Managed secure IT | no matter what

¿CÓMO EVITAR SER VÍCTIMA DE LAS BRECHAS DE DATOS?

Volverse víctima de una brecha de datos, te hace al menos 10 veces más vulnerable como individuo y aún más si se forma parte de una red empresarial de la que dependen las operaciones de un negocio de escala pequeña o grande.

Lo peor del caso es que ser víctima de un ataque de phishing o malware hace que cualquier miembro de un equipo de trabajo sea 400 más propenso a que roben su cuenta personal, sus datos sensibles e incluso sus accesos a las bases de datos del lugar donde trabaja.

Security

Esto lo dice un estudio reciente llevado a cabo por ingenieros de Google usando sus propias apps como cajas de petri y sus propias herramientas para monitorear lo que pasa cuando alguien descuida el manejo de su información en internet.

Ya hemos hablado bastante de cómo funciona el phishing, pero resulta cada vez más difícil no caer en una trampa como esta pues los cibercriminales usan formas cada vez más creativas y complejas para robar la información de los internautas.

Lo mismo pasa con las campañas de infección masiva que roban los datos de millones de usuario y exponen su información personal, así como los datos de los lugares donde hacen negocios todos los días.

El año pasado, al menos mil 900 millones de nombres de usuarios y contraseñas fueron expuestos en brechas de datos, mientras que 788 mil víctimas potenciales de keyloggers, perdieron su información a manos de hackers que usaron sus contraseñas para robar fondos de las empresas para las que trabajaban y secuestrar el uso de sus bases de datos.

Si un solo empleado de una compañía o negocio pequeño o mediano pierde su información por una brecha de datos, todas las operaciones de su equipo se hallan en peligro de corromperse completamente pues un ataque de esta magnitud hace que cualquier negocio o empresa se vea afectado tras un ataque de ransomware, por ejemplo.

Se sabe que las empresas más propensas a sufrir este tipo de vulneraciones son las que continúan almacenando su información y confiando sus operaciones en sistemas on-premise que pueden ser fácilmente corrompibles por terceros.

Una de las maneras más efectivas de protegerse es activar el modo de autenticación de usuario en dos pasos, pero es solo cuestión de tiempo para que los cibercriminales averiguen formas más complejas de burlar este cerco.

Por ello, a decir de los expertos, la mejor manera de protegerse es acudiendo a un experto que ofrezca consultorías de seguridad con el fin de concientizar a todo el equipo de trabajo de los peligros de hacer un uso irresponsable de sus datos.

Conceptos como higiene de seguridad e inteligencia de amenazas locales y globales, pueden resultar desconocidos en un negocio mediano o pequeño, pero con la orientación adecuada, pueden convertirse en herramientas clave para mantener a flote cualquier empresa ante los retos y dificultades del siglo en curso.

Security

Los expertos en seguridad pueden orientar a cualquier CEO o CIO en conceptos tan importantes como cercos de blindaje digital, cifrado, tecnologías Cloud, Internet of Things, Megadata, seguridad basada en firmas, firewalls, análisis de comportamiento, segmentación de red, VPNs y soluciones de punto aislado, entre otras herramientas diseñadas para no convertirse en víctima de una brecha de datos que acabe por destruir desde dentro un negocio.

En un mundo donde hay cada vez más ataques como WannaCry o NotPetya, ambas campañas que en 2017 hicieron que empresas de todo el mundo perdieran miles de millones de dólares y la confianza del público, lo más recomendable es invertir en ciberseguridad y asesoramiento de expertos certificados y actualizados en todas las maneras de contrarrestar las amenazas de los cibercriminales.

Síguenos en nuestras redes sociales:

MexisMX

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

Mexis TI

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