Código de prácticas de seguridad del consumidor en relación con el Internet de las cosas

Título

Código de prácticas de seguridad del consumidor en relación con el Internet de las cosas

Fecha

Octubre del 2018

Resumen ejecutivo

Debido a que cada vez conectamos más dispositivos de nuestros hogares al Internet, los productos y electrodomésticos que tradicionalmente se han utilizado sin conexión, ahora forman parte del "Internet de las cosas" (IdC).

El IdC representa una nueva etapa en cómo la tecnología se vuelve cada vez más común en nuestros hogares, haciendo la vida de las personas más fácil y agradable. Dado que la gente confía una gran cantidad de datos personales a los dispositivos y servicios en línea, ahora la seguridad cibernética de estos productos es tan importante como la seguridad física de nuestros hogares.

El objetivo de este Código de prácticas es asistir a todas las partes involucradas en el desarrollo, la fabricación y la distribución del IdC para consumidores, con una serie de normas que garanticen que los productos sean seguros por diseño y para hacer que sea más sencillo para las personas estar seguras en un mundo digital.

Este Código de prácticas reúne, en trece normas enfocadas en las consecuencias, lo que generalmente se considera como buenas prácticas de seguridad del IdC. Ha sido desarrollado por el Departamento de Cultura, Medios y Deporte (DCMS, por sus siglas en inglés), en conjunto con el Centro Nacional de Seguridad Cibernética (NCSC, por sus siglas en inglés), y busca lograr el compromiso de la industria, las asociaciones de consumidores y el ámbito académico. El proyecto del Código se publicó en marzo del 2018, como parte del informe Seguridad por diseño.[1]

Introducción

El Internet de las cosas (IdC) brinda excelentes oportunidades a las personas. Sin embargo, se ha descubierto que, en la actualidad, una gran cantidad de dispositivos del mercado no cumplen con las medidas de seguridad básicas. Las personas deben poder beneficiarse de las tecnologías conectadas de manera segura, confiando en que las medidas de seguridad y privacidad correspondientes se están cumpliendo 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 prácticas establece las medidas concretas para que los fabricantes del IdC y otros participantes mejoren la seguridad del consumidor en relación con los productos del IdC y sus servicios correspondientes. Implementar sus trece normas ayudará a proteger la privacidad y seguridad de los consumidores, haciendo que para ellos sea más sencillo usar sus productos de forma segura. También reducirá las amenazas de ataques distribuidos de denegación de servicio (DDoS, por sus siglas en inglés) que se presentan en los dispositivos y servicios del IdC con poca seguridad.

Las normas reúnen lo que generalmente se considera como buenas prácticas de seguridad del IdC. Estas se centran en las consecuencias en lugar de la normativa, lo que da a las organizaciones la versatilidad de innovar e implementar soluciones de seguridad apropiadas para sus productos.

Este Código de prácticas no es una solución milagrosa para resolver todos los problemas de seguridad. La única forma en que una organización puede tener éxito en la creación de un IdC seguro es enfocándose en la seguridad e invirtiendo en un ciclo de vida de desarrollo seguro. Los productos y servicios se deben diseñar tomando en cuenta la seguridad, desde el desarrollo del producto y a través de todo su ciclo de vida. Las organizaciones también deben evaluar regularmente los riesgos de seguridad cibernética pertinentes a sus productos y servicios e implementar las medidas apropiadas para solucionarlos.

Las cadenas de suministro de productos del IdC pueden ser complejas e internacionales y por lo general involucran a diversos fabricantes de componentes y proveedores de servicios. El objetivo del Código es iniciar y facilitar un cambio positivo en la seguridad en toda la cadena de suministros.

Varios organismos de la industria y foros internacionales están creando recomendaciones y normas de seguridad para el IdC.[2] Este Código de prácticas está diseñado para complementar y apoyar esos esfuerzos, así como los estándares de seguridad cibernética pertinentes ya publicados. Se creó directamente con la industria, con la esperanza de que se utilice en los futuros planes de aseguramiento de calidad y marcas de confianza relacionados con el IdC para el consumidor.

La implementación del Código de prácticas 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 exige que los datos personales se procesen de forma segura.[3]

Implementación

El Código de prácticas está respaldado por un documento de resumen que vincula cada una de estas normas con los principales estándares, recomendaciones y directrices de la

[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) de la RGPD se refiere a la "integridad y confidencialidad" de los datos personales.

industria.[4] Este documento contextualiza mejor las trece normas del código y ayuda a la industria a implementarlas. Este documento también muestra la relación entre el Código y el trabajo que han realizado, con respecto a la seguridad del IdC, un gran número de organizaciones mundiales.

Organización por prioridades y estructura

Las primeras tres normas tienen prioridad, porque tomar medidas en cuanto a las contraseñas predeterminadas, la divulgación de vulnerabilidades y las actualizaciones de seguridad aportará la mayor cantidad de beneficios a corto plazo.

El texto de apoyo explica la lógica y detalla en mayor profundidad cada norma. Las notas explicativas adicionales al final del documento responden a las preguntas frecuentes.

Destinatarios

Se proporciona una indicación para cada norma, en cuanto a qué participante tendrá la responsabilidad principal de la implementación. Los participantes se definen como:

Fabricantes de dispositivos	La entidad que crea y ensambla el producto final con conexión a Internet. Un producto final puede contener los productos de muchos otros fabricantes distintos.
Proveedores de servicios del IdC	Empresas que ofrecen servicios como redes, almacenamiento en la nube y transferencia de datos, que se ofrecen como parte de las soluciones del IdC. Es posible que se ofrezcan dispositivos con conexión a Internet como parte del servicio.
Desarrolladores de aplicaciones móviles	Entidades que desarrollan y proporcionan aplicaciones que se usan en dispositivos móviles. Por lo general se ofrecen como una forma de interactuar con los dispositivos como parte de una solución del IdC.
Vendedores minoristas	Los vendedores de los productos que tienen conexión a Internet y servicios asociados a los consumidores.

Terminología

El uso del término "datos confidenciales seguros" pretende diferenciarlos de otros tipos de datos confidenciales por ejemplo, los datos de categoría especial (oficialmente conocidos como "datos personales confidenciales") según lo definido en el RGPD. Los datos confidenciales seguros 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 para mantener la coherencia; generalmente se considera que los consumidores son los usuarios finales de los productos y servicios del IdC.

Alcance de aplicación

Este Código de prácticas se aplica a los productos del IdC para el consumidor, que están conectados a Internet o a redes domésticas y a servicios asociados. Una lista parcial de ejemplos incluye lo siguiente:

- Juguetes de niños y monitores infantiles conectados a Internet,
- Productos de seguridad con conexión a Internet, como detectores de humo y cerraduras de puertas,
- Televisores, altavoces y cámaras inteligentes
- Accesorios inteligentes ponibles para monitorear la salud,
- Sistemas de alarma y automatización del hogar con conexión a Internet,
- Electrodomésticos con conexión a Internet (por ejemplo, lavadoras, refrigeradores),
- Asistentes de hogar inteligente.

Aquí, los servicios asociados se consideran como los servicios digitales que están vinculados con los dispositivos del IdC, por ejemplo, aplicaciones móviles, almacenamiento o computación en la nube e interfaces de programación de aplicaciones (API) de terceros para servicios como la mensajería.

Revisión

El Departamento de Cultura, Medios y Deporte revisará regularmente el Código y publicará actualizaciones, al menos cada dos años. Comuníquese con securebydesign@culture.gov.uk para mantenerse informado.

Normas

1) No utilizar contraseñas predeterminadas

Todas las contraseñas de los dispositivos IdC serán únicas y no se podrán restablecer bajo ningún valor de fábrica universal predeterminado.

Muchos dispositivos del IdC se venden con nombres de usuario y contraseñas predeterminados universales (como "admin, admin"), los cuales se espera que el consumidor cambie. Esto ha sido origen de muchos problemas de seguridad en el IdC y dicha situación debe eliminarse. Deben seguirse las prácticas recomendadas para contraseñas y otros métodos de autenticación.[5]

Se dirige principalmente a: Fabricantes de dispositivos

2) Implementar una política de divulgación de vulnerabilidades

Todas las empresas que proporcionan dispositivos y servicios con conexión a Internet deberán proporcionar un servicio de punto de contacto público, como parte de una política de divulgación de vulnerabilidades, para que los investigadores de seguridad y otras personas puedan informar de problemas. Deberán solucionarse de forma oportuna las vulnerabilidades divulgadas.

Tener conocimiento sobre la vulnerabilidad de la seguridad les permite a las empresas reaccionar. Las empresas también deben supervisar continuamente para identificar y enmendar las vulnerabilidades de la seguridad en sus propios productos y servicios, como parte de un ciclo de vida de seguridad del producto. En primera instancia, debe informarse directamente a los participantes afectados por las vulnerabilidades. Si esto no es posible, las vulnerabilidades pueden reportarse a las autoridades nacionales.[6] En las notas explicativas se incluyen más detalles sobre los diferentes pasos que deben tomarse en las distintas circunstancias. También se invita a que las empresas a compartir la información con los organismos competentes de la industria.[7]

Se dirige principalmente a: Fabricantes de dispositivos, proveedores de servicios del IdC y desarrolladores de aplicaciones móviles

---

[5] Para ver las normas consulte, por ejemplo: NCSC, 2016, 'Password Guidance: Simplifying Your Approach' (Orientación sobre contraseñas: simplificando su enfoque), https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach. Vea también: NIST, 2017, 'NIST Special Publication 800-63B: Digital Identity Guidelines - Authentication and Lifecycle Management' (Publicación especial de NIST 800-63B: Pautas de identidad digital - Autenticación y administración de vida útil), 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] Los organismos competentes de la industria incluyen a la Asociación GSM (GSMA, por sus siglas en inglés) y a la IoT Security Foundation. Guidance on Coordinated Vulnerability Disclosure (Normas de divulgación coordinada de vulnerabilidades) está disponible en la IoT Security Foundation, que hace referencia a la Norma ISO/IEC/29147 sobre la divulgación de vulnerabilidades. El programa Coordinated Vulnerability Disclosure (Divulgación coordinada de vulnerabilidades) a nivel de la industria de la GSMA se encuentra en https://www.gsma.com/cvd.

3) Mantener el software actualizado

Los componentes del software en dispositivos con conexión a Internet deben poder actualizarse de forma segura. Las actualizaciones deben ser oportunas y no afectar la función del dispositivo. Debe publicarse una política sobre el término de la vida útil de los dispositivos finales en la que se indique de manera explícita la duración mínima del período durante el cual un dispositivo recibirá actualizaciones de software, y el motivo de la duración del período de asistencia. Se debe dejar en claro para los consumidores la razón por la que cada actualización es necesaria y debe ser sencillo implementarlas. Para dispositivos limitados que no se puedan actualizar físicamente, el producto se debe aislar y reemplazar.

También se debe garantizar el origen de los parches de seguridad y se deben entregar a través de un medio seguro. Siempre que sea posible, las funciones básicas de un dispositivo deben seguir funcionando durante una actualización; un reloj, por ejemplo, debe seguir dando la hora, un termostato para el hogar debe seguir funcionando y una cerradura debe seguir abriendo y cerrando. Esto puede parecer principalmente una consideración del diseño, pero si no se toma en cuenta o se controla adecuadamente, se puede transformar en un serio problema de seguridad para algunos tipos de dispositivos y sistemas.

Las actualizaciones del software se deben poner a disposición después de la venta de un dispositivo, y enviarlas a los dispositivos durante un período adecuado. Este período de asistencia de actualizaciones de software debe dejarse claro al consumidor en el momento en que se adquiere el producto. El distribuidor o los fabricantes deben informar al consumidor que se requiere la actualización. Las condiciones del período de asistencia de reemplazo para dispositivos con restricciones que no tienen la posibilidad de actualizar el software deben ser claras.

Se dirige principalmente a: Fabricantes de dispositivos, proveedores de servicios del IdC y desarrolladores de aplicaciones móviles

4) Guardar las credenciales y los datos confidenciales de forma segura

Las credenciales se almacenarán de forma segura dentro de los servicios y en los dispositivos. No se admiten credenciales fijas codificadas en el software del dispositivo.

La ingeniería inversa de dispositivos y aplicaciones puede descubrir fácilmente credenciales como nombres de usuario y contraseñas fijos codificados en los programas. Los métodos sencillos de ocultamiento que también se utilizan para oscurecer o cifrar esta información codificada fija se pueden burlar muy fácilmente. Los datos confidenciales que se deben almacenar de forma segura incluyen, por ejemplo, claves criptográficas, identificadores de dispositivo y vectores de inicialización. Deben utilizarse mecanismos de almacenamiento confiables y seguros, como los que proporcionan un entorno de ejecución confiable y un almacenamiento asociado seguro y confiable.

Se dirige principalmente a: Fabricantes de dispositivos, proveedores de servicios del IdC, desarrolladores de aplicaciones móviles

5) Comunicarse de forma segura

Los datos confidenciales, lo que incluye cualquier control y gestión remota, se deben codificar en tránsito, de acuerdo con las propiedades de la tecnología y el uso. Todas las claves deben administrarse de forma segura.

Se recomienda firmemente el uso de estándares de Internet abiertos, revisados por pares.

Se dirige principalmente a: Fabricantes de dispositivos, proveedores de servicios del IdC, desarrolladores de aplicaciones móviles

6) Reducir las superficies expuestas a ataques

Todos los dispositivos y servicios deben funcionar bajo el "principio de privilegio mínimo", los puertos sin uso se deben cerrar, el hardware no deben tener accesos innecesarios expuestos, los servicios no deben estar disponibles si no se usan y el código se debe reducir a la funcionalidad necesaria para los servicios que se van a operar. El programa debe funcionar con los privilegios apropiados, teniendo en cuenta tanto la seguridad como la funcionalidad.

El principio del privilegio mínimo es la base de una buena ingeniería de seguridad y se aplica tanto al IdC como a cualquier otro campo.

Se dirige principalmente a: Fabricantes de dispositivos, proveedores de servicios del IdC

7) Garantizar la integridad del software

El software en dispositivos del IdC se debe verificar mediante mecanismos de arranque seguro. Si se detecta un cambio no autorizado, el dispositivo debe advertir al consumidor/administrador que existe un problema y no debe conectarse a otras redes más amplias que no sean las necesarias para cumplir la función de alerta.

La capacidad de recuperarse de forma remota de estas situaciones debe basarse en un estado de funcionamiento adecuado conocido, es decir, almacenar de forma local una versión de un estado de funcionamiento adecuado para usarla como recuperación segura y llevar a cabo la actualización del dispositivo. Esto evitará la denegación de servicio y visitas de mantenimiento o retiros del producto costosos, al mismo tiempo que controla el riesgo potencial de que un atacante pueda tomar el control del dispositivo alterando la actualización u otros mecanismos de comunicación de la red.

Se dirige principalmente a: Fabricantes de dispositivos

8) Asegurar que los datos personales estén protegidos

Cuando los productos o servicios procesan datos personales, deben hacerlo de conformidad con las leyes de protección de datos aplicables, como el Reglamento General de Protección de Datos (RGPD) y la Ley de protección de datos del 2018. Los fabricantes

de dispositivos y los proveedores de servicios del IdC deben proporcionar información clara y transparente a los consumidores con respecto a cómo se utilizan sus datos, quién lo hace y con qué fines, para cada dispositivo y servicio. Esto también se aplica a cualquier tercero que pueda estar involucrado (incluidos los anunciantes). Cuando los datos personales se procesan basándose en el consentimiento de los consumidores, estos deben obtenerse de forma válida y legal, y debe darse a los consumidores la oportunidad de retirar dicho consentimiento en cualquier momento.

Esta norma garantiza que:
i) Los fabricantes, proveedores de servicios y desarrolladores de aplicaciones del IdC respeten las obligaciones de protección de datos cuando desarrollen y entreguen productos y servicios;
ii) Los datos personales se procesen de conformidad con la ley de protección de datos;
iii) Los usuarios reciban asistencia para garantizar que las operaciones de procesamiento de datos de sus productos sean coherentes y que funcionen tal como se indica;
iv) Los usuarios cuenten con mecanismos para proteger su privacidad mediante la configuración del dispositivo y la funcionalidad del servicio de manera apropiada.

Se dirige principalmente a: Fabricantes de dispositivos, proveedores de servicios IdC, desarrolladores de aplicaciones móviles, distribuidores

9) Hacer que los sistemas sean flexibles en casos de desconexión o cortes de energía

La flexibilidad debe estar integrada en los dispositivos y servicios del IdC cuando así lo requiera su uso o el uso de otros sistemas que los utilicen, considerando la posibilidad de interrupciones a las redes de datos y de energía eléctrica. Dentro de lo posible, los servicios del IdC deben seguir operando y ser funcionales de forma local en caso de una desconexión de la red, y se deben recuperar sin problemas después de un corte de energía eléctrica. Los dispositivos deben poder volver a la red en un estado razonable y de forma ordenada, en lugar de una reconexión a gran escala.

Los consumidores confían cada vez más en los sistemas y dispositivos del IdC para usos prácticos cada vez más importantes que pueden ser relevantes para la seguridad o tener un impacto en sus vidas. Una de las medidas que se pueden tomar para aumentar la flexibilidad es mantener los servicios funcionando de manera local en caso de que exista una pérdida de conexión a la red. Otras medidas pueden incluir el establecimiento de conexiones redundantes a servicios, además de mitigar ataques de DDoS. El nivel de flexibilidad necesario debe ser proporcional y estar determinado por el uso, pero se deben considerar a otros que puedan depender del sistema, servicio o dispositivo, ya que es posible que exista un impacto mayor del esperado.

Se dirige principalmente a: Fabricantes de dispositivos, proveedores de servicios del IdC

10) Supervisar los datos de telemetría del sistema

Si se obtienen datos de telemetría de los dispositivos y servicios del IdC, como datos de uso y de medición, se deben supervisar para identificar irregularidades en la seguridad.

La supervisión de la telemetría, incluidos los datos de registro, es útil para la evaluación de la seguridad y permite que se identifiquen a tiempo y se solucionen las circunstancias fuera de lo común, lo que reduce los riesgos de seguridad y permite una solución rápida de los problemas. Sin embargo, de acuerdo con la Norma 8, el procesamiento de datos personales se debe mantener al mínimo y debe informarse a los consumidores sobre qué tipo de datos se recopilan y las razones para ello.

Se dirige principalmente a: Proveedores de servicios del IdC

11) Facilitar la eliminación de datos personales por parte de los consumidores

Dispositivos y servicios deben configurarse de tal manera que los datos personales se puedan eliminar fácilmente de ellos cuando exista una transferencia de propiedad, cuando el consumidor desee borrarlos o cuando quiera deshacerse del dispositivo. Los consumidores deben recibir instrucciones claras sobre cómo eliminar sus datos personales.

Los dispositivos del IdC pueden cambiar de dueño y tarde o temprano tendrán que reciclarse o desecharse. Deben proporcionarse mecanismos que permitan al consumidor mantener el control y eliminar su información personal de los servicios, dispositivos y aplicaciones.

Se dirige principalmente a: Fabricantes de dispositivos, proveedores de servicios del IdC, desarrolladores de aplicaciones móviles

12) Hacer que la instalación y el mantenimiento de los dispositivos sean sencillos

La instalación y el mantenimiento de los dispositivos del IdC deben requerir de pasos mínimos y seguir las prácticas recomendadas de seguridad en la utilización. Los consumidores también deben recibir indicaciones sobre cómo configurar su dispositivo de forma segura.

Los problemas de seguridad causados por una configuración inadecuada o por la confusión del consumidor se pueden reducir y, en ocasiones, eliminar cuando se resuelve adecuadamente la complejidad y el diseño deficiente en las interfaces de usuario. Una guía clara para los usuarios acerca de cómo configurar los dispositivos de forma segura también puede reducir su exposición a amenazas.

Se dirige principalmente a: Fabricantes de dispositivos, proveedores de servicios del IdC, desarrolladores de aplicaciones móviles

13) Validar los datos de entrada

Debe validarse el ingreso de datos a través de interfaces de usuario y la transferencia a través de las interfaces de programación de la aplicación (API) o entre redes en servicios y dispositivos.

Los sistemas se pueden alterar por datos con un formato incorrecto o códigos transferidos a través de distintos tipos de interfaz. Con frecuencia, los atacantes emplean herramientas

automáticas para aprovechar las brechas y debilidades que surgen como resultado de la falta de validación de los datos. Los ejemplos incluyen, entre otros, datos que:
i) No son del tipo esperado, por ejemplo, un código ejecutable en lugar de texto ingresado por el usuario.
ii) Están fuera de rango, por ejemplo, un valor de temperatura que está por sobre los límites de un sensor.

Se dirige principalmente a: Fabricantes de dispositivos, proveedores de servicios del IdC, desarrolladores de aplicaciones móviles

Notas explicativas adicionales

Norma 1 sobre no utilizar contraseñas predeterminadas: Aunque se han hecho muchos esfuerzos por eliminar la dependencia en las contraseñas y proporcionar métodos alternativos de autenticación de usuarios y sistemas, algunos productos del IdC siguen llegando al mercado con nombres de usuario y contraseñas predeterminados, desde interfaces de usuario hasta protocolos de redes. Esta no es una práctica aceptable y debe dejar de usarse. La seguridad de los dispositivos se puede fortalecer aún más otorgándoles identidades únicas e inalterables.

Norma 2 sobre la divulgación coordinada de vulnerabilidades (CVD, por sus siglas en inglés): La CVD está estandarizada por la Organización Internacional de Normalización (ISO), es fácil de implementar y se ha probado que es exitosa en algunas grandes empresas de software de todo el mundo.[8] Sin embargo, la CVD aún no se establece en la industria del IdC y es posible que algunas empresas se sientan renuentes a trabajar con los investigadores de seguridad. La CVD le da a los investigadores de seguridad una forma de ponerse en contacto con las empresas para informarles sobre problemas de seguridad, lo que las pone un paso adelante de la amenazas de explotación maliciosa, y les da la oportunidad de resolver las vulnerabilidades antes de realizar una divulgación pública.

Las empresas que proporcionan dispositivos y servicios con conexión a Internet tienen el deber de preocuparse por terceros que puedan resultar perjudicados debido a que no tienen establecido un programa de CVD. Además, las empresas que comparten su información a través de los organismos de la industria pueden ayudar a otras que puedan estar teniendo el mismo problema.

Es posible que las divulgaciones exijan distintos enfoques, dependiendo de las circunstancias:
Vulnerabilidades relacionadas con un solo producto o servicio: el problema se debe informar directamente a los participantes afectados (por ejemplo, fabricante del dispositivo, proveedor de servicio del IdC o desarrollador de aplicaciones móviles). El origen de estos informes puede ser los investigadores de seguridad o los pares de la industria. Si después de hacer contacto con el fabricante del dispositivo u otro participante afectado, no actúan de manera oportuna, entonces es posible informar sobre un problema directamente al NCSC.

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

Vulnerabilidades sistémicas: Puede ocurrir que un participante, como un fabricante de dispositivos, descubra un problema que afecte posiblemente a todo el sistema. Si bien la reparación del propio producto del fabricante de dispositivos es muy importante, compartir esta información con la industria y los consumidores puede aportar un gran beneficio. Asimismo, es posible que los investigadores de seguridad también busquen informar de dichas vulnerabilidades del sistema. En este caso, un organismo de la industria competente y pertinente puede coordinar una respuesta a mayor escala. El NCSC puede proporcionar asesoría y orientación al organismo de la industria competente para poder proporcionar una respuesta coordinada.

Una "manera oportuna" de actuar sobre las vulnerabilidades varía considerablemente y es distinta según el caso, sin embargo, la norma para completar los procesos de vulnerabilidad no supera los 90 días. Una reparación de física del dispositivo puede tardar mucho más que una de software. Además, es posible que una reparación que se deba implementar en los dispositivos tarde más en comenzar, comparada con una reparación de un software de servidor.

Norma 3 sobre mantener actualizado el software: Las actualizaciones de seguridad del software son una de las cosas más importantes que una empresa puede hacer para proteger a sus clientes y al ecosistema técnico en general. Las vulnerabilidades a menudo provienen de componentes de software que no se consideran relacionados con la seguridad. Por tanto, como principio general, todo el software debe mantenerse actualizado y recibir buen mantenimiento. Se pueden enviar reparaciones preventivas a los dispositivos, por lo general, como parte de actualizaciones automáticas, que pueden eliminar vulnerabilidades de seguridad antes de que puedan explotarse. Controlar esto puede ser complejo, especialmente si hay que lidiar con actualizaciones en la nube, actualizaciones de dispositivos y actualizaciones en otros servicios. Por tanto, es esencial contar con un plan de implementación y control claro, así como la transparencia con el consumidor acerca del estado actual del soporte de actualización.

En muchos casos, publicar actualizaciones de software involucrará a distintas dependencias de otras organizaciones, como fabricantes de subcomponentes. Esta no es una razón para no llevar a cabo las actualizaciones: el objetivo del Código de prácticas es impulsar un cambio positivo en cuanto a la seguridad a través de toda la cadena de suministros de software. También existen algunas situaciones en las que los dispositivos no pueden aceptar los parches de software. Algunos dispositivos muy limitados entrarán en esta categoría y para estos se debe implementar un plan de sustitución, que debe comunicarse al consumidor de forma clara. Este plan debe detallar un programa para saber cuándo deben reemplazar las tecnologías y, cuando corresponda, saber en qué fecha finaliza el soporte para el software y el hardware.

Es posible que para los consumidores sea importante que un dispositivo siga funcionando. Esta es la razón por la cual una actualización "no debe impactar en el funcionamiento de un dispositivo", siempre que sea posible. En especial, los dispositivos que cumplen una función importante para la seguridad no se deben apagar por completo en caso de una actualización; debe haber una capacidad de funcionamiento mínimo del sistema, por ejemplo, mantener el funcionamiento de un sistema de calefacción o una alarma antirrobo.

Los fabricantes de esos tipos de dispositivos también deben considerar avanzar a una arquitectura más flexible.

Es importante tener en cuenta que los mecanismos de actualización de software son vías de ataque y se les debe prestar mucha atención para garantizar su seguridad.

Norma 5 sobre la comunicación segura: La idoneidad de los controles de seguridad y el uso del cifrado depende de muchos factores, lo que incluye el contexto de uso.[9] Debido a que la seguridad está en constante evolución, es difícil dar consejos normativos sobre las medidas de cifrado sin el riesgo de que dichos consejos queden obsoletos en un corto plazo. Los ejecutores deben asegurarse de que su producto satisfaga las necesidades de los usuarios y, al mismo tiempo, sea resistente a los ataques en el cifrado.

Norma 7 sobre garantizar la integridad del software: Si un dispositivo del IdC detecta que sucede algo irregular con el software, debe poder informarlo a la persona correcta. En algunos casos, es posible que los dispositivos tengan la capacidad de entrar en modo de administración; por ejemplo, es posible que exista un modo de usuario para un termostato en una habitación, que no permita modificar otros ajustes. En estos casos, es apropiado que exista una alerta para el administrador, ya que la persona tiene la capacidad de darle respuesta.

Norma 9 sobre hacer que los sistemas sean flexibles en casos de desconexión o cortes de energía: El objetivo de esta norma es garantizar que los servicios del IdC se mantengan funcionando, ya que la adopción de dispositivos del IdC en todos los aspectos de la vida de los consumidores va en aumento, y esto incluye funciones que son importantes para la seguridad personal. El impacto en la vida de las personas puede ser predominante si, por ejemplo, una puerta con conexión a Internet pierde la conexión y alguien se queda afuera sin poder entrar. Otro ejemplo es un sistema de calefacción doméstica que se apaga debido a un ataque DDoS contra los servicios de la nube. Es importante tener en cuenta que pueden aplicar otras regulaciones relacionadas con la seguridad, pero la clave es evitar que las interrupciones en el servicio eléctrico o de red sean la causa de estos [problemas].

[9] Puede encontrarse orientación disponible, por ejemplo, en el NCSC en https://www.ncsc.gov.uk/guidance/tls-external-facing-services.