La cibercriminalidad será un quebradero de cabeza en 2016

29/12/2015

La multiplicación de prácticas de extorsión, el perfeccionamiento de los ataques por correo electrónico o la pérdida del control de los aparatos conectados a internet se presentan como las mayores amenazas para 2016, según los expertos en cibercriminalidad, que cada vez temen más la posibilidad de un atentado a distancia.

Para el Círculo Europeo de Seguridad de Sistemas de Información, que agrupa a las organizaciones del sector, las mayores amenazas son el cibersabotaje y el ciberterrorismo.

"El ataque informático es un sistema amplio, que va a tener efectos medioambientales y humanos, por ejemplo contaminar el agua, hacer explotar una fábrica, descarrilar un tren", explica la asociación.

Los hackers, ya sean estados, mafias o grupos armados, usan métodos cada vez más sofisticados para "romper" los sistemas informáticos de sus blancos. Hace un año y medio, un pirata informático logró parar el funcionamiento de un alto horno de una fundición en Alemania, un ejemplo de cómo un ciberataque puede afectar a sectores estratégicos.

La empresa estadounidense Varonis, que fabrica aplicaciones de seguridad informática, plantea por ejemplo que si un pirata elige como blanco la campaña presidencial en Estados Unidos, habría muchas repercusiones. "Expondría la identidad de los donantes, sus números de tarjeta de crédito, sus afinidades políticas, que son confidenciales", explica la empresa.

Para lograr sus objetivos, muchos piratas informáticos utilizan la técnica del 'caballo de Troya', que consiste en introducir un 'malware' (una aplicación maliciosa) en los aparatos de algún empleado, para que el virus pueda avanzar hacia las unidades centrales. Para ejecutar esta técnica, los piratas envían correos cada vez más personalizados a las víctimas para que una de ellas abra un enlace o un archivo adjunto que está infectado.

Este método también es utilizado para el chantaje, ya que después de haber descargado los datos, desencriptándolos si es necesario, los piratas pueden pedir una recompensa a cambio de no revelarlos.

Esta forma de ataque también puede permitir que una empresa espíe a la competencia.

"El próximo año, o en los próximos años, creo que va a haber casos serios de este tipo", plantea Jérôme Robert, director de marketing de la consultora francesa Lexsi.

- Una amenaza para los teléfonos inteligentes -

"Hay muchas empresas que ya han usado detectives privados; no hay motivos para que no hagan lo mismo en el ciberespacio", destacó.

Otra preocupación para los especialistas es la falta de protección de los teléfonos inteligentes, donde los usuarios almacenan gran cantidad de datos personales y que concentran gran parte de la actividad en internet. "Hoy hay casi más teléfonos inteligentes que ordenadores. Los teléfonos están encendidos casi las 24 horas, nos siguen a todos lados", destaca Thierry Karsenti, vicepresidente técnico de la empresa antivirus israelí Check Point.

El ejecutivo explica que estos aparatos tienen una mayor conectividad que un PC, disponen de micrófonos y cámara de fotos y almacenan una gran cantidad de información profesional y personal. "Es bastante más molesto que un pirata intervenga tu teléfono que tu ordenador", afirmó Karsent, quien señala que es paradójico que estos aparatos estén mucho menos protegidos que los ordenadores.

En este sentido, el pago a través del móvil puede incitar a los piratas a interesarse por romper los códigos para tener acceso a estos aparatos.

En el mundo actual, con el creciente desarrollo del internet de los objetos, también se plantean nuevos desafíos.

Para Lam Son Nguyen, experto en seguridad de Intel Security, "muchas veces estos aparatos están concebidos sin tener en cuenta el tema de la seguridad", por lo que advierte de que van a ser susceptibles de ser un blanco para los malhechores.