Departamento de Seguridad Nacional de los Estados Unidos

PRINCIPIOS ESTRATÉGICOS PARA LA SEGURIDAD DE LA INTERNET DE LAS COSAS (IoT)

Versión 1.0

15 de noviembre de 2016

Homeland Security

INTRODUCCIÓN Y VISIÓN GENERAL

El crecimiento de los dispositivos, sistemas y servicios conectados a la red que conforman el Internet de las cosas (IoT)[1] crea inmensas oportunidades y beneficios para nuestra sociedad. Sin embargo, la seguridad de la IO no ha seguido el rápido ritmo de la innovación y el despliegue, creando importantes riesgos económicos y de seguridad. Este documento explica estos riesgos y ofrece un conjunto de principios no vinculantes y sugerencias de buenas prácticas para alcanzar un nivel de seguridad responsable para los dispositivos y sistemas que las empresas diseñan, fabrican, poseen y operan.

Crecimiento y prevalencia del Internet de los objetos

Los dispositivos conectados a Internet permiten conexiones sin fisuras entre personas, redes y servicios físicos. Estas conexiones ofrecen eficiencia, usos novedosos y experiencias personalizadas que resultan atractivas tanto para los fabricantes como para los consumidores. Los dispositivos conectados a la red ya son omnipresentes, e incluso esenciales, en muchos aspectos de la vida cotidiana, desde los rastreadores de fitness, los marcapasos y los coches, hasta los sistemas de control que suministran agua y energía a nuestros hogares. La promesa que ofrece la IO es casi ilimitada.

Prioridad a la seguridad del IoT

Aunque las ventajas del IoT son innegables, la realidad es que la seguridad no sigue el ritmo de la innovación. A medida que integramos cada vez más las conexiones de red en la infraestructura crítica de nuestra nación, los procesos importantes que antes se realizaban manualmente (y que, por tanto, gozaban de cierta inmunidad contra la ciberactividad maliciosa) son ahora vulnerables a las ciberamenazas. Nuestra creciente dependencia nacional de las tecnologías conectadas a la red ha crecido más rápido que los medios para asegurarlas.

El ecosistema de la IO introduce riesgos que incluyen a los actores maliciosos que manipulan el flujo de información hacia y desde los dispositivos conectados a la red o que manipulan los propios dispositivos, lo que puede conducir al robo de datos sensibles y a la pérdida de la privacidad de los consumidores, a la interrupción de las operaciones comerciales, a la ralentización de la funcionalidad de Internet a través de ataques de denegación de servicio distribuidos a gran escala y a posibles interrupciones de las infraestructuras críticas.

El año pasado, en un ciberataque que inutilizó temporalmente la red eléctrica en algunas partes de Ucrania, el mundo vio las consecuencias críticas que pueden tener los fallos en los sistemas conectados.
Dado que nuestra nación depende ahora del buen funcionamiento de las redes para llevar a cabo muchas actividades vitales, la seguridad de la IO es ahora una cuestión de seguridad nacional.

[1] En este contexto, el término IoT se refiere a la conexión de sistemas y dispositivos con fines principalmente físicos (por ejemplo, detección, calefacción/refrigeración, iluminación, accionamiento de motores, transporte) a redes de información (incluida Internet) a través de protocolos interoperables, a menudo incorporados en sistemas integrados.

Es imperativo que el gobierno y la industria trabajen juntos, rápidamente, para garantizar que el ecosistema del IoT se construya sobre una base que sea confiable y segura. En 2014, el Comité Asesor de Telecomunicaciones de Seguridad Nacional (NSTAC) del Presidente destacó la necesidad de actuar con urgencia.

> La adopción del IoT aumentará tanto en velocidad como en alcance, y [tendrá] un impacto en prácticamente todos los sectores de nuestra sociedad. El reto de la nación es garantizar que la adopción de la IO no genere riesgos indebidos. Además, en .... hay un pequeño margen, que se está cerrando rápidamente, para garantizar que la adopción de la IO se realice de forma que se maximice la seguridad y se minimicen los riesgos. Si el país no lo hace, tendrá que afrontar las consecuencias durante generaciones. [2]

El momento de abordar la seguridad de la IO es ahora mismo. Este documento sienta las bases para el compromiso con los sectores público y privado en estas cuestiones clave. Es un primer paso para motivar y enmarcar las conversaciones sobre las medidas positivas para la seguridad de la IO entre los desarrolladores de la IO, los fabricantes, los proveedores de servicios y los usuarios que compran y despliegan los dispositivos, servicios y sistemas. Los siguientes principios y prácticas sugeridas proporcionan un enfoque estratégico sobre la seguridad y mejoran el marco de confianza que sustenta el ecosistema de la IO.

Visión general de los principios estratégicos

Muchas de las vulnerabilidades del IoT podrían mitigarse mediante las mejores prácticas de seguridad reconocidas, pero demasiados productos actuales no incorporan ni siquiera las medidas de seguridad básicas. Hay muchos factores que contribuyen a este déficit de seguridad. Uno de ellos es que puede no estar claro quién es responsable de las decisiones de seguridad en un mundo en el que una empresa puede diseñar un dispositivo, otra suministrar el software que lo compone, otra operar la red en la que está integrado el dispositivo y otra desplegarlo. Este reto se ve magnificado por la falta de normas y estándares internacionales completos y ampliamente adoptados para la seguridad de la IO. Otros factores que contribuyen a ello son la falta de incentivos para que los desarrolladores aseguren adecuadamente los productos, ya que no necesariamente asumen los costes de no hacerlo, y el conocimiento desigual de cómo evaluar las características de seguridad de las opciones que compiten.

Los siguientes principios, expuestos en la siguiente sección, ofrecen a las partes interesadas una forma de organizar su pensamiento sobre cómo abordar estos retos de seguridad de la IO:

Incorporar la seguridad en la fase de diseño

Actualizaciones avanzadas de seguridad y gestión de vulnerabilidades

Basarse en prácticas de seguridad probadas

[2] Informe del Comité Asesor de Seguridad Nacional de Telecomunicaciones al Presidente sobre el Internet de los objetos, 19 de noviembre de 2014.

Priorizar las medidas de seguridad según el impacto potencial

Promover la transparencia en el IoT

Conéctese con cuidado y deliberadamente

Al igual que con todos los esfuerzos de ciberseguridad, la mitigación de los riesgos de la IO es una responsabilidad compartida entre el gobierno y el sector privado en constante evolución. Las empresas y los consumidores son generalmente responsables de tomar sus propias decisiones sobre las características de seguridad de los productos que fabrican o compran. El papel del gobierno, fuera de ciertos contextos regulatorios específicos y actividades de aplicación de la ley, es proporcionar herramientas y recursos para que las empresas, los consumidores y otras partes interesadas puedan tomar decisiones informadas sobre la seguridad de la IO.

Alcance, objetivo y público

El objetivo de estos principios no vinculantes es dotar a las partes interesadas de prácticas sugeridas que ayuden a tener en cuenta la seguridad cuando desarrollan, fabrican, implementan o utilizan dispositivos conectados a la red. En concreto, estos principios están pensados para:

1. Los **desarrolladores de la IO** deben tener en cuenta la seguridad cuando se diseña y desarrolla un dispositivo, un sensor, un servicio o cualquier componente de la IO;
2. **Los fabricantes de IoT** deben mejorar la seguridad tanto de los dispositivos de consumo como de los gestionados por los proveedores;
3. Los **proveedores de servicios,** que implementan servicios a través de dispositivos IoT, deben considerar la seguridad de las funciones ofrecidas por esos dispositivos IoT, así como la seguridad subyacente de la infraestructura que permite estos servicios; y
4. **Consumidores de nivel industrial y empresarial** (incluidos el gobierno federal y los propietarios y operadores de infraestructuras críticas) para que sirvan de líderes a la hora de involucrar a los fabricantes y proveedores de servicios en la seguridad de los dispositivos del IoT.

PRINCIPIOS ESTRATÉGICOS PARA ASEGURAR LA IOT

Los principios que se exponen a continuación están diseñados para mejorar la seguridad de la IO en toda la gama de actividades de diseño, fabricación y despliegue. La adopción generalizada de estos principios estratégicos y de las prácticas sugeridas asociadas mejoraría drásticamente la postura de seguridad de la IO. Sin embargo, no existe una solución única para mitigar los riesgos de seguridad de la IO. No todas las prácticas que se enumeran a continuación serán igualmente relevantes en la diversidad de dispositivos de la IO. Estos principios están pensados para ser adaptados y aplicados a través de un enfoque basado en el riesgo que tenga en cuenta los contextos empresariales pertinentes, así como las amenazas y consecuencias particulares que pueden resultar de los incidentes relacionados con un dispositivo, sistema o servicio conectado a la red.

Incorporar la seguridad en la fase de diseño

La seguridad debe ser evaluada como una parte integral

componente de cualquier dispositivo conectado a la red. Aunque hay excepciones, en demasiados casos los impulsos económicos o la falta de conciencia de los riesgos hacen que las empresas impulsen la comercialización de dispositivos sin tener en cuenta su seguridad. Incorporar la seguridad en la fase de diseño reduce las posibles interrupciones y evita el esfuerzo, mucho más difícil y costoso, de intentar añadir seguridad a los productos una vez desarrollados e implantados. Al centrarse en la seguridad como una característica de los dispositivos conectados a la red, los fabricantes y proveedores de servicios también tienen la oportunidad de diferenciarse en el mercado. Las prácticas que se exponen a continuación son algunas de las formas más eficaces de tener en cuenta la seguridad en las primeras fases de diseño, desarrollo y producción.

¿Cuáles son las posibles consecuencias de no incorporar la seguridad durante el diseño?

No diseñar y aplicar las medidas de seguridad adecuadas podría perjudicar al fabricante en términos de costes financieros, costes de reputación o costes de retirada del producto. Aunque todavía no existe una jurisprudencia consolidada que aborde el contexto de la IO, cabe esperar que se apliquen los principios tradicionales de responsabilidad civil por productos defectuosos.

PRÁCTICAS SUGERIDAS:

Habilite la seguridad por defecto mediante nombres de usuario y contraseñas únicos y difíciles de descifrar. Los nombres de usuario y las contraseñas de los dispositivos IoT suministrados por el fabricante son

a menudo nunca son cambiadas por el usuario y son fáciles de descifrar. Las redes de bots operan buscando continuamente dispositivos IoT que estén protegidos por nombres de usuario y contraseñas conocidos por defecto. Los controles de seguridad fuertes deben ser algo que el consumidor industrial tenga que desactivar deliberadamente en lugar de activar deliberadamente.

Construya el dispositivo utilizando el sistema operativo más **reciente** que sea técnicamente viable y económicamente factible. Muchos dispositivos IoT utilizan sistemas operativos Linux, pero pueden no utilizar el sistema operativo más actualizado. Utilizar el sistema operativo actual garantiza que las vulnerabilidades conocidas se habrán mitigado.

Utilice **hardware que incorpore características de seguridad** para reforzar la protección e integridad del dispositivo. Por ejemplo, utilice chips informáticos que integren la seguridad a nivel de transistor, incrustados en el procesador, y que proporcionen cifrado y anonimato.

Diseñar teniendo en cuenta la interrupción del sistema y del funcionamiento. Comprender las consecuencias que podría tener el fallo de un dispositivo permitirá a los desarrolladores, fabricantes y proveedores de servicios tomar decisiones de seguridad más informadas y basadas en el riesgo. Siempre que sea posible, los desarrolladores deben construir dispositivos IoT para que fallen de forma segura, de modo que el fallo no conduzca a una mayor interrupción del sistema.

Promover las actualizaciones de seguridad a
nd Gestión de la vulnerabilidad

Incluso cuando la seguridad se incluye en la fase de diseño, pueden descubrirse vulnerabilidades en los productos después de que se hayan desplegado. Estos fallos pueden mitigarse mediante parches, actualizaciones de seguridad y estrategias de gestión de vulnerabilidades. Al diseñar estas estrategias, los desarrolladores deben tener en cuenta las implicaciones de un fallo del dispositivo, la durabilidad del producto asociado y el coste previsto de la reparación. En ausencia de la capacidad de desplegar actualizaciones de seguridad, los fabricantes pueden enfrentarse a la decisión de elegir entre una costosa retirada del mercado o dejar en circulación dispositivos con vulnerabilidades conocidas.

ENFOQUE: NTIA Multi-
Proceso de las partes interesadas en la aplicación de parches y actualizaciones

La Administración Nacional de Telecomunicaciones e Información (NTIA) ha convocado un proceso de múltiples partes interesadas en relación con la "Actualizabilidad y los parches de la Internet de los objetos" para reunir a las partes interesadas y compartir la variedad de opiniones sobre la actualizabilidad y los parches de seguridad, y establecer objetivos más concretos para la adopción por parte de toda la industria.

PRÁCTICAS SUGERIDAS:
Considere la posibilidad de **asegurar el dispositivo a través de las conexiones de red o por medios automatizados**. Lo ideal sería que los parches se aplicaran automáticamente y que aprovecharan las protecciones criptográficas de integridad y autenticidad para solucionar más rápidamente las vulnerabilidades.
Considere la posibilidad de **coordinar las actualizaciones de software entre los proveedores de terceros** para abordar las vulnerabilidades y las mejoras de seguridad a fin de garantizar que los dispositivos de los consumidores tengan el conjunto completo de protecciones actuales.
Desarrollar **mecanismos automatizados para abordar las vulnerabilidades**. En el ámbito de la ingeniería de software, por ejemplo, existen mecanismos para incorporar la información de los informes sobre vulnerabilidades críticas procedentes de las comunidades de investigadores y hackers en tiempo real. Esto permite a los desarrolladores abordar esas vulnerabilidades en el diseño del software, y responder cuando sea apropiado.
Desarrollar una política relativa a la divulgación coordinada **de vulnerabilidades**, incluyendo las prácticas de seguridad asociadas para abordar las vulnerabilidades identificadas. Una política de divulgación coordinada debe involucrar a los desarrolladores, fabricantes y proveedores de servicios, e incluir información sobre cualquier vulnerabilidad reportada a un equipo de respuesta a incidentes de seguridad informática (CSIRT). El US Computer Emergency Readiness Team (US-CERT), el Industrial Control Systems (ICS)-CERT, y otros CSIRTs proporcionan regularmente alertas técnicas, incluso después de incidentes importantes, que proporcionan información sobre las vulnerabilidades y su mitigación.

Basarse en prácticas de seguridad reconocidas

Muchas de las prácticas probadas que se utilizan en la seguridad tradicional de las TI y las redes pueden aplicarse a la IO. Estos enfoques pueden ayudar a identificar vulnerabilidades, detectar irregularidades, responder a posibles incidentes y recuperarse de daños o interrupciones en los dispositivos IoT.

ENFOQUE EN: Marco de gestión de riesgos de ciberseguridad del NIST

El Instituto Nacional de Normas y Tecnología (NIST) publicó un marco para la gestión de los riesgos de ciberseguridad que ha sido ampliamente adoptado por la industria privada, integrado entre sectores y dentro de las organizaciones. El marco es ampliamente reconocido como una piedra de toque integral para la gestión de riesgos cibernéticos de las organizaciones https://www.nist.gov/cyberframework. Aunque no es específico de la IO, el marco de riesgos proporciona un punto de partida para considerar los riesgos y las mejores prácticas.

PRÁCTICAS SUGERIDAS:

Comience con **las prácticas básicas de seguridad de software y ciberseguridad** y aplíquelas al ecosistema del IoT de forma flexible, adaptable e innovadora.

Consulte las **orientaciones sectoriales** pertinentes, cuando existan, como punto de partida para considerar las prácticas de seguridad. Algunas agencias federales abordan las prácticas de seguridad para los sectores únicos que regulan. Por ejemplo, la Administración Nacional de Seguridad del Tráfico en las Carreteras (NHTSA) ha publicado recientemente unas directrices sobre las mejores prácticas de ciberseguridad para los vehículos modernos que abordan algunos de los riesgos únicos que plantean los vehículos autónomos o semiautónomos. Del mismo modo, la Administración de Alimentos y Medicamentos publicó un proyecto de orientación sobre la gestión de la ciberseguridad en losdispositivos médicos después de su comercialización.

Practicar la defensa en profundidad. Los desarrolladores y fabricantes deben emplear un enfoque holístico de la seguridad que incluya defensas en capas contra las amenazas a la ciberseguridad, incluidas las herramientas a nivel de usuario como posibles puntos de entrada para los actores maliciosos. Esto es especialmente valioso si los mecanismos de parcheo o actualización no están disponibles o son insuficientes para abordar una vulnerabilidad específica.

Participar en **plataformas de intercambio de información** para informar de las vulnerabilidades y recibir información oportuna y crítica sobre las ciberamenazas y vulnerabilidades actuales de los socios públicos y privados. El intercambio de información es una herramienta fundamental para garantizar que las partes interesadas sean conscientes de las amenazas a medida que surgen3. El Centro Nacional de Integración de la Ciberseguridad y las Comunicaciones (NCCIC) del Departamento de Seguridad Nacional (DHS), así como los centros de análisis e intercambio de información (ISAC) multiestatales y sectoriales y las organizaciones de análisis e intercambio de información (ISAO), son ejemplos de ello.

[3] "Information Sharing", National Cybersecurity and Communications Information Center.

Priorizar las medidas de seguridad según el impacto potencial

Los modelos de riesgo difieren sustancialmente en el ecosistema del IoT. Por ejemplo, los consumidores industriales (como los propietarios y operadores de reactores nucleares) tendrán consideraciones diferentes a las de un consumidor minorista. Las consecuencias de un fallo de seguridad en los distintos clientes también variarán significativamente. Por lo tanto, centrarse en las posibles consecuencias de una interrupción, una infracción o una actividad maliciosa en todo el espectro de consumidores es fundamental para determinar hacia dónde deben dirigirse los esfuerzos particulares de seguridad y quién es el más capacitado para mitigar las consecuencias significativas.

¿Deben centrarse las medidas de seguridad del IoT en el dispositivo del IoT?

Dado que el propósito de todos los procesos de IoT es tomar información en un punto físico y motivar una decisión basada en esa información (a veces con consecuencias físicas), las medidas de seguridad pueden centrarse en una o más partes del proceso de IoT. Como se ha señalado anteriormente, los riesgos de la IO comienzan con el dispositivo específico, pero ciertamente no se limitan a él. Los desarrolladores, fabricantes y proveedores de servicios deben considerar los riesgos específicos del dispositivo IoT, así como del proceso y el servicio, y tomar decisiones basadas en el impacto relativo sobre los tres en cuanto a dónde deben aplicarse las medidas más sólidas.

PRÁCTICAS SUGERIDAS:

Conocer el **uso y el entorno previsto del dispositivo**, siempre que sea posible. Este conocimiento ayuda a los desarrolladores y fabricantes a tener en cuenta las características técnicas del dispositivo IoT, cómo puede funcionar el dispositivo y las medidas de seguridad que pueden ser necesarias.

Realice un **ejercicio de "red-teaming"**, en el que los desarrolladores intenten activamente eludir las medidas de seguridad necesarias en las capas de aplicación, red, datos o física. El análisis resultante y la planificación de la mitigación deberían ayudar a priorizar las decisiones sobre dónde y cómo incorporar medidas de seguridad adicionales.

Identificar y autenticar los dispositivos conectados a la red, especialmente para los consumidores industriales y las redes empresariales. La aplicación de medidas de autenticación para los dispositivos y servicios conocidos permite al consumidor industrial controlar aquellos dispositivos y servicios que están dentro de sus marcos organizativos.

Promover la transparencia en el IoT

En la medida de lo posible, los desarrolladores y fabricantes deben conocer su cadena de suministro**,** es decir, si hay vulnerabilidades asociadas con los componentes de software y hardware proporcionados por proveedores ajenos a su organización. La dependencia de las numerosas soluciones de software y hardware de bajo coste y fácil acceso que se utilizan en la IO puede dificultar esta tarea. Dado que los desarrolladores y fabricantes dependen de fuentes externas para obtener soluciones de software y hardware de bajo coste y fácil acceso, es posible que no puedan evaluar con precisión el nivel de seguridad incorporado en los componentes al desarrollar e implantar dispositivos conectados a la red. Además, dado que muchos dispositivos del IoT utilizan paquetes de código abierto, los desarrolladores y fabricantes pueden no ser capaces de identificar las fuentes de estos componentes.

Una mayor concienciación podría ayudar a los fabricantes y a los consumidores industriales a identificar dónde y cómo aplicar las medidas de seguridad o incorporar redundancias. En función del perfil de riesgo del producto en cuestión, los desarrolladores, fabricantes y proveedores de servicios estarán mejor equipados para mitigar adecuadamente las amenazas y vulnerabilidades con la mayor rapidez posible, ya sea mediante la aplicación de parches, la retirada del producto o el aviso al consumidor.

PRÁCTICAS SUGERIDAS:

Llevar a cabo evaluaciones de riesgo de extremo a extremo que tengan en cuenta tanto los **riesgos** internos como los de terceros **proveedores,** siempre que sea posible. Los desarrolladores y fabricantes deben incluir a los vendedores y proveedores en el proceso de evaluación de riesgos, lo que creará transparencia y les permitirá conocer las posibles vulnerabilidades de terceros y promoverá la confianza y la transparencia. La seguridad debe ser revisada de forma continua a medida que el componente de la cadena de suministro es reemplazado, eliminado o actualizado.

Considere la posibilidad de crear un **mecanismo de divulgación pública para utilizar los informes de vulnerabilidad**. Los programas de Bug Bounty, por ejemplo, se basan en métodos de crowdsourcing para identificar vulnerabilidades que los propios equipos de seguridad internos de las empresas pueden no detectar.

Considerar la posibilidad de desarrollar y emplear una **lista de materiales de software** que pueda utilizarse como medio para crear una confianza compartida entre vendedores y fabricantes. Los desarrolladores y fabricantes deberían considerar la posibilidad de proporcionar una lista de los componentes de hardware y software conocidos en el paquete del dispositivo de una manera que tenga en cuenta la necesidad de proteger las cuestiones de propiedad intelectual. Una lista puede servir como herramienta valiosa para que otros en el ecosistema de la IO entiendan y gestionen su riesgo y parcheen cualquier vulnerabilidad inmediatamente después de cualquier incidente.

Conéctese con cuidado y deliberadamente

Los consumidores de IoT, especialmente en el contexto industrial, deben considerar deliberadamente si la conectividad continua es necesaria dado el uso del dispositivo IoT y los riesgos asociados a su interrupción. Los consumidores de IoT también pueden ayudar a contener las posibles amenazas que plantea la conectividad a la red conectándose de forma cuidadosa y deliberada, y sopesando los riesgos de una posible infracción o fallo de un dispositivo IoT frente a los costes de limitar la conectividad a Internet.

En el actual entorno de red, es probable que cualquier dispositivo IoT pueda sufrir una interrupción durante su ciclo de vida. Los desarrolladores, fabricantes y consumidores de IoT deben tener en cuenta cómo una interrupción afectará a la función principal del dispositivo IoT y a las operaciones comerciales tras la interrupción.

¿Necesitan todos los dispositivos en red una conexión continua y automática a Internet?

En 2015, la Comisión Federal de Comercio publicó una guía llamada "Start with Security: A Guide for Businesses" para ayudarles a determinar esta misma cuestión. Aunque puede ser conveniente tener un acceso continuo a la red, puede no ser necesario para el propósito del dispositivo -y los sistemas-; por ejemplo, los reactores nucleares, donde una conexión continua a internet abre la oportunidad de una intrusión de consecuencias potencialmente enormes.

PRÁCTICAS SUGERIDAS:

Informe a los consumidores de IoT sobre la finalidad prevista de las conexiones de red. Las conexiones directas a Internet pueden no ser necesarias para operar las funciones críticas de un dispositivo IoT, especialmente en el entorno industrial. La información sobre la naturaleza y la finalidad de las conexiones puede servir de base para las decisiones de los consumidores.

Haz conexiones intencionadas. Hay casos en los que al consumidor le interesa no conectarse directamente a Internet, sino a una red local que pueda agregar y evaluar cualquier información crítica. Por ejemplo, los sistemas de control industrial (ICS) deben protegerse mediante los principios de defensa en profundidad publicados por https://ics- cert.us-cert.gov/recommended_practices.

Incorporar **controles que** permitan a los fabricantes, proveedores de servicios y consumidores desactivar las conexiones de red o puertos específicos cuando sea necesario o se desee para permitir **una conectividad selectiva**. Dependiendo de la finalidad del dispositivo IoT, proporcionar a los consumidores orientación y control sobre la implementación final puede ser una práctica acertada.

CONCLUSIÓN

Nuestra nación no puede permitirse una generación de dispositivos IoT desplegados sin tener en cuenta la seguridad. Las consecuencias son demasiado elevadas dado el potencial de daño a nuestra infraestructura crítica, nuestra privacidad personal y nuestra economía.

Al tiempo que el DHS publica estos principios, reconocemos los esfuerzos que están llevando a cabo nuestros colegas de otras agencias federales y el trabajo de las entidades del sector privado para avanzar en las arquitecturas e instituir prácticas para abordar la seguridad del IoT. Este documento es un primer paso para fortalecer esos esfuerzos mediante la articulación de principios de seguridad generales. Pero seguramente se necesitarán más pasos.

El DHS identifica cuatro líneas de esfuerzo que deberían ser emprendidas por el gobierno y la industria para fortificar la seguridad del IoT.

CUATRO LÍNEAS DE ESFUERZO:
Coordinar a todos los departamentos y agencias federales para comprometerse con las partes interesadas en la IO y explorar conjuntamente formas de mitigar los riesgos que plantea la IO. El DHS, junto con sus socios federales, seguirá colaborando con los socios de la industria para determinar los enfoques que pueden mejorar aún más la seguridad de la IO, y para promover la comprensión de las tendencias tecnológicas en evolución que pueden abordar los riesgos de la IO. Los esfuerzos futuros también se centrarán en la actualización y aplicación de estos principios, a medida que se perfeccionen y comprendan mejor las mejores prácticas y enfoques.
Concienciar a las partes interesadas sobre los riesgos asociados a la IO. Es importante que las partes interesadas sean conscientes de los riesgos de la IO para que puedan posicionarse para hacerles frente. El DHS acelerará las iniciativas de concienciación, educación y formación del público, en colaboración con otros organismos, el sector privado y socios internacionales. El DHS, junto con otros organismos, también emprenderá iniciativas más directamente adaptadas a sectores concretos y consumidores individuales.
Identificar y avanzar en los incentivos para incorporar la seguridad de la IO. Los responsables políticos, los legisladores y las partes interesadas deben considerar formas de incentivar mejor los esfuerzos para mejorar la seguridad de la IO. En el entorno actual, con demasiada frecuencia no está claro quién es responsable de la seguridad de un determinado producto o sistema. Además, los costes de una seguridad deficiente no suelen ser asumidos por quienes están mejor posicionados para aumentar la seguridad. El DHS y todas las demás partes interesadas deben considerar cómo la responsabilidad civil, los ciberseguros, la legislación, la reglamentación, la gestión voluntaria de la certificación, las iniciativas de establecimiento de normas, las iniciativas voluntarias a nivel de la industria y otros mecanismos podrían mejorar la seguridad sin dejar de fomentar la actividad económica y la innovación pionera. En el futuro, el DHS se reunirá con sus socios para debatir estas cuestiones críticas y solicitar ideas y comentarios.
Contribuir a los procesos de desarrollo de normas internacionales para la IO. La IO forma parte de un ecosistema global, y otros países y organizaciones internacionales están empezando a evaluar muchas de estas mismas consideraciones de seguridad. Es importante que las actividades relacionadas con la IO no se dividan en conjuntos de normas o reglas incoherentes. A medida que el DHS se centra cada vez más en los esfuerzos de la IO, debemos comprometernos con nuestros

socios internacionales y el sector privado para apoyar el desarrollo de normas internacionales y garantizar que se alinean con nuestro compromiso de fomentar la innovación y promover la seguridad.

El DHS espera con interés estos próximos pasos de colaboración. Juntos podemos, y debemos, afrontar estos complejos retos. Al hacerlo, nos aseguraremos de que nuestro futuro conectado a la red no sólo sea innovador, sino también seguro y construido para durar.

APÉNDICE: ORIENTACIONES Y RECURSOS ADICIONALES

Los principios de este documento se han desarrollado sobre la base de la información recogida en los informes de la industria, y a través de las discusiones con la industria privada, las asociaciones comerciales, las entidades no gubernamentales y los socios federales, especialmente con el NIST y la NTIA.

Departamento de Seguridad Nacional

- https://www.dhs.gov/sites/default/files/publications/draft-lces-security-comments-508.pdf
- https://www.dhs.gov/publication/security-tenets-lces
- https://www.dhs.gov/sites/default/files/publications/security-tenets-lces-paper-11-20-15-508.pdf

Otras entidades federales

- Comité Consultivo de Telecomunicaciones para la Seguridad Nacional
    1. Informe final del NSTAC sobre el Internet de los objetos

- NTIA
    1. Notificación y solicitud de comentarios sobre los beneficios, desafíos y posibles funciones del Gobierno para fomentar el avance de la Internet de los objetos
        a) Comentarios
    2. Libro Verde - Ciberseguridad, Innovación y Economía de Internet, 2011
    3. Nuevas ideas sobre el emergente Internet de los objetos
    4. Declaraciones del subsecretario Simpson en el taller sobre el fomento del avance de la de la Internet de las cosas, 9/9/2016
        a) Anuncio para fomentar el avance del taller sobre la Internet de los objetos
    5. Recurso/revisión/catalogación del Grupo de Trabajo de Política de Internet sobre las ventajas, los retos y las posibles funciones del gobierno para fomentar el avance de la Internet de los objetos.

- NIST
    1. Marco de ciberseguridad
    2. Programa de Sistemas Ciberfísicos (CPS)
        a) Borrador del Grupo de Trabajo Público (PWG) sobre Sistemas CiberfísicosCPS) Marco de trabajo de la versión 1.0
            - Se aceptan comentarios hastael 9/2/2015

3. Programa Smart-Grid
4. Grupo de Trabajo Técnico Internacional sobre el Marco deCiudades Inteligentes habilitadas por la IO
5. Publicación especial (SP) 800-183 del NIST, Network of Things, 28 de julio de 2016.
    a) Comunicado de prensa del NIST

- Comisión Federal de Comercio
    1. Informe del personal de la FTC, "Internet of Things: Privacy & Security in a Connected World", enero de 2015.

- Congreso de los Estados Unidos
    1. Audiencia del Comité de Comercio, Ciencia y Transporte del Senado, "El mundo conectado: Examinando el Internet delos objetos".
    2. Resolución bipartidista unánime del Senado (S. Res. 110) en la que se pide una estrategia nacional que guíe el desarrollo del Internet de los objetos.
    3. Comisión de Energía y Comercio de la Cámara de Representantes: "El Internet de los objetos: Explorando la próximafrontera"
- Oficina de Contabilidad del Gobierno
    1. Compromiso de la GAO con el DHS: La GAO está actualmente comprometida con el DHS en materia de IoT, código 100435 [carta de notificación del 15 de enero de 2016 disponible a través de este enlace].
        a) Estado/entrada en la más reciente, 3 de junio de 2016 Lista de compromisos activos de la GAO relacionados conel DHS

Fuentes externas

La lista de recursos adicionales se proporciona únicamente como referencia y no constituye un respaldo del Departamento de Seguridad Nacional (DHS). El DHS no respalda ningún producto, servicio o empresa comercial.

- Consejo del Atlántico
    1. Hogares inteligentes e Internet de las cosas - http://www.atlanticcouncil.org/publications/issue-briefs/smart-homes-and-the-internet-of-things
- Yo soy la caballería
    1. Marco de ciberseguridad de cinco estrellas para el sector de la automoción - https://iamthecavalry.org/5star
    2. Juramento hipocrático para los dispositivos médicos conectados - https://iamthecavalry.org/oath
- Alianza para la Confianza en Línea

1. Las mejores prácticas de los consumidores

- Consorcio de Internet Industrial: http://www.iiconsortium.org/IISF.htm
- Proyecto abierto de seguridad de las aplicaciones web (OWASP)
    1. Proyecto del Internet de las cosas https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
    2. Guía de seguridad de la Internet de los objetos https://www.owasp.org/index.php/IoT_Security_Guidance
- Safecode.org mejores prácticas industriales relevantes www.safecode.org
- AT&T
    1. Explorando la seguridad del IoT
- Symantec
    1. Una arquitectura de referencia de la Internet de las cosas https://www.symantec.com/content/dam/symantec/docs/white-papers/iot-security-reference-architecture-en.pdf