Los desafíos en ciberseguridad para 2017

18/12/2016

Los ataques a las cuentas de Yahoo, Twitter y el bitcoin demostraron una vez más que nadie es inmune a los hackers, cada vez más sofisticados.

Los virus siguen reinventándose y aumentando y se dirigen a los datos de más valor: números de la seguridad social, tarjetas de crédito, datos de salud, correos electrónicos y contraseñas.

Cuando falta menos de un mes para la llegada de 2017, los expertos del foro ESET de seguridad informática adelantaron cuáles serán las amenazas a tener en cuenta en los próximos doce meses.

Las aplicaciones para móviles, por ejemplo, guardan datos personales muy valiosos para los hackers: desde las preferencias y la localización de los usuarios hasta los datos bancarios en aquellas que permiten compras.

En tanto, el negocio de los videojuegos en línea continúa creciendo y los ciberataques con él. En los últimos años, los usuarios de PlayStation y Xbox, dos de las plataformas más extendidas en el mundo, han sido las principales víctimas.

Por otro lado, uno de los motivos por los que la amenaza de los virus sobrevuela a los gamers es que los usuarios aún no hacen lo suficiente para protegerse.
El desarrollo creciente de choces autónomos y casas automatizadas implica también nuevos ámbitos a los que los hackers pueden sacar partido.

Se calcula que solo en 2016 hubo seis mil 400 millones de dispositivos conectados a internet (móviles, televisores, relojes, neveras) y se teme que el próximo año aumenten los delitos de secuestro de esos objetos, es decir, que se instale un virus que bloquea, por ejemplo, una cámara de seguridad, y se pida dinero a cambio de

desbloquearla.

SOFISTICADOS CIBERATAQUES

El año que viene se verá una evolución de la práctica que los cibercriminales llevaron a cabo hasta ahora: recurrían a programas maliciosos que bloquean los equipos y exigían el pago de un rescate para liberar el disco duro.

Según la consultora Gartner, para 2017 habrá más de 322 millones de weareables (como relojes inteligentes, bandas deportivas y monitores de glucosa) conectados a Internet y de acuerdo a los expertos del foro ESET, el 39 por ciento de las empresas de salud no sabe cómo protegerse ante un ciberataque. Otro escenario perfecto para los hackers, que pueden obtener datos confidenciales sobre la identidad de los pacientes.

La administración pública, el sistema financiero, las centrales y redes de energía y la industria nuclear siempre fueron objetivos muy codiciados por los hackers por el valor que tiene la información que consiguen de ellas. La amenaza que se prevé para el próximo año se debe a que la actualización de los sistemas de protección de esas infraestructuras es escasa.

La compañía Check Point añade a esa lista los ataques a la nube, donde cada vez hay más datos almacenados. Infectar con un virus a un proveedor de servicios cloud afectaría a todos los clientes que almacenan sus datos allí, por lo que con un solo ataque los hackers consiguen acceso a los sistemas de multitud de empresas.

Los datos de los informes presentan un escenario complejo y alarmante sobre la seguridad en 2017. No obstante, las predicciones presentadas en este material pueden contribuir a que los usuarios desarrollen sus planes de ciberseguridad y se mantengan un paso por delante de los hackers.