Managed secure IT | no matter what

RECOMENDACIONES PARA NO SER VÍCTIMA DE ESTAFAS CIBERNÉTICAS

Patrón Bitcoin, empresa especializada en servicios de consultoría de Estimaciones de firmas de seguridad internacionales indican que en el último semestre de 2017, los ataques cibernéticos aumentaron un 89%, respecto al mismo periodo del año anterior.

En México, por otra parte, 8 de cada 10 empresas han sido víctimas de algún tipo de fraude.

Fortalece tus contraseñas

Tal vez parezca el paso más obvio, pero te impresionaría saber que, según un estudio reciente, al menos 48% de los usuarios de servicios de internet no cuentan con las medidas de protección básicas como contraseñas de acceso a sus cuentas, dispositivos y herramientas de productividad.

Incluso importantes agencias de seguridad y defensa estratégica de países como Estados Unidos fallan en este aspecto, lo que le da a los cibercriminales la oportunidad perfecta de destrozar sus sistemas desde dentro.

Pide a tu CIO que construya un sistema confiable de contraseñas que proteja cada paso de tus operaciones y evite que los clientes, proveedores o incluso empleados se vuelvan eslabones débiles de tu cadena de seguridad.

Pasa de los Discos Duros al Cloud

Un importante número de empresas suele almacenar toda su información en uno o varios Discos Duros físicos que, de fallar, paralizarán todas sus operaciones.

Algunos CIO's incluso confían en la vieja estrategia de copiar la información de un Disco Duro a otro de respaldo para "proteger la información" de cualquier falla, sin embargo, se ha comprobado en más de una ocasión que esa forma de proteger la data solo retrasa lo inevitable: perder la información por un ciberataque o un accidente.
Actualmente, la única forma segura de proteger información importante es almacenándola en un "Disco Duro virtual" ubicado en el Cloud, lejos de posibles fallas por interrupciones en el suministro eléctrico y de los ataques de los hackers.

Consulta a un experto en este ecosistema para saber qué herramientas del Cloud satisfacen mejor tus necesidades y cuál es la mejor manera de migrar a ella sin perder información.

Evita el mal uso del correo electrónico

Tener una cuenta de correo corporativo protegida y bajo la celosa mirada de un equipo de expertos en seguridad cibernética no sirve de nada si los empleados que la usan diariamente no lo hacen correctamente.

En el pasado ha habido casos en los que grandes empresas como Yahoo o PayPal sufren la pérdida de millones de cuentas de sus usuarios por un simple error de logueo cometido por uno de sus empleados.

La tarea de un CIO en este aspecto es la de establecer un código de Buenas Prácticas que enseñe a usar correctamente el correo electrónico de la empresa con el fin de evitar que el equipo de trabajo lo use para atender asuntos personales, realizar descargas no autorizadas o para ingresar a ciertas aplicaciones públicas.

No obedecer esta guía puede derivar, ya sea en una infección de Spam, hasta la parálisis de una compañía secuestrada por un cibercriminal.

Recuerda que la seguridad informática es tan fuerte como su eslabón más débil.

Las redes sociales

Una empresa que no tiene presencia en Facebook, Twitter, YouTube o Instagram prácticamente no existe para su público, pero es justo esa necesidad de estar en tantos lugares a la vez, la que abre la puerta a nuevas amenazas.

El empleado que lleve las cuentas de redes sociales debe obedecer un protocolo de seguridad integral que proteja tanto el equipo en el que trabaja (para evitar infectar al resto de la red), como la imagen y prestigio de la empresa en redes sociales.

Ha habido casos recientes en los que los cibercriminales secuestran las redes sociales de una compañía de clase mundial en los que piden millones de dólares como rescate.

Tras contratar a un experto en soluciones de seguridad, se descubrió que los responsables del ataque habían entrado a la red a través de una fisura en el cerco de seguridad provocada por un descuido de su Community Manager.

Construye un protocolo de seguridad en torno a las redes sociales para evitar convertirte en víctima de un fraude o ataque llevado a cabo por cibercriminales.

Construye un plan de protección bien balanceado

Ya que seguiste todas las recomendaciones que te compartimos, ahora toca transmitírselas a tu equipo de trabajo, pero si estas son demasiado estrictas, serán pasadas por alto, así que debes balancear productividad con seguridad.

Cambiar una contraseña cada semana es una forma segura de proteger la red de la compañía, pero si lo exiges así a tu equipo, probablemente te enfrentes a un gran número problemas de acceso y a muchos usuarios necesitando que les restablezcan su contraseña, entre otros contratiempos.

Busca una manera de combinar seguridad con facilidad de uso y si no sabes cómo hacerlo, acude a un experto en protección cibernética para que juntos diseñen un plan de prevención y contención de emergencias digitales.

Actualiza todo

Este paso es fundamental para mantener los firewalls, antivirus, anti-spywares y sistemas operativos actualizados en cuanto a las nuevas amenazas que pululan en la red, pero tarde o temprano un cibercriminal sabrá adelantarse a cualquier parche o actualización para atacar tu empresa.

Cloud

La mejor manera de asegurarte que tu red está al día es migrando al Cloud, ecosistema que siempre está en constante actualización y bajo la vigilancia de expertos que saben cuáles son las amenazas del presente y del futuro.

Es cada vez más necesario buscar una organización dedicada a este tipo de soluciones para empresas de cualquier calibre, con el fin de obtener orientación sobre qué pasos seguir en el camino hacia la protección integral de tu negocio.

Síguenos en nuestras redes sociales:

MexisMX

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

Mexis TI

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