Managed secure IT | no matter what

EL ATAQUE A LAS REDES WPA2 QUE OBLIGÓ A LA INDUSTRIA A MUDARSE AL WPA3

Por años, el estándar WPA2 se usó para proteger el intercambio de datos mediante conexiones inalámbricas a internet.

Desde su creación, se creyó que este protocolo de seguridad se encargaría de hacer del wifi una de las conexiones más seguras del mundo, sin embargo, una vulnerabilidad hallada recientemente en su código demostró lo contrario.

Security

Para ser más exactos, los hackers no explotaron solo una vulnerabilidad para romper el cerco de seguridad de WPA2, sino que usaron varias a través del método conocido como KRAK (Key Reinstallation Attacks), que no son más que una serie de ataques al sistema de cifrado de las conexiones inalámbricas que abren, casi de manera accidental, una brecha en el cerco de seguridad de WPA2 para dejarlo vulnerable a cualquier infección de malware.

Afortunadamente, esta vulnerabilidad quedó expuesta en un evento de ciberseguridad en Dallas, Texas, por lo que ningún cibercriminal pudo explotarla, pero su violación sí dejó bien en claro que llegó la hora de confiar la seguridad de nuestras redes inalámbricas a un protocolo mucho más fiable.

De no llegar la solución a esta vulnerabilidad, el mundo tendrá que conectarse a redes inseguras que podrían quedar indefensas ante un ataque y esto, aplicado a una empresa, podría dejarlas completamente a la merced de los cibercriminales.

Actualmente se plantea usar el protocolo WPA3 para proteger las redes wifi de todo el planeta, pero mientras este no haya sido probado completamente, las empresas de todo el mundo quedarán expuestas ante los ataques de cualquier hacker que quiera afectarlas.

Si un cibercriminal puede explotar la vulnerabilidad en tu cerco de protección de redes inalámbricas, podrá hacerse de tu contraseña, tomar el control de todos tus equipos, robar tu base de datos, infectar cada equipo con malware y, en el peor de los casos, paralizar tus actividades productivas a través del ransomware.

Debido al alcance de la vulnerabilidad en WPA2, ningún respaldo está seguro y tanto las PCs, como las Macs, podrían convertirse en objetivos de hackers capaces de robar toda la información de tu negocio en cuestión de minutos.

Por el momento, cambiar las contraseñas de las redes inalámbricas es un paso recomendable para protegerse, pero este método no es más que un paliativo en lo que llega la verdadera medicina: un protocolo más fuerte en la forma del WPA3.

En lo que esto sucede, una empresa debe modernizarse y actualizar sus sistemas de seguridad, ya sea a través de nuevos antivirus o migrando toda su información a un entorno seguro, de fácil acceso y vigilado bajo los más estrictos estándares de calidad: el de la Nube.

El WPA3 promete proteger nuestras redes inalámbricas, pero así como el WEP (que al principio se creyó inviolable y fue vulnerado en 2001), el WPA, que también dejó de ser confiable pocos años después de su implementación y su sucesor ya vulnerado, podría verse comprometido en cuestión de tiempo, por lo que confiar los assets de tu compañía a un nuevo protocolo de seguridad inalámbrica no será sino una solución temporal a las amenazas de seguridad a las que se enfrenta día con día.

Consulta a un experto en seguridad para que recomiende los mejores métodos de protección para las bases de datos de tu negocio, sus herramientas y la información más valiosa que maneje todos los días.

Las amenazas de seguridad que vienen en 2018 serán más letales que las del año pasado y la única manera de mantenerse protegido de estas es a través de un sistema inteligente de protección empresarial que combata cualquier peligro sin importar su procedencia, naturaleza o potencia.

Síguenos en nuestras redes sociales:

MexisMX

Servicios Administrados Mexis, S.A. de C.V.

Mexis TI

Servicios Administrados Mexis, S.A. de C.V.