Publicado en Madrid el 10/03/2022

DXC Technology presenta en "RootedCON Madrid 2022" cómo aplicar de forma avanzada Machine Learning en Ciberseguridad

El protagonismo creciente del Machine Learning y su papel clave en la ciberseguridad fueron el eje de la ponencia de Jesús Domínguez Belinchón, responsable de Identidad Digital dentro del área de Ciberseguridad de DXT Technology, en el marco del RootedCON Madrid 2022 que se clausura el próximo sábado

Bajo el enunciado “Desde los inicios de Akinator a poder ser Tom Cruise en Tinder”, Jesús Domínguez Belinchón repaso la historia reciente del ML, empezando en el ámbito lúdico con el famoso Akinator de 2007, “un juego capaz de leer el pensamiento” al desarrollo de Shazam, “la aplicación que identifica canciones”, el más reciente autopilot de Tesla, y el último gran logro, el “Deep Fake”.

Un recorrido que lleva a las aplicaciones más innovadoras y actuales del ML dentro del ámbito de los EDR (Endpoint Detection and Response), una tecnología de ciberseguridad que monitorea continuamente un "punto final" para mitigar amenazas cibernéticas maliciosas.

Según Jesús Domínguez Belinchón, lo próximo que se verá son ataques de phishing en el ámbito de las videoconferencias “donde creeremos estar hablando con alguien que no es quien dice ser”.

DXC, patrocinadora del evento, analizó las diferencias entre tres tecnologías muy próximas como la IA, el Machine Learning y el Deep Learning y explicó errores frecuentes en la aplicación de estas tecnologías en ámbitos más comerciales, en campos como el reconocimiento facial, el ocio, los robots domésticos o los vehículos autónomos que bien fallan o abren puertas a los ciberdelincuentes.

Machine Learning y Ciberseguridad

Al abordar el papel del ML en la ciberseguridad, Domínguez Belinchón señaló que hasta hace poco los antivirus se basaban en listas negras “y hoy utilizan la capacidad del ML para detectar amenazas: cuando veo un pájaro que anda como un pato, nada como un pato y grazna como un pato, lo llamo pato. Si algo tiene pinta de ser un virus, es un virus, ya que el motor ha sido entrenado para detectar una amenaza en sus miles de variantes desde el momento 0, lo que permite parar la infección”.

El ponente destacó las capacidades de identificación de ataques y vigilancia digital del ML y explicó el liderazgo y expertise de DXC y su oferta de soluciones end-to-end y servicios de consultoría en ciberseguridad.

“Gracias a la capa de aprendizaje y obtención de patrones, se llega a crear una baseline en relación a la cual, cualquier desviación que se produzca puede indicar una situación anómala que puede incurrir en un ataque, fuga de información o cualquier otro riesgo de Seguridad”, explicó.

Domínguez Belinchón finalizó su intervención hablando “del futuro que nos espera”, donde "nos enfrentaremos a los riesgos provocados por las debilidades de determinados modelos generados por la IA y los Deep Fakes, que permiten simular identidades en fotografías y videos, personas que no existen o clonaciones de voz que pueden llevar a la ciberextorsión, los perfiles falsos en RRSSS, las fake news, la violación de los accesos biométricos y al daño reputacional de las empresas".

Datos de contacto:
María Guijarro
622836702

Nota de prensa publicada en: Madrid

Categorías: Nacional Telecomunicaciones E-Commerce Ciberseguridad