Publicado en Madrid el 14/10/2024

DXC Technology identifica cinco tendencias en ciberseguridad que marcarán el futuro a partir de 2025

Octubre es el Mes de la Concienciación sobre la Ciberseguridad, lo que representa una excelente oportunidad para que las organizaciones, tanto públicas como privadas, revisen sus objetivos de ciberseguridad, evalúen sus avances y se preparen para los retos futuros. Presentan cinco tendencias emergentes que están transformando la forma en que se dirigen los programas de seguridad para defenderse de las ciberamenazas

1. La IA es un actor clave en la lucha contra la ciberdelincuencia

La IA ofrece importantes ventajas gracias a su capacidad para procesar grandes cantidades de datos, identificar patrones y detectar indicios de un intento de ataque. También es una herramienta útil para detectar actividades maliciosas en un sistema o red y detectar anomalías o comportamientos sospechosos.

Además, la IA automatiza muchas tareas manuales y laboriosas de ciberseguridad, liberando tiempo y recursos para que los equipos de ciberseguridad se centren en otros aspectos clave de su trabajo.

Pero mientras la industria de la ciberseguridad se centra en cómo utilizar la IA para detener a los malos actores, los ciberdelincuentes a menudo utilizan la propia IA para aumentar la velocidad, la escala y la intensidad de sus ataques.

Por ejemplo, los correos electrónicos de phishing han evolucionado de simples correos engañosos a otros más avanzados, difíciles de detectar y mucho más peligrosos. Los atacantes también utilizan con éxito los deepfakes -una forma de IA que puede usarse para crear imágenes, sonidos y vídeos engañosos convincentes- para perpetrar fraudes o manipular a la audiencia para que actúe.

Y la naturaleza adaptativa de la IA es una de sus características más potentes en los ataques de ingeniería social, que manipulan a las personas para que faciliten información sensible o pongan en peligro la seguridad.

Al utilizar la IA en estos ataques, los ciberdelincuentes pueden parecer más creíbles y dignos de confianza, lo que lleva a más víctimas a caer en intentos de fraude o manipulación, que podrían comprometer el sistema.

2. Ciber, cibernético en todas partes

Ahora más que nunca se está más conectado a los teléfonos, aplicaciones, canales sociales, servicios de mensajes de texto y otras cosas, lo que puede tener consecuencias devastadoras para las

organizaciones y las personas si no se aplica una adecuada concienciación cibernética.

Y el aumento de los incidentes de ciberseguridad ha coincidido con el cambio al trabajo a distancia, ya que los delincuentes tratan de aprovechar la mayor superficie de ataque disponible para atacar. La seguridad perimetral desplegada en la oficina ya no sirve para defender adecuadamente a los empleados en este nuevo entorno o con las modernas capacidades interconectadas.

Se utilizan los teléfonos y las aplicaciones que contienen para casi todo: desde recibir actualizaciones en directo y mensajes de texto de amigos en las redes sociales hasta publicar actualizaciones de trabajo en LinkedIn o participar en aplicaciones de juegos. "Esto ha aumentado las posibilidades de que los agresores se fijen en ti y te ataquen a ti o a los miembros de tu familia para cometer fraudes o abusos online".

Por ejemplo, un solo clic en un enlace aparentemente inofensivo en WhatsApp puede abrir la puerta a las ciberamenazas y comprometer la información personal y, potencialmente, poner en riesgo los datos de una organización. "Y al compartir en exceso información sensible sobre tus acontecimientos vitales o tu trabajo en los canales sociales, puedes ponerte en peligro a ti mismo y a tu empresa".

Durante años se ha tratado de controlar los dispositivos y sistemas de Shadow IT en el lugar de trabajo que se conectan a las redes sin permiso, lo que puede dar lugar a vulnerabilidades de seguridad, problemas de cumplimiento y un aumento del riesgo de violación de datos. "Ahora, nos enfrentamos a la IA en la sombra (el uso de sistemas y herramientas de IA dentro de una organización sin aprobación o supervisión formal), que es un problema creciente y tiene consecuencias reales en torno a la confidencialidad de nuestros datos, y debemos implementar capacidades para detectar y controlar continuamente posibles ciberataques".

3. Los ataques pueden dirigirse contra infraestructuras críticas -y contra los hogares-
Cuando se va la luz o se corta el gas, es poco probable que la mayoría de la gente piense que es el resultado de un fallo de ciberseguridad industrial. Pero la tecnología operativa es un campo de batalla emergente para los ciberataques, ya que los sistemas que controlan y automatizan las fábricas y las infraestructuras civiles críticas (incluidas las centrales eléctricas, las plantas de tratamiento de agua y las presas) se están convirtiendo en un objetivo.

Con unos actores de amenazas empeñados en causar daños a nuestra sociedad, hay que estar preparados para responder a este tipo de incidentes y recuperarse de ellos con la mayor eficacia posible, minimizando al mismo tiempo las pérdidas.

Y con las continuas tensiones geopolíticas, la amenaza cibernética de la OT podría seguir creciendo, presionando a las industrias para que se aseguren de ir un paso por delante mediante la protección de la ciberseguridad en todas sus operaciones.

4. Los acontecimientos mundiales pueden aumentar el nivel de amenaza

En tiempos de crisis, es habitual un recrudecimiento de los ciberataques. Los actores de las amenazas suelen trabajar duro aprovechándose de personas, sistemas y recursos gubernamentales vulnerables para obtener beneficios financieros, políticos o de otro tipo.

Como resultado, los datos de muchas empresas, la información de acceso potencial, la información de clientes, el código fuente y otros datos críticamente sensibles podrían acabar en manos de delincuentes o adversarios patrocinados por el Estado que quieren hacer daño.

Estos ataques pueden tener profundas implicaciones para las infraestructuras críticas y los sectores industriales de todo el mundo. Por ejemplo, en lugar de dirigirse directamente a los usuarios finales, los atacantes comprometen ahora la propia cadena de suministro, convirtiéndose en un vector primario para las violaciones de datos a gran escala y los incidentes cibernéticos. Estos efectos en la cadena de suministro afectan profundamente al panorama tecnológico moderno, que se basa en un modelo de responsabilidad compartida.

5. La IA es un multiplicador de fuerza

A medida que las organizaciones se enfrentan a la complejidad de las crecientes ciberamenazas, necesitan personas con las capacidades adecuadas para proteger sus datos y sistemas.

Se oye hablar mucho de cómo se está ampliando la brecha mundial de competencias en ciberseguridad, lo que deja a muchas organizaciones vulnerables ante las crecientes ciberamenazas. Y la falta de profesionales cualificados se debe en gran medida a lo rápido que han evolucionado el sector de la ciberseguridad y las ciberamenazas. Casi de la noche a la mañana, las empresas se han dado cuenta de que necesitan un profesional dedicado a la ciberseguridad -o todo un equipo- en plantilla.

Una forma de gestionarlo es ampliando el grupo de candidatos para incorporar a los más jóvenes y formarlos en el puesto de trabajo. Esto puede incluir a candidatos que quizá no tengan los conocimientos especializados necesarios, pero que tienen potencial analítico, capacidad para resolver problemas y promesa técnica. Y si se imparte la formación adecuada a los empleados actuales, las organizaciones pueden facilitarles la movilidad profesional y convertirlos en la primera línea de defensa frente a posibles amenazas.

Además, la IA y el aprendizaje automático pueden funcionar como un multiplicador de fuerza para los equipos de seguridad más pequeños, lo que da a las organizaciones una mejor oportunidad contra las cepas más nuevas de malware.

No se trata de sustituir unos conocimientos valiosos y escasos, sino de aumentarlos mediante el uso de la IA para ayudar a los sobrecargados analistas de seguridad, profesionales de gestión de identidades y personal de respuesta a incidentes, que necesitan clasificar una cantidad cada vez mayor de información para hacer su trabajo. Y con la ayuda de la IA para automatizar las funciones de los analistas a la velocidad de la máquina, los equipos de seguridad pueden centrar su atención en tareas de mayor valor.

Datos de contacto:
María Guijarro
GPS Imagen y Comunicación, S.L.
622836702

Nota de prensa publicada en: Madrid

Categorías: Nacional Inteligencia Artificial y Robótica Madrid Ciberseguridad Otros Servicios Innovación Tecnológica Digital