EPICENTRO CDMX: LA ANGUSTIA BAJO LOS PIES

Newsweek®

EN ESPAÑOL

NEWSWEEKESPANOL.COM
NEWSWEEK.COM

14-10-2018

COSECHAR AGUA DE LLUVIA

Solución para la escasez

ADEMÁS:

• LAS MUJERES QUE SE SOBREPUSIERON A LA GUERRA • VIRIDIANA ÁLVAREZ EN LAS CIMAS DEL MUNDO
• "RUSIA ESTÁ MATÁNDOME LENTAMENTE" • EDICIÓN ESPECIAL: TECNOLOGÍA Y SEGURIDAD EN NUESTRA ERA

Argentina: $31.00
Bolivia: Bs25.00
Chile: $2130.00
Colombia: $8,900.00
Costa Rica: ₡1,900.00
Ecuador: S/.87,600.00
El Salvador: 31.00
Guatemala: Q27.00
Honduras: L75.00
México: $40.00
Nicaragua: C$95.00
Panamá: ฿3.50
Paraguay: ₲16,500.00
Perú: S/.11.00
Puerto Rico: US$3.50
Rep. Dominicana: RD$157.00
Uruguay: $87.50
EE. UU. :$5.00

42
0 040232 904479

Seguridad informática: acciones a favor y tendencias en contra

¿Qué hacer a modo de prevención? No dejar nada a la suerte.

Cuando el 2018 se adentra a su último tercio se ha detectado que ha habido más de 8,000 ataques a empresas y entidades financieras y de gobiernos en todo el mundo, incluido México, asegura la investigadora en seguridad de ESET Latinoamérica, Cecilia Pastorino.

De continuar esta tendencia, los ciberataques superarán los sucedidos en 2017, ya que la incidencia de dichas embestidas está en crecimiento, según se dio a conocer en el ESET Security Report 2018.

Una de las estrategias de hackeo más utilizadas por los cibercriminales es la llamada "watering hole". Esta consiste en colocar programas malignos *(malware)* dentro de los sistemas de las organizaciones y esperar a que algún usuario interno se infecte para después aprovechar esa vulnerabilidad y obtener la información a la que solo los usuarios de la empresa tienen acceso.

Se le llama "watering hole" (abrevadero) por los animales que en la naturaleza se resguardan en los pozos de agua a esperar a que sus víctimas se acerquen. Es la estrategia que se utilizó para atacar el Sistema de Pagos Electrónicos Interbancarios (SPEI) del Banco de México.

Pero no todo el peligro se halla en las computadoras. El celular de un ejecutivo trabajando en la red gratuita de un aeropuerto es una vulnerabilidad latente, pues estos puntos de wifi gratuito no cuentan con la seguridad mínima requerida por una empresa y se pueden infectar de *malware* y convertirse en bots para un probable ataque.

Los celulares no solo transmiten información de trabajo, pues también resguardan datos personales, contactos de familiares, agendas e, incluso, datos biométricos.

Por otra parte, la creciente adopción del internet de las cosas está aumentando la utilización de monitoreo de las cosas —valga la redundancia—, lo que pone en exposición los hábitos y frecuencia de consumos que abren la puerta a ataques por "ingeniería social".

IHS Markit (Information Handling Services), empresa londinense encargada de ofrecer información a entidades públicas y de gobierno, prevé que para 2023 las ventas globales de automóviles ascenderán a 72.5 millones de vehículos con acceso constante a internet. Eso significa que casi 69 por ciento de vehículos de pasajeros estarán compartiendo información con fuentes externas, lo que los convertirá en una red móvil avanzada. Un núcleo de información conectada y constantemente disponible.

El sector automotriz está tomando medidas para prevenir ataques que no pondrían únicamente en riesgo la operación del vehículo, pues habrá la probabilidad de ataque a cuentas personales, historiales de navegación y monitoreo del vehículo y sistemas de peaje.

¿Qué hacer a modo de prevención? No dejar nada a la suerte. Los oficiales de seguridad de la información deben estar conscientes de que la seguridad informática no se limita a contar con infraestructura sólida. La labor de cualquier equipo o individuo encargado de ofrecer seguridad informática es adoptar medidas desde implementar las mejores prácticas hasta ejecutar normas para responder a incidentes una vez que ocurren.

Según tendencias identificadas por Wired, una de las acciones que se deben tomar de manera inmediata es ejecutar pruebas de penetración. Una prueba de penetración es, en esencia, un ciberataque controlado, permitir que un experto en hackeo ético acceda a aplicaciones, sistemas y redes de las empresas y detecte e informe las vulnerabilidades que podrían utilizarse para comprometer la seguridad de la información y tomar acciones correctivas.

También existen tendencias en seguridad que debemos considerar. Organizaciones de todos los tamaños saben que deben protegerse con *firewalls* (contrafuegos) y puntos de seguridad física y lógica. Pero también saben que por sí solos no hacen la diferencia, tanto como las bolsas de aire en un auto no reducen las posibilidades de verse involucrado en un accidente.

La inteligencia artificial y el *machine learning* (aprendizaje automático) son un mecanismo que se puede explorar para evitar la creciente ola de ciberataques. Los *hackers* utilizan inteligencia artificial para generar ataques más poderosos en menor tiempo, ¿pero qué tal si se crean sistemas que aprendan a defenderse por sí mismos?

Esto es lo que está haciendo IBM con el Watson Project, que alimenta constantemente a su máquina de inteligencia artificial con información, métodos y procedimientos de hackeo que son analizados y procesados para orquestar protección actualizada.

Si bien los ciberataques se hacen con máquinas, quienes los planean, ejecutan y en su momento resuelven son humanos, por lo que los oficiales informáticos deben trabajar en conjunto con las áreas de capital humano para mejorar la ciberhigiene de la empresa. Este es un proceso para que los empleados tengan presente siempre la seguridad dentro y fuera de la empresa y en sus hogares. ●

POR ALBERTO RODRÍGUEZ; IMAGEN: ADOBE STOCK