(index.html)

CRITERIOS

¿Qué podemos esperar, en el 2018 para la Seguridad de la Información?

Edgar Vega Briceño (http://edgar.academy/)
Edgar.vega.briceño@una.cr (mailto:Edgar.vega.briceno@una.cr)

El 2017 tuvo grandes eventos que encendieron las alarmas a otro nivel en lo que respecta ataques contra la Seguridad de la Información: aumento de correos maliciosos con virus y manipulación de sitios web falsos llamados *Phishing*, virus de secuestro de información y rescates millonarios (*Ransomware*), la brecha de seguridad descubierta en grandes empresas mundiales como Equifax, ataques patrocinados por gobiernos para la manipulación de la información a su beneficio, entre muchos otros que probablemente hayan escuchado y leído en los medios, y si no lo hizo, ahora debería darle más importancia a este tipo de noticias pues para el 2018 el nivel de alerta debe ser alto ya que los ciber atacantes serán más inteligentes y persuasivos.

Los ataques a dispositivos del Internet de las Cosas aumentarán

Gracias a que hoy en día la conectividad a Internet es mucho amplia que antes, millones de dispositivos ahora están conectados a esta Red mundial, no solamente un usuario mediante una laptop o PC de escritorio, estos dispositivos incluyen teléfonos inteligentes, consolas de video juegos, impresoras, electrodomésticos, automóviles, cámaras de vigilancia, asistentes personales inteligentes como el Alexa de Amazon o el *Home* de Google y muchas nuevas "cosas" conectadas. Muchos de estos dispositivos tienen poca o carecen de alguna protección en contra de ciberdelincuentes que quieren ganar el control de estos dispositivos y sumarlos a su red de dispositivos que

posteriormente utilizan para realizar envíos masivos de *spam* o envíos masivos de tráfico de Internet causando lentitud en la navegación de Internet o acceso a ciertos sitios o aplicaciones web denegando el servicio a los usuarios. Estas redes que se crean a través de dispositivos controlados por atacantes se llaman *botnets* (redes de dispositivos bajo control de un ciber delincuente sin que el dueño se percate) y para este año 2018 se volverá un dolor de cabeza a pesar de los grandes esfuerzos por desactivar estas redes a nivel mundial por parte de empresas de seguridad y gobiernos. Hace falta cooperación internacional ya que estas redes están formadas por dispositivos del Internet de la Cosas alrededor del mundo. Debe mantener los sistemas operativos de sus computadoras actualizados, con antivirus actualizados y cuidar de no instalar programas que de sitios web no confiables o que le pidan instalarlos sin dejar claro su objetivo.

El Ransomware al acecho

WannaCry y *Petya* los virus que hicieron sucumbir cientos de miles de empresas y usuarios a nivel mundial en el 2017 por el secuestro de la información de sus computadoras y pidiendo un rescate económico para recuperarla, iniciaron con una nueva era de extorsión digital. Definitivamente esta evolución de amenaza cibernética debe recordarnos que los ciber delincuentes innovan dramáticamente creando virus cada vez más agresivos. La evolución seguirá en objetivos menos tradicionales este 2018, buscaran objetivos más rentables como el secuestro de dispositivos del Internet de las Cosas y también atacarán empresas directamente para causar ciber sabotaje e interrupción de operaciones en sus servicios de redes, nube, servicios de correo electrónico y aplicaciones web, siendo la única forma de evitarlo o detenerlo accediendo a peticiones económicas. Ya no bastará solamente con que las organizaciones hagan respaldo de su información sensible, sino que, deberán encontrar innovadoras formas de asegurar la información incluyendo la Inteligencia Artificial. La Sociedad civil debe mantenerse informada y capacitarse en Seguridad Informática, asistir a charlas, foros y estar atentos a grupos y páginas en redes sociales que discuten y comunican noticas que se refieren a Ciberseguridad. Las Universidades por otro lado, deben buscar nuevas y renovadas ofertas académicas que preparen a nuestros profesionales en TIC para afrontar grandes retos que vienen en Ciberseguridad, no solo en el 2018, sino en los próximos años con mucha más fuerza, creatividad y agresividad.

(*) Académico Sede Regional Chorotega

CAMPUS DIGITAL

Marzo 2018 - Año XXVIII N° 295

Oficina de Comunicación, Universidad Nacional. Apartado 86-3000, Heredia - Costa Rica. Teléfonos (506) 2237-5929 y 2277-3224, FAX: (506) 2237-5929. Correo electrónico: campus@una.ac.cr Edición digital: www.campus.una.ac.cr (http://www.campus.una.ac.cr)

Directora: Maribelle Quirós Jara.
Editor: Víctor J. Barrantes C.
Periodistas: Víctor J. Barrantes C., Gerardo Zamora Bolaños, Silvia Monturiol Fernández, Johnny Núnez Zúñiga, Laura Ortiz Cubero, Maribelle Quirós Jara,
Asistente editorial: Andrea Hernández Bolaños y Ana Lucía Vargas.
Diseño de página: José Luis Sánchez Pino josesanchez@engineer.com (mailto:josesanchez@engineer.com)