Publicado en CDMX el 11/09/2017

# [1 de cada 5 dispositivos conectados a Internet de las cosas en México es vulnerable: Avast](http://www.notasdeprensa.es)

## Webcams y monitores de bebé son vulnerables y representan un riesgo para la privacidad y seguridad de las personas

 Avast, el líder global en productos de seguridad digital para usuarios y empresas, reveló los resultados de su última investigación sobre dispositivos inteligentes en México, incluyendo webcams, monitores de bebé, impresoras y routers. Investigadores de Avast encontraron que 20.7% de los dispositivos conectados a Internet de las cosas son vulnerables a ciberataques, poniendo en riesgo la seguridad y privacidad de las personas. Entre los dispositivos se encuentran tanto webcams como monitores de bebé, de los cuales el 13.8% son vulnerables, lo que podría ser utilizado para espiar tanto a adultos como a niños. Además, el 21.3% de las impresoras no son seguras. Sin embargo, el mayor riesgo se encuentra en los routers, Avast encontró que 66.6% de los routers en México son vulnerables. A través de routers vulnerables, los ciberdelincuentes pueden acceder a otros dispositivos conectados a la misma red, como webcams, televisores inteligentes, o aparatos de cocina inteligentes. En general, cualquier dispositivo vulnerable puede ser utilizado para infectar a otros, para agregarlos a una botnet, o tomar el control de ellos y perjudicar a su propietario. Esto incluye cocina inteligente y dispositivos domésticos a los cuales los ciberdelincuentes pueden dar órdenes de manera remota. Los fabricantes de dispositivos inteligentes también recolectan y almacenan información privada de los usuarios, incluyendo comportamiento de búsqueda y utilización del dispositivo, contactos, y detalles de tarjeta de crédito, lo que representa un riesgo adicional si ésta información llega a ser interceptada por ciberdelincuentes. Como el 13.8% de webcams y monitores de bebé en México son vulnerables, los ciberdelincuentes pueden acceder fácilmente a ellos y observar a las personas en espacios privados o incluso transmitir los videos en vivo directamente a Internet. `Con miles de dispositivos vulnerables esparcidos alrededor del mundo, los ciberdelincuentes pueden crear una botnet para atacar y tirar servidores y sitios web, como lo vimos el pasado otoño, cuando el proveedor de servicios de dominio, Dyn, fue atacado, lo que interrumpió el tráfico a sitios importantes, incluyendo Amazon, Twitter y Reddit` dijo Ondrej Vlcek, CTO, Vicepresidente ejecutivo y director general de consumo en Avast. `También los routers son la puerta a la red Alerta para los medios doméstica, y por lo tanto, crean un punto de entrada fácil para que los hackers ataquen redes domésticas mexicanas, si éstas no están debidamente protegidas, por ejemplo, porque el software está desactualizado o porque se está usando una contraseña débil´. Es simple para cualquier persona, incluyendo ciberdelincuentes, escanear la dirección y puertos IP a través de Internet y clasificar cuál dispositivo está conectado a cada dirección IP. Con un esfuerzo extra y algo de conocimiento, los hackers también pueden encontrar el tipo de dispositivo (webcam, impresora, cafeteria, refrigerador, etc.) marca, modelo y versión de software que utiliza. A continuación ellos pueden comparar ésta información en listas públicas disponibles de los dispositivos vulnerables para saber cuál de ellos no es seguro. Para asegurar los dispositivos conectados contra ataques, los usuarios necesitan contribuir para hacer que Internet sea un lugar seguro, manteniendo el software actualizado y eligiendo contraseñas fuertes y complejas. Avast está abordando la seguridad de Internet de las cosas de las siguientes maneras: • Wi-Fi Inspector es parte de Avast 2017 versión gratuita y premium, disponibles en www.avast.com. Wi-Fi Inspector escanea las redes domésticas buscando dispositivos vulnerables y permite a los usuarios solucionar, mediante instrucciones paso a paso, cualquier problema de seguridad. • Chime es una plataforma que se asienta sobre el router y lo hace inteligente, de manera que pueda protegerse a sí mismo y a todos los dispositivos que se conectan a él. El concepto surgió de la idea de que un router podría agregar una capa extra de seguridad para un hogar inteligente y también actuar como central de conexión entre los dispositivos inteligentes del hogar. Avast tiene un partner en Estados Unidos de América, que utiliza la plataforma con su router. El nuevo sistema de Wi-Fi inteligente de Amped Wireless´ALLY, que recientemente obtuvo un premio CES a la innovación, ofrece a los usuarios agregar una capa extra de seguridad a sus dispositivos conectados a Internet de las cosas, lo que también incluye control parental y filtros de contenido, los cuales pueden manejarse fácilmente mediante una aplicación móvil. Avast (www.avast.com), líder global en productos de seguridad digital, protege a más de 400 millones de personas online. Avast ofrece productos bajo las marcas Avast y AVG que protegen a las personas de las amenazas en internet y del escenario de amenazas de Internet de las Cosas en constante evolución. La red de detección de amenazas de la compañía se encuentra entre las más avanzadas en el mundo, utilizando tecnologías de aprendizaje automático e inteligencia artificial para detectar y detener amenazas en tiempo real. Los productos de seguridad digital de Avast para Móvil, PC o Mac están mejor clasificados y certificados por V-100, AV-Comparatives, AV-Test, OPSWAT, ICSA Labs, West Coast Labs, entre otros. Avast cuenta con el respaldo de las principales firmas globales de capital privado CVC Capital Partners y Summit Partners

**Datos de contacto:**

Flor Carreño

Marketing Q S

56152198

Nota de prensa publicada en: [https://www.mexicopress.com.mx/1-de-cada-5-dispositivos-conectados-a-internet\_1](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: E-Commerce Software Ciberseguridad Dispositivos móviles



[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)