Publicado en Ciudad de México el 10/08/2018

El rol crítico de los proveedores de telecomunicaciones en la protección de los hogares inteligentes

La colaboración entre los proveedores de banda ancha y los vendedores de sistemas de seguridad constituye una poderosa relación que permite a los consumidores mantener a salvo sus hogares y dispositivos inteligentes

Gagan Singh, SVP & GM Mobile de Avast (LSE: AVST), líder global en productos de ciberseguridad, comparte la visión que juegan los proveedores de telecomunicaciones en la protección de los hogares inteligentes, destacando los riesgos que enfrentan tanto los consumidores como la industria, y como resolver el desafío de la amenaza a la seguridad de los dispositivos inteligentes.

Se espera que el número de dispositivos inteligentes del hogar alcancen los 38.5 billones en 2020, de acuerdo con Juniper Research. La cifra incluye todos los dispositivos, desde parlantes hasta lavarropas inteligentes, diseñados para hacer las vidas de esos hogares más sencillas. Dichos dispositivos inteligentes vienen desafortunadamente con un potencial de vulnerabilidad de seguridad que puede poner las casas y los datos de sus dueños en peligro, así como afectar negativamente sus negocios. Sin embargo, asegurar estos dispositivos conectados a Internet de las Cosas (IoT, por sus siglas en inglés) es un desafío, dada la diversidad de artefactos y sistemas con los que se comunica.

Los riesgos que enfrentan los consumidores

Los atacantes pueden penetrar cualquier dispositivo inteligente a través de la red doméstica si su punto de acceso, el router, no está asegurado contra estas amenazas de intrusión, lo cual puede ocasionar una amplia variedad de ataques.

IoT es un ejemplo en el cual las debilidades en la ciberseguridad pueden abrir paso a amenazas a la seguridad física. Un buen ejemplo de ello son los dispositivos de IoT hackeados, que pueden informar a los atacantes si los dueños de casa están o no en ella, según el dispositivo que estén usando.

Un riesgo muchas veces menospreciado cuando se habla de dispositivos de IoT es la posibilidad de que se pueda filtrar información personal, así como el registro de los movimientos de los dispositivos.

Los hackers no necesitan hackear el servidor de una compañía para apoderarse de información, en cambio pueden ir directamente al dispositivo del usuario. Los motores de búsqueda de IoT, que son capaces de hacer listas de dispositivos vulnerables y que pueden ser aprovechados para intrusiones, están disponibles libremente en internet. Si un hacker consigue ingresar a todos o la mayoría de los dispositivos de IoT en la casa de alguna persona, será capaz de monitorear sus movimientos, escuchar sus conversaciones privadas y potencialmente atacar a esa persona o vender a otros la

información que ha colectado, como los datos de su cuenta bancaria o de su tarjeta de crédito, para que se aprovechen de ella.

Los riesgos que los proveedores de telecomunicaciones y otros enfrentan

Una de las amenazas más comunes que actualmente apunta hacia los dispositivos de IoT pasa inadvertida por los consumidores, pero tiene un considerable impacto negativo en los proveedores de banda ancha y en otras compañías. La esclavización de los dispositivos inteligentes para que se comporten como bots en una botnet, permite a los cibercriminales usar dispositivos infectados para llevar adelante varios ataques, incluidos ataques de DDoS que ponen fuera de servicio a los servidores

Los cribercriminales usan los ataques de DDoS para hacer que una red quede no disponible y para ello buscan abrumar a la máquina objeto de dicho ataque con un enorme número de solicitudes de acceso, enviadas desde múltiples dispositivos. Esto sobrecarga al computador objetivo, atascando su ancho de banda y luego volviendo imposibles las conexiones legítimas. Para el usuario, los ataques de DDoS pueden pasar fácilmente inadvertidas dado que corren en el background del computador. Sin embargo, pueden causar grandes daños a las compañías.

Resolviendo el desafío de la amenaza a la seguridad de los dispositivos inteligentes

Los fabricantes de dispositivos están bajo presión para producir dispositivos inteligentes y sacarlos al mercado rápidamente y a un precio accesible. No ven la seguridad como una prioridad o no están muy familiarizados con ella, lo que implica que distribuyen dispositivos vulnerables y con una seguridad muy baja que con frecuencia no pueden ser actualizados por los consumidores.

El enfoque actual sobre cómo brindar seguridad a los dispositivos de IoT es más un enfoque de `hágalo usted mismo´ que un abordaje estructurado -una brecha que está generando grandes oportunidades para los cibercriminales. Los consumidores, por ejemplo, pueden tomar medidas básicas para proteger sus dispositivos inteligentes, pero simplemente no hay suficientes opciones disponibles para darles una protección total en este momento. Adicionalmente, cuando se trata de implementar las opciones que figuran en los manuales de seguridad, con base en 30 años de experiencia en la industria de seguridad, Avast sabe que la mayoría de los usuarios son blandos al cumplir con los pasos básicos como actualizar el firmware o las contraseñas por defecto, si los usuarios eligen cumplirlos las medidas que pueden tomar son a menudo limitadas.

Las autoridades pueden hacer cumplir los estándares y leyes de la industria que los fabricantes aún deben cumplir, pero incluso si las leyes existen no son suficientes para proteger a los consumidores.

Los proveedores de telecomunicaciones y quienes comercializan soluciones de seguridad son dos jugadores que desempeñan un rol importante en la seguridad de los artefactos conectados al IoT. Si trabajan en conjunto pueden resolver los retos del consumidor relativos a cómo proteger sus redes domésticas y sus dispositivos. Los proveedores de banda ancha se encuentran en una posición

privilegiada para proporcionar seguridad dado que a menudo proveen el router, las redes que contienen los datos del usuario y realizan la conexión en los aparatos de uso diario de los usuarios. Además, tienen el poder para erigir una infraestructura y una red seguras, que le permitan al usuario confiar en la seguridad de su conexión.

Los proveedores de servicios de seguridad, por otro lado, pueden vigilar el flujo de datos a través de la red y usar tecnología de machine learning e inteligencia artificial para entender esos datos, identificar anomalías y bloquearlas. Como resultado, las soluciones de seguridad pueden identificar a los ataques en el momento en el que ocurren y responder a ellos en tiempo real, cuando las anomalías ocurren en el tráfico de un hogar inteligente. La clave para hacer esto exitosamente recae en la big data, pues a mayor cantidad de datos e insights proveniente de su base de usuarios que tenga un proveedor de servicios de seguridad, mejores posibilidades tendrán sus soluciones de detectar amenazas nunca antes vistas.

Con la cifra de dispositivos de IoT creciendo exponencialmente, a la par que aumenta la cifra de amenazas que los tienen en la mira, es imperativo que los proveedores de banda ancha y los comercializadores de soluciones de seguridad trabajen juntos para brindar a los consumidores soluciones simples y robustas que protejan su vida digital.

Datos de contacto:
Marketing Q
Agencia de Relaciones Públicas
56152196

Nota de prensa publicada en: Ciudad de México

Categorías: Telecomunicaciones Comunicación Hardware Tecnología Software Seguridad