LA INFRAESTRUCTURA DE TI SE BLINDA CON IA

PANDUIT™

Algunos ataques a la infraestructura de TI pueden terminar en un verdadero desastre para quienes tienen bajo su responsabilidad la información de sus usuarios. Sin embargo, la situación puede ser aún más crítica si la información comprometida puede vulnerar la seguridad y estabilidad de una ciudad o de un país entero

La historia demuestra que los ataques dirigidos a la infraestructura utilizando tecnología informática son tan factibles y efectivos, e incluso más dañinos que los ataques físicos que usan armamento convencional.

También es importante resaltar que los ataques no se perpetran exclusivamente a los organismos gubernamentales sino también a entidades que pongan en riesgo las finanzas, la salud o los bienes tanto del estado como de las empresas y la sociedad en general.

Latinoamérica es un escenario crítico en el que los ataques a baluartes estratégicos para la gobernabilidad de las naciones.

El caso de Costa Rica, que comprometió varios ministerios de la nación y otras entidades administrativas, fue seguido por ataques a otras naciones: Colombia, Ecuador, Bolivia, Chile, México, han sido blanco de importantes ataques a entidades críticas tanto públicas como de defensa y ahora las naciones de América Latina tienen como parte de su rutina de defensa estar al tanto de los riesgos constantes que yacen en la Red.

Según la Organización de Estados Americanos, OEA, en su estudio **Las consideraciones de los ataques de *Ramsonware* en las Américas** afirma que en la región existen organizaciones como Guacamaya dedicadas al activismo digital utilizando el sabotaje o la publicación de información de valor de entidades públicas o financieras; también existen grupo como Conti, de origen ruso y dedicado al robo y el tráfico ilegal de la información.

Los casos se hacen más preocupantes al agregar **Inteligencia Artificial** a la ecuación de defensa, pues este nuevo componente exige nuevos esfuerzos por parte de las entidades que se encargan de prevenir el éxito de los ataques sin importar de dónde provengan.

De cualquier manera, es necesario que las naciones afronten cualquier tipo de ataque. Por esto, la OEA ha llegado al despliegue de un modelo que proteja la infraestructura crítica de las naciones.

> Una estrategia nacional servirá para incorporar la protección y la resiliencia de las infraestructuras críticas en otros planes nacionales al comprender los riesgos conexos, identificar oportunidades para que diferentes actores públicos y privados refuercen la seguridad y la resiliencia y servirá también como base para los cambios y decisiones que se requieran en los ámbitos financiero, político o normativo. En la estrategia pueden tratarse temas como la mitigación, la respuesta, la recuperación o la adaptación a las condiciones e incertidumbres futuras.

es lo que concluye la Comisión de Seguridad Hemisférica del Consejo Permanente de la OEA en el documento *Guía práctica para la protección de infraestructura crítica contra todo tipo de peligro*, presentado en febrero 24 de 2024

G2.0

La infraestructura de TI se protege con IA

La Inteligencia Artificial puede mejorar significativamente la infraestructura de tecnología de la información para la defensa al mejorar la ciberseguridad, el análisis predictivo y la conciencia operativa. **Aquí hay algunas formas en que la IA puede mejorar la infraestructura de defensa:**

Detección de amenazas: Los algoritmos de IA destacan en el procesamiento de grandes cantidades de datos para identificar patrones indicativos de amenazas cibernéticas en tiempo real.

Detección y prevención de intrusiones: La IA puede analizar el comportamiento de la red para identificar nuevos patrones de ataque, haciendo que los sistemas de defensa sean más resilientes.

Gestión de vulnerabilidades: Las herramientas impulsadas por IA pueden automatizar la exploración de vulnerabilidades, priorizar las vulnerabilidades y sugerir estrategias de remedio de manera eficiente.

Caza de amenazas: La IA complementa a los analistas humanos en descubrir patrones ocultos y vectores de ataque potenciales para un enfoque de defensa proactiva.

Respuesta a incidentes: La IA puede automatizar tareas de respuesta a incidentes como la triage de alertas y acciones de respuesta, reduciendo los tiempos de respuesta y mejorando los procesos de toma de decisiones.

Estrategias de ciberseguridad para las naciones

De acuerdo con el *Government Technology Indider*, la IA debe tomarse como una de las principales herramientas para la protección de la infraestructura de TI y de todas las infraestructuras críticas de una nación y sus principales funciones en la actualidad se centran en:

Análisis predictivo: La IA puede mejorar las capacidades de análisis predictivo para una mejor planificación estratégica y anticipación de amenazas.

Conciencia operativa: La IA ayuda a mejorar la conciencia operativa al procesar y analizar vastas cantidades de datos para la toma de decisiones informadas.

Consideraciones de implementación: La firma de consultoría *ValueSEC*, enfoca su análisis hacia los temas que deben tratar las naciones para mejorar el impacto de sus objetivos de defensa en estos dos frentes:

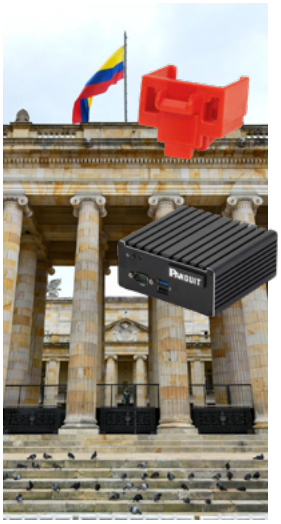
Directrices éticas: Establecer directrices éticas para el uso de la IA, abordando los sesgos, priorizando los derechos humanos y garantizando la transparencia en las operaciones es crucial.

Educación y formación: Invertir en educación y formación de la fuerza laboral para mejorar la experiencia técnica en la utilización efectiva de aplicaciones de IA.

Al aprovechar las tecnologías de IA de manera efectiva, la infraestructura de defensa puede fortalecerse para combatir las amenazas cibernéticas en evolución y mejorar las capacidades de seguridad nacional. La integración de la IA en los sistemas de defensa se considera un imperativo estratégico para abordar desafíos complejos con mayor eficiencia, precisión y rapidez.

¿Cómo mejorar la seguridad desde la infraestructura?

Panduit ofrece diversas soluciones de ciberseguridad para mejorar las medidas de seguridad de la información en la infraestructura de TI. Algunas soluciones específicas incluyen:



Dispositivos de Bloqueo: Panduit proporciona dispositivos como enchufes RJ45 de bloqueo y dispositivos de bloqueo para asegurar conexiones, reducir el tiempo de inactividad de la red, prevenir brechas de seguridad de datos y proteger contra el robo de *hardware*.

Software IntraVUE™: Este *software* de Panduit aumenta la conciencia sobre la infraestructura física, ofreciendo visibilidad en los dispositivos y niveles de conectividad para identificar y resolver problemas rápidamente.

Soluciones de Seguridad de Infraestructura de Red: Panduit ofrece soluciones para mitigar riesgos en aplicaciones empresariales, de centros de datos y de automatización industrial, mejorando las medidas de seguridad de la información sin obstaculizar las mejoras del servicio o las inversiones en TI.

Estas soluciones contribuyen a **fortalecer la ciberseguridad en la infraestructura de TI** al proporcionar herramientas para asegurar conexiones, aumentar la visibilidad en la infraestructura de red y mitigar eficazmente los riesgos de seguridad.