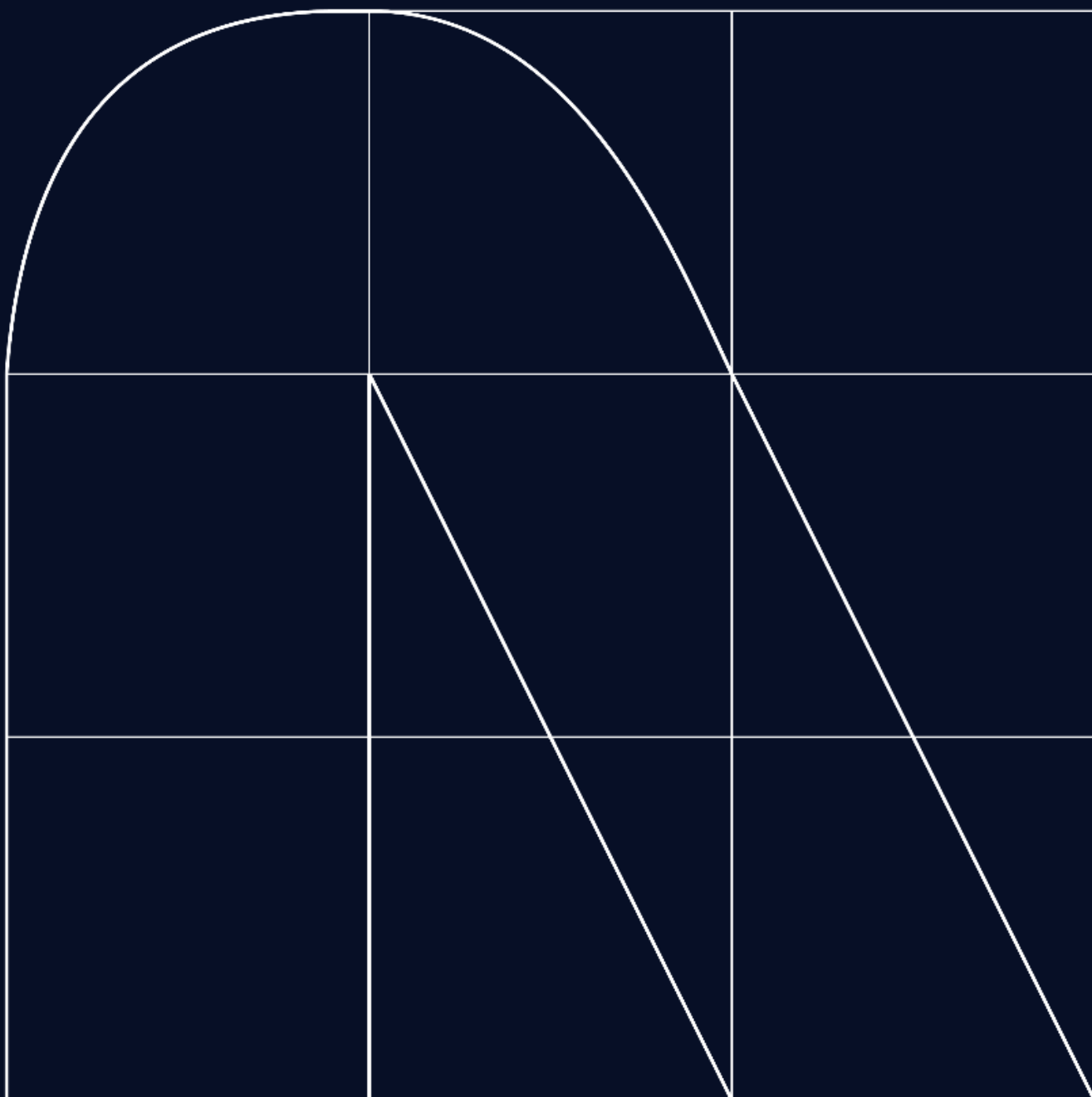
Número 92 | Julio 2024

NTT DATA

Radar

El magazine de ciberseguridad



El impacto de la inteligencia artificial en la ciberseguridad

Por David Sandoval Rodríguez-Bermejo

El impacto de la inteligencia artificial en la sociedad actual es innegable y deja atrás una época de cambios (internet, redes sociales, 5G ...), abriendo la puerta a un cambio de época. Si bien es cierto que esta tecnología es extremadamente potente, su nivel de madurez es aún bastante prematuro. Hasta hace unos años, trabajar con redes neuronales requería un nivel de conocimiento bastante técnico. Sin embargo, actualmente la inteligencia artificial se ha democratizado y ya no es necesario saber qué sucede bajo el capó para poder conducir el coche. Esta democratización unida a las capacidades digitales ya inherentes en la sociedad actual ha contribuido a que su adopción sea extremadamente rápida.

El problema de adoptar una tecnología de este calibre sin aportar formación ni concienciar a la población es bastante crítico. Desde el punto de vista de la productividad, al no comprender qué hay entre bambalinas no se le saca el máximo partido (por ejemplo, haciendo correctamente los prompts). Sin embargo, este desconocimiento tiene un impacto aún mayor desde el punto de vista de la ciberseguridad debido a los riesgos asociados que conlleva (y que pasan desapercibidos).

Integrar soluciones poco maduras en entornos de producción implica ampliar la superficie de ataque de forma exponencial. Actualmente, la literatura está investigando cómo atacar tanto los modelos como sus integraciones dentro del ecosistema de un cliente. En esta línea se han cometido distintos ataques como: extraer innumerables licencias de Windows; romper las protecciones de los modelos para responder crímenes de la humanidad; o comprar un coche por un euro a través de un chatbot de una empresa.

El problema es que el riesgo no está sólo en el uso (desde el punto de vista del consumo de tecnología), sino también en su uso como palanca para traccionar y optimizar nuestros esfuerzos productivos. Muchas compañías hacen uso de LLMs para desarrollar sus productos sin comprobar y auditar correctamente el código.

Es sabido que muchos de estos modelos de generación de código se han entrenado con Github, Gitlab y otros repositorios públicos (de los que se estima que el 70% de estos tiene alguna vulnerabilidad). Esto implica que, probabilísticamente hablando (y con la madurez actual), el código que genere será vulnerable.

Otro ataque interesante fruto de la falta de concienciación sobre esta tecnología se da bajo el concepto de alucinación. Muchas veces (debido a su funcionamiento) la IA se “inventa” las respuestas. A priori, esta invención no supone un problema, la respuesta es errónea y se descarta. Sin embargo, muchos actores maliciosos han decidido sacar provecho a las alucinaciones generando estos paquetes que se inventa la IA (y que a priori no deberían existir) para saltarse todas las protecciones de seguridad de una forma rápida y sencilla.

Por último, otro riesgo crítico de la IA está relacionado con el honor y la reputación. Como consecuencia de las capacidades generativas de la IA se pueden clonar voces, vídeo y suplantar a personas en distintos contextos. Este hecho, sumado a la facilidad de obtener datos para realizar el ataque (a través de las redes sociales), rompe con la frontera entre la realidad y el mundo virtual, y nos deja desamparados ante estos ataques. Si bien es cierto que el ataque no es real, sus daños sí lo son.

El objetivo de este artículo no es meter miedo sobre la inteligencia artificial sino concienciar sobre su mal uso y advertir que, debido a su nivel de madurez, se debe utilizar con mucha cautela. Para mitigar estos riesgos, se recomienda adoptar metodologías existentes como OWASP LLMs en las que se proporcionan las recomendaciones básicas para implantar soluciones de IA generativa basadas en LLMs en los entornos de producción.

Suscríbete a RADAR

David Sandoval Rodríguez-Bermejo
Cybersecurity Expert Architect

LA IA GENERATIVA ESTÁ REVOLUCIONANDO EL MERCADO, Y LOS ATACANTES LO SABEN

Cibercrónica por Alejandro Bernal Almeyda

Un reciente estudio de la IBM Institute for Business Value1 puso en evidencia que el 64% de los CEOs se enfrenta a una constante presión de sus inversores, acreedores y prestamistas para acelerar la adopción de IA generativa en sus compañías; en contraparte, el 84% manifestó preocupación respecto a los ataques de ciberseguridad a los que podría conducir esta adopción.

Parte fundamental de una adopción de la IA generativa a nivel corporativo es entender los potenciales riesgos asociados a esta tecnología emergente que deben ser mitigados, algunos de estos riesgos asociados a ataques específicamente diseñados para este tipo de IA tal como el prompt injection, y otros asociados a explotación de vulnerabilidades dentro de un esquema de ataque a la cadena de suministros (supply chain attack).

Los ataques de tipo prompt injection manipulan los LLMs (Large Language Models) a través del empleo de entradas maliciosas con el objetivo de anular los prompts del sistema; los prompts son las instrucciones iniciales que fueron provistas a la IA por su desarrollador, y su evasión puede resultar en la IA generando respuestas engañosas o revelando información sensible.

En setiembre del 2023, un estudiante universitario llamado Kevin Liu, de la Stanford University, llevó a cabo un prompt injection hacia el chat de Bing (Microsoft): al pedirle a Bing que “ignore instrucciones previas” y que escriba lo que está al “principio del documento anterior”, Liu incitó al modelo de IA que divulga sus instrucciones iniciales, que fueron escritas por OpenAI o Microsoft y que generalmente están ocultas al usuario.

Recientemente, mientras esta crónica se escribe, The Synopsys Cybersecurity Research Center (CyCR) anunció la presencia de un nuevo prompt injection que explota una vulnerabilidad de seguridad para robar datos; esta vulnerabilidad, que tiene reservado el código CVE-2024-5184, se encontró en el servicio de EmailGPT, un servicio de API y una extensión de Google Chrome que ayuda a los usuarios a escribir correos de Gmail usando los modelos GPT de OpenAI.

Alrededor de los LLMs aparecen una serie de componentes complementarios que permiten extender sus capacidades, entre ellos los agentes, chains y plugins que explotan el poder de las LLMs y permite a los usuarios construir aplicaciones que busquen información en una base de datos o que resuelvan un problema; el riesgo se empieza a dar cuando esas extensiones al LLM se construyen sin un concepto de seguridad: dado que la salida de un LLM sirve como entrada hacia estas extensiones, y la salida del LLM proviene de una entrada hecha por un usuario (un prompt), un atacante puede alterar el comportamiento de uno de estos componentes si ha sido diseñado de manera incorrecta.

Algunos ejemplos se pueden encontrar en documentación pública:

- Tres vulnerabilidades de LangChain identificadas y verificadas por el NVIDIA AI Red Team:
    - CVE-2023-29374 - el llm_match permite la ejecución remota de código arbitrario (RCE)
    - CVE-2023-32786 - APIChain.from_llm_and_api_docs permite explotación de SSRF (server-side request forgery)
    - CVE-2023-32785 - SQLDatabaseChain permite los ataques de inyección SQL

- Tres vulnerabilidades reportadas por Protect AI en mayo del 2024 a través de su plataforma bug bounty llamada huntr, que impacta a aplicaciones LLM open-source:
    - CVE-2024-4078 - esta vulnerabilidad puede permitir a un atacante la ejecución remota de código arbitrario en el servidor (LoLLMs)
    - CVE-2024-3153 - esta vulnerabilidad permite a un atacante apagar el servidor a través de un endpoint para cargar archivos (AnythingLLM)
    - CVE-2024-3104 - esta vulnerabilidad puede permitir a un atacante la ejecución remota de código arbitrario en el servidor (AnythingLLM)
- The Synopsys Cybersecurity Research Center (CyCR) descubrió una vulnerabilidad en la aplicación EmbedAI, aplicación que permite a los usuarios interactuar con los documentos a través de capacidades LLM. Esta vulnerabilidad ha sido catalogada con el código CVE-2024-5185 y, de ser explotada, puede conducir a accesos no autorizados o ataques de data poisoning.

La adopción de la IA generativa debe ir acompañado de una estrategia de seguridad similar a cualquier otra aplicación convencional, que incluya una protección end-to-end desde la concepción, aplicando conceptos de Zero Trust, principio de mínimo privilegio, Security by Design, entre otros.

Alejandro Bernal Almeyda
Cybersecurity Lead Architect

Inteligencia Artificial: Navegando la frontera entre la defensa y el ataque

Por Mafalda Maciel Querido

Hemos comprobado que la Inteligencia Artificial no es solo una nueva palabra de moda o una tendencia "sexy" en el mundo de las tecnologías. De hecho, la Inteligencia Artificial incorpora campos que ya conocemos desde hace mucho, como el Aprendizaje Automático (Machine Learning) y el Aprendizaje Profundo (Deep Learning), con pruebas demostradas, y ahora tiene un nuevo enfoque. Sin embargo, su rápida evolución y uso por parte de la sociedad, como ya han demostrado varios estudios, nos preocupa a los profesionales de la ciberseguridad.

Podemos ver el problema desde dos perspectivas. Por un lado, sabemos que esta tecnología cambiará la forma en que trabajamos, acelerará procesos lentos, permitirá aumentar la productividad y combatir la falta de profesionales en este campo. Las organizaciones que no se suban al tren de la innovación, inevitablemente quedarán rezagadas, como ya hemos visto históricamente. Por otro lado, sabemos que la línea que separa los aspectos positivos de los peligros inminentes que nos trae la Inteligencia Artificial es delgada, y que, por lo general, los atacantes siempre intentan estar un paso adelante. Como cualquier héroe, la Inteligencia Artificial también tendrá su villano.

Son innegables los impactos positivos que la Inteligencia Artificial aporta a la ciberseguridad: una mayor y mejor automatización en la detección y respuesta a amenazas, con la posibilidad de analizar volúmenes masivos de datos a velocidades sin precedentes y, por lo tanto, identificar anomalías de manera más rápida, lo que permite a los equipos de seguridad anticipar riesgos y amenazas de manera más efectiva, y también ayudar en esta crisis de recursos humanos especializados que estamos experimentando; un análisis de patrones y comportamientos más rápido; sistemas adaptativos que evolucionan para hacer frente a nuevas amenazas; aumento de la previsibilidad y de la capacidad y velocidad de la toma de decisiones basada en datos e información concreta. En resumen, la Inteligencia Artificial puede y debe ser utilizada como una herramienta aliada, que nos ayuda en términos de productividad, análisis de información y rapidez de respuesta en este entorno de rápida transformación en el que vivimos.

Sin embargo, como cualquier tecnología, también trae nuevos riesgos y, para la ciberseguridad, representa un nuevo factor de rapidez, sofisticación y alcance de los ataques. A medida que las barreras de defensa evolucionan, también lo hacen las tácticas utilizadas por agentes maliciosos. La automatización lleva a la explotación de vulnerabilidades a gran escala que, beneficiándose también de la adaptabilidad de los sistemas, aprenden nuevas formas de sortear las barreras de seguridad a medida que las encuentran; tácticas de engaño y evasión que imitan el comportamiento humano legítimo, dificultando su detección; el reconocimiento orientado por Inteligencia Artificial que permite un análisis exhaustivo y más rápido de posibles objetivos, identificando vulnerabilidades y puntos de entrada en la infraestructura de una organización; la capacidad de crear mensajes de phishing, smishing y vishing altamente dirigidos y convincentes, que junto con el uso de deepfake, eleva todo el campo de la ingeniería social a un nivel más sofisticado, impredecible y difícil de detectar, y trae una nueva disrupción en lo que respecta a las precauciones y mecanismos de defensa con los que debemos dotar a nuestros colaboradores.

Además del conflicto moral y ético que surge del uso de la Inteligencia Artificial Generativa -sobre la cual cada vez más instituciones, estatales y no estatales, están investigando- y de los peligros relacionados con la compartición no intencionada de datos personales e información sensible, ya sea por desconocimiento, falta de medidas tecnológicas para su prevención, o incluso descuido, surge una exposición aumentada de lo que muchos consideran el eslabón más débil, y para otros, la primera línea de defensa de las organizaciones: el elemento humano.

El uso masivo de esta nueva tecnología acaba de comenzar, y ya tiene un alcance mayor que cualquier otra tecnología o plataforma vista anteriormente, y las consecuencias ya se están sintiendo. Aunque aún no existen estudios de gran alcance sobre el impacto que la Inteligencia Artificial tendrá en la seguridad de la información y la ciberseguridad desde el punto de vista del riesgo humano, ni análisis estadísticos muy concretos, ya están surgiendo los primeros casos de ataques perpetrados con base en tecnologías de Inteligencia Artificial Generativa.

La concienciación de los colaboradores y de la sociedad en general en materia de Seguridad de la Información sigue siendo uno de los puntos menos evidentes y de mayor dificultad de ejecución. Aún tenemos el desafío de preparar y alertar a los colaboradores de las organizaciones sobre los riesgos y la importancia de la seguridad, y hacerlo eficazmente y que dé resultados, resultados difíciles de medir, porque las variables son muchas y difíciles de cuantificar y calificar.

Entonces, ¿cómo debemos proceder frente a estas nuevas y mejoradas amenazas? ¿Cómo enseñamos a detectar ataques cada vez más creíbles, a simple vista? ¿Cómo detectamos comportamientos anómalos cuando cada vez se asemejan más a los nuestros? ¿Tendremos que reinventarnos, y reinventar la forma en que concienciamos a nuestros colaboradores? En este momento, surgen dudas para las cuales, por ahora, tenemos pocas respuestas concretas.

Los equipos de seguridad deben repensar su enfoque, adoptando una postura proactiva y adaptándose a la nueva realidad generada por la implementación de tecnologías defensivas avanzadas, con un enfoque central en la maximización de la automatización, la detección de amenazas, la agilidad operativa y la mejora de la toma de decisiones. La necesidad apremiante de superar las limitaciones de recursos es, sin lugar a duda, un área donde la Inteligencia Artificial emerge como una aliada esencial.

La dependencia de la IA no solo como una solución para la falta de recursos, sino como un enfoque estratégico para enfrentar riesgos y amenazas en constante evolución, es imperativa. En este sentido, la reorganización de los equipos de seguridad debe incorporar no solo la implementación de tecnologías avanzadas, sino también la exploración continua de nuevas metodologías que estén alineadas con los desafíos emergentes.

La construcción de una cultura de seguridad sólida es crucial para la eficacia a largo plazo, involucrando no solo la capacitación de los colaboradores con conocimientos actualizados, sino también la promoción de una mentalidad vigilante en las actividades diarias, tanto profesionales como personales. Debemos fomentar el análisis crítico, la desconfianza constructiva y la aplicación de buenas prácticas en todos los aspectos de la vida cotidiana, estableciendo así una línea de defensa sólida.

En última instancia, la convergencia de la tecnología y la ciberseguridad es un área desafiante que requiere la unión estratégica de la Inteligencia Artificial con las capacidades humanas. Reconocer la inevitabilidad de esta batalla tecnológica de titanes y abrazar la Inteligencia Artificial como un aliado indispensable es la clave para fortalecer las organizaciones contra las amenazas emergentes.

Mafalda Maciel Querido
Cybersecurity Project Manager

Construyendo una inteligencia artificial segura y efectiva: La clave del AI TRiSM en la ciberseguridad moderna

Por Melanie Brenis Valencia

En los últimos años, la inteligencia artificial (IA) ha experimentado un crecimiento exponencial, transformando sectores clave y mejorando la eficiencia operativa de un sinfín de organizaciones. Sin embargo, ésta también ha traído consigo una serie de riesgos significativos, lo que puede ser evidenciado mediante los siguientes casos:

- Mayo 2022: El Departamento de Justicia de Estados Unidos hace público que el algoritmo PATTERN, utilizado para determinar la elegibilidad de liberación anticipada de determinadas personas en custodia federal, se encuentra siendo revisado por el sesgo racial que le es inherente. Según relatos de medios locales, el algoritmo PATTERN mostraba disparidades significativas al sobrestimar el riesgo de reincidencia criminal en minorías raciales.

- Febrero 2024: Se hace público un fallo judicial en contra de Air Canadá, debido a que su chatbot proporcionó información falsa sobre determinadas políticas de la aerolínea a un cliente. Según relatos de medios locales, el chatbot cometió graves errores al "alucinar" políticas inexistentes, lo que llevó al cliente a perder su vuelo. Dicho caso resaltó la importancia de la supervisión y verificación de la IA.

Como podemos apreciar, los riesgos y/o desafíos actuales entorno a la IA subrayan la necesidad de contar con enfoques robustos que puedan garantizar una implementación segura y efectiva, lo que es clave traer a colación el concepto de **AI TRiSM**.

En términos generales, AI TRiSM (AI Trust, Risk and Security Management, por sus siglas en inglés) es un conjunto de soluciones y/o marcos de trabajo enfocados **en asegurar la confianza (Trust), minimizar los riesgos (Risk) y garantizar el manejo de la seguridad (Security Management)** en el uso de sistemas de IA por parte de las organizaciones. Su objetivo es asegurar aspectos transversales de los sistemas de IA tales como gobernanza, confiabilidad, eficacia y protección de datos.

A través de los casos previamente mencionados, podemos advertir que los sistemas de IA pueden ser vulnerables a ataques malintencionados, sesgos inherentes e incluso fallos operativos que pueden comprometer la integridad de los datos y la confianza de quienes los utilizan o consumen. Precisamente, por ello, el concepto de AI TRiSM es relevante pues proporciona un conjunto de soluciones para gestionar y mitigar los riesgos de la IA, asegurando así que las implementaciones no solo sean efectivas en términos operativos y económicos, sino también seguras y éticas.

Ahora bien, para cumplir con tal objetivo, ¿qué engloba realmente el AI TRiSM? Éste se encuentra conformado por 4 pilares fundamentales, que, de manera sucinta, se resumen en los siguientes:

- **Explicabilidad y monitoreo de modelo:** Enfocado en lograr que los sistemas de IA sean más transparentes. Por un lado, la explicabilidad se refiere a que los sistemas de IA deben ser capaces de explicar sus decisiones y procesos internos de una manera clara y concisa a quienes los utilizan/consumen. Por otro lado, el monitoreo de modelo se refiere a la supervisión continua del rendimiento y el comportamiento de los sistemas de IA para detectar posibles sesgos, datos envenenados, fugas de información, entre otras cuestiones.

- **ModelOps:** Enfocado en la gobernanza end-to-end y gestión del ciclo de vida de los sistemas de IA, esto es, prácticas y procesos operativos para la implementación, gestión y mantenimiento de sistemas de IA en entornos de producción. ModelOps incluye actividades como el despliegue automatizado de modelos, la monitorización del rendimiento en tiempo real, la gestión de versiones y la optimización continua de los modelos.

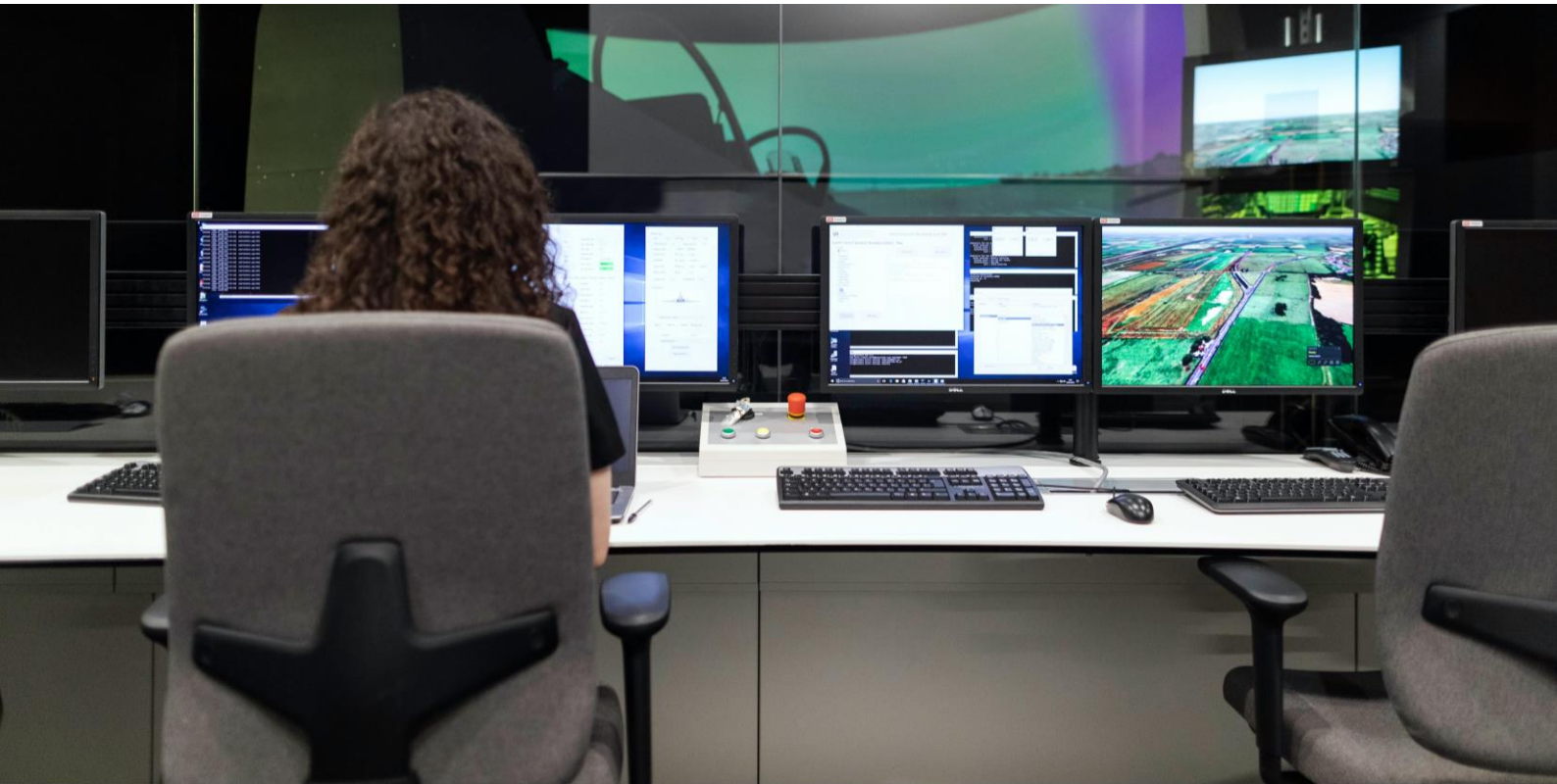
- **Seguridad de aplicaciones:** Enfocado en la detección y bloqueo de ataques hacia/sobre los sistemas de IA. Incluye medidas para protegerlos contra amenazas y vulnerabilidades, y de esa forma, garantizar la integridad, confidencialidad y disponibilidad de los datos que utilizan. Este pilar es de suma relevancia pues los ataques maliciosos hacia la IA conllevan pérdidas y daños no solo económicos, sino también reputacionales.

- **Privacidad:** Enfocado en la protección de la información personal y sensible utilizada en el desarrollo y despliegue de los sistemas de IA. Ello incluye el diseño de sistemas de IA que minimicen la recopilación y el uso de datos personales, así como la implementación de medidas de anonimización, encriptación y control de acceso para proteger la privacidad de los titulares de la información.

En ese sentido, podemos concluir que el AI TRiSM con los 4 pilares fundamentales que lo conforman, es clave para una gestión de la IA de manera efectiva, segura y ética, lo cual puede derivar en una ventaja competitiva para las organizaciones. Alineado a ello, según Gartner, para el 2026, los sistemas de IA de las organizaciones que operen la transparencia, la confianza y la seguridad lograrán una mejora del 50 % en términos de adopción, objetivos empresariales y aceptación de los usuarios.

Adoptar AI TRiSM no es la implementación de un conjunto de medidas técnicas, sino más bien un compromiso hacia un futuro digital confiable y ético.

Melanie Brenis Valencia
Cybersecurity Consultant



Retos de la ciberseguridad en la era de la inteligencia artificial: un camino hacia la democratización responsable

Tendencias por Mauro Pereira Almeida

En un mundo cada vez más digital, la proliferación de la Inteligencia Artificial (IA) ha impulsado la innovación y la eficiencia operativa de las organizaciones a niveles sin precedentes. Sin embargo, esta marea de progreso no está exenta de desafíos, especialmente en lo que respecta a la ciberseguridad. La democratización del acceso a la IA, aunque es un vector de inclusión digital, amplifica la necesidad de estructuras sólidas de seguridad de la información.

Uno de los retos más urgentes en este trayecto es la gestión y el control del acceso. En un contexto en el que la IA es capaz de procesar y analizar enormes volúmenes de datos a una velocidad vertiginosa, es crucial garantizar que solo los usuarios autorizados tengan acceso a información sensible y/o confidencial. Implantar accesos con privilegios mínimos y gestionar correctamente quién tiene acceso a qué es una premisa que no se puede pasar por alto. Mecanismos estrictos de identificación, autenticación y definición de privilegios de acceso son esenciales para evitar la exposición no deseada de datos y garantizar el cumplimiento de normativas estrictas como el Reglamento General de Protección de Datos (RGPD).

La clasificación y protección de la información es también un pilar crucial en este debate. Es esencial que las organizaciones implanten sistemas robustos capaces de identificar, clasificar y proteger la información, teniendo en cuenta su grado de sensibilidad. Este proceso debe ser continuo, adaptable y capaz de responder con prontitud a la dinámica volátil del ciberespacio.

Por otro lado, la transparencia y la formación son elementos claves en la gestión de los riesgos asociados a la IA. Las organizaciones deben invertir en la formación de sus empleados, no solo en términos de principios básicos de ciberseguridad, sino también sobre las implicaciones éticas y legales del uso de la IA. Crear una cultura consciente de la seguridad es vital para mitigar los riesgos y promover el uso responsable de la IA.

La colaboración entre las distintas partes interesadas -de los organismos reguladores, el mundo académico, la industria y la sociedad civil- es otro elemento crucial para construir un ecosistema de IA seguro y responsable. La creación de reglamentos, normas de seguridad y el intercambio de buenas prácticas son medidas esenciales para afrontar los retos inherentes a la ciberseguridad en el contexto de la IA.

En resumen, la democratización del acceso a la IA, si bien es un paso alentador hacia la inclusión digital, requiere un enfoque reflexivo y diligente de la ciberseguridad. Las organizaciones, como protagonistas en este campo, tienen la responsabilidad de incorporar prácticas de seguridad sólidas, fomentar la educación y colaborar activamente con la comunidad en general para garantizar que la revolución de la IA se desarrolle de forma segura y beneficiosa para todos. La concienciación, la formación y la colaboración multidisciplinaria son, por tanto, piedras angulares para garantizar que navegamos por las agitadas aguas de la innovación tecnológica con seguridad y confianza.

Artículo originalmente publicado en CNN Portugal en noviembre 2023

Mauro Pereira Almeida
Cybersecurity Director

Vulnerabilidades

Vulnerabilidad crítica en el plugin wpDataTables de WordPress

Fecha: 31 de mayo de 2024
CVE: CVE-2024-3820

CVSS: 10

CRÍTICA

Descripción

Se ha descubierto una vulnerabilidad crítica en el *plugin* wpDataTables – WordPress Data Table, Dynamic Tables & Table Charts Plugin para WordPress. Esta vulnerabilidad, identificada como CVE-2024-3820, se debe a un escape insuficiente en el parámetro proporcionado por el usuario '*id_key*' de la acción *AJAX wdt_delete_table_row*.

Este fallo podría permitir a atacantes no autenticados inyectar consultas SQL adicionales en las consultas existentes, lo que puede ser usado para extraer información confidencial de la base de datos.

Esta vulnerabilidad afecta únicamente a la versión premium del *plugin*.

Productos afectados

La vunerabilidad afecta a los siguientes productos:

- wpDataTables: versiones hasta la 6.3.1 (incluida).

Solución

Se recomienda a los usuarios afectados que actualicen a la versión 6.3.2, que ya ha sido lanzada por los desarrolladores del plugin con los parches de seguridad correspondientes.

- wpDataTables: Actualizar a la versión 6.3.2 y posteriores.

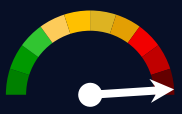
Además, se recomienda implementar medidas de seguridad adicionales, como el uso de *firewalls* para aplicaciones web (WAF), y la monitorización regular de los sitios web en busca de actividades sospechosas, realizando auditorías de seguridad periódicas.

Referencias

- nvd.nist.gov
- wpdatatables.com
- www.wordfence.com

Vulnerabilidad crítica en aplicaciones ThinkPHP

Fecha: 5 de junio de 2024
CVEs: CVE-2018-20062 y 1 más



CVSS: 9.8

CRÍTICA

Descripción

Se ha detectado una campaña de explotación activa dirigida a aplicaciones ThinkPHP vulnerables a CVE-2018-20062 y CVE-2019-9082 (vulnerabilidades publicadas hace varios años), orquestada por un grupo de ciberamenazas de origen Chino desde octubre de 2023. Los ataques provienen de IPs asociadas con servidores del proveedor "Zenlayer" en Hong Kong.

Los atacantes descargan un archivo ofuscado desde otro servidor ThinkPHP comprometido para obtener acceso inicial e instalan una *web shell* llamada "Dama" para mantener acceso persistente al servidor, permitiendo acciones como la escalada de privilegios y el escaneo de puertos de red.

Productos afectados

Las versiones de los productos afectados son las siguientes:

- ThinkPHP: versiones anteriores a 5.0.23
- NoneCMS: versiones anteriores a 1.3.0
- Open Source BMS: versiones anteriores a 1.1.1

Solución

Se recomienda a los usuarios afectados que actualicen a las versiones más recientes que no incluyen el código vulnerable:

- ThinkPHP 5.0.23 y posteriores
- NoneCMS 1.3.0 y posteriores
- Open Source BMS 1.1.1 y posteriores

Se aconseja a los usuarios verificar y limpiar sus sistemas de estas versiones afectadas.

Referencias

- nvd.nist.gov (CVE-2018-20062)
- nvd.nist.gov (CVE-2019-9082)
- www.akamai.com

Parches

ALTA

Parcheada vulnerabilidad *zero-day* en Check Point Gateway VPN

Fecha: 26 de mayo de 2024
CVE: CVE-2024-24919

Descripción

Check Point ha publicado un *hotfix* para el *zero-day* crítico en su producto VPN Security Gateway con IPsec, el cual permitía un acceso remoto no autorizado, pudiendo llevar a un atacante potencial a desplazarse lateralmente y obtener privilegios de administrador del dominio.

El fabricante ha indicado que, en un pequeño número de clientes, se han encontrado numerosos intentos de acceso no autorizado a los productos VPN intentando explotar esta vulnerabilidad.

Adicionalmente, Check Point ha creado un *script* de validación de acceso remoto que puede ser cargado en 'SmartConsole' y ejecutado para revisar los resultados.

Productos afectados

La vulnerabilidad afecta a los siguientes productos:

- CloudGuard Network
- Quantum Maestro
- Quantum Security Gateways
- Quantum Spark Appliances

Las versiones específicas afectadas son: R80.20.x, R80.20SP (EOL), R80.40 (EOL), R81, R81.10, R81.10.x, y R81.20.

Solución

Se recomienda encarecidamente actualizar a las siguientes versiones:

- Quantum Security Gateway y CloudGuard Network Security: R81.20, R81.10, R81, R80.40
- Quantum Maestro y Quantum Scalable Chassis: R81.20, R81.10, R80.40, R80.30SP, R80.20SP
- Quantum Spark Gateways: R81.10.x, R80.20.x, R77.20.x

Referencias

- support.checkpoint.com
- blog.checkpoint.com

ALTA

SolarWinds publica parches para múltiples vulnerabilidades

Fecha: 4 de junio de 2024
CVE: CVE-2024-28996 y 2 más

Descripción

SolarWindws ha informado en su boletín de seguridad nuevos parches para corregir 3 nuevas vulnerabilidades de seguridad que afectan a la plataforma SolarWinds Platform 2024 y al FTP Serv-U MFT. La actualización corrige múltiples vulnerabilidades de severidad alta.

A continuación, se detallan algunas de estas vulnerabilidades:

- En primer lugar, la vulnerabilidad CVE-2024-28996, descubierta por un miembro de la OTAN, podría permitir a un atacante realizar una inyección SQL, permitiendo de esta forma consultar la base de datos de SolarWinds para obtener información de red.

- La vulnerabilidad CVE-2024-28995, de tipo *Path Traversal*, permite a los atacantes acceder a directorios y archivos fuera del directorio raíz del servidor. La severidad de se basa en la baja complejidad del ataque al poder ser explotada de forma remota y sin interacción de ningún usuario.

Productos afectados

Los productos afectados por esta vulnerabilidad son los siguientes:

- SolarWinds Serv-U 15.4.2 HF 1 y versiones anteriores (CVE-2024-28995).
- Plataforma SolarWinds 2024.1 SR 1 y versiones anteriores (CVE-2024-28996, CVE-2024-28999 y CVE-2024-29004).

Solución

Aplicar las últimas actualizaciones disponibles en la versión SolarWinds 2024.2 lanzadas por el fabricante.

Referencias

- solarwinds.com
- documentation.solarwinds.com

Eventos

SANS London (1 y 6 julio)
El SANS London July 2024 es un evento que se llevará a cabo en Londres, Reino Unido, durante 5 días. Este evento, al cual se puede acceder también vía online, tiene como objetivo ofrecer entrenamientos prácticos en diversas áreas de ciberseguridad tales como gestión de incidentes, inteligencia de amenazas, análisis forense digital y entre otras.
Link

2024 DataConnect Conference (11-12 julio)
El DataConnect Conference 2024 tendrá lugar del 11 al 12 de julio en Columbus, Ohio, y está organizado por Women in Analytics. Este evento incluye conferencias magistrales, paneles y talleres en temas de data analytics, machine learning e inteligencia artificial. Es un foro inclusivo que promueve el aprendizaje, la colaboración y el networking entre profesionales de diversos sectores. Además, habrá una sesión de reclutamiento y un espacio para startups.
Link

AI Summit 2024 (17 julio)
El AI Summit 2024 se celebrará el 17 de julio en San Diego, en el marco de la Esri User Conference. Este evento, que también puede ser asistido de manera virtual, explorará los últimos avances en GeoAI e IA generativa, y su aplicación en ArcGIS. Los asistentes aprenderán sobre nuevas herramientas y técnicas para la extracción y análisis de datos, y podrán escuchar casos de éxito en el uso de IA. Además, se ofrecerán oportunidades para expandir redes profesionales y colaborar con expertos de la industria.
Link

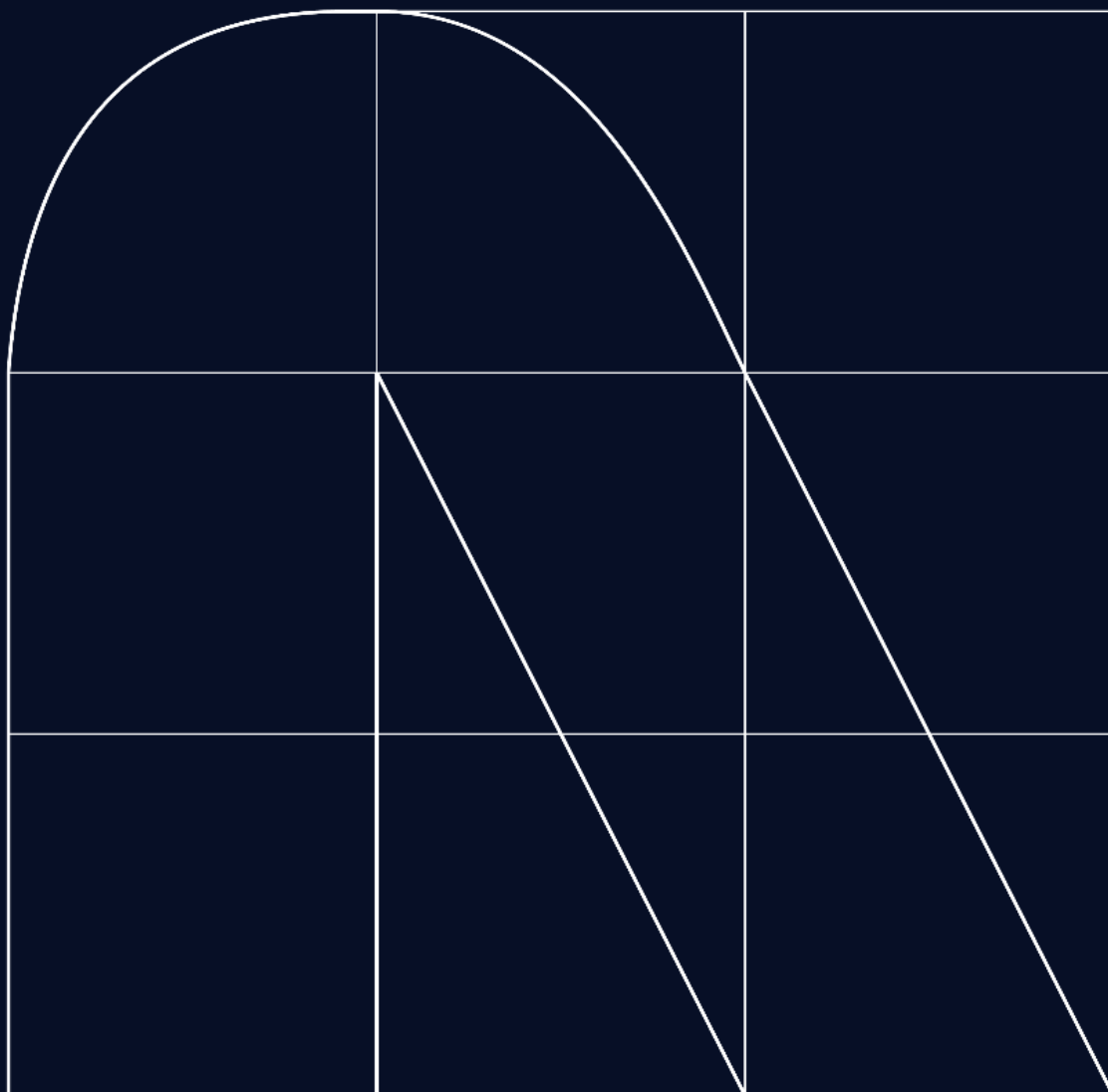
Gartner Security & Risk Management Summit Tokio (24 – 26 julio)
El Gartner Security & Risk Management Summit Tokyo 2024 es un evento que se llevará a cabo en Tokio, Japón, del 24 al 26 de julio. En este evento, se abordarán diversos temas clave, como IA generativa, gestión de riesgos, seguridad en la nube y entre otros. Asimismo, los asistentes podrán participar en sesiones con expertos sobre inteligencia de amenazas, respuesta a incidentes y el papel crítico de los factores humanos en la construcción de sistemas de seguridad resilientes.
Link

Recursos

Foresight Cybersecurity Threats For 2030 - Update 2024: Extended report
La ENISA (European Union Agency for Cybersecurity) publicó la segunda edición del estudio «ENISA Foresight Cybersecurity Threats for 2030», que representa un análisis y una evaluación exhaustivos de las nuevas amenazas a la ciberseguridad previstas para el año 2030. El informe reevalúa las diez principales amenazas previamente identificadas y sus respectivas tendencias, al tiempo que explora la evolución a lo largo de un año.
Link

AI RMF Generative AI Profile
El NIST (National Institute of Standards and Technology) publicó el documento «Generative AI Profile», desarrollado a lo largo del año pasado y basado en las aportaciones del grupo de trabajo público sobre IA generativa, formado por más de 2.500 miembros. Este documento permite ayudar a las organizaciones a identificar los riesgos únicos que plantea la IA generativa y propone acciones para la gestión de riesgos de la IA generativa que mejor se alineen con sus objetivos y prioridades.
Link

ChatGPT-4o
OpenAI, la empresa responsable de ChatGPT, anunció el lanzamiento de ChatGPT-4o, una versión gratuita de ChatGPT 4.0, la versión más avanzada del chatbot conversacional que inauguró la carrera por la IA generativa. GPT-4o acepta como entrada cualquier combinación de texto, audio, imagen y vídeo y genera cualquier combinación de salidas de texto, audio e imagen. Puede responder a entradas de audio en tan sólo 232 milisegundos, con una media de 320 milisegundos, lo que es similar al tiempo de respuesta humana en una conversación.
Link



Powered by the cybersecurity NTT DATA team

es.nttdata.com