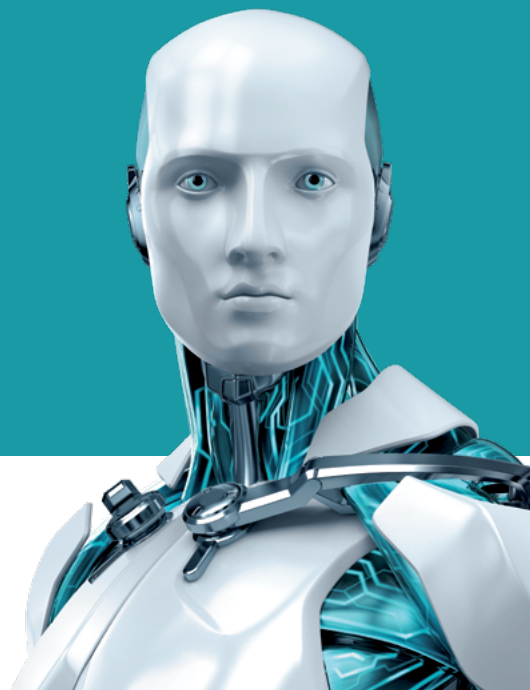
PROTECCIÓN COMPLETA PARA UN HOGAR INTELIGENTE

Autor:
Tony Anscombe

Investigadores:
Juraj Bartko, Ivan Bešina, **Miloš Čermák,**
Milan Fránik, Štefan Svorenčík, **Kacper Szurek**



ENJOY SAFER TECHNOLOGY™

CONTENIDOS

1. INTERNET DE LAS COSAS

La Internet de las cosas (Internet of Things o IoT) se ha convertido en un término muy común a nivel mundial, tanto en lo laboral como en el hogar, y en un sentido literal podría usarse para referirse a cualquier cosa que se encuentre conectada a Internet. Sin embargo, si te preguntas qué tipos de dispositivos se incluyen en la IoT, es probable que recibas distintas respuestas. La misma puede incluir desde smartphones, lamparitas inteligentes, dispositivos para monitorear la actividad física, parlantes inteligentes y lavavajillas, hasta sensores de calidad del agua en estaciones de bombeo.

En los últimos años, con el incremento de los dispositivos interconectados, muchos analistas comenzaron a hacer predicciones sobre cómo sería el futuro: 50 mil millones para 2020 fue el número que citó en una presentación en 2017 el ex CEO de Ericsson Hans Vestberg. Ocho años después, la expectativa inicial en torno al sector industrial ha disminuido y los números citados son más conservadores. En la actualidad, Ericsson ofrece una visión más matizada: estima que para 2022 se pronostican alrededor de 29 mil millones de dispositivos conectados, de los cuales alrededor de 18 mil millones estarán relacionados con la IoT.

Si bien continuará el debate sobre los números, lo cierto es que muchos de estos dispositivos serán de consumo, que pueden brindar numerosos beneficios a los hogares pero que también pueden atentar contra la privacidad y la seguridad de los usuarios. Los sensores integrados a los productos del hogar inteligente, con sus micrófonos, cámaras, interfaces con GPS, y ni hablar de la interoperabilidad, son objetivos muy atractivos para los ataques de malware. Al obtener el control de estos dispositivos, los ciberdelincuentes no solo pueden atacar otros dispositivos en la red de un usuario, sino también espiar y recopilar datos confidenciales y personales.

Un equipo de especialistas de ESET ha analizado algunos de estos populares dispositivos de la IoT, como cámaras, balanzas, sensores y sistemas de

administración del hogar. Este informe técnico detalla la investigación que llevaron a cabo y analiza específicamente los problemas de privacidad que surgen al crear un hogar inteligente básico. Por supuesto, aquí mencionamos los problemas evidentes que encontraron en dispositivos específicos.

Como no existe una definición ampliamente aceptada de lo que constituye un "hogar inteligente", para la elaboración de este documento oficial decidimos centrar nuestra atención sólo en los dispositivos de la IoT que aparentan estar destinados principalmente al mercado de consumo.

Podría decirse que una casa verdaderamente inteligente requeriría una remodelación importante y un gran compromiso financiero inicial para crear un entorno intuitivo y automático que anticipe y se adapte al estilo de vida cambiante de los ocupantes en tiempo real. La atracción para los consumidores es ahorrar energía y gastos a largo plazo a la vez que aumentan la comodidad y la conveniencia.

En la actualidad, esta situación está fuera del alcance de muchos, por lo que un hogar inteligente para la mayoría de nosotros será una pequeña incursión en el mundo de la IoT, con un número limitado de dispositivos bien ubicados que añaden conveniencia, comodidad o innovación. Uno de los desafíos que enfrenta incluso la implementación más básica de una casa inteligente, es la interoperabilidad entre dispositivos de diferentes fabricantes para proporcionar una experiencia armoniosa y unificada.

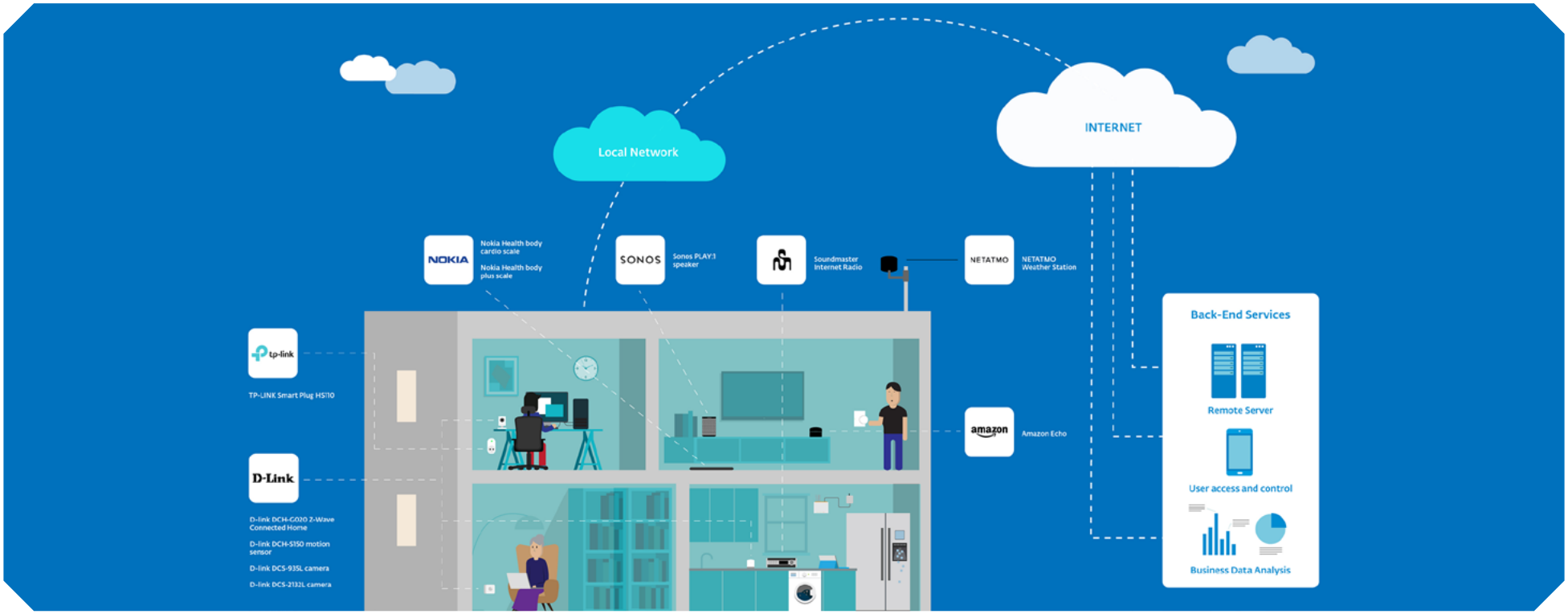
Cada dispositivo proporciona un conjunto de características diseñadas para mantenernos informados sobre nuestras actividades o permitirnos realizar ciertas acciones. Las personas tienen (o deberían tener) inquietudes sobre los riesgos que surgen de la posibilidad de compartir datos de manera inadvertida o inapropiada acerca de sus hábitos o su estilo de vida. Hoy en día, el gran volumen de datos compartidos justifica plenamente estas preocupaciones.

Recientemente, Nathan Ruser, un joven universitario australiano que estudia seguridad internacional en la Universidad Nacional de Australia, destacó el riesgo que presenta un dispositivo en particular. En un tweet el 27 de enero de 2018, Ruser señaló un problema de seguridad operativa para el personal militar que usaba una app de entrenamiento físico de Strava. La aplicación utiliza la ubicación GPS de teléfonos celulares para rastrear rutas para trotar, andar en bicicleta o realizar otras actividades de acondicionamiento físico. De forma predeterminada, los usuarios permiten el intercambio anónimo de sus datos para que Strava pueda generar un mapa de calor que muestre las rutas más populares. El ejemplo destacado por Ruser fue la Base Aérea de Bagram en Afganistán, que muestra las rutas regulares de trote utilizadas por el personal militar de los Estados Unidos allí destinado. Éste es un buen ejemplo de una aplicación popular que recopila datos y los acumula para generar resultados útiles y divertidos, pero en este caso plantea problemas obvios de seguridad. Intentar encontrar una ruta para trotar cuando uno está lejos de casa ahora es simple, pero las consecuencias para la seguridad y la privacidad no son evidentes de inmediato.

2. HOGAR INTELIGENTE

Cada "cosa" en el término "Internet de las cosas" se refiere a un dispositivo, y hay muchos tipos de dispositivos que se pueden conectar, desde cámaras, balanzas, sensores y sistemas de administración del hogar, hasta implantes de monitoreo cardíaco o automóviles o sensores de monitoreo para el ganado. Las oportunidades de interconexión son ilimitadas. Por ejemplo, San José, California, se ha comprometido a crear una ciudad inteligente que, según afirman, ofrecerá un entorno más seguro, inclusivo y fácil de usar para sus residentes. El proyecto promete usar una plataforma de la IoT que combina los vehículos con una infraestructura de tecnologías de sensores inteligentes para mejorar la seguridad, la movilidad y la optimización del sistema de tránsito.

Los escritores de ciencia ficción alguna vez imaginaron un mundo regulado



por dispositivos interconectados utilizados en la vida cotidiana. Hoy, ese mundo se está convirtiendo rápidamente en una realidad y un claro ejemplo podría ser una cámara de seguridad que comienza a grabar cuando se activa un sensor de movimiento y envía una alerta a tu teléfono. En términos simples, los elementos que componen este escenario de interconectividad son: el dispositivo, la red a la que se encuentra conectado, el dispositivo que lo controla o interactúa con él (probablemente un smartphone) y por último el servicio en la nube que almacena los datos o actúa como canal para entregar los datos al teléfono. Potencialmente, se podría implementar un componente más: un sistema de administración hogareña que incluya un dispositivo principal o concentrador y que tiene como objetivo proporcionar una interfaz única integrada para administrar todos los dispositivos conectados que brindan servicios en el hogar.

Existen varios escenarios principales para controlar y comunicarse con los dispositivos, y como consumidores estamos familiarizados con al menos dos de ellos: Bluetooth y Wi-Fi. Si, por ejemplo, hay un dispositivo que sólo necesita ser controlado localmente por un smartphone, entonces se podría usar una tecnología inalámbrica de corto alcance como Bluetooth o Wi-Fi. En los sistemas de automatización del hogar donde se usa un concentrador, es común encontrar uno o más de los protocolos de comunicación Z-Wave, BidCoS y ZigBee, que proporcionan una transferencia de datos de baja latencia y tienen un menor consumo de energía que el Wi-Fi. El concentrador se conecta a través de Wi-Fi o Ethernet por cable, lo que permite la conexión desde dispositivos remotos o servicios en la nube.

3. POLÍTICA DE PRIVACIDAD Y RECOPILACIÓN DE DATOS

Cada fabricante debe tener una política de privacidad o un documento similar que explique cómo se recopilan y utilizan los datos por un dispositivo, o a través de sus servicios asociados. A veces las políticas son imprecisas y difíciles de entender y, en algunos casos, hasta difíciles de encontrar, mientras que otras demuestran un esfuerzo excepcional por parte de la empresa para que sean lo más comprensibles y legibles posible.

Las empresas también tienden a hacer que las políticas de privacidad abarquen una gama más amplia de eventualidades de las que pueden ocurrir en la realidad, por lo que es posible que no recopilen todos los datos que se establecen en la política. Las políticas son documentos complejos que requieren considerables recursos legales para escribirse, modificarse y mantenerse, de modo que suelen enumerar todo lo que el sistema pueda llegar a recopilar para garantizar su vigencia en el futuro. Por supuesto, esto significa que si usted acepta la política hoy, la empresa podría llegar a recopilar esos datos adicionales el día de mañana.

Aquí no cuestionaremos los motivos u otros aspectos de la recopilación de datos; nuestro objetivo es tomar una visión holística de los datos que se recopilan en general para proporcionar servicios en una casa inteligente básica. Al observar la cantidad y el detalle de los datos recopilados, surge la preocupación de que un individuo pueda estar compartiendo de más sin saberlo.

La mayoría de los dispositivos y servicios recopilarán datos personales básicos que pueden incluir el nombre, la dirección, la fecha de nacimiento, el correo electrónico y el número de teléfono. Los datos que cada dispositivo puede recopilar figuran en la política de privacidad correspondiente publicada por la empresa en cuestión. A menudo, las empresas usan el término "pero sin limitarse a", lo que significa que, si lo desean, pueden recopilar más de lo que se describe en la lista.

Cuando los dispositivos son controlados por un servicio diferente al ofrecido por los fabricantes que los crearon, los datos también pueden ser recopilados por el proveedor de servicios de terceros. Por ejemplo, los productos D Link que usan el servicio en la nube también pueden ser controlados por Alexa de Amazon. Un comando simple como "Alexa, dile a mydlink que encienda la cámara del garage" significa que tanto mydlink como Amazon conocen no sólo las instrucciones, sino también el dispositivo y la forma en que se usa. Las consecuencias de todos los comandos enviados a diferentes dispositivos desde diferentes fabricantes y que fluyen a través de un solo proveedor de servicios pueden ser más convenientes para el usuario final, pero algunos lo ven como una entidad capaz de construir un perfil completo del estilo de vida de los ocupantes del hogar.

4. DISPOSITIVOS VULNERABLES

¿Encontramos vulnerabilidades? Sí.

Como empresa de seguridad informática, nos interesaba brindar un panorama sobre los niveles de seguridad que poseen ciertas aplicaciones y dispositivos, y por ello elegimos y evaluamos 12 productos de 8 proveedores y en el presente documento presentamos 11 de ellos. Uno de los productos mostró vulnerabilidades significativas, y como valoramos el compromiso con la divulgación responsable y la naturaleza colaborativa de la industria de seguridad de TI, decidimos no compartir la información y suministrar a la empresa en cuestión detalles de las vulnerabilidades detectadas en su dispositivo. Se trata de un panel de control de automatización del hogar capaz de administrar sensores de movimiento, controles de calefacción, motores de persianas, sensores de ambiente y enchufes inteligentes. El dispositivo tiene una serie de vulnerabilidades, entre las que se incluyen:

- *El proceso de inicio de sesión desde la red local no está completamente autenticado. La opción predeterminada es permitir el inicio de sesión automático, lo que evita la necesidad de usar credenciales estándar como ID de usuario y contraseña. El fabricante menciona este problema en una alerta de seguridad y recomienda deshabilitar la opción predeterminada.*
- *Como ocurre con casi todos los sistemas de hogares inteligentes, un servicio en la nube brinda la funcionalidad para administrar los dispositivos conectados desde un solo lugar. Pero en este caso, las comunicaciones enviadas al servicio en la nube no están cifradas.*
- *El servicio en la nube del fabricante tiene la capacidad de establecer una conexión de red privada virtual (VPN) con los dispositivos remotos. Una vez que se establece este túnel, podría ser posible cambiar la configuración de la red remota. Esto podría otorgarle acceso a la red local a usuarios no autorizados.*
- *El acceso al servicio en la nube requiere el registro del usuario, pero si los detalles del usuario fueron comprometidos, el acceso de la VPN a la red remota podría presentar un riesgo considerable.*

Los dispositivos restantes que probamos y detallamos en este documento demuestran que es necesario investigarlos antes de tomar la decisión de compra. Por ejemplo, las cámaras D-Link y el enchufe inteligente TP-link Smart Plug tienen problemas de seguridad bien documentados. La principal preocupación respecto a las cámaras es la falta de cifrado en la transmisión de video, en este caso, tienen una débil autenticación.

Hay cámaras disponibles que son seguras y cifran la transmisión de video, tanto en tiempo real como cuando se almacenan. Los dispositivos que probamos pertenecían a una marca reconocida, lo que sugiere que la "marca registrada" no necesariamente significa seguridad, al menos cuando se trata de cámaras.

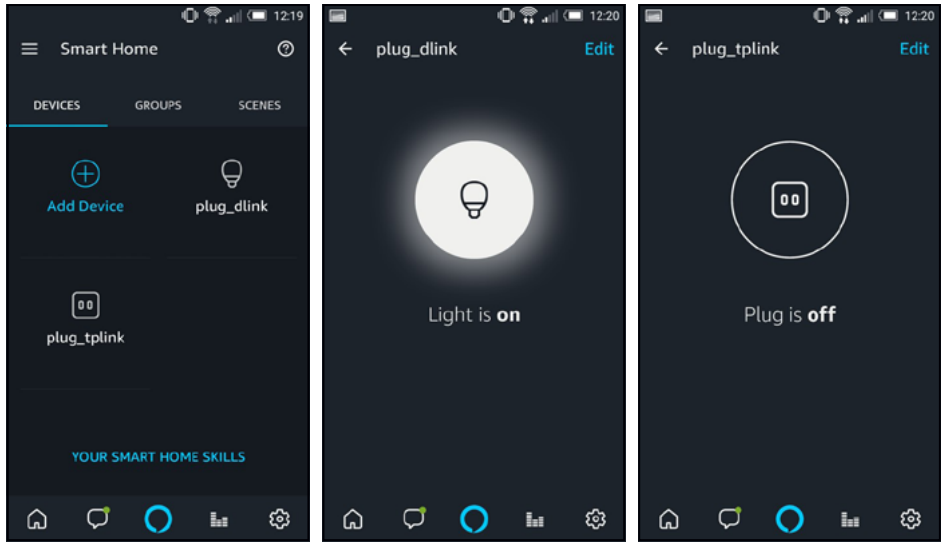
5. PRIVACIDAD, UNA ENORME PREOCUPACIÓN

¿A la gente le preocupa la privacidad? Sí.

Cada dispositivo de la prueba recopiló datos diferentes para facilitar su funcionalidad y en la mayoría de los casos los datos parecían ser acordes al servicio que se brindaba. El Soundmaster Internet Radio, sin una política de privacidad obvia ni términos significativos, activó una alerta roja para nuestros investigadores. Si no hay una política establecida, entonces no se puede tomar una decisión objetiva.

Las preocupaciones más importantes son planteadas por los asistentes inteligentes activados por voz, en este caso Alexa. Un servicio que actúa como canal para todos los demás dispositivos y luego almacena todas

las interacciones, potencialmente está creando un cofre del tesoro para un cibercriminal. No se está cuestionando la reputación del dispositivo ni los servicios de Amazon; no obstante, un hacker inteligente que intente recopilar datos personales para el robo de identidad podría crear un ataque de suplantación de identidad y obtener acceso a las cuentas de Amazon del cliente.



Las imágenes de arriba son ejemplos de la funcionalidad Smart Home de la app Alexa.

Con Alexa, ¿uno puede estar seguro? Posiblemente.

Si decides utilizar este asistente inteligente, configura tus parámetros de seguridad.

- *Configura la solicitud de un PIN cuando realices compras por voz o, mejor aún, evita comprar a través de la voz.*
- *Entrena a Alexa para reconocer tu voz y limita la funcionalidad sólo a tus instrucciones reconocidas.*
- *Cuando no necesites usar el asistente, apágalo o silencia el micrófono.*

6. EVALUACIONES DE ESET EN DISPOSITIVOS INTELIGENTES

a. Amazon

Amazon Echo (2nd Gen)

Amazon Echo es un asistente virtual de manos libres y activado por voz que utiliza el servicio Alexa de Amazon para procesar los comandos del usuario, como reproducir música, configurar alarmas o controlar los dispositivos domésticos inteligentes que sean compatibles con Alexa.

Sus siete micrófonos y su tecnología de cancelación de ruidos garantizan que Alexa podrá escuchar sus comandos dentro de una habitación, incluso mientras está reproduciendo música.

Con audio omnidireccional de 360°, es capaz de reproducir música envolvente en toda la habitación, combinada con el procesamiento Dolby y la respuesta de base dinámica.

Cada vez más fabricantes están incorporando la compatibilidad para Alexa a través de "habilidades" que le otorgan el control de otros dispositivos y servicios, permitiéndole así administrar el hogar inteligente desde un único dispositivo controlado por voz.

Términos de uso de Alexa

https://www.amazon.com/gp/help/customer/display.html?nodeId=201809740

Los productos compatibles con Alexa recopilan y envían a Amazon la siguiente información:

Sus interacciones con Alexa
Las entradas de voz
Listas de reproducción de música
Sus listas de tareas y de compras a través de Alexa.

Tus productos habilitados para Alexa:

Tipo de dispositivo
Nombre
Funcionalidades
Estado
Conectividad de red
Ubicación

Amazon puede actualizar automáticamente el firmware de ciertos productos auxiliares en nombre del fabricante correspondiente.

Nota: Esto no incluye detalles de la política de privacidad general de Amazon, sólo los detalles del servicio de Alexa.

Seguridad y privacidad

Si posee un Amazon Echo, entonces probablemente su mejor amigo sea Alexa, un dispositivo al que le puede hacer un número ilimitado de preguntas, así como darle instrucciones y recibir respuestas educadas y rápidas. Si piensas en una casa inteligente, este es un dispositivo casi imprescindible. El mismo puede realizar una amplia gama de servicios tanto directamente como a través de conexiones de terceros que haya aprobado, por ejemplo, reproducir música, leer noticias, consultar su calendario, armar su lista de tareas y, por supuesto, comprar cosas a través de su cuenta de Amazon.

Echo está constantemente escuchando sus comandos y es controlado por su voz; permanece inactivo hasta que reconoce la "palabra de activación". Esta palabra activa a Alexa y le permite darle un comando directo o uno vinculado a una habilidad, explicado en el siguiente párrafo. La instrucción se transmite a Amazon para su análisis y se genera una respuesta. Estas interacciones están asociadas a su cuenta de Amazon y luego las puede revisar.

Si la interacción está relacionada con un tercero, por ejemplo, le está preguntando a la app Health Mate de Nokia cuánto pesa, Nokia no recibe la solicitud de audio, sino la solicitud de su peso. Para que esta interacción sea posible, es necesario conectar la cuenta de terceros a Alexa para que la información esté disponible. Esto se conoce como una "habilidad de Alex".

Las interacciones de audio se almacenan en tu cuenta de Amazon y se asocian a ella. Puedes eliminarlas individualmente en la aplicación Alexa o en bloques a través del sitio Web de Amazon. ¿Los usuarios suelen tomarse el tiempo para revisar lo que se está almacenando y eliminar todo lo que se considere personal? Probablemente no.

Los datos podrían ser esclarecedores para un comerciante. Tus interacciones le habrán informado a Amazon qué productos te gustaría comprar y de quién, qué música escuchas, qué otros productos conectados tienes, etc. Esta recopilación de datos permite construir un perfil con detalles muy específicos sobre tu estilo de vida: el sueño de un especialista en marketing y potencialmente también de un ciberdelincuente. Es importante que enfaticemos una vez más que tu eres quien tiene el control y que aquí no hay nada oculto, ya que puedes ver las interacciones y eliminarlas cuando desees. Además, si te preocupa demasiado tu privacidad, siempre puedes desactivar Alexa, ya sea por completo o simplemente silenciando el micrófono.

Con las noticias tan frecuentes de filtraciones de datos, cualquier asistente digital activado por voz podría ser motivo de preocupación. Si, por ejemplo, alguien obtiene acceso a tu usuario y contraseña de la cuenta de Amazon, podrá escuchar tus interacciones con Alexa. La profundidad de la información

almacenada en las interacciones podría causar vergüenza y ser un problema de privacidad.

Pero hay precauciones que usted puede tomar.

- *Configura el reconocimiento de voz para que sólo tu puedas usar Alexa, lo que impedirá que los visitantes de tu casa se diviertan con él.*
- *Elimina las grabaciones de interacciones pasadas.*
- *Considera no conectar otros dispositivos si crees que los datos son demasiado personales.*
- *Apaga Alexa cuando no lo necesites.*
- *Protege tu cuenta de Amazon con autenticación en dos fases. Esto impedirá el acceso en caso de que tus datos de inicio de sesión caigan involuntariamente en manos equivocadas.*

b. D-Link

Dispositivos

D-Link DCH-G020 Connected Home

El DCH-G020 es un concentrador para hogares conectados que funciona como un canal central para conectar todos sus dispositivos mydlink Wi-Fi y Z-Wave. Si se usa en combinación con sensores domésticos, puede alertarlo cuando se abren puertas o ventanas o cuando detecta movimiento. Con el servicio en la nube mydlink Home, simplifica la configuración de una casa inteligente sin la necesidad de suscripciones ni cargos adicionale.

D-Link DCH-S150 Motion Sensor

El sensor DCH-S150 detecta movimiento y puede vincularse con otros dispositivos para realizar acciones predefinidas; por ejemplo, si se combina con una cámara, puede capturar un video, o si se combina con un Smart Plug, puede encender las luces. Las notificaciones y alertas se pueden enviar a dispositivos móviles o por correo electrónico.

D-Link DCS-935L Camera

El dispositivo DCS-935L es una cámara conectada capaz de capturar imágenes claras y nítidas. Cuenta con calidad de video HD de 720p, visión nocturna de hasta casi 5 metros, y tecnología de detección de sonido y movimiento. Las notificaciones y alertas se pueden enviar a dispositivos móviles o por correo electrónico. La visualización remota es gratuita a través de navegadores Web y dispositivos móviles cuando se ve a través del servicio en la nube de D Link, llamado mydlink.

D-Link DCS-2132L Camera

La cámara DCS-2132L proporciona la capacidad de transmitir directamente imágenes de video de alta calidad para fines de seguridad y vigilancia, u otros. Aloja su propio servidor Web y tiene una CPU integrada, lo que significa que se puede acceder desde cualquier navegador Web a través de Internet. El dispositivo integrado tiene infrarrojo para video nocturno, detección de movimiento, un micrófono y un altavoz.

"mydlink" es un servicio en la nube que proporciona las capacidades de configuración, control y monitoreo de todos sus dispositivos D Link compatibles. Al acceder a través de apps de dispositivos móviles o de un navegador Web, te proporciona una central única desde donde puedes ver las cámaras o el estado de la red del hogar inteligente.

Política de privacidad

https://www.mydlink.com/privacyPolicy

Cada producto mydlink recopilará algunos o todos de los siguientes datos:

Voz
Sonido

Rostro
Temperatura
Luz ambiente
Vapor de agua en el aire
Niveles de CO_2
Precipitación
Humedad en el aire
Decibelios de ruido
Movimiento captado por los sensores
Datos de uso de las utilidades
Configuración de la app
Planificación
Alertas
Notificaciones
Ubicación del producto dentro de las instalaciones
SSID (nombre de Wi-Fi)
Contraseña de Wi-Fi
Señales de audio y video

Amazon Echo Habilitado

Sí

Seguridad y privacidad

La comunicación desde un dispositivo móvil al servicio en la nube mydlink está cifrada, al igual que la conexión entre el dispositivo y los servidores D Link.

Sin embargo, las actualizaciones de firmware son entregadas por HTTP en lugar de HTTPS, lo que significa que un atacante podría inyectar malware en la actualización, ya que la secuencia de datos no está cifrada. Nuestro intento de tomar el control o cambiar la operación del dispositivo mediante la creación de una actualización modificada provocó que fallara la instalación. Esto prueba que se realizan verificaciones en el paquete de actualización a pesar del hecho de que los datos entregados no están cifrados. Curiosamente, cambiar sólo unos pocos bytes sin importancia no impidió que la actualización se llevara a cabo.

Las cámaras incluidas en la prueba de hogar inteligente de ESET tienen puntos débiles, algunos de los cuales han sido documentados en otras pruebas. Por ejemplo, AV Test en Alemania probó el dispositivo D Link DCS-2132L y le otorgó sólo una estrella de cinco, ya que detectó una serie de importantes problemas de seguridad. Un año después, todavía siguen los problemas, como la autenticación HTTP que es básica, y el cifrado del flujo de video que sigue siendo insuficiente y reversible, así como accesible a través de una dirección IP pública. Sin embargo, la cámara se controla desde la app mydlink, que está cifrada. Pero si la transmisión de video en sí está poco protegida, entonces las preocupaciones de seguridad y privacidad se centran en el contenido capturado. Si se utiliza una cámara para controlar la actividad de los surfistas en una playa, podría argumentarse que revertir el cifrado para ver cuán grande es la ola sería una pérdida de tiempo y esfuerzo. Sin embargo, una cámara colocada dentro del hogar tendría implicaciones de seguridad y privacidad muy diferentes.

Es decepcionante que después de un examen exhaustivo realizado por AV Test en enero de 2017, los problemas continúen siendo los mismos 12 meses después.

c. NETAMTO

NETAMTO Weather Station

La estación meteorológica NETATMO tiene dos módulos: un módulo para exterior que proporciona acceso en tiempo real a las condiciones climáticas, y un módulo para interior que supervisa las condiciones en interiores, como

la calidad del aire. A través de una red colectiva de dispositivos NETATMO, puede ver las variaciones de las condiciones climáticas locales y en otras ubicaciones.

Política de privacidad

https://www.netatmo.com/en-US/site/terms

La política de privacidad de NETATMO no es tan detallada como algunas de las otras. La redacción es generalizada y sólo menciona categorías de datos en lugar de ejemplos específicos de los datos reales que se recopilan. Esto significa que los usuarios pueden desconocer la realidad de lo que se está recopilando, almacenando o compartiendo. Sin embargo, al comprar una estación meteorológica NETATMO, una de las principales propuestas de compra es el Mapa Meteorológico (consulte el vínculo y la descripción a continuación).

Cuando utiliza los servicios, se recopilan los siguientes datos en forma automatizada:

> Datos personales y mediciones
> Uso
> Su actividad con los servicios
> Dirección de IP

NETATMO comparte datos personales anonimizados agregados con terceros

Amazon Echo Habilitado

Sí

Seguridad y privacidad

NETATMO te proporciona un Mapa Meteorológico para que puedas ver el estado del tiempo en cualquier ubicación donde haya un dispositivo instalado que comparta sus hallazgos. Si eliges participar en el Mapa Meteorológico, se compartirán los datos de tu sensor para exterior. Los datos del sensor para interior permanecen privados. Si eliges no compartir, solo verá su dispositivo en el mapa.

Si decides compartir los datos de tu dispositivo, entonces la ubicación es específica. Ingresa al vínculo del Mapa Meteorológico más arriba y selecciona uno de los dispositivos. Se muestra la dirección de la calle en los detalles a la derecha. Lo único que falta es el número de la casa. De todas formas, si abres un mapa de Google en otra ventana del navegador y compara las direcciones podría llegar a determinar la dirección real.

¿Compartir tu dirección es motivo de preocupación? Sí. ¿Alguna vez recibiste una llamada diciendo que se ha identificado un problema con tu equipo portátil o su sistema operativo Windows? Si es así, se trata de una de las muchas estafas de soporte técnico diseñadas para cobrarle por un servicio que usted no necesita. Imagina que la llamada es un poco más específica y, en vez de intentar adivinar si tienes o no una computadora portátil con Windows, la persona que llama hace preguntas específicas sobre tu estación meteorológica. Este conocimiento validado sobre los dispositivos exactos que están instalados en tu casa puede hacer que sea mucho más difícil detectar una llamada fraudulenta.

NETATMO tuvo problemas en 2015 por la filtración de sus credenciales de Wi-Fi de texto plano. Resolvieron estos problemas mediante una actualización del firmware. Una vez conectado, el dispositivo descarga automáticamente la última versión de firmware desde la nube. Si bien no se entrega a través de SSL, se codifica utilizando un método patentado.

d. Nokia Health

Dispositivos

Nokia Health Body+ Scale

El Nokia Health Body+ Scale es mucho más que una balanza de baño. Proporciona información adicional con precisión, como el índice de masa corporal, la grasa corporal, el porcentaje de agua, la masa muscular y la masa ósea. Con la app Health Mate, puedes hacer un seguimiento de tu progreso y recibir consejos de entrenamiento que te ayudarán a alcanzar tus objetivos.

Nokia Health Body Cardio Scale

El dispositivo Nokia Health Body Cardio Scale añade la funcionalidad de salud cardíaca al Nokia Health Body+ Scale y permite realizar un seguimiento de tu salud cardiovascular a través de un monitor de frecuencia cardíaca.

Política de privacidad

https://health.nokia.com/us/en/legal/privacy-policy

Cuando usa productos y servicios de salud digital de Nokia, la política de privacidad establece que Nokia puede necesitar recopilar los siguientes datos:

Datos de identidad

- Dirección de IP
- Imágenes y videos

Datos de la actividad

- Cantidad de pasos
- Distancia recorrida
- Cantidad de patadas en natación
- Cantidad de calorías quemadas
- Tipo de actividad
- Nivel de actividad
- Duración de la sesión deportiva

Datos de medidas corporales

- Peso
- Musculatura
- Grasa corporal
- Salud
- Frecuencia respiratoria
- Presión sanguínea

Datos ambientales

- Nivel de ruido
- Nivel de luz
- Nivel de temperatura
- Concentración de CO_2

Datos de posicionamiento y ubicación

Amazon Echo Habilitados

Sí

Seguridad y privacidad

La privacidad de los datos relacionados con la salud es fundamental. La política de privacidad de Nokia establece:

Algunos servicios pueden permitirte compartir tus datos personales con otros usuarios del servicio o con otros servicios y sus usuarios. Antes de divulgar cualquier dato personal u otra información que pueda ser accesible para otros usuarios, considéralo cuidadosamente.

Cuando nos fijamos en la naturaleza personal de los datos recopilados, compartirlos puede parecer inapropiado: sin embargo, es cierto que una

persona que está intentando bajar de peso puede motivarse más si comparte información sobre la cantidad de pasos caminados o el peso perdido. En general, una vez que se comparten los datos, incluso con otros miembros de la familia o amigos, hay que considerar que son públicos, ya que le ha pasado el control a otra persona.

El equipo de investigación de ESET analizó más detenidamente el dispositivo debido al tipo de datos recopilados, y el comentario real del equipo fue "la seguridad de este dispositivo es relativamente buena". Nos propusimos intentar acceder a los datos que fluyen entre la balanza o la app Health Mate y el servicio en la nube con el que se comunican y el servicio en la nube asociado.

Logramos lanzar un ataque Man-in-the-Middle (MitM) entre la app de Android y la nube, pero para lograrlo, fue necesario rootear el dispositivo Android e instalar un certificado raíz para MitM. Como la balanza se comunica con el dispositivo Android y las actualizaciones de firmware se entregan a través de la app, el ataque MitM nos permitió interceptar las actualizaciones de firmware. La descarga se cifra con SSL, y luego fluye a través del dispositivo Android hasta la balanza. Se pueden hacer modificaciones del firmware y luego grabarla en la balanza a través de la conexión Bluetooth, pero para hacerlo es necesario presionar un botón de modo de configuración en la misma balanza, lo que significa que la persona tiene que estar presente físicamente, de modo que un ataque remoto no es factible.

La modificación del firmware para bajar el nivel de seguridad de las comunicaciones con la balanza desde HTTPS a HTTP fue exitosa. Los datos que se transmitieron de esta forma fueron legibles. Sin embargo, incluso así, los datos y parámetros que se transmitieron no se pudieron determinar fácilmente.

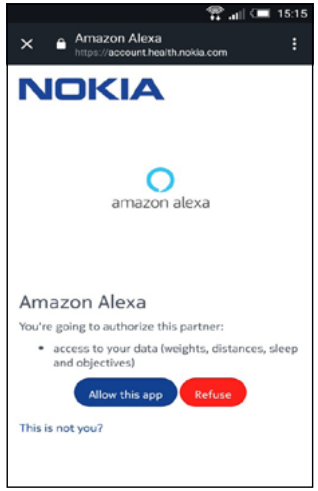
En resumen, es muy poco probable encontrar un escenario donde un hacker pueda acceder al teléfono, rootear el dispositivo, interceptar la descarga del firmware, reescribirlo, luego presionar el botón de configuración de la balanza e instalar el nuevo firmware. Y si lo hiciera, la información que recopilaría no tendría sentido sin una extensa ingeniería inversa.

Otra característica curiosa de la balanza es su pronosticador del tiempo. Si la balanza conoce tu ubicación, que toma de tu teléfono, entonces podrá ver el pronóstico local en la pantalla de la balanza mientras te estás pesando. Queda por ver si se trata de un riesgo para la seguridad o la privacidad, pero compartir tu ubicación con una balanza parece algo innecesario.

El mayor riesgo con las balanzas es que los usuarios compartan más datos de los necesarios a través de redes sociales o que un tercero tenga acceso a información personal confidencial. El tercero en el que nos centramos en este documento es Amazon Echo. Al vincular Nokia Scale con Amazon Echo, puede formularle preguntas a Alexa sobre los datos almacenados en su cuenta de Health Mate. En la página Web de Amazon donde se detalla la activación de la habilidad para Nokia y las ofertas, aparece la siguiente declaración:

https://www.amazon.com/Nokia-Apps-Distribution-LLC-Health/dp/B0786NLDBF

Nota: Alexa y Amazon, Inc. no almacenan ni conservan tus datos de Nokia Health, pero las interacciones de voz asociadas con tu cuenta de Amazon pueden contener tus datos de Nokia Health Mate.



Cuando se vincula a Alexa y otorga permiso a Amazon para acceder a tu cuenta de Nokia Health Mate, se muestra la pantalla de arriba. Ten en cuenta que se menciona específicamente que estás otorgando a Amazon Alexa acceso a datos personales, incluidos el peso, la distancia, el sueño y sus objetivos.

Al preguntarle a Alexa su peso, la declaración de política de privacidad debería asegurarte que Amazon no está almacenando los datos de tu cuenta de Nokia Health Mate. Sin embargo, los está almacenando en forma de interacciones de voz asociadas con tu cuenta de Amazon. Recuerda: si accede a tus interacciones de voz en la aplicación Alexa, podrás ver todas las interacciones en forma escrita y podrás volver a reproducir el audio original. No obstante, tu eres quien tiene el control: puedes eliminar estas interacciones y, opcionalmente, puedes revisar la precisión de tus interacciones con Alexa.

El problema de volver a poner el control en manos del usuario para eliminar estas interacciones es que muchos no sabrán que están almacenadas, e incluso si lo saben, la tarea de eliminarlos suele ser demasiado ardua e infrecuente.

e. Sonos

Sonos PLAY:1 Speaker

Sonos PLAY: 1 es un altavoz conectado a Wi-Fi que puede transmitir música independientemente del estado de su dispositivo móvil. No más interrupciones debido a un problema de conectividad con Bluetooth.

Combinado con un Amazon Echo o Dot, puede controlar verbalmente la melodía, la lista de reproducción o la emisora de radio que se está reproduciendo. Se pueden sincronizar varios altavoces en diferentes salas para reproducir la misma canción o cada uno puede disfrutar de una canción diferente al mismo tiempo.

Política de privacidad

https://www.sonos.com/en-us/legal/privacy

La política establece que Sonos puede recopilar:

Tipo de producto
Tipo de dispositivo controlador
Sistema operativo del controlador
Información de la versión del software
Fuente de contenido (entrada de línea de audio)
Entrada de señal (por ejemplo, Dolby)
Información sobre antenas Wi-Fi
Configuraciones de audio
Orientación del producto
Nombres de las salas que haya asignado
Ajustes usando Sonos Trueplay
Temperatura del producto
Información del Wi-Fi (intensidad de la señal)
Servicios de música a los que se conecta (para algunos servicios, inicie sesión con el nombre de usuario, pero no con la contraseña)
Con qué frecuencia utilizas la app Sonos en comparación con otros mecanismos de control
Flujo de interacciones dentro de la app Sonos
Con qué frecuencia utilizas los controles físicos de la unidad
Datos de ubicación cuando la app está en uso
Duración de uso
Duración del uso del servicio de música
Información de combinaciones de productos y salas
Información de comandos, reproducir, pausar, cambiar el volumen, saltar pistas, información sobre pistas, lista de reproducción, contenedor de la emisora de radio, lista de reproducción de Sonos, favoritos de Sonos.

Amazon Echo Habilitado

Sí

Seguridad y privacidad

Es importante tener en cuenta que este dispositivo es un altavoz que está habilitado para Wi-Fi en lugar de Bluetooth. Esto elimina la necesidad de que un dispositivo emparejado, por ejemplo un teléfono celular, tenga que estar cerca, y permite que las funciones de audio del teléfono funcionen de manera independiente.

La app Sonos, u otra que conozca la existencia del dispositivo, transmiten su deseo de reproducir audio a toda la red. Como el altavoz está en modo de escucha permanente, verá la transmisión de esta solicitud y reproducirá el audio solicitado.

Se requiere una cuenta de Sonos para trabajar con la app. El altavoz se conecta con frecuencia a los servidores de Sonos. Hay dos conexiones: una es una permanente mientras que la otra es por hora. Ambas están protegidas con cifrado. La conexión permanente no es una sorpresa, ya que el altavoz funciona con Alexa de Amazon. Pedirle a Alexa que reproduzca una pista en su altavoz Sonos requeriría una conexión entre los servidores de Sono y el altavoz para poder transmitirla.

La política de privacidad de Sonos establece que captura las interacciones con la app y los servicios de música a los que se conecta. Esto es de esperar,

ya que casi todos los servicios de música ofrecen recomendaciones sobre la música que le puede llegar a gustar.

La política también establece que se almacenan los nombres de las habitaciones que asigna al dispositivo. Esto es comprensible, ya que necesita poder especificar en qué dispositivo desea reproducir una pista, por ejemplo, "Alexa por favor toque 'Beautiful' de James Blunt en el altavoz de la cocina". Si alguien obtiene acceso a esta información, posiblemente esté compartiendo más información de la necesaria, dependiendo del nombre de las habitaciones. Por ejemplo, si tienes altavoces en las habitaciones de tus hijos, al ponerles sus nombres puede estar inadvertidamente compartiendo datos con Sonos sobre los miembros de su familia.

Ahora hay una nueva versión del altavoz disponible, el Sonos One. Esta versión combina la funcionalidad del altavoz y del Amazon Echo. El parlante de Sonos en efecto cumple la función de Amazon Echo. En este escenario, la política de privacidad de Sonos deja en claro que Sonos no retiene las interacciones con Alexa.

f. Woerlein

Soundmaster Internet Radio IR4000SW

Esta moderna radio por Internet con su atractivo diseño y una práctica manija para su transporte es el compañero perfecto para aquellos que buscan una radio que no deje nada que desear. La radio por Internet IR4000SW en color blanco también admite la recepción de bandas DAB+ y FM PLL, por lo que puede almacenar sus emisoras favoritas en memoria y, por lo tanto, acceder fácilmente a ellas. El dispositivo se conecta a Internet por Wi-Fi. Además, tiene puerto USB. [Descripción traducida de amazon.de.].

Política de privacidad

No pudimos encontrar una política de privacidad relacionada con los productos de la empresa. Existe una política de privacidad en alemán para los visitantes del sitio Web de la empresa. No obstante, los visitantes de otros idiomas no podrán entenderla, ni siquiera los de habla inglesa. Pueden comprar los productos en inglés pero no leer la política. Es cierto que existe el Traductor de Google, pero los matices pueden perderse en la traducción, lo que es extremadamente importante en documentos legales.

Amazon Echo Habilitado

No

Seguridad y privacidad

Ante la falta de una política de privacidad, debemos confiar en nuestra investigación para comprender qué comunicación se está llevando a cabo entre el dispositivo e Internet. En primer lugar, al configurar el dispositivo para que se conecte a la red Wi-Fi, la contraseña no se oculta mientras se

escribe, por lo que cualquier persona que esté cerca podría ver la contraseña en texto sin cifrar. Si alguien accediera al dispositivo físicamente, por ejemplo, en un lugar público, como una oficina o un negocio, podrá acceder a las credenciales de Wi-Fi haciendo clic en las configuraciones. Si una empresa desarrolla sus productos teniendo en cuenta la seguridad desde el diseño como requisito previo, entonces es poco probable que se la contraseña se muestre en texto sin cifrar o que se pueda acceder a ella sin autenticación.

Al seleccionar una emisora de radio, se envía una instrucción en texto sin cifrar a mediayou.net, que parece ser un portal para acceder al contenido de radio online. mediayou.net conocerá la dirección IP de la radio que se conecta a ella, la emisora de radio solicitada, así como el tiempo y la duración de la escucha.

Tampoco hay ninguna política de privacidad en el sitio Web de mediayou.net. Incluso cuando se creó la cuenta en el sitio, no se ofreció ninguna política de privacidad ni términos de uso. Investigar el dominio mediayou.net para establecer quién lo posee es inútil, ya que los detalles del dominio están ocultos detrás de un escudo de privacidad, lo cual resulta un tanto irónico.

Al no conocer qué datos (si los hay) puede llegar a recopilar y conservar el sistema, entonces uno debe suponer el peor de los casos: es decir, que la empresa recopilará todo lo que pueda y se lo venderá a quien sea y de la forma que quiera. En una época en que los datos personales tienen valor y el robo de identidad es un problema creciente, ésta es una situación inaceptable.

g. TP-Link

TP Link Smart Plug HS110

El TP Link Smart Plug le permite conectar un dispositivo estándar no inteligente y controlarlo directamente desde su smartphone. Encender en forma remota un ventilador, las luces o hervir una pava de agua sin tener que reemplazar los dispositivos viejos por nuevos dispositivos inteligentes y conectados es una forma económica de comenzar un hogar inteligente.

Política de privacidad

http://www.tp-link.com/us/privacy

Versión de firmware
Dirección IP
Dirección MAC
Otra información de identificación, como nombres e imágenes que lo asocien con los usuarios de la cuenta
Su ubicación
Dispositivos
Escenas
Detalle de configuración del dispositivo
Información demográfica
Detalles de la cuenta de terceros
Programaciones
Grabaciones de audio y video
Uso del dispositivo por terceros, como cuando un sensor de movimiento detecta movimiento
Nombre del dispositivo, nombre del grupo, nombre de la ubicación (que puede configurar el usuario)
Dirección IP
Ubicación

Información del dispositivo móvil

Amazon Echo Habilitado

Sí

Seguridad y privacidad

Cuando nos propusimos crear nuestra casa inteligente básica, seleccionamos los dispositivos según el precio, la disponibilidad y la popularidad. Tomar un dispositivo que no esté conectado o no sea "inteligente" y controlarlo a través de su fuente de alimentación es bastante rentable y conveniente. Por ejemplo, es posible que desees hervir una pava de agua sin tener que ir hasta la cocina a prenderla. Entonces, antes de irte a la cama, dejas el botón de la pava encendido, y cuando te despiertas, lo único que tienes que hacer es activar el enchufe inteligente de manera remota o a través de un servicio de activación de voz como Amazon Alexa.

Este dispositivo tiene vulnerabilidades bien documentadas que incluyen un cifrado fácilmente reversible entre el dispositivo y la app Kasa de TP Link utilizada para controlarlo, problemas de validación de certificados y posibles ataques Man-in-the-Middle.

El 5 de enero de 2018, TP Link publicó una declaración de vulnerabilidad donde detallaba algunos problemas con WPA2 Security debido al exploit KRACK. Sin embargo, KRACK constituye un problema para toda la industria y los dos investigadores que detectaron la falla divulgaron los detalles en octubre de 2017. En la declaración de TP Link, el enchufe inteligente HS110 figura como corregido siempre y cuando el usuario esté usando el firmware correcto, que se distribuye mediante la app Kasa.

Al buscar las "vulnerabilidades de tp link hs110" online, encontramos más de 2600 resultados. El contenido de la página de resultados debería ser una advertencia para cualquier comprador potencial. Entre los primeros resultados, si ignoramos el problema con el exploit KRACK mencionado anteriormente, encontramos términos como "Ingeniería inversa de TP Link HS110", "Autenticación débil de TP LINK HS110" y "Cómo hackear dispositivos que usan TP Link"...'.

Comprar un enchufe económico en un intento de reutilizar un dispositivo que, de lo contrario, no se podría conectar a Internet como parte de un hogar inteligente puede parecer una solución muy rentable, pero, como puede ver en este caso, no siempre está libre de problemas.

7. CONCLUSIÓN – ¿ES SEGURO?

¿Es seguro tener un hogar inteligente? Posiblemente.

En sus inicios, el objetivo de este proyecto era crear una casa inteligente que imitara lo que podría ser un hogar "típico". La preocupación principal de nuestro equipo de investigación era: "¿Qué pasa si no encontramos ningún problema?" ¡Qué gran avance sería para la IoT si realmente no hubiéramos encontrado motivo de preocupación, y nuestra recomendación para todos los que sientan la necesidad de comenzar a construir esa casa inteligente fuera "siga adelante"! Lamentablemente, este no es el caso, y de hecho, la conclusión que estoy escribiendo ahora difiere mucho de lo que había imaginado al principio

Ningún dispositivo o software está exento de tener vulnerabilidades potenciales. Sin embargo, podemos juzgar a las empresas en función de cómo reaccionan ante la divulgación de una falla en sus productos. Algunos de los dispositivos probados tenían vulnerabilidades que se han solucionado rápidamente con nuevo software y firmware. Si dichas divulgaciones no se reconocen rápidamente y se reparan las vulnerabilidades, la elección de un dispositivo alternativo sería la respuesta más adecuada. Si utiliza el sentido común y la precaución, es posible comenzar a construir una casa inteligente. A continuación se presentan las principales consideraciones que debería tener en cuenta antes de comprar componentes o embarcarse en este viaje.

- *Investigue posibles vulnerabilidades antes de comprar (requisito obligatorio para tomar una decisión). Haga una búsqueda simple de los ejemplos que detallamos a continuación. Esto le dará un panorama de los problemas conocidos.*

Vulnerabilidad de seguridad de "nombre del dispositivo"
Vulnerabilidad de seguridad de "nombre de la marca del dispositivo
Brecha de privacidad de "nombre de la marca del dispositivo
Fuga de datos de "nombre de la marca del dispositivo

- *¿El fabricante actualiza el firmware y el dispositivo puede actualizarse automáticamente o, como mínimo, se le notifica al usuario a través de una app o por correo electrónico? Consulte el sitio Web del fabricante o haga una búsqueda online para encontrar la información.*
- *Lea la política de privacidad. Comprender qué datos se recopilan, almacenan o comparten lo ayudará a tomar una decisión sobre si el dispositivo debe estar conectado a la red en general o si es preferible mantenerlo aislado. Y si el uso de los datos no se considera seguro, entonces por supuesto no compre el dispositivo.*
- *Tenga cuidado al compartir datos en las redes sociales o con los sistemas de un fabricante. Si comparte su ubicación, dispositivo y patrón de uso puede estar dándoles a los cibercriminales la información suficiente para estafarlo o iniciar un ataque dirigido.*
- *Los asistentes personales inteligentes controlados por voz son muy convenientes. Pero ellos también manejan todos sus datos. Piense cuidadosamente cuánto le dice a su asistente, o cuánta información es capaz de reunir en su nombre.*

Cada persona que lea este documento tendrá una opinión diferente sobre qué información personal está dispuesta a divulgar, ya sea a un único fabricante o a una empresa que tenga una vista agregada de distintos dispositivos. La recopilación por los proveedores de servicios de Internet de los datos del hogar, el estilo de vida, la salud e incluso la navegación, y su disponibilidad potencial para una sola entidad sólo debe permitirse tras una cuidadosa consideración de las consecuencias. A medida que las empresas van descubriendo nuevas formas de rentabilizar los datos recopilados por los dispositivos de la IoT, la industria necesita autorregularse, o los gobiernos deberán fortalecer la legislación sobre privacidad de una forma similar a la implementación de las normativas GDPR en la Unión Europea.

Febrero 2018

ENJOY SAFER TECHNOLOGY™

ESET, spol. s r.o.

Aupark Tower, 16th Floor
Einsteinova 24, 851 01 Bratislava
Slovak Republic