NOTA DE PRENSA
14 / 02 / 2019

Las interacciones confiables serán críticas en 2019, según el informe de predicciones de ciberseguridad de Forcepoint

> Expertos en ciberseguridad advierten de los riesgos en la infraestructura crítica y la información de inteligencia nacional, las amenazas en la identificación biométrica y la excesiva dependencia a la inteligencia artificial (IA) en el ámbito de la ciberseguridad

Forcepoint, líder mundial en seguridad cibernética, ha lanzado hoy su Informe de Predicciones de Seguridad Cibernética 2019, en el que especialistas en seguridad, investigadores de inteligencia del comportamiento y científicos de datos ofrecen orientación sobre las sofisticadas amenazas a las que se enfrentarán las organizaciones en los próximos meses.

El informe examina siete áreas en las que los riesgos aumentarán en 2019. Los expertos de Forcepoint ofrecen un análisis exhaustivo de las tendencias en tecnología y la motivación detrás de los ciberataques, con el fin de que los líderes empresariales, gubernamentales y sus equipos de seguridad puedan prepararse mejor ante la nueva ola de amenazas. Las empresas y los gobiernos se enfrentan a un mundo hiperconvergente en el que los sistemas conectados ponen en riesgo no solo los datos críticos y la propiedad intelectual, sino también la seguridad física. El informe explora estas áreas y concluye que, cuando las personas pueden trabajar con confianza, aprovechando los datos de manera creativa y con total libertad mediante la tecnología, las empresas pueden innovar de manera segura para crear valor.

“La industria de la seguridad cibernética y los hackers dedican sus esfuerzos en un ciclo interminable de intrusión, reacción y evasión, un verdadero juego del gato y el ratón”, explica Raffael Marty, vicepresidente de investigación e inteligencia de Forcepoint. *“Necesitamos romper este ciclo. La investigación de estas predicciones nos obliga a dar un paso atrás y apreciar la totalidad de la situación sin enfrascarnos tanto en los detalles. Los profesionales de la ciberseguridad y los líderes empresariales tienen que adaptarse a los cambios en función del riesgo que representan, lo que les permite liberar lo bueno*

mientras detienen lo malo".

Lidiar con la transformación digital y la confianza

El Informe de Forcepoint sobre Predicciones de Seguridad Cibernética para 2019 explora el impacto de las empresas que confían en los proveedores de servicios en la nube, de la confianza del usuario final en la protección de sus datos personales mediante biometría y el potencial de la confianza en toda la cadena de suministro.

En una encuesta de clientes de Forcepoint , el 94% señaló la seguridad como un tema importante al migrar a la nube. El 58% está buscando activamente proveedores dignos de confianza con una sólida reputación en seguridad y el 31% está limitando la cantidad de datos que alojan en la nube por razones de seguridad.

"Una forma de aumentar la confianza y recuperar el control es a través del modelado del comportamiento de los usuarios, o específicamente, de sus identidades digitales, para entender las razones detrás de su actividad", continuó Marty. *"Comprender cómo actúa un usuario en la red y dentro de las aplicaciones puede identificar anomalías de comportamiento que ayudan a fundamentar las respuestas que se adaptan al riesgo".*

Predicciones de Forcepoint: siete áreas de riesgo para 2019

Entre los aspectos destacados del informe de este año se incluyen:

• **Dirigidos al borde del abismo**

Los consumidores, agotados por las intrusiones y el abuso de sus datos personales, han llevado a las organizaciones a introducir nuevas medidas para garantizar la privacidad del usuario dentro de los servicios que brindan. 'Edge Computing' o "computación en el borde" ofrece a los consumidores un mayor control de sus datos manteniéndolos en su teléfono inteligente o portátil. Las soluciones actuales deben superar la falta de confianza de los consumidores quienes temen que los datos se filtren a la nube exitosamente.

• **Interrupción industrial de IoT a escala**

Los ataques a IoT del consumidor son frecuentes, pero la posibilidad de interrupciones en la manufactura e industrias similares hace que la amenaza sea aún más seria. Meltdown y Specter han brindado a los hackers una forma de atacar las vulnerabilidades de hardware; la infraestructura en la nube puede ser la siguiente.

• **El invierno de la Inteligencia Artificial**

Si la Inteligencia Artificial (IA) trata de reproducir la cognición, ¿existe realmente la IA en la ciberseguridad? ¿Cómo aprovecharán los hackers la desaceleración de la financiación de AI? Cuando se confía en los algoritmos y los datos analíticos para conducir un automóvil, para enfocar las decisiones en la atención médica y para alertar a los profesionales de seguridad sobre posibles incidentes de pérdida de datos, ¿hasta dónde debe llegar esta confianza? ¿Las afirmaciones de los proveedores sobre la efectividad de la IA se compararán con la realidad de los ataques cibernéticos sofisticados?

• **Un reflejo falso**

A medida que persisten los ataques de phishing, los trucos de los hackers como “SIM Swaps” (intercambio de tarjeta SIM) quebrantan la efectividad de algunos métodos de la autenticación de dos factores (2FA), como los mensajes de texto. La biometría ofrece seguridad adicional al usar datos más específicos de cada usuario final, pero las nuevas vulnerabilidades en el software de reconocimiento facial llevan a los expertos a poner fe en la biometría del comportamiento.

Contacto de prensa:

JAVIER MODUBAR ALVAREZ
info@ingecom.net
944395678
http://www.ingecom.net