Código de conducta para la seguridad del Internet de las cosas de los consumidores

Título

Código de conducta para la seguridad del Internet de las cosas de los consumidores

Fecha

Octubre de 2018

Resumen ejecutivo

A medida que conectamos más dispositivos a Internet en nuestros hogares, los productos y electrodomésticos que tradicionalmente estaban fuera de línea se están convirtiendo en parte del «Internet de las cosas» (IoT, por sus siglas en inglés).

El IoT representa un nuevo capítulo sobre cómo la tecnología se vuelve cada vez más común en nuestros hogares, haciendo que la vida de las personas sea más fácil y placentera. A medida que las personas confían cada vez más datos personales a los dispositivos y servicios en línea, la seguridad cibernética de estos productos es ahora tan importante como la seguridad física de nuestros hogares.

El objetivo de este Código de conducta es ayudar a todas las partes involucradas en el desarrollo, fabricación y venta minorista de IoT de consumo con un conjunto de directrices para garantizar que los productos sean seguros por naturaleza y para facilitar que las personas mantengan su seguridad en el mundo digital.

Este Código de conducta reúne, en trece directrices centradas en los resultados, lo que se considera en general una buena práctica en la seguridad del IoT. Ha sido desarrollado por el DCMS (del inglés *Department for Digital, Culture, Media and Sport*, Departamento de contenidos digitales, cultura, medios de comunicación y deporte) junto con el NCSC (del inglés *National Cyber Security Centre*, Centro nacional de ciberseguridad) y sigue las normas del sector, las asociaciones de consumidores y los ámbitos académicos. El Código se publicó por primera vez como borrador en marzo de 2018 como parte del informe Secure by Design.[1]

Introducción

El Internet de las cosas (IoT) ofrece grandes oportunidades para las personas. Pero se ha descubierto que un número significativo de dispositivos en el mercado hoy en día carecen de medidas de seguridad básicas. Las personas deben poder beneficiarse de las tecnologías conectadas de forma segura, con la confianza de que existen medidas de seguridad y de privacidad adecuadas para proteger su actividad en línea.

[1] DCMS, 2018, 'Secure by Design: Improving the cyber security of consumer Internet of Things: Report', https://www.gov.uk/government/publications/secure-by-design.

Este Código de conducta establece pasos prácticos para los fabricantes de IoT y otras partes interesadas del sector para mejorar la seguridad de los productos IoT de consumo y sus servicios asociados. La aplicación de sus trece directrices contribuirá a proteger la privacidad y seguridad de los consumidores, a la vez que les facilitará el uso seguro de sus productos. También mitigará la amenaza de ataques por DDoS (del inglés *Distributed Denial of Service*, denegación de servicio distribuido) que se lanzan desde dispositivos y servicios del IoT mal protegidos.

Las directrices aportan lo que se considera una buena práctica en la seguridad del IoT. Se centran en los resultados, en lugar de ser prescriptivos, lo que proporciona a las organizaciones flexibilidad para innovar e implementar soluciones de seguridad adecuadas para sus productos.

Este Código de conducta no es un remedio mágico para resolver todos los desafíos de seguridad. Una organización solo puede tener éxito en la creación de un IoT seguro si cambia a una nueva mentalidad en materia de seguridad e invierte en un ciclo de vida de desarrollo seguro. Los productos y servicios deben diseñarse teniendo en cuenta la seguridad, desde el desarrollo del producto hasta su ciclo de vida completo. Las organizaciones también tienen que evaluar periódicamente los riesgos de seguridad cibernética relevantes para sus productos y servicios e implementar medidas apropiadas para abordarlos.

Las cadenas de suministro de productos IoT pueden ser complejas e internacionales, y suelen contar con la participación de numerosos fabricantes de componentes y proveedores de servicios. El objetivo del Código es iniciar y facilitar cambios de seguridad positivos en toda la cadena de suministro.

Una serie de organismos del sector y foros internacionales han desarrollado recomendaciones de seguridad y estándares para el IoT.[2] El presente Código de conducta se ha diseñado para complementar y respaldar esos esfuerzos y los estándares de ciberseguridad publicados. Se ha creado directamente con el sector con la esperanza de que los planes de garantía y marca de confianza futuros relacionados con el IoT del consumidor se adapten a él.

La implementación del Código de conducta puede ayudar a las organizaciones a cumplir con las leyes de protección de datos aplicables. Por ejemplo, el Reglamento general de protección de datos (RGPD) de la UE requiere que los datos personales se procesen de forma segura.[3]

Implementación

El Código de conducta está respaldado por un documento de asignación que vincula cada una de sus directrices con los principales estándares, recomendaciones y orientación del

[2] PETRAS, 2018, 'Summary literature review of industry recommendations and international developments on IoT security', https://www.gov.uk/government/publications/secure-by-design.
[3] El artículo 5 (1) (f) del RGPD se refiere a la «integridad y confidencialidad» de los datos personales.

sector.[4] Este documento brinda un contexto adicional a las trece directrices del Código y ayuda al sector a implementarlas. Este documento también muestra la relación entre el Código y el trabajo sobre seguridad del IoT que un amplio número de organizaciones internacionales están llevando a cabo.

Priorización y estructura

Las tres primeras directrices se consideran prioritarias porque la acción en las contraseñas predeterminadas, la divulgación de vulnerabilidades y las actualizaciones de seguridad proporcionan los mayores beneficios de seguridad a corto plazo.

En el texto adicional se expone el razonamiento y se añade más información para cada directriz. Las notas explicativas adicionales al final del documento responden a las preguntas frecuentes.

Audiencias

Se proporciona una indicación para cada directriz sobre qué parte interesada es la principal responsable de la implementación. Las partes interesadas se definen como:

Fabricante de dispositivos	Entidad que crea un producto conectado a Internet final ensamblado. Un producto final puede contener los productos de muchos otros fabricantes diferentes.
Proveedores de servicios del IoT	Empresas que ofrecen servicios tales como redes, almacenamiento en la nube y transferencia de datos que forman parte de soluciones del IoT. Se pueden ofrecer dispositivos conectados a Internet como parte del servicio.
Desarrolladores de aplicaciones móviles	Entidades que desarrollan y proporcionan aplicaciones que se ejecutan en dispositivos móviles. Normalmente se ofrecen como una forma de interactuar con dispositivos como parte de una solución del IoT.
Minoristas	Vendedores de productos conectados a Internet y servicios asociados a los consumidores.

Terminología

El uso del término «datos sensibles a la seguridad» tiene como objetivo diferenciar entre otros tipos de datos confidenciales, por ejemplo, datos de categorías especiales (formalmente conocidos como «datos personales sensibles») como se define en el RGPD. Los datos sensibles a la seguridad podrían incluir, por ejemplo, vectores de inicialización criptográfica.

[4] DCMS, 2018, 'Mapping of IoT Security Recommendations, Guidance and Standards to the Code of Practice for Consumer IoT Security', https://www.gov.uk/government/publications/secure-by-design.

El término «consumidor» se utiliza en todo el documento por coherencia; en general se puede considerar que los consumidores son los usuarios finales de los productos y servicios del IoT.

Ámbito de aplicabilidad

Este Código de conducta se aplica a los productos del IoT para los consumidores que están conectados a Internet o a una red doméstica y los servicios asociados. Entre una lista no exhaustiva de ejemplos se incluyen:

- Juguetes infantiles y monitores para bebés conectados
- Productos relacionados con la seguridad conectados, como detectores de humo y cerraduras de puertas
- Cámaras, televisores y altavoces inteligentes
- Sistemas de seguimiento de salud portátiles
- Sistemas de alarma y domótica conectados
- Electrodomésticos conectados (por ejemplo, lavadoras, frigoríficos)
- Asistentes de hogar inteligentes.

Los servicios asociados se consideran aquí como los servicios digitales que están vinculados a dispositivos IoT, por ejemplo, aplicaciones móviles, informática/almacenamiento en la nube e interfaces de programación de aplicaciones (API) de terceros para servicios tales como mensajería.

Revisión

El DCMS revisará periódicamente el Código y publicará actualizaciones, al menos cada dos años. Póngase en contacto con securebydesign@culture.gov.uk para mantenerse informado.

Directrices

1) Ausencia de contraseñas predeterminadas

Todas las contraseñas de dispositivos IoT serán únicas y no podrán restablecerse a ningún valor universal predeterminado de fábrica.

Muchos dispositivos IoT se venden con nombres de usuario y contraseñas universales por defecto (como «admin, admin») que el consumidor tiene que cambiar. Este ha sido el origen de muchos problemas de seguridad del IoT y en la práctica se tiene que eliminar. Deben seguirse las mejores prácticas sobre contraseñas y otros métodos de autenticación.[5]

Principalmente se aplica a: Fabricantes de dispositivos

2) Implementación de una política de divulgación de vulnerabilidades

Todas las compañías que ofrecen dispositivos y servicios conectados a Internet deben proporcionar un punto de contacto público como parte de una política de divulgación de vulnerabilidades para que los investigadores de seguridad y otras personas relevantes puedan informar de los problemas. Se debe actuar sobre las vulnerabilidades reveladas de manera oportuna.

El conocimiento de una vulnerabilidad de seguridad permite a las compañías responder. Las compañías también deben supervisar, identificar y rectificar continuamente las vulnerabilidades de seguridad dentro de sus propios productos y servicios como parte del ciclo de vida de la seguridad del producto. Se debe informar de las vulnerabilidades directamente a las partes interesadas afectadas en primera instancia. Si eso no es posible, se puede informar a las autoridades nacionales.[6] En las notas explicativas se incluye más información sobre los diferentes enfoques a tener en cuenta en diferentes circunstancias. También se recomienda a las compañías a compartir información con los organismos competentes del sector.[7]

Principalmente se aplica a: Fabricantes de dispositivos, proveedores de servicios del IoT y desarrolladores de aplicaciones móviles

3) Mantenimiento del software actualizado

---

[5] Para obtener ayuda, consulte, por ejemplo: NCSC 2016, 'Password Guidance: Simplifying Your Approach', https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach. Véase también: NIST, 2017, 'NIST Special Publication 800-63B: Digital Identity Guidelines - Authentication and Lifecycle Management', https://pages.nist.gov/800-63-3/sp800-63b.html#sec5.

[6] En el Reino Unido, los informes de vulnerabilidades se pueden enviar a https://www.ncsc.gov.uk/contact.

[7] Entre los organismos competentes del sector se incluyen la GSMA y la IoT Security Foundation. La Guía sobre la divulgación coordinada de vulnerabilidades está disponible en IoT Security Foundation, que hace referencia al estándar ISO/IEC 29147 sobre revelación de vulnerabilidades. El programa de Divulgación de vulnerabilidades coordinadas a nivel industrial de la GSMA se encuentra en https://www.gsma.com/cvd.

Los componentes de software en dispositivos conectados a Internet deben poder actualizarse de forma segura. Las actualizaciones deben ser oportunas y no deben afectar al funcionamiento del dispositivo. Se publicará una política de fin de vida útil para dispositivos finales que indique de forma explícita el tiempo mínimo durante el cual un dispositivo recibirá actualizaciones de software y las razones de la duración del período de asistencia. Las necesidades de cada actualización deben quedar claras para los consumidores y la actualización se debe implementar de manera sencilla. Para dispositivos restringidos que no se pueden actualizar físicamente, el producto se tiene que poder aislar y reemplazar.

También se debe garantizar la procedencia de los parches de seguridad y deben enviarse a través de un canal seguro. Las funciones básicas de un dispositivo deben seguir funcionando durante una actualización siempre que sea posible, por ejemplo, un reloj debe continuar indicando la hora, un termostato doméstico aún debería funcionar y un candado debería continuar desbloqueando y bloqueando. Esto puede parecer principalmente una consideración de diseño, pero puede convertirse en un problema de seguridad crítico para algunos tipos de dispositivos y sistemas si no se considera o gestiona correctamente.

Se deben proporcionar actualizaciones de software después de la venta de un dispositivo y enviarse a los dispositivos durante un período adecuado para el dispositivo. Este período de asistencia de la actualización de software debe indicarse de forma clara al consumidor en el momento de adquirir el producto. El minorista o los fabricantes deben informar al consumidor de la necesidad de una actualización. Para dispositivos restringidos sin posibilidad de actualización de software, las condiciones y el período de asistencia de reemplazo deben quedar claros.

Principalmente se aplica a: Fabricantes de dispositivos, proveedores de servicios del IoT y desarrolladores de aplicaciones móviles

4) Almacenamiento de las credenciales y los datos sensibles a la seguridad de manera segura

Todas las credenciales se almacenarán de forma segura en los servicios y en los dispositivos. No se admitirán las credenciales codificadas en el software del dispositivo.

La ingeniería inversa de dispositivos y aplicaciones puede descubrir fácilmente credenciales como nombres de usuario y contraseñas codificados en el software. Los métodos sencillos de ofuscamiento también utilizados para ocultar o encriptar esta información codificada se pueden descifrar fácilmente. Los datos confidenciales que deben almacenarse de forma segura incluyen, por ejemplo, claves criptográficas, identificadores de dispositivos y vectores de inicialización. Se deben usar mecanismos de almacenamiento seguros y confiables, como los provistos por Trusted Execution Environment y el almacenamiento confiable y seguro asociado.

Principalmente se aplica a: Fabricantes de dispositivos, proveedores de servicios del IoT, desarrolladores de aplicaciones móviles

5) Comunicación segura

Los datos sensibles a la seguridad, incluidos cualquier gestión y control remotos, se deben cifrar en tránsito, de acuerdo con las propiedades de la tecnología y el uso. Todas las claves deben gestionarse de forma segura.

Se recomienda encarecidamente el uso de estándares de Internet abiertos y revisados por pares.

Principalmente se aplica a: Fabricantes de dispositivos, proveedores de servicios del IoT, desarrolladores de aplicaciones móviles

6) Minimización de las superficies de ataque expuestas

Todos los dispositivos y servicios deben operar bajo el «principio de mínimo privilegio»; los puertos que no se utilicen se deben cerrar, el hardware no debe exponer innecesariamente el acceso, los servicios no deberían estar disponibles si no se usan y el código debe minimizarse a la funcionalidad necesaria para que el servicio funcione. El software debe ejecutarse con los privilegios adecuados, teniendo en cuenta tanto la seguridad como la funcionalidad.

El principio de mínimo privilegio es la piedra angular de una buena ingeniería de seguridad, aplicable tanto al IoT como a cualquier otro campo de aplicación.

Principalmente se aplica a: Fabricantes de dispositivos, proveedores de servicios del IoT

7) Garantía de la integridad del software

El software de dispositivos IoT debe verificarse utilizando mecanismos de arranque seguros. Si se detecta un cambio no autorizado, el dispositivo debe alertar al consumidor/administrador del problema y no debe conectarse a redes más amplias que las necesarias para realizar la función de alerta.

La capacidad de recuperación remota de estas situaciones debe basarse en un estado conocido oportuno, como el almacenamiento local de una versión conocida adecuada para permitir que el dispositivo se recupere y se actualice de forma segura. Eso evitará la denegación de servicio y las retiradas o visitas de mantenimiento costosas, mientras se gestiona el riesgo de una posible adquisición del dispositivo por parte de un atacante subvirtiendo la actualización u otros mecanismos de comunicación de red.

Principalmente se aplica a: Fabricantes de dispositivos

8) Garantía de protección de los datos personales

Cuando los dispositivos o servicios procesan datos personales, lo deben hacer en conformidad con la ley de protección de datos aplicable, como el Reglamento general de protección de datos (RGPD) y la Ley de protección de datos de 2018. Los fabricantes de dispositivos y los proveedores de servicios del IoT deben proporcionar a los consumidores

información clara y transparente sobre cómo se usan sus datos, quién los envía y con qué fines, para cada dispositivo y servicio. Esto también se aplica a los terceros que puedan estar involucrados (incluidos los anunciantes). Cuando los datos personales se procesan con el consentimiento de los consumidores, este se debe obtener de forma válida y lícita, y los consumidores deben tener la oportunidad de retirarlo en cualquier momento.

Esta directriz garantiza que:
i) Los fabricantes de IoT, los proveedores de servicios y los desarrolladores de aplicaciones cumplen con las obligaciones de protección de datos cuando desarrollan y proporcionan productos y servicios.
ii) Los datos personales se procesan en conformidad con la ley de protección de datos aplicable.
iii) Se ayuda a los usuarios a garantizar que las operaciones de procesamiento de datos de sus productos sean consistentes y que funcionen según lo especificado.
iv) Se proporciona a los usuarios los medios para preservar su privacidad al configurar la funcionalidad del dispositivo y del servicio de manera adecuada.

Principalmente se aplica a: Fabricantes de dispositivos, proveedores de servicios del IoT, desarrolladores de aplicaciones móviles, minoristas

9) Creación de sistemas resistentes a las interrupciones

La capacidad de recuperación debe incorporarse a los dispositivos y servicios del IoT cuando así lo requiera su uso o mediante otros sistemas de confianza, teniendo en cuenta la posibilidad de interrupciones en las redes de datos y la alimentación. En la medida de lo posible, los servicios del IoT deben permanecer operativos y localmente funcionales en el caso de una pérdida de red y deben recuperarse limpiamente en el caso de una restauración por una pérdida de energía. Los dispositivos deben poder regresar a una red en un estado sensible y de manera ordenada, en lugar de volver a conectarse a gran escala.

Los consumidores confían en los sistemas y dispositivos IoT para casos de uso cada vez más importantes que pueden ser relevantes para la seguridad o tener un gran impacto en la vida. El mantenimiento de los servicios en ejecución local si hay una pérdida de la red es una de las medidas que se pueden tomar para aumentar la capacidad de recuperación. Otras medidas pueden incluir la creación de redundancia en servicios, así como mitigaciones contra ataques DDoS. El nivel de resiliencia necesario debe ser proporcional y debe estar determinado por el uso, pero se debe considerar a otros que pueden confiar en el sistema, servicio o dispositivo, ya que puede haber un impacto más amplio del esperado.

Principalmente se aplica a: Fabricantes de dispositivos, proveedores de servicios del IoT

10) Supervisión de los datos de telemetría del sistema

Si se recopilan datos de telemetría de los dispositivos y servicios del IoT, como el uso y los datos de medición, se deben supervisar las anomalías de seguridad.

La supervisión de la telemetría, incluidos los datos de registro, es útil para la evaluación de la seguridad y permite identificar y resolver las circunstancias inusuales de manera temprana, minimizando el riesgo de seguridad y permitiendo una rápida mitigación de problemas. Sin embargo, en conformidad con la directriz 8, el procesamiento de datos personales debe mantenerse al mínimo y se debe proporcionar a los consumidores información sobre qué datos se recopilan y las razones para ello.

Principalmente se aplica a: Proveedores de servicios del IoT

11) Facilitación a los consumidores de la eliminación de datos personales

Los dispositivos y servicios deben configurarse de modo que los datos personales puedan eliminarse fácilmente cuando se realice una transferencia de propiedad, cuando el consumidor desee eliminarlos o cuando desee deshacerse del dispositivo. Los consumidores deben recibir instrucciones claras sobre cómo eliminar sus datos personales.

Los dispositivos IoT pueden cambiar de dueño y eventualmente serán reciclados o eliminados. Se pueden proporcionar mecanismos que permitan al consumidor mantener el control y eliminar los datos personales de los servicios, dispositivos y aplicaciones.

Principalmente se aplica a: Fabricantes de dispositivos, proveedores de servicios del IoT, desarrolladores de aplicaciones móviles

12) Facilitación de la instalación y el mantenimiento de los dispositivos

La instalación y el mantenimiento de dispositivos IoT se debe realizar en un número mínimo de pasos y deben seguir las mejores prácticas de seguridad sobre usabilidad. Los consumidores también deben recibir orientación sobre cómo configurar su dispositivo de forma segura.

Los problemas de seguridad causados por la confusión o mala configuración del consumidor se pueden reducir y, a veces, eliminarse abordando adecuadamente la complejidad y el diseño deficiente en las interfaces de usuario. Una información clara a los usuarios sobre cómo configurar dispositivos de forma segura también puede reducir su exposición a las amenazas.

Principalmente se aplica a: Fabricantes de dispositivos, proveedores de servicios del IoT, desarrolladores de aplicaciones móviles

13) Validación de los datos de entrada

Se validará la entrada de datos a través de interfaces de usuario y transferidas a través de interfaces de programación de aplicaciones (API) o entre redes en servicios y dispositivos.

Los sistemas se pueden alterar debido a datos formateados incorrectamente o códigos transferidos a través de diferentes tipos de interfaz. Normalmente, los atacantes emplean herramientas automatizadas para explotar posibles brechas y debilidades que surgen como

resultado de no validar los datos. Algunos ejemplos incluyen, sin carácter restrictivo, datos que:
i) No son del tipo esperado, por ejemplo, código ejecutable en lugar de texto ingresado por el usuario.
ii) Están fuera de rango, por ejemplo, un valor de temperatura que sobrepasa los límites de un sensor.

Principalmente se aplica a: Fabricantes de dispositivos, proveedores de servicios del IoT, desarrolladores de aplicaciones móviles

Notas explicativas adicionales

Directriz 1 sobre la ausencia de contraseñas predeterminadas: Si bien se ha trabajado mucho para eliminar la dependencia de las contraseñas y proporcionar métodos alternativos de autenticación de usuarios y sistemas, algunos productos IoT todavía se están comercializando con nombres de usuario y contraseñas predeterminados desde interfaces de usuario hasta protocolos de red. Esta práctica no es aceptable y debe suspenderse. La seguridad del dispositivo se puede fortalecer aún más teniendo identidades únicas e inmutables.

Directriz 2 sobre CVD (del inglés Coordinated Vulnerability Disclosure, divulgación de vulnerabilidad coordinada): La CVD está estandarizada por la Organización internacional de normalización (ISO), es fácil de implementar y se ha demostrado su éxito en algunas grandes compañías de software de todo el mundo.[8] Sin embargo, la CVD aún no está establecida en el sector del IoT y algunas compañías pueden mostrarse reticentes a tratar con investigadores de seguridad. La CVD proporciona un camino para que los investigadores de seguridad se pongan en contacto con las empresas para informarles de los problemas de seguridad que ponen a la empresa por delante de la amenaza de la explotación maliciosa y brindarles la oportunidad de resolver las vulnerabilidades antes de una divulgación pública.

Las compañías que proporcionan dispositivos y servicios conectados a Internet tienen el deber de cuidar a terceros que puedan verse perjudicados por su incapacidad de tener un programa de CVD en su lugar. Además, las compañías que comparten esta información a través de organismos del sector pueden ayudar a otras personas que puedan estar sufriendo el mismo problema.

Las divulgaciones pueden requerir diferentes enfoques según las circunstancias: Vulnerabilidades relacionadas con productos o servicios únicos: se debe informar del problema directamente a la parte interesada afectada (por ejemplo, fabricante del dispositivo, proveedor de servicios del IoT o desarrollador de aplicaciones móviles). Las fuentes de estos informes pueden ser investigadores de seguridad o compañeros del sector. Si, después de ponerse en contacto con el fabricante del dispositivo u otra parte interesada

[8] International Organization for Standardization, 2014, 'ISO/IEC 29147 - Vulnerability Disclosure', https://www.iso.org/standard/45170.html.

afectada, no actúan de manera oportuna, entonces es posible informar del problema directamente al NCSC.

Vulnerabilidades sistémicas: Puede ser que una parte interesada, como un fabricante de dispositivos, descubra un problema potencialmente sistémico. Si bien es fundamental corregirlo en el propio producto del fabricante del dispositivo, es importante que el sector y los consumidores compartan esta información. De manera similar, los investigadores de seguridad también pueden informar de dichas vulnerabilidades sistémicas. En este caso, un organismo competente del sector relevante puede coordinar una respuesta de mayor escala. El NCSC puede proporcionar asesoramiento y orientación al organismo competente del sector para ofrecer la respuesta coordinada.

Una «manera oportuna» para actuar sobre las vulnerabilidades varía considerablemente y es específica del incidente; sin embargo, el estándar de facto para que se complete el proceso de vulnerabilidad no debe superar los 90 días. Una corrección de hardware puede tardar mucho más tiempo en tratarse que una corrección de software. Además, una solución que se debe implementar en los dispositivos puede tardar más tiempo en implementarse que una solución de software del servidor.

Directriz 3 sobre el mantenimiento del software actualizado: Las actualizaciones de seguridad del software son una de las acciones más importantes que una empresa puede hacer para proteger a sus clientes y al ecosistema técnico más amplio. Las vulnerabilidades a menudo provienen de componentes de software que no se consideran relacionados con la seguridad. Por lo tanto, como principio general, todo el software debe mantenerse actualizado y en buen estado. Las correcciones se pueden enviar a los dispositivos de forma preventiva, normalmente como parte de las actualizaciones automáticas, que pueden eliminar las vulnerabilidades de seguridad antes de que sucedan. Su gestión puede ser compleja, especialmente si hay actualizaciones en la nube, actualizaciones de dispositivos y otras actualizaciones de servicio con las que tratar. Por lo tanto, es esencial contar con un plan de gestión e implementación claro, así como transparencia para los consumidores sobre el estado actual del soporte de actualización.

En muchos casos, la publicación de actualizaciones de software implicará múltiples dependencias en otras organizaciones, como los fabricantes de subcomponentes. Eso no es un motivo para denegar las actualizaciones: el objetivo del Código de conducta es instigar un cambio de seguridad positivo en toda la cadena de suministro de software. También hay algunas situaciones en las que no se pueden aplicar parches a los dispositivos. Algunos dispositivos ultrarrestringidos entrarán en esta categoría y para ellos se necesita un plan de reemplazo que se debe comunicar claramente al consumidor. Este plan debe detallar un cronograma de reemplazo de las tecnologías, cuándo se debe realizar y cuándo finaliza el servicio técnico para hardware y software.

Puede ser de vital importancia para los consumidores que un dispositivo siga funcionando. Esta es la razón por la cual una actualización no debe «afectar al funcionamiento de un dispositivo» cuando sea posible. En particular, los dispositivos que cumplen una función relevante para la seguridad no deben apagarse completamente en el caso de una actualización; tiene que haber alguna capacidad funcional mínima del sistema, por ejemplo, mantener el funcionamiento de un sistema de calefacción o una alarma antirrobo. Los

fabricantes de este tipo de dispositivos también deberían considerar avanzar hacia una arquitectura más resistente.

Es importante tener en cuenta que los mecanismos de actualización de software son un vector de ataque y se debe prestar atención para garantizar que estén protegidos.

Directriz 5 sobre la comunicación segura: La idoneidad de los controles de seguridad y el uso del cifrado depende de muchos factores, incluido el contexto de uso.[9] Como la seguridad está en constante evolución, es difícil dar consejos prescriptivos sobre las medidas de cifrado sin el riesgo de que tales consejos queden obsoletos rápidamente. Los implementadores deben asegurarse de que su producto pueda satisfacer las necesidades de los usuarios y a la vez siga siendo resistente a los ataques de cifrado.

Directriz 7 sobre la garantía de la integridad del software: Si un dispositivo IoT detecta que ha sucedido algo inusual con su software, debe ser capaz de informar a la persona adecuada. En algunos casos, los dispositivos pueden tener la capacidad de estar en modo de administración; por ejemplo, puede haber un modo de usuario para un termostato en una habitación que impida que se cambien otras configuraciones. En estos casos, una alerta al administrador es apropiada ya que esa persona tiene la capacidad de actuar sobre la alerta.

Directriz 9 sobre la creación de sistemas resistentes a las interrupciones: El objetivo de esta guía es garantizar que los servicios del IoT sigan en funcionamiento a medida que aumenta la adopción de dispositivos IoT en todos los aspectos de la vida del consumidor, incluso en funciones que son relevantes para la seguridad personal. El impacto en la vida de las personas podría ser prevalente si, por ejemplo, se pierde una conexión a Internet en una puerta conectada y alguien se quede fuera. Otro ejemplo es un sistema de calefacción doméstica que se apaga debido a un ataque DDoS contra un servicio en la nube. Es importante tener en cuenta que pueden aplicarse otras reglamentaciones relacionadas con la seguridad, pero la clave es evitar que las interrupciones sean la causa de estos [problemas].

[9] Puede encontrar más ayuda disponible, por ejemplo, del CNSC en https://www.ncsc.gov.uk/guidance/tls-external-facing-services.