Seguridad y privacidad en el Internet de las Cosas

Daniel García
Director gerente de ISMS Forum

Es habitual encontrar en la prensa generalista titulares y menciones sobre un empleado desleal que provoca una fuga de información o un *cracker* que opera desde un paraíso digital y que se lucra de la extorsión a usuarios y empresas. Pero también sobre los efectos de programas maliciosos, de la inserción de *malware*, del *phising*, de APTs, de accesos indebidos a la red empresarial o de ataques de denegación de servicio, entre otros. Éstas constituyen las principales amenazas cibernéticas a las que estados, empresas, proveedores de tecnologías y servicios tienen que hacer frente en la era digital y que deben gestionar para minimizar su impacto en sus procesos de negocio, al mismo tiempo que comienzan a ser una preocupación para la seguridad y la privacidad de las personas en sus propios hogares.

Cada día surgen nuevas amenazas que cambian de forma, e incluso el modo en que causan un impacto, pero también nuevas tecnologías que multiplican los puntos de entrada de todas ellas. Tecnologías conectadas que alteran la clasificación tradicional de amenazas y que se encuentran dentro y fuera de la organización, en las ciudades, en la industria, en las infraestructuras, en los medios de transporte e, incluso, en las personas.

Las tecnologías conectadas son, por tanto, los activos que todos los actores implicados deben proteger, no solo para mantener los principios tradicionales de confidencialidad, integridad y disponibilidad, sino también para preservar el desarrollo seguro a todos los niveles de la denominada sociedad de la información.

Con el objetivo de fomentar el conocimiento y las buenas prácticas en aspectos de seguridad y privacidad en las tecnologías enmarcadas en el concepto Internet de las Cosas (IoT, por sus siglas en inglés), desde el Centro de Estudios en Movilidad e Internet de las Cosas, iniciativa de ISMS Forum Spain, se ha puesto a disposición del sector una aproximación sobre el estado actual y las implicaciones de seguridad y privacidad en el Internet de las Cosas.

Capítulos

A lo largo de este primer estudio se pueden encontrar cuatro capítulos en los que se define el estado actual del fenómeno Internet de las Cosas, se analizan los principales vectores de ataque asociados y los aspectos legales y se presenta un manual de buenas prácticas junto a una marca de garantía de confianza en ciberseguridad para entornos bajo la denominación IoT.

Estado del Arte del Internet de las Cosas. A lo largo de las páginas de este primer apartado, se aborda la evolución de la tecnología y su aplicación en un mundo hiperconectado. Analiza cuáles son los componentes tecnológicos que intervienen en el marco de tecnologías conectadas, en qué sectores de mercado influye, quiénes son los receptores de los productos y qué aspectos de seguridad son relevantes.

Análisis de los vectores de ataque del Internet de las Cosas. Un segundo capítulo desarrolla el conjunto de áreas de análisis de los vectores de ataque. Tiene como objeto identificar y definir las áreas de análisis asociadas a la superficie de exposición y a los vectores de ataque propios de los dispositivos IoT, con el propósito de poder evaluar las potenciales debilidades y vulnerabilidades de seguridad y/o privacidad que afectan a este tipo de dispositivos y a sus servicios o plataformas asociadas.

El conjunto de áreas de análisis identificadas permitiría evaluar de manera global la seguridad de cualquier dispositivo o solución IoT, pudiendo existir vulnerabilidades de

Cada día surgen nuevas amenazas que cambian de forma e incluso el modo en que causan un impacto, pero también nuevas tecnologías que multiplican los puntos de entrada de todas ellas

seguridad comunes entre diferentes áreas, como por ejemplo debilidades en los mecanismos de autentificación, autorización, cifrado (en reposo y en tránsito), tanto en el interfaz web de gestión del dispositivo IoT, como en su comunicación con "la nube" o con aplicaciones móviles, en otros servicios de red que éste proporciona, etc.

Impacto de las tecnologías IoT y dispositivos móviles en la privacidad de las personas. El tercer apartado analiza el impacto de las tecnologías IoT en la vida de los individuos a través de casos de uso, proponiendo medidas correctoras desde el ámbito legal, contractual y regulatorio. Recomienda la adopción de medidas bajo la premisa *Privacy by Design* y *Privacy by Default,* que permiten clarificar las cláusulas de privacidad y las políticas de protección de datos, evitando así que no se generen situaciones de desprotección para el usuario.

La falta de virtualidad de las políticas de protección de datos y de las cláusulas de información previas al consentimiento, unido a los problemas técnicos de recogida del propio consentimiento en los objetos conectados, hacen recomendable la adopción de medidas tendentes a obligar a que los dispositivos IoT sean *privacy conformance* desde su diseño y, por defecto, que se basen en *privacy-enhancing technologies* (PET).

Buenas prácticas en dispositivos IoT y Marca de Garantía. El último apartado tiene como objetivo la definición de cuáles son las mejores prácticas orientadas hacia productos canalizados al consumidor final, así como proporcionar un mecanismo de confianza que avale el seguimiento de las mismas: la marca de garantía de confianza en ciberseguridad para la gama de productos conectados de entornos no críticos. Los dominios que aborda el manual de buenas prácticas son la seguridad en el diseño, el gobierno y seguridad en el ciclo de vida comercial, la protección en el hardware/firmware, la seguridad en las comunicaciones, la seguridad en los sistemas y la seguridad jurídica.

Asimismo, el estudio concluye que los estándares de calidad o sellos de confianza son una vía muy adecuada para establecer un marco de referencia donde confluyen usuarios, fabricantes y desarrolladores. De este modo, todos los productos quedan bajo unos estándares que aseguran unos parámetros mínimos de calidad y seguridad, garantizando la privacidad de los usuarios.

Desarrollo

El estudio ha sido desarrollado por el Centro de Estudios en Movilidad e Internet de las Cosas de ISMS Forum bajo la dirección de Francisco Lázaro y la coordinación de Juan Manuel Zarzuelo (Estado del Arte del Internet de las Cosas), Raúl Siles (Análisis de los vectores de ataque del Internet de las Cosas), Paloma Llaneza (Impacto de las tecnologías IoT y dispositivos móviles en la privacidad de las personas) y Jorge Hurtado y Antonio Fontiveros (Buenas prácticas en dispositivos IoT y Marca de Garantía), sumados al más de medio centenar de colaboradores que hacen posible esta iniciativa.

Finalmente, cabe destacar que el estudio *Estado del arte e implicaciones de seguridad y privacidad en el Internet de las Cosas* se encuentra disponible en la web de ISMS Forum, bajo la url www.ismsforum.es/estudioCEM. ■

Las tecnologías conectadas son activos que todos los actores implicados deben proteger para preservar el desarrollo seguro de la denominada sociedad de la información.