

Seguridad informática: predicciones para 2017

La seguridad informática presenta nuevos desafíos constantemente, así que ir por delante de las amenazas a la seguridad que aparecen cada año no es tarea fácil. Aun así, con un poco más de dedicación y previsión, las empresas podrían haber evitado muchos de los ataques que se produjeron en 2016.

¿Les ocurrirá lo mismo en 2017?
¿O serán más proactivas en materia de seguridad?
Continúe leyendo para conocer las diez amenazas que vaticina Fujitsu.

1



Cuidado con los puntos ciegos de la red

Los puntos ciegos de la seguridad, como PowerShell, seguirán siendo el talón de Aquiles de muchas empresas que pasen por alto los riesgos que implican.

2

¿Aparecerán ordenadores más inteligentes que ofrezcan una seguridad más inteligente?



Los ordenadores son cada vez más inteligentes. No paran de aprender trucos nuevos. Esto conlleva la aparición de formas completamente nuevas de abordar la seguridad. No obstante, no se confíe. Los piratas informáticos siguen utilizando los mismos trucos de siempre para burlar los controles de seguridad.

3



Los bancos siguen en primera línea de guerra

El año pasado, los piratas informáticos lograron deslizarse entre las grietas de seguridad para apoderarse de millones de dólares de los principales bancos. Pese a que se han implantado medidas de contención, es posible que se produzcan más intentos de ataques contra los bancos este año.

4

Los ataques se centrarán en los dispositivos móviles



Probablemente esté leyendo esto en un teléfono. ¿Sabe si es seguro? Tenga cuidado con los nuevos ataques que amenazan sus datos personales, como el ransomware que toma las fotos como rehenes.

5



Veremos en qué medida las "ciudades inteligentes" hacen honor a su nombre

El diseñador de las vallas publicitarias inteligentes para las autopistas probablemente nunca pensó que estas serían el blanco de los piratas informáticos para mostrar mensajes políticos. Se pondrán a prueba los límites de los sistemas inteligentes. No les quite el ojo a sus plataformas de control.

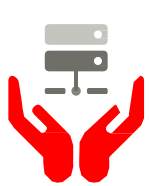
6

La recuperación rápida será necesaria para la protección de la reputación



Tengan los controles de seguridad que tengan, las empresas seguirán sufriendo ataques informáticos. Por ello, si no pueden recuperarse rápidamente, estos perjudicarán a su negocio y a su reputación. ¿Está preparado para el desafío?

7



Las empresas desearán confiar sus datos a las opciones más seguras

El Reglamento general de protección de datos está ya a la vuelta de la esquina. Esto significa que los inversores, los accionistas, los clientes y los reguladores desearán que sus datos se mantengan sanos y salvos.

8

Los clientes globales estarán ojo avizor en cuanto a las cadenas de suministro



Puede que ya haya protegido todos sus datos confidenciales, pero ¿y su cadena de suministro? Las grandes empresas solo querrán trabajar con las cadenas de suministro que sepan cómo gestionar la seguridad de los datos.

9



Las juntas directivas se interesarán por la seguridad de la TI

Los directivos empiezan a abrir los ojos y enfrentarse a la realidad. Una seguridad de TI deficiente es perjudicial para las empresas, tanto en términos de ingresos como de imagen de marca. No obstante, no siempre comprenderán la jerga técnica, así que el personal de TI sénior tendrá que explicarse en un lenguaje más asequible.

10

El mayor problema seguirán siendo los cimientos

Ojalá pudiéramos afirmar que todos los problemas de seguridad se deberán a los astutos piratas informáticos. Sin embargo, el verdadero villano es mucho más aburrido. No estar al día de las prácticas básicas de TI es lo que más le deja expuesto a las vulneraciones.



Si hay algo que nos ha enseñado el 2016, es que las empresas ignoran los avances de la seguridad cibernética bajo su propia responsabilidad. Aunque nadie es invulnerable a los ataques, estar alerta y mantener el orden aumenta las posibilidades de evitarlos, así como las interrupciones que causan.

Visite el sitio web [Secure Thinking](#) para obtener más información acerca de la protección de su empresa frente a las amenazas informáticas.