Martes, 26 de agosto de 2016.

'Empresas ven lejos la posibilidad de ser víctimas de ciberataques'

Las empresas están expuestas a cuatro amenazas digitales frecuentes y deberían crear estrategias.

Según expertos, las empresas no destinan suficientes recursos para crear medidas de seguridad dentro de sus organizaciones.

Foto:
Rirchie B. Tongo/ EFE

Por: REDACCIÓN TECNOLOGÍA

25 de septiembre 2017 , 05:45 p.m.

Aunque numerosas firmas de ciberseguridad han indicado que no hay medidas de protección total para los ecosistemas digitales, el **configurar estrategias de seguridad digital fue la recomendación principal de los expertos** durante el Foro sobre Ciberseguridad, organizado por Certicámara S.A y Symantec. En el evento, líderes de tecnología y seguridad de la información de empresas privadas y entidades

públicas de varias ciudades colombianas expresaron sus recomendaciones sobre ciberseguridad.

Las estrategias de las empresas deben ser “defensivas, preventivas y correctivas”, de esta manera tanto la ciudadanía como las organizaciones pueden mitigar el impacto de las amenazas en sus entornos electrónicos y proteger sus sistemas e información privada.

Según el Gaula de la Policía Nacional, en Colombia, se han registrado 12 casos de ataques cibernéticos a empresas establecidas en el país, provenientes de países europeos y asiáticos. Frente a casos como estos, Fredy Bautista, Jefe del Centro Cibernético Policial, aseguró que un evento de cibercrimen “generalmente proviene de varias jurisdicciones, pues cada uno de los actores que están involucrados en las amenazas puede estar ubicado en diferentes países del mundo”.

Durante el foro, **presentaron el siguiente top 4 de amenazas cibernéticas**:

- La contaminación de búsquedas en Google: Esta modalidad ocurre cuando páginas fraudulentas realizan pauta con palabras claves y nombres de bancos y entidades financieras que dirigen a los usuarios a sitios diferentes a los originales.
- Los perfiles falsos en redes sociales: Representan un riesgo tanto de suplantación del usuario, como de potenciales engaños a menores, extorciones y amenazas bajo el anonimato.
- Las Apps peligrosas: Pocas personas confirman los permisos otorgados a las aplicaciones cuando se descargan en los dispositivos móviles, pero además, los usuarios pueden descargar también un virus en sus dispositivos móviles. Son más vulnerables las tiendas de aplicaciones para Android.
- La falsificación de correos corporativos: La suplantación de correos, por ejemplo provenientes de la DIAN, suelen buscar extraer información mediante el engaño. Aprovechando la información que está enviando la

entidad, para poder firmar electrónicamente las declaraciones de renta, se han reportado casos de suplantación.

Según David Kummers, especialista en seguridad de redes de la organización Certicámara, **las organizaciones no invierten los recursos económicos de una forma eficiente para su protección ante ciberamenazas**.

Krummers considera que las empresas por lo general no destinan lo suficiente para crear medidas de seguridad acordes a sus activos de información, lo que las hace vulnerables. Aunque lo suficiente no se refiere solamente a el dinero sino también al talento humano y el tiempo de los integrantes de las organizaciones. En el mismo sentido, **lo "más preocupante" es que las organizaciones "ven lejos la posibilidad de convertirse en víctimas de algún ataque cibernético"**, dijo.

El experto considera que al implementar una estrategia de seguridad digital, las organizaciones deben tener en mente tres propósitos: la protección, la prevención y la detección.

En materia de protección, las organizaciones pueden "implementar herramientas como certificados de servidor seguro, utilizar cifrados fuertes y un WAF (firewall que protege los servidores de aplicaciones web de determinados ataques específicos en Internet)".

Para prevención, las organizaciones "deben contar con escaneos de vulnerabilidades y centros de operaciones de ciberseguridad".

Finalmente, para la detección, el especialista recomienda que las organizaciones implementen escaneos de malware, sistemas de monitoreo de aplicaciones, entre otras herramientas para prevenir ataques de denegación de servicio.

Martes, 26 de agosto de 2016.

REDACCIÓN TECNOLOGÍA