Una red Wi-Fi vulnerable puede poner en peligro los datos de tu organización

28/06/2022

L**a seguridad de la información pasó a ser una de las mayores prioridades de los negocios hoy en día y una de las mayores preocupaciones de los usuarios, ya que nadie quiere ver sus datos expuestos y ninguna organización quiere enfrentar las graves consecuencias** -legales, reputacionales y financieras- de una violación de su red Wi-Fi.

Hace unas semanas, un analista de ciberseguridad descubrió de manera inesperada que mediante la herramienta rsync (utilizada para sincronización de archivos) pudo volcar archivos del sistema de la red del hotel en el que se alojaba en Qatar a su propio ordenador.

A través de una pasarela HSMX (HSMX Gateway), accedió a una gran cantidad de información sensible que se hallaba en un servidor FTP utilizado con fines de back-up. Esto incluía

datos personales de huéspedes como sus habitaciones, correos electrónicos y números de móvil.

Por si fuera poco, l**os archivos que se descargó no solo eran del propio complejo en el que se encontraba, sino también de todo el grupo, formado por 629 hoteles en más de 40 países.**

Además, no solo estarían en peligro esos datos personales, ya que la vulnerabilidad que encontró permite a los ciberatacantes emplear otras técnicas. Por ejemplo, podrían suplantar la landing page de acceso Wi-Fi al hotel de tal manera que los huéspedes, al conectarse, vean una landing falsa que les pide introducir otros datos personales aún más sensibles, como números de tarjetas de crédito que después podrían emplear para sustracción del dinero de sus cuentas o para su venta en la Dark Web.

Este hallazgo pone de manifiesto lo insegura que pueden llegar a ser las redes Wi-Fi públicas y cómo suponen una gran vía de acceso que pone en riesgo tanto a sus usuarios como a las propias organizaciones que las gestionan.

En este contexto, los especialistas de WatchGuard aconsejan una serie de medidas que pueden y deben tomarse para proteger estas redes:

– Los responsables de TI o de ciberseguridad de las organizaciones deben asegurarse de que cuentan con todos sus servidores y programas de terceros actualizados con sus parches convenientemente instalados, para reducir las posibilidades de que exploten sus vulnerabilidades. Para ello, pueden servirse de gestores de parches que automaticen y faciliten estos procesos.

– Para una gestión de las redes Wi-Fi sencilla y segura, han de emplear soluciones avanzadas que sean fácilmente gestionables desde la nube y que cuenten con Puntos de Acceso Wi-Fi 6 con cifrado WPA3. De esta manera, se asegura un Entorno Inalámbrico Confiable para todos.

– A su vez, estos Puntos de Acceso han de estar integrados en una red segura que disponga de dispositivos Firewall avanzados con grandes capacidades de seguridad avanzada como sandboxing en la nube, antimalware con tecnología de IA, correlación de amenazas y filtrado de DNS.

– Por último, es recomendable que los usuarios y clientes que se conecten a cualquier red Wi-Fi pública, por muy protegida que pueda parecer, lo hagan mediante redes VPN protegidas y que dispongan de Firewalls virtuales.