Asimismo, John es el Director de la Fundación para la Seguridad del IoT.

Asegurar el Internet de las cosas
Biografías de los colaboradores

Luis Muñoz, Director del Grupo de planificación de redes y comunicaciones móviles de la Universidad de Cantabria

La investigación del catedrático Luis Muñoz se centra en las técnicas avanzadas de transmisión de datos, redes multisalto inalámbricas heterogéneas, Internet de las cosas, ciudades inteligentes y métodos matemáticos aplicados a las telecomunicaciones. Ha participado en diversos proyectos nacionales y europeos de investigación en los que fue, entre otros, director técnico de SmartSantander.

Andrey Nikishin, Director de proyectos especiales y futuras tecnologías de Kaspersky Lab

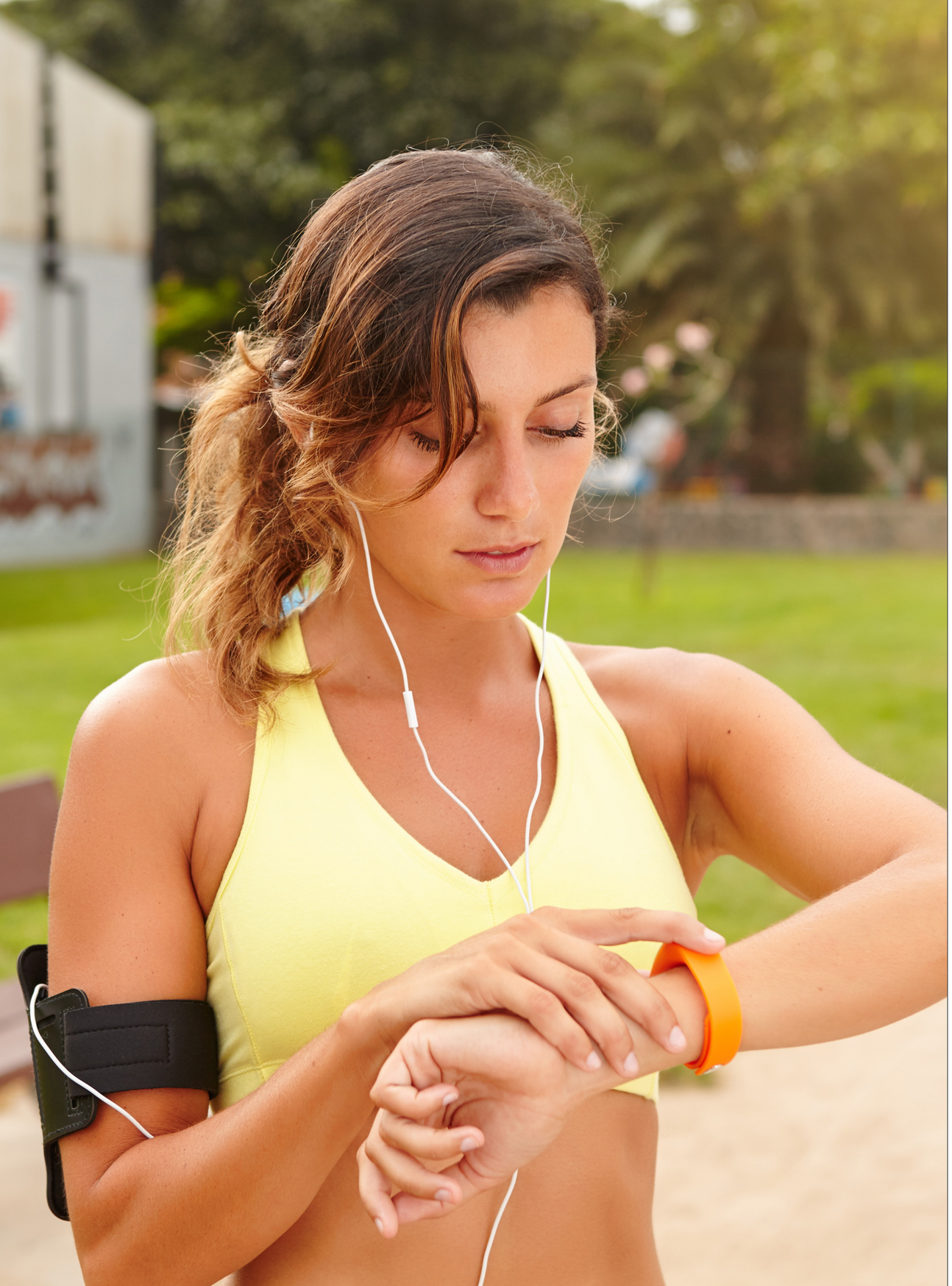
En Kaspersky Lab, Andrey trabajó como director de ingeniería y arquitectura de software antes de incorporarse al departamento de marketing estratégico como director de estrategia de productos. Antes de su puesto actual, dirigió el departamento de investigación y desarrollo de tecnologías de contenidos y de la nube. Andrey tiene experiencia desarrollando sus propios programas antivirus.

Bertrand Ramé, Director de redes y operadores de SIGFOX

Bertrand desarrolla alianzas de SIGFOX en Europa y Latinoamérica. Cuenta con 25 años de experiencia en el sector de las telecomunicaciones, principalmente en el desarrollo de negocio y la dirección general. Desarrolló la mitad de su trayectoria profesional en EE.UU. y en el Reino Unido, trabajando para empresas como AT&T y Telecom Italia.

Jaime Sanz, Gestor técnico de cuentas de telecomunicaciones en Intel Corporation Iberia

Jaime presta apoyo a las cuentas de telecomunicaciones en Europa centrándose especialmente en Telefónica para NFV, centros de datos, seguridad e IoT. En Intel ha desempeñado distintas funciones de apoyo técnico para ventas y marketing, y está licenciado en Ingeniería Informática por la Universidad Pontificia de Salamanca.



Introducción_

El Internet de las cosas no tiene precedentes en lo que a ámbito y escala se refiere, cambiando la sociedad y el modo en que interactúan las personas con su entorno de innumerables y complejas formas. Es totalmente lícito decir que estamos muy lejos de comprender las ramificaciones y consecuencias involuntarias de lo que estamos haciendo a día de hoy, y mucho menos de lo que llegará mañana y en un futuro más lejano. Quizá el asunto más acuciante sea el de la seguridad.

«Internet de las cosas podría ser un término relativamente nuevo, pero el concepto no lo es. Muchos de los problemas de seguridad, los malos actores y los ataques perpetrados contra el mismo, distan mucho de ser nuevos», afirma Antonio Guzmán de ElevenPaths, empresa filial de Telefónica. «Lo que es diferente es la escala de las redes implicadas, la heterogeneidad de los dispositivos, la increíble confianza en el cloud computing y el nivel de exposición de los dispositivos conectados a estas redes. Por este motivo, asegurar el Internet de las cosas es un verdadero reto».

«IoT está dejando rápidamente obsoletas las leyes necesarias para regular y normalizar las medidas de seguridad», afirma Belisario Contreras, Gerente del Programa para el Comité Interamericano contra el Terrorismo en la Organización de los Estados Americanos. «Esta velocidad de desarrollo también está afectando a las cuestiones de compatibilidad, ya que las medidas de seguridad para algunos dispositivos y plataformas pueden no ser compatibles con otros al aparecer versiones más recientes».

Y, según Guzmán, «muchos de los problemas potenciales son simplemente los mismos problemas de seguridad superpuestos sobre la infraestructura a escala masiva».

Todo esto está suponiendo un reto empresarial, así como un reto tecnológico.

«Cada vez es más evidente que la seguridad del IoT es un tema a debate en la sala de juntas y no solo un coste operativo o un problema tecnológico», afirma John Moor de la Fundación para la Seguridad del IoT. «Especialmente las grandes empresas tienen mucho que perder, y están comenzando a aparecer litigios legales en EE.UU. en los que la obligación que tienen las organizaciones de cuidar a sus clientes está siendo objeto de investigación».

«En mi opinión, ya estamos viendo cómo el Internet de las cosas está cambiando

> Hasta ahora se ha puesto mucho interés sobre las oportunidades de innovación en torno a IoT, y relativamente poco sobre sus puntos débiles.

nuestra sociedad. Como ejemplo de ello, la mayoría de las tareas realizadas por los proveedores de servicios, usuarios y otras personas están siendo supervisados de forma exhaustiva, lo que nos permite medir la eficiencia del trabajo desempeñado. Está claro que IoT cambiará nuestras vidas aún más que Internet», afirma Luis Muñoz, catedrático del Departamento de Ingeniería de Comunicaciones de la Universidad de Cantabria y unas de las fuerzas rectoras de SmartSantander. «Cuando comenzamos a implantar las redes máquina a máquina (M2M) en el año 2000 para gestionar las flotas de transporte, nos concentramos en un nicho muy concreto. Pero ahora, después de 15 años, IoT está presente en todas partes».

«IoT trae consigo numerosas ventajas. Como cliente, estoy muy satisfecho de contar con IoT, me hace la vida mucho más fácil», afirma Andrey Nikishin, Director de futuras tecnologías de Kaspersky. «Sin embargo, toda evolución conlleva nuevos riesgos en los que no habíamos pensado. Pongamos como ejemplo la invención del teléfono. Al principio, nadie se paró a pensar en el fraude telefónico, realmente, nadie lo previó. Todo elemento nuevo conlleva nuevos riesgos y nuevas vías para la delincuencia».

«Lo mismo sucede con el Internet de las cosas. La conectividad e interoperabilidad de los sistemas IoT son un paraíso, si no para los delincuentes, sí para los hooligans. Por supuesto, podemos desarrollar escenarios de prueba y predecir los comportamientos, pero en un mundo conectado no se puede hacer eso. Las personas son, por su propia naturaleza, impredecibles, creativas e ingeniosas. Y está en la naturaleza del software que las personas cometan errores y otros se aprovechen de ello».

Para John Moor de la Fundación para la Seguridad del IoT, los matices y la escala causan complejidad y agravan el reto.

«En la seguridad, limitado y pequeño suelen ser aspectos positivos. Si se limita el espacio y el tamaño de la base de código, entonces se reduce la superficie de ataque. Cuando observamos la oportunidad del Internet de las cosas, solemos mirar a escala masiva y la hiperconectividad. Desde el punto de vista de la seguridad, se trata de una propuesta abrumadora», afirma Moor. «Hasta ahora se ha puesto mucho interés sobre las oportunidades de innovación en torno a IoT, y relativamente poco sobre sus puntos débiles. Si no tenemos cuidado podríamos caminar como sonámbulos hacia numerosos problemas, algunos de los cuales pueden no haberse presentado antes».

«Tenemos que clasificar los retos. Se suele hablar de IoT como si se tratara de una sola cosa, si bien en realidad son muchos los dispositivos IoT que están ahí. La seguridad dependerá del contexto y será útil pensar en ella dentro de dicho contexto, pensar por ejemplo en el "IoT del consumidor", el "IoT en casa" o el "IoT de asistencia sanitaria". Esto marcará una diferencia enorme».

Es una cuestión de enfoque; la seguridad no es necesariamente una prioridad.

«El Internet de las cosas está creciendo exponencialmente, pero no al ritmo que cabría esperar», afirma Jaime Sanz, Gestor técnico de cuentas de telecomunicaciones en Intel Corporation Iberia. «Cosas como las ciudades inteligentes o los coches conectados añaden valor, pero también existe la necesidad de observar cómo los productos crearán una cadena de valor. Existe una dirección, aunque de momento está orientada a la conectividad, la funcionalidad, el ahorro de energía y similares, y no tanto a las normas o la seguridad».

Para Guzmán, director científico de ElevenPaths, el problema radica en entender las exigencias que plantean un nuevo territorio y la oportunidad respecto a la tecnología. «En el Internet de las cosas, suelen definirse barreras para los entornos industriales o la infraestructura crítica. El tipo y el número de objetos aumentará hasta incluir todos los objetos o dispositivos presentes en nuestra vida diaria y que reivindican contar con potencia informática», explica. «En IoT, los dispositivos funcionan conjuntamente para facilitarnos las tareas de la vida cotidiana, haciéndolas más eficientes y sostenibles».

«Según la tarea optimizada, se suele hablar de los denominados lugares inteligentes: redes inteligentes, contadores inteligentes, hogares inteligentes, ciudades inteligentes y similares», afirma Guzmán. «Sin embargo, esta cooperación solo es posible si los dispositivos están conectados entre sí y equipados con mecanismos de identificación que les identifiquen de manera única frente a todos los demás dispositivos conectados a Internet. La necesidad de interconexión e identificación, e incluso la necesidad de procesar la información generada o consumida por estos objetos, se convierte en un problema pendiente de resolver cuando nos damos cuenta del número estimado de "cosas" que forma parte del IoT».

En este informe se analizarán tres temas específicos: la necesidad de normas universales de seguridad, acceso y control; el choque entre la tecnología de la información y una red de cosas más antigua y consolidada (la tecnología operativa); y la necesidad de recuperarse de las vulnerabilidades, incluyendo su efecto sobre los usuarios.

Control y acceso: la verdadera lucha para el Internet de las cosas_

Una innovación tecnológica de la que todo el mundo habla crece de forma imparable. Fabricantes, viejos y nuevos, se lanzan al mercado. Se aportan nuevas ideas, se crean nuevos mercados y si existen nuevos estándares, se destruyen.

Se trata de un patrón familiar a la vanguardia de la tecnología, y el Internet de las cosas no difiere de las anteriores oleadas de innovación. La estandarización se encuentra en una situación comprometida y, con ella, la seguridad.

Se trata de un ciclo familiar, probablemente necesario, que infunde ímpetu, oportunidad e innovación en un momento crítico. Podría afirmarse que el IoT se encuentra en ese punto: a punto de alcanzar la madurez. Ese punto en el que la creación y la aprobación de las normas de seguridad, los controles y la comunicación se hacen también más necesarios.

¿Libre o patentada? ¿Una innovación sin restricciones o un buen conjunto de estándares? En periodos de rápida innovación, este tipo de dilemas son de especial importancia y es necesario abordarlos antes de pasar a una etapa en la que se creará y definirá una normativa estable y de establecimiento de estándares.

Al mismo tiempo, en comparación con el despegue de otras grandes redes (el telegrama, el teléfono analógico, el teléfono móvil e incluso el mismo Internet), su adopción será caótica y no planificada.

Los hitos históricos señalados solían ser monolíticos, programados y ejecutados minuciosamente, normalmente por grandes empresas u organismos gubernamentales (en el caso de las redes telefónicas, normalmente por el servicio postal nacional). Pese a ello, como explica el vicepresidente de Gartner y destacado analista Jim Tully[2]: «Las soluciones IoT raramente se adquieren como un paquete de trabajo y simplemente se despliegan sin más en una empresa». Lo mismo sucede con nuevos despliegues soportados en muchas ocasiones en infraestructuras previamente nacionalizadas y que son el pilar del Internet moderno».

Desde una perspectiva más general, las grandes implementaciones en toda una ciudad podrían coincidir con el

modelo histórico, pero cabe destacar que en el futuro cada una de las empresas añadirá sus propias capas de IoT sobre dichas instalaciones. Asimismo, a un nivel más pequeño, las personas (y cada vez más dispositivos y aplicaciones individuales) buscarán la forma de conectarse a dicha infraestructura.

Así pues, la pregunta a realizarse es la siguiente: ¿Qué entidad controla qué y cómo se transmite la información entre redes?

Ritmo frente a control

Con el Internet de las cosas, la aplicación de las normas vigentes, y la creación de normas nuevas ha tropezado con un ritmo frenético de innovación. Aquí, las empresas necesitan salvaguardar su propiedad intelectual a medida que fabrican y venden cosas que nadie más puede hacer.

Lo irónico es que con el fin de aprovechar las ventajas de los dispositivos y servicios de IoT, el hardware y software deben ser abiertos e interoperables. La seguridad en el dispositivo, la aplicación y las capas de red es fundamental. Pero a medida que se incrementa el ritmo de aprobación, también lo hacen la complejidad, la variedad de implementación y la oportunidad de los ataques maliciosos o errores involuntarios.

A esto cabe añadir el hecho de que numerosos fabricantes de IoT son relativamente nuevos en el mundo del software[3]. Hasta ahora, los productos se centraban en el valor del hardware en lugar de evaluar el valor total del hardware combinado con las capas de software. Aunque la investigación de Gartner hace referencia a la administración de licencias y derechos para esta nueva clase de proveedores de software, podría decirse que el riesgo es igualmente aparente en lo relativo a la creación de seguridad desde cero.

La colaboración entre dispositivos conectados en el Internet de las cosas requiere, por su propia naturaleza, transparencia y confianza mutua entre los dispositivos, y eso se basa en mecanismos universales de identificación y control. Es absolutamente necesario combinar la transparencia con un control de la precisión. Debe haber un modo de hacerlo entre todos los dispositivos, más allá de los protocolos existentes, y también debe haber un modo de recopilar y gestionar a una escala hasta el momento desconocida.

«Es poco probable que la solución venga de los fabricantes contratados, es más probable que venga de las grandes empresas que tienen más que perder», afirma Moor, Director de la Fundación para la Seguridad del IoT. «Si usted no es un fabricante de electrónica de renombre, le preocupará menos perder la reputación o la marca que si fuera un proveedor importante con grandes inversiones que supongan millones de nodos finales. Si

en cambio se encuentra en una posición intermedia, es probable que exista menos riesgo para su reputación. Debe establecerse la confianza en IoT, y las empresas que sean flexibles y mantengan una posición firme ante las amenazas de seguridad serán las que tengan éxito».

«Actualmente existe una evolución del tipo de productos conectados y de productos novedosos como por ejemplo los cepillos de dientes conectados. El sector consumo es particularmente vulnerable, ya que existen numerosos productos de bajo coste en el mercado de origen y fabricación dudosa».

Es importante recordar también las raíces del IoT y las bases sobre las que gran parte del mismo se ha construido.

«Cuando comenzamos a integrar M2M en las flotas de transporte, se trataba de un trabajo pionero», afirma el catedrático Luis Muñoz. «Años más tarde, la normativa europea obligó a integrar esta tecnología en todos los camiones que superaran un peso determinado. Lo mismo está sucediendo con nuestras ciudades. Hace una década, pocos servicios urbanos integraban la tecnología M2M. A día de hoy, debido al crecimiento de la población previsto, así como a la necesidad de mejorar la calidad de vida de los ciudadanos, la mayor parte de los servicios en la ciudad deben ser supervisados, con el objetivo de mejorar su eficiencia. Los ciudadanos desean participar activamente en esta nueva era».

Para Jaime Sanz de Intel, es necesaria una estrategia con un planteamiento arquitectónico que englobe tanto la tecnología como los datos.

«Estamos implicados en todas las partes de la cadena de valor del IoT, desde el centro de datos hasta el circuito integrado auxiliar de los dispositivos periféricos, salvo microprocesadores y sensores. Creemos que una arquitectura integral segura es fundamental», afirma Sanz. «La protección de los datos, desde el extremo hasta la nube, así como en el nivel del dispositivo, es una necesidad. En tercer lugar, tenemos en cuenta la protección del centro de datos».

«Hay dos ámbitos en lo que se refiere a la protección de las puertas de enlace. En primer lugar, proteger el dispositivo antes de que se ponga en funcionamiento con una combinación del Intel SoC Hardware Root of Trust y especificaciones de UEFI. Y en segundo lugar asegurar los datos mediante la codificación de datos, la protección de la integridad y las listas blancas».

> El sector consumo es particularmente vulnerable, ya que existen numerosos productos de bajo coste en el mercado de origen y fabricación dudosa

Dos mundos chocan: IT y OT en el Internet de las cosas_

La mayoría de las personas están muy familiarizadas con las tecnologías de la información. Sin embargo, no tantas conocen la presencia de controles industriales o incluso no son conscientes de ella. No obstante, la tecnología operativa es omnipresente. Controla los suministros de agua, electricidad y gas que consumimos, y además hace funcionar las fábricas que producen las cosas que compramos y utilizamos.

Los relojes inteligentes de hoy en día son maravillas de la informática y representan una capacidad de procesamiento muy superior a la de los primitivos ordenadores electrónicos utilizados para que el hombre aterrizara en la luna. El ordenador que controlaba las barras de combustible en Chernobyl tenía capacidades equivalentes a un microordenador modelo B de la BBC, un dispositivo educativo introducido por primera vez en 1981. Estos dos hechos suelen sacarse a colación, pero sorprendentemente se suele olvidar un aspecto tanto del Apolo Guidance Computer[4] como del SKALA[5]: no se necesita una gran capacidad de procesamiento para alcanzar resultados extraordinarios, especialmente en aplicaciones muy específicas.

La práctica de informatizar los controles industriales, conocida como tecnología operacional u OT (por sus siglas en inglés), es anterior a la informática cliente actual. Se basa en requisitos para los controles necesarios para automatizar los servicios públicos, como la generación de energía eléctrica, el suministro de gas o agua, así como la industria, del modo más fiable y seguro posible. Mientras que la IT (tanto en términos de software como de hardware) se ha caracterizado normalmente por su rápida iteración e innovación a costa, algunas veces, de la fiabilidad y de otros factores, la OT se ha diseñado desde cero para ofrecer un control y una medición predecibles.

IT, por su propia naturaleza, se ha diseñado para interconectarse, mientras que OT es casi exactamente lo contrario. Sin embargo, la conexión de ambas genera importantes beneficios. Solo en estos últimos años la combinación de IT y OT ha resultado ser práctica y atractiva.

«Una combinación de los mundos de IT y OT nos permite incorporar los datos en tiempo real de los dispositivos en el campo de la lógica empresarial de una organización», afirma Guzmán de

ElevenPaths, empresa filial de Telefónica. «La combinación de IT y OT muestra algunas lecciones muy importantes sobre cómo se puede asegurar el futuro Internet de las cosas».

«El legado de la OT ha supuesto que la mayoría de las implementaciones de IoT tengan un protocolo patentado que utiliza la seguridad mediante la oscuridad como mecanismo de defensa. No obstante, la explosión en la cantidad de dispositivos y negocios verticales está ayudando a impulsar las iniciativas que pretenden crear estándares abiertos para la comunicación; algunos ejemplos son MQTT, Zwave y ZigBee. Es probable que estos contribuyan a crear normas de seguridad más abiertas y útiles».

Una de las lecciones más recientes que hemos aprendido es que un espacio vacío equivale a la inexistencia de una defensa. Unos ingenieros de las instalaciones de Natanz (Irán) descubrieron, muy a su pesar, que las personas introducen y seguirán introduciendo lápices USB[6] en los PC que controlan la tecnología operativa. Los proveedores también son vectores de ataque[7]. Es más, las partes interesadas tienen la intención de utilizar ingeniería inversa y diseñar ataques personalizados para entrar en los sistemas si el valor que aporta hacerlo es significativo para ellas. A medida que se incrementa el tamaño y el alcance de las redes IoT operadas por suministradores de servicios públicos, ciudades y grandes compañías, se incrementa también el valor de dichos premios.

Sin embargo, OT ha tardado décadas en desarrollarse, y ha dado a los programadores tiempo, ámbito y presupuesto para realizar un cuidadoso trabajo de planificación y enfoque de la integración de sistemas como la ERP (planificación de recursos empresariales), así como la conectividad a la intranet e internet. Los creadores de IoT no cuentan con el mismo plazo de ejecución sobre el que considerar la integración y la seguridad. Francamente, su situación es diferente, en un momento en el que se llevan a cabo numerosas implementaciones de IoT en Internet, donde deben abrirse a la integración o quedar expuestas a posibles escenarios de ataque.

«IT y OT tienen filosofías diferentes. Biológicamente, no son completamente diferentes, pero las prioridades de sus creadores sí que lo son. Los ingenieros de OT quieren mantener procesos que funcionen las 24 horas del día, los 7 días de la semana, sin interrupción. Cualquier interrupción del proceso tecnológico supone un problema, por lo que el desarrollo se inclina hacia el objetivo de evitar la interrupción», afirma Nikishin de Kaspersky. «Sin embargo, para los ingenieros de IT, la disponibilidad del sistema no es la prioridad principal.

Asegurar el Internet de las cosas
Dos mundos chocan: IT y OT en el Internet de las cosas

> El objetivo principal del IoT es diseñar todos los dispositivos teniendo en cuenta la seguridad desde el principio.

El problema principal es mantener la integridad de los datos. El principal activo en la red de la oficina son los datos y, de nuevo, esto sesga el desarrollo».

«Cuando ambos converjan, se observarán algunos problemas. Los informáticos desean mantener la seguridad de los datos, lo que significa poner parches a los problemas lo antes posible. No obstante, la aplicación de parches para OT implica detener el proceso tecnológico y esto se contradice con los objetivos del ingeniero de OT. Dar con un terreno común representa un verdadero reto».

«Añadir IoT aporta multitud de beneficios y productividad. Por cierto, este proceso es imparable e inevitable. El problema principal del Internet de las cosas es que se basa en la idea de la conectividad. Desde el momento en que entran en el mundo conectado, surgen los problemas».

OT sigue siendo una preocupación para el futuro, entre otras razones porque las implementaciones de OT son increíblemente longevas.

«La seguridad de los datos, así como la fiabilidad del funcionamiento, son muy importantes», afirma Nikishin. «Ni que decir tiene que IoT influye en nuestra vida diaria. El objetivo principal del IoT es diseñar todos los dispositivos teniendo en cuenta la seguridad desde el principio. De otro modo, asegurarlos es casi imposible».

«Este dispositivo deberá diseñarse desde el principio para que sea seguro. Nuestra idea es obligar a todos los fabricantes de dispositivos industriales – SCADA, PLC y PLM – a rediseñar todos sus sistemas de forma segura y obligar a los clientes a sustituir su estructura de control existente por una nueva. Un sistema deberá ser seguro desde su diseño. Si se fija en lo que hizo Siemens después de Stuxnet, verá a lo que me refiero. Trabajaron mucho para mejorar considerablemente la seguridad de su OT. Aunque conseguir que los clientes cambiaran sus sistemas, que podrían haber funcionado perfectamente en los mismos PLC y PLM durante 10 o 15 años, resultó más problemático. Dicho de otro modo, los usuarios vieron el coste, creyeron que sus sistemas no estaban rotos y se negaron a arreglarlos».

Según Contreras de la OEA, la llegada del IoT y la creciente interconexión de los entornos de IT y OT ayudaron a impulsar el cambio en el sector de OT y también atribuyeron nuevas responsabilidades al personal técnico.

«No hace tanto tiempo que el espacio vacío se consideraba seguridad suficiente para OT. El crecimiento de IoT difumina considerablemente los límites y las OT están apareciendo ahora en el

mundo de la IT con mayor conectividad y vectores de amenaza. Se prevé que los ingenieros y otros miembros del personal técnico hagan frente a las necesidades de IT y OT. Lo mismo ocurrirá con los técnicos de ciberseguridad», afirma Contreras. «El papel de IoT como recopilador, distribuidor y receptor de datos hará que la IT y la OT respondan mejor a los problemas o a los cambios ambientales, y les permitirá trabajar con mayor flexibilidad y eficiencia. También requerirá que los CIO estudien el flujo de información y se cuestionen cómo se almacenan los datos de la empresa. Esto también supondrá una oportunidad de negocio, ya que con esta correlación de datos ahora muchas empresas pueden proyectar el desarrollo basándose en una información mejor».

«Tambi`én debemos considerar las necesidades y las limitaciones de la sociedad. Al principio fueron las empresas, centros de investigación y similares los que impulsaron la tecnología de IoT porque veían una oportunidad única en ella. Tuvo que transcurrir algo más de tiempo para que los ciudadanos vieran los beneficios que dicha tecnología podría aportarles y, por tanto, trasladarles de una postura reacia a una más entusiasta. Como ya he comentado, IoT está promoviendo implícitamente un cambio de comportamiento», afirma Luis Muñoz.

«Los santanderinos están cada vez más capacitados para utilizar e interpretar la información que les proporciona IoT y sus servicios compatibles. Esto demuestra claramente que estamos superando una de las amenazas siempre mencionadas, es decir, la brecha digital. En este sentido, diría que más que el reto tecnológico al que nos enfrentamos cuando iniciamos el proyecto SmartSantander, nos encontramos ante un nuevo modo de manejarnos y vivir en la ciudad. En resumen, estábamos remodelando el ecosistema de la ciudad avanzando hacia un nuevo paradigma basado en los conocimientos y el uso intensivo de las TIC».

Asegurar el Internet de las cosas: antes y después_

Las redes creadas por IoT serán algunas de las más grandes que en el mundo se hayan visto jamás, haciéndolas enormemente atractivas para los piratas informáticos.

Según lo establecido en la ley de Metcalfe[8], el valor de las redes IoT es enorme, convirtiéndolas en objetivos significativos para los piratas informáticos motivados por la codicia o por razones políticas. Sin embargo, si IoT representa ahora una difícil tarea para la seguridad, a medida que aumenta la cantidad de redes, operadores, consumidores y dispositivos, también lo es el riesgo de que se produzca una vulneración eficaz.

Parte del problema es la escala. La gran cantidad de dispositivos, redes, aplicaciones, plataformas y actores crea un intrincado problema[9] cuya complejidad solo aumentará a medida que lo haga la infraestructura para apoyar, atender y extraer valor del IoT.

Las intenciones de los diseñadores (que priorizan la protección por encima de la seguridad, como hemos observado anteriormente) también pueden suponer un problema.

«Tenemos que sacrificar la heterogeneidad de los dispositivos por la capacidad de controlarlos y asegurarlos», afirma Guzmán de ElevenPaths. «La capa de seguridad de IoT debe contemplar los sistemas de protección a todos los niveles: capa de red, capa de aplicación y dispositivos IT».

Gestionar las vulnerabilidades y responder a los ataques o a las infracciones es ahora posible gracias a la cantidad y el alcance relativamente reducidos de los dispositivos IoT. Lograr que se implementen los procesos de seguridad, generación de informes y resolución para los dispositivos conectados a Internet antes de que se produzca el primer ataque catastrófico, será absolutamente vital.

Recientes pruebas de concepto, como la infracción de la seguridad en 1,4 millones de Jeeps Chrysler[10] que podían actualizarse mediante una transmisión aérea y controlarse de forma remota por un pirata informático, demuestran los problemas potenciales que existen al conectar dispositivos IoT a las redes.

También cabe destacar que un ataque no tiene por qué forzar necesariamente el cambio. Un accidente, un resbalón accidental o un simple error también podrían ser catastróficos; retrocedamos, por ejemplo, al caso del Gusano Morris[11] en 1988. Aunque la escala y la variedad bien podrían ayudar a evitar daños

Asegurar el Internet de las cosas
Asegurar el Internet de las cosas: antes y después

significativos, el ritmo de desarrollo, la escala y el crecimiento de IoT siguen permitiendo resultados potenciales mucho más perjudiciales que los nunca vistos en los entornos informáticos más tradicionales.

«Equilibrar la creatividad de la invención frente a la necesidad de garantizar la seguridad es complejo, pero también necesario», afirma Guzmán. «Y mientras que, a simple vista, puede parecer que frena la innovación, es todo lo contrario. He mencionado la seguridad mediante el diseño, y no es algo que necesariamente frene la innovación», afirma Nikishin de Kaspersky.

«Asimismo, la innovación lanza al mercado a empresas nuevas, pero no es justo tachar a los nuevos competidores como más peligrosos que los demás. Numerosos fabricantes actuales intentan adaptar sus diseños existentes con consecuencias inesperadas. Por ejemplo, existen numerosas ventajas para los consumidores que tienen contadores inteligentes de los servicios públicos. Pero en España, en concreto, la introducción de estos contadores ha sacado a la luz algunos problemas. Los usuarios pueden piratearlos para registrar un consumo inferior y eso supone una pérdida de ingresos. Algunos contadores utilizaban 3G para transmitir las lecturas y hubo quien encontró el modo de utilizarlo para obtener acceso gratuito a Internet. Estamos hablando de un país en el que hay instalados entre 30 y 40 millones de contadores inteligentes».

«La cuestión es que esto no supone una negligencia; se trata de las consecuencias imprevistas de las que he hablado antes, junto con un cambio fundamental en el enfoque que deben adoptar los fabricantes. Esta clase de empresa diseña para la seguridad, y no existe norma de certificación ni de seguridad para los dispositivos IoT a la que hacer referencia. Se trata de un problema con los fabricantes e ingenieros consolidados, que piensan principalmente en la protección en lugar de pensar en la seguridad».

«Y después nos encontramos con las empresas nuevas. Una empresa a la que hemos ayudado fabrica dispositivos domésticos inteligentes: detectores de movimiento, contadores de electricidad, controladores de temperatura y sensores de todo tipo. Almacenan y procesan gran cantidad de datos en la nube y las

> Es importante comprender que una gran conectividad conlleva una gran responsabilidad.

decisiones sobre dichos datos también se toman allí. Esto permitió que la empresa creara unos sistemas muy inteligentes que se adaptan a las necesidades domésticas, y que desarrollara nuevos productos y servicios con mucha rapidez».

«Ninguno de estos datos estaba cifrado. Aunque encender o apagar una luz no parecería tan importante, cualquier persona que quisiera asaltar su casa podría estar realmente interesada en el modelo de ocupación del hogar. Asimismo, dado que las decisiones se toman en la nube, ¿qué sucede si no existe un 100 % de conectividad en todos estos dispositivos domésticos?».

Moor, vicepresidente de Desarrollo de Segmentos de IoT de NMI, considera que un triple enfoque es lo más satisfactorio.

«Debemos pensar primero en la seguridad y asegurar por defecto», afirma Moor. «No se puede tratar precipitadamente la seguridad después de que se produzca el suceso. No obstante, algunas empresas tienen que intentarlo y hacerlo cuando ya se han lanzado al mercado. Les motiva la oportunidad de mercado de entrar precipitadamente en la conectividad sin conocer las repercusiones. Es importante comprender que una gran conectividad conlleva una gran responsabilidad».

«Puede que no se cree un problema a sí mismo, pero puede ocasionarlo a otras personas en otro lugar, y cuantos más problemas se encuentre el mercado, más lento será el ritmo de adopción porque el riesgo y la incertidumbre predominarán. Cuando alguien puede irrumpir en la red de su casa a través de su hervidor conectado (lo que, por cierto, sería posible), usted empieza a considerar lo que hay en las redes domésticas de interés para los delincuentes de todas las denominaciones».

«En segundo lugar», afirma Moor, «tenemos que desarrollar la resiliencia. Nadie fabrica un producto irrompible, pero las posibilidades de que se piratee aumentan a medida que el producto alcanza más éxito y se vuelve más generalizado. Las empresas tienen que pensar cómo responder a los ataques cuando se utilizan sus productos. Y tienen que ofrecer seguridad en todo el ciclo de vida. Justo desde su fabricación, los activos que cree tener se validan y certifican. Incluso en el terreno de los chips, Texas Instruments e IBM están colaborando para crear identificadores

únicos en los chips para realizar un seguimiento de los mismos a lo largo de su ciclo de vida. En caso de aplicarse IoT, no se encuentran necesariamente en los dispositivos desechables. Algunos pueden durar décadas. Si pensamos en temas como las actualizaciones de software, existen numerosas dificultades. Cuando pienso en la cantidad de dispositivos conectados que tengo solo en mi casa, la idea de que se actualicen todos constantemente causa pánico. Entonces surgirá el mercado de segunda mano». w«Por último, observamos la adecuación al propósito. La seguridad en IoT no ofrece una solución universal. Aquí estamos hablando de contexto. La aplicación determinará una serie de factores que determinarán el enfoque que adoptarán las empresas para asegurar sus sistemas. Por ejemplo, la economía de la implementación de millones de dispositivos dictará el coste de fabricación, el suministro de sistemas, el mantenimiento de los regímenes de seguridad, etc.; asimismo, la criticidad de dichos sistemas determinará el nivel de seguridad necesario (véase como ejemplo un implante médico y la amenaza de pirateo frente a la de una bombilla)».

Antonio Guzmán de ElevenPaths, ve el problema en términos de antiguas dificultades aplicadas a las nuevas infraestructuras y a gran escala.

«Deben volver a considerarse los enfoques tradicionales», afirma Guzmán. «Los esquemas donde conviven la prevención, la detección y las estrategias de respuesta permiten soluciones que supervisen continuamente tanto el interior como el exterior de la infraestructura para prevenir el ataque, emitir una alerta en caso de que se esté produciendo uno y, si consigue llevarse a cabo, poner en marcha la recuperación y la respuesta».

«Sin embargo, para IoT, la escala hace que las soluciones actuales sean ineficaces e ineficientes. Tenemos que proponer un nuevo modo de asegurar lo que es una nueva oleada de tecnologías que pueden funcionar a la escala que nosotros o cualquiera pueda prever. Debemos abordar cuatro capas OSI fundamentales: de transporte, física y de infraestructura, de aplicación, de dispositivo y red. Menciono OSI porque estas capas no son nuevas; forman parte de la composición original de las redes Ethernet, pero las dificultades que presentan como parte del Internet de las cosas tienen magnitudes superiores a las que nos habíamos tenido que enfrentar como sociedad en el pasado».

> “Tenemos que proponer un nuevo modo de asegurar lo que es una nueva oleada de tecnologías que pueden funcionar a la escala que nosotros o cualquiera pueda prever.

Conclusión_

Las redes que cree IoT serán las mayores que se hayan visto jamás, y esto las hace enormemente valiosas para los piratas informáticos.

Mucho antes de que el Internet de las cosas llegase a formar parte del lenguaje común, era evidente que el mundo se quedaría sin direcciones posibles para los dispositivos conectados a Internet disponibles a través de la IP v4 (4 294 967 296, para ser exactos).

Aunque el Internet de las cosas no se ampliará de tal modo que consuma las 3,4*1038 direcciones disponibles en un futuro próximo, es evidente que ya está creciendo mucho más rápido (y con una base de usuarios informados mucho más amplia) que su mayor predecesor: el propio Internet. Esto es fuente de gran preocupación. Las personas, dispositivos, aplicaciones, redes e infraestructura física deben estar protegidos y el mejor modo de hacerlo es trabajar y basarse en normas comunes.

«Cada nueva tecnología viene acompañada de obstáculos, expectativas y, en ocasiones, grandes amenazas», afirma Bertrand Ramé, Director de redes y operaciones de SIGFOX. «En Sigfox, consideramos tanto la integridad del dispositivo como la privacidad de los datos de los usuarios, especialmente cuando vamos a conectar casi cualquier cosa física a Internet. Además, las aplicaciones IoT pueden necesitar implementar diferentes niveles de seguridad para adaptarse a la criticidad, el presupuesto y el consumo de energía de la empresa, por encima de lo exigido por los gobiernos, los fabricantes y las instituciones».

«Estamos todavía en el inicio del Internet de las cosas», afirma Moor. «Creo que sabremos que lo hemos conseguido cuando se vuelva invisible y las personas dejen de hablar de IoT, y se centren más en las experiencias y en los servicios nuevos y valiosos aún por descubrir. Cuando se haya generalizado y el “Internet de las cosas” haya desaparecido de la conciencia pública, cuando los objetos físicos que uno alquile o compre se configuren solos y se mantengan solos, entonces lo habremos conseguido. Para llegar hasta ahí, el Internet de las

> El Internet de las cosas permitirá que las personas, empresas y países tengan más control sobre su tecnología, así como un acceso a la información mayor que nunca.

cosas de hoy en día debe ser fiable en estado salvaje y sobre todo, seguro».

«El Internet de las cosas permitirá que las personas, empresas y países tengan más control sobre su tecnología, así como un acceso a la información mayor que nunca. El principal problema de seguridad asociado a IoT es el riesgo generalizado de que una vulnerabilidad pueda derribar todo un sistema. No obstante, esto no debería disuadirnos de aprovechar estas innovaciones», afirma Contreras de la OEA.

«A medida que implementemos IoT en nuestra red, querremos formular las siguiente preguntas: "¿Los beneficios potenciales de IoT serán superiores a los riesgos potenciales en esta circunstancia concreta?", "¿Está protegida mi red con medidas de seguridad actualizadas, y el programador de IoT guarda un buen registro de la seguridad?" y "¿Sé cómo y dónde se almacenan los datos recogidos, y es seguro el lugar de almacenamiento y está protegido con medidas como contraseñas y códigos?". Si tenemos en cuenta estas cuestiones, podemos dar la bienvenida a la innovación de IoT al mismo tiempo que mantenemos nuestra capacidad de responder con rapidez si nuestra ciberseguridad se ve amenazada».

«Con el fin de aprovechar las ventajas del IoT de forma segura, necesitaremos un triple enfoque de seguridad. En primer lugar, deben establecerse normas y reglamentos para el desarrollo y la implementación del software de IoT. En segundo lugar, debe haber confianza y un diálogo constante entre los programadores y los operadores; y, por último, debe haber una mayor comprensión holística de la ciberseguridad, teniendo en cuenta el IoT y el modo en que conecta los sistemas IT y OT».

Los esfuerzos de normalización están en marcha y están demostrando ser satisfactorios. Sin embargo, es fundamental encontrar el modo de garantizar cómo la multiplicidad de actores puede interoperar y comunicar los requisitos, necesidades y riesgos de seguridad a escalas que eclipsan los problemas actuales. No es necesariamente algo que tengamos o que vayamos a tener pronto. No obstante, necesitamos trabajar para conseguirlo. De hecho, debemos hacerlo.

Anexo_

1,2 Gartner – Gartner's 2015 Hype Cycle for Emerging Technologies Identifies the Computing Innovations That Organizations Should Monitor
http://www.gartner.com/newsroom/id/3114217

3 Gartner – Gartner's 2015 Hype Cycle for Emerging Technologies Identifies the Computing Innovations That Organizations Should Monitor
http://www.gartner.com/document/3143217

4 Computer Weekly – Apollo 11: The computers that put man on the moon
http://www.computerweekly.com/feature/Apollo-11-The-computers-that-put-man-on-the-moon

5 Chernobyl Nuclear Power Plant: Control Room
http://kiev2010.com/2010/06/chernobyl-nuclear-power-plant-i-control-room

6 IEEE Spectrum: The real story of Stuxnet
http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

7 Engadget – Stuxnet worm entered Iran's nuclear facilities through hacked suppliers
http://www.engadget.com/2014/11/13/stuxnet-worm-targeted-companies-first

8 P2P Foundation – Metcalfe's Law
http://p2pfoundation.net/Metcalfe's_Law

9 Rittel, Webber – Dilemmas in a General Theory of Planning
http://www.uctc.net/mwebber/Rittel+Webber+Dilemmas+General_Theory_of_Planning.pdf

10 Wired – Hackers Remotely Kill a Jeep on the Highway—With Me in It
http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway

11 ZDNet – The Morris Worm: Internet malware turns 25 | ZDNet
www.zdnet.com/article/the-morris-worm-internet-malware-turns-25

Telefonica

securely powered by

ElevenPaths

Para más información sobre ElevenPaths, visita elevenpaths.com o síguenos en Twitter @ ElevenPaths y LinkedIn.