EL TRABAJO
Desde 1929 informando al Valle de Aconcagua

Fecha: 06/11/2024 Audiencia: 8.700 Sección: OPINION
Vpe: $325.027 Tirada: 2.900 Frecuencia: 0
Vpe pág: $990.000 Difusión: 2.900
Vpe portada: $990.000 Ocupación: 32,83%

Cómo aprovechar la IA para avanzar en la ciberseguridad

Por: Alfredo Taborga, Gerente de Soluciones para la Protección de Datos en Dell Technologies

Las organizaciones están involucradas en una partida de ajedrez de alto riesgo contra ciberdelincuentes que utilizan Inteligencia Artificial (IA). Si bien esta tecnología ofrece un inmenso potencial para impulsar la innovación y la eficiencia en todas las industrias, también introduce una nueva generación de amenazas cibernéticas. Según el estudio Catalizadores de Innovación de Dell Technologies, en América Latina el 65% de los líderes encuestados teme que la GenAI introduzca nuevos retos a nivel de seguridad y privacidad.

Los ataques habilitados por GenAI presentan algunos desafíos únicos para las organizaciones. Por ejemplo, las campañas de phishing son cada vez más sofisticadas y la GenAI permite a los estafadores imitar mejor el comportamiento humano. Con la tecnología actual, algunos ciberdelincuentes realizan *deep fakes* para imitar a amigos, familiares o colegas. A nivel de software, también se observan casos de malware que se adapta de tal forma que no se logra una detección exitosa.

Ante este escenario surge la pregunta, ¿Cómo deberían responder las organizaciones ante los ataques actuales, pero aún más importante, cómo pueden estar cada vez mejor preparadas?

1- Fortalecer las prácticas de seguridad para la adopción de la IA

Si bien no existe una «solución milagrosa», es necesario comenzar a implementar buenas prácticas de seguridad, especialmente a medida que las organizaciones aceleran la adopción de la IA.

Comience garantizando que el entorno y el patrimonio de TI sean seguros tanto a nivel de diseño como de desarrollo e implementación del producto. La incorporación de funciones de seguridad como la autenticación multifactor y los controles de acceso basados en roles agrega otra capa para minimizar las vulnerabilidades, además garantiza un monitoreo continuo para detectar y responder ante un ataque.

Las organizaciones también están adoptando cada vez más arquitecturas de Zero Trust para fortalecer sus entornos, enfoque que funciona según el principio de que no se confía en ninguna entidad dentro o fuera de la red de forma predeterminada y que requiere verificación para acceder a los recursos de la red. La implementación de Zero Trust reduce efectivamente el riesgo de ataques cibernéticos al permitir solo actividades verificadas y necesarias.

2- Adopte soluciones de seguridad que incorporen IA

Una vez que tenga una base de seguridad sólida, adopte la misma tecnología que los actores de amenazas usan contra nosotros: la IA. La incorporación de soluciones de seguridad habilitadas por la IA puede ayudar a las organizaciones a desarrollar ciber resiliencia y mantenerse por delante de los actores de amenazas.

La seguridad habilitada por la IA son soluciones efectivas que las organizaciones pueden usar de manera proactiva y reactiva para identificar y responder a las amenazas. Al equipar a sus colaboradores con herramientas que utilizan capacidades de aprendizaje automático, autoaprendizaje y defensa adaptativa, será posible detectar y responder mejor a las amenazas.

3- Añada elementos humanos en la seguridad de la IA

Además de construir una base de seguridad sólida, las organizaciones deben reconocer que los empleados son su primera línea de defensa. Cada trabajador necesita una comprensión básica de cómo la IA hace que las amenazas sean más sofisticadas, cómo detectarlas y qué hacer cuando algo no parece correcto. Esto se volverá más importante a medida que los atacantes desplieguen ataques avanzados de suplantación de identidad creados por deepfakes que añaden una fachada convincente a las bien practicadas técnicas de ingeniería social de los delincuentes. Los profesionales de la seguridad también requieren capacitación específica en IA para tener el conocimiento y las habilidades necesarias para comprender cómo los posibles atacantes podrían usar la tecnología.

El panorama de la ciberseguridad está en constante cambio. Las organizaciones que priorizan la seguridad basada en IA y una cultura de aprendizaje continuo están mejor posicionadas para navegar en el cambiante panorama de amenazas. En definitiva, adoptar un enfoque de seguridad proactivo y adaptable le permitirá a las empresas aprovechar con confianza el poder transformador de la IA y construir un futuro más re-