Número 101 | Abril 2025

NTT DATA

Radar

El magazine de ciberseguridad

Ciberseguridad: Protegiendo el futuro con innovación

Por Andrea Isabel Muñoz Parreño

En la actualidad, algunos de los retos que presentan las organizaciones son el constante cambio y evolución de la tecnología, así como el comportamiento de los consumidores y clientes. Ello hace que deban innovar constantemente para mantenerse a la vanguardia y ser competitivos a la hora de ofrecer productos y servicios. Este desafío empresarial no es indiferente a la ciberseguridad, pues la misma también debe mantenerse al día, como *core* de la estrategia empresarial, a fin de ser una catapulta para el crecimiento y no una traba del mismo.

Las nuevas tendencias como el uso de inteligencia artificial, la adopción de la nube o la computación cuántica, entre otras, hacen que los retos de protección sean cada vez más complejos y requieran de una estrategia innovadora con aliados fuertes, tecnologías ágiles y personal capacitado. El mismo uso y tendencia de la inteligencia artificial abre nuevos vectores de ataque y aumenta la velocidad en la que una organización puede ser atacada.

La gran pregunta es: ¿cómo estar al día en las nuevas tendencias? ¿Como definir una estrategia que cubra los riesgos más importantes de una organización y que sea sostenible en el tiempo?

La respuesta a estas grandes preguntas no solo se encuentra en la participación de empresas expertas como parte de la estrategia de los CISOs, sino también en la comunidad, en el compartir de tendencias e innovación en foros especializados en ciberseguridad que permitan que las empresas trabajen de forma alineada, que puedan compartir sus experiencias y preocupaciones, así como traer nuevas ideas.

La conferencia RSA 2025 (RSAC), que se realiza en San Francisco (EEUU) desde 1995, trae esa oportunidad de participar en la comunidad, de hablar de nuevas tendencias y acercarse a colegas expertos de ciberseguridad y CISOs de todas partes del mundo en un mismo foro. Cada año, el RSA tiene un título diferente, este año será “Muchas voces, una sola comunidad”, lo cual está totalmente alineado a la idea de compartir conocimiento e ideas innovadoras que se alineen a las nuevas tecnologías.

Desde NTT DATA, estaremos presentes en el RSA del 28 de abril al 1 de mayo, compartiendo con nuestros clientes, trayendo nuevas tendencias, y realizando demos innovadoras, como:

- **Security Insights:** plataforma de seguridad que proporciona información operativa de los múltiples dominios de seguridad.
- **Data Resilience:** centrada en la capacidad que tiene una empresa para responder ante incidentes de seguridad.
- **MXDR for Integrated Threat Management:** para la protección avanzada de incidentes como tendencia de SOC.
- **Consumer IAM:** se analizará cómo atacar el manejo de identidades, sin dejar de lado el cumplimiento normativo y la experiencia de usuario.
- **Zero Trust Application Access:** mostrará cómo las organizaciones pueden observar, detectar y proteger el tráfico de aplicaciones críticas en tiempo real.

Espero que disfrute mucho del contenido de esta revista así como de las demos que vamos a presentar.

Andrea Isabel Muñoz Parreño
Cybersecurity Manager

Privacidad en la IA: Un actor relevante habilitado que opera algunas veces sin los controles necesarios

Cibercrónica por Jaime Tovar Prieto

Para nadie es un misterio que el uso de la IA se ha convertido en una herramienta fundamental para el apoyo de tareas personales, laborales y, en algunos casos, emocionales. En esta cibercrónica, quiero hablar sobre el uso de la IA en cualquiera de sus variantes y de uno de los casos de "abuso" que ha ocurrido debido al uso de esta tecnología, lo cual ha derivado en incidentes de seguridad relacionados con la fuga de información por la ausencia parcial de controles de seguridad adecuados.

Para abordar el tema central de esta cibercrónica, me gustaría poner el foco en un incidente que quizá no ha sido muy conocido en el mundo de la tecnología, pero que ha tenido un impacto significativo en algunas empresas, entendiendo que en algunos eventos no siempre indican la causa raíz.

Lo que pasa en Las Vegas, se queda en Las Vegas o, ajustado para este escenario, lo que se indexa en Bing, se queda en Bing. Así comienza este relato. Para esta crónica tenemos a un actor principal llamado Copilot y un actor de reparto llamado Bing (que se lleva un premio Oscar sin lugar a duda). Todo esto nos lleva a mediados de 2024, cuando la empresa de seguridad Lasso observa un post en LinkedIn en el que se acusa a OpenAI de exponer datos de repositorios privados de GitHub (plataforma de repositorio de código). Ante este alerta, que llama la atención por sí sola, Lasso se pone manos a la obra en la búsqueda de la razón detrás de tal afirmación y del comportamiento tan particular que este post indicaba.

Después de esfuerzos de búsqueda y consultas en ChatGPT (inteligencia artificial propia de OpenAI), no se logran obtener indicios claros sobre este comportamiento. Al intentar realizar accesos directos a algunos de los repositorios supuestamente públicos, no era posible, ya que estos eran privados en ese momento, lo que hace imposible el acceso sin una autenticación y autorización vigente y válida.

Al continuar con las consultas recurrentes sobre ChatGPT, esta firma realiza preguntas sobre sus propios repositorios, en donde ChatGPT sigue indicando respuestas poco concluyentes sobre sus repositorios, es decir, fueron poco informativas y no proporcionaban más que conceptos generales sobre la organización y tipos de tecnologías que pudiera tener. Entonces, ¿qué está ocurriendo?

La respuesta llegó tiempo después, cuando se realizan las mismas preguntas o validaciones en Copilot (inteligencia artificial propia de Microsoft), donde era posible obtener información sobre la estructura de aquellos repositorios, ya saben, nombres de carpetas, anidamiento, tamaños de archivos, entre otros; pero que, en el momento de la consulta, eran privados. Curioso.

La respuesta no era más difícil ni menos sencilla, depende de cómo se quiera ver. Simplemente era Bing siendo Bing; este había logrado indexar el contenido a través de sus arañas y había realizado *caché* sobre aquellos repositorios que había detectado públicos en algún momento en el tiempo, muy similar a Wayback Machine (es la máquina del tiempo en internet, donde es posible acceder al estado de un sitio público en Internet en un momento determinado en el tiempo).

¿Y si fue Bing, por qué Copilot lo tiene?

Lo anterior ocurre debido a que Copilot usa Bing como buscador para realizar búsquedas, lo cual es muy válido y funcional. Basado en lo anterior, fue posible obtener lo catalogado o conocido como Datos Zombi, los cuales son datos que no son utilizados continuamente o tienen poco uso (algo muy similar a datos del tipo *cold*) y que están disponibles.

Con claridad sobre lo ocurrido, Lasso realiza el respectivo escalamiento a Microsoft para que tome las acciones pertinentes, obteniendo una respuesta efectiva a su requerimiento y aplicándose las soluciones respectivas por parte de esta. Adicionalmente, Lasso notifica a otras empresas afectadas por este comportamiento.

Hasta aquí nada fuera de lo común, pero para nada normal. Es importante no normalizar este tipo de incidentes pues la filtración de información es muy relevante y puede conllevar un impacto económico y afectación de marca, sin mencionar la fuga de los secretos propios de la marca, algo similar a lo que le ocurrió a Kaspersky hace algún tiempo.

Desde mi punto de vista, hasta el momento el único culpable son los administradores, quienes dejaron expuestos los repositorios como públicos, lo cual es un error, entendiendo lo que contenían.

Año nuevo, búsquedas nuevas

Esto nos lleva a mediados de enero de 2025, más exactamente al 14 de enero. En este momento, Lasso decide realizar nuevas búsquedas en Bing de repositorios indexados, obteniendo un mensaje con el código 404 (código de error HTTP que indica que un recurso no existe o fue movido) para varios recursos consultados, lo que obedecería a una respuesta esperada. Con lo anterior, ¿estaríamos tranquilos? La respuesta más obvia es sí.

En búsqueda de indagar un poco más sobre si es posible acceder a estos repositorios, se hace uso nuevamente de Copilot, donde el resultado no fue el mismo ni mucho menos el esperado, pues fue posible observar la estructura del repositorio y fragmentos de código buscado, el cual no fue posible acceder a través de la búsqueda realizada previamente por Bing.

¿Entonces, por qué es posible acceder?

Esto se traduce o se podría entender que la solución realizada por Microsoft no fue completa, pues es posible acceder a información privada que alguna vez fue pública a través de Copilot, ya que este aún podría llegar a acceder al caché que, para 2024, fue deshabilitado para el consumo de usuario, pero posiblemente para Copilot no.

Algo que, en mi humilde parecer, es muy particular y llamativo. Con lo anterior, no estoy invocando a que se utilice esto como una práctica para saltar controles de seguridad, ni nada por el estilo, solo que es llamativo al ojo de alguien que requiera información especial y que hoy no está disponible.

Para más información, se puede consultar el blog de Lasso (enlace) donde se puede obtener más información técnica sobre cómo realizar este tipo de búsquedas (con carácter educativo).

Conclusiones generales

- **Publicación de información**: la información es un activo muy valioso para cualquier organización y debe ser tratada de la misma forma. Toda información debe ser catalogada, priorizada y tratada según lo indique su nivel de confidencialidad.
- **Presentación de resultados de la IA**: en este punto creo que, si bien es cierto que la IA es un producto "vivo" basado en su modelo de evolución, es de vital importancia revisar un poco más sobre el componente ético y el tópico de privacidad, donde se aborde la casuística expuesta en este relato. Con lo anterior, no quiero decir que la postura no sea la adecuada, solo que es prudente hacer un poco más de énfasis y que, muy posiblemente, hará parte de su evolución.
- **Bloqueo parcial de la IA en la organización**: actualmente existen soluciones de fabricantes en el mercado que pueden realizar funciones de DLP para IA, los cuales pueden evitar que usuarios accedan a IAs, carguen o visualicen información sensible en las IAs y, con ello, reducir la posibilidad de fuga de información.

Jaime Tovar Prieto
Cybersecurity Architect

Criptografía post-cuántica

Artículo por César Huanayque Vilca

En la era digital actual, donde la información es un activo invaluable, la seguridad de la información se ha convertido en un pilar fundamental para individuos, empresas y gobiernos por igual. En ese sentido, la criptografía se ha consolidado como un pilar fundamental para proteger la confidencialidad, integridad y autenticidad de los datos. A lo largo de las últimas décadas, la criptografía ha evolucionado significativamente, adaptándose a las crecientes amenazas y demandas de seguridad en diversos sectores de la industria.

La criptografía, con sus sofisticadas técnicas de cifrado, ha desempeñado un papel necesario en la protección de datos sensibles y la garantía de comunicaciones seguras, utilizando algoritmos matemáticos de cifrado para proteger datos y transacciones. Su aplicación es crítica en todos los sectores económicos, incluyendo Gobierno y defensa.

Sin embargo, el panorama de la seguridad informática está en constante evolución, y el advenimiento de la computación cuántica plantea nuevos desafíos que requieren una reevaluación de los paradigmas de seguridad existentes.

La computación cuántica tiene el potencial de transformar múltiples industrias, aunque enfrenta desafíos técnicos importantes, como el desarrollo de cúbits estables y confiables. Adicionalmente, con su capacidad para realizar cálculos que superan las capacidades de las computadoras clásicas, y en la evolución de las computadoras cuánticas, tendrían el potencial de socavar la eficacia de muchos algoritmos criptográficos ampliamente utilizados. Esta disrupción potencial exige una investigación exhaustiva en nuevas estrategias de criptoanálisis que permitan evaluar la robustez de los sistemas criptográficos frente a las capacidades de la computación cuántica.

Los algoritmos criptográficos ampliamente utilizados, como RSA, ECC y Diffie-Hellman, se basan en problemas matemáticos que son difíciles de resolver para las computadoras clásicas, pero que podrían ser vulnerables a los ataques de las computadoras cuánticas. Esto significa que la información cifrada con estos algoritmos podría ser descifrada por atacantes con acceso a tecnología cuántica suficientemente avanzada.

El papel de la inteligencia artificial (IA)

La IA está revolucionando el criptoanálisis, ofreciendo nuevas herramientas para analizar, atacar y defender sistemas criptográficos.

- **Análisis potenciado:** la IA automatiza y mejora el análisis de patrones en datos cifrados, optimiza ataques de fuerza bruta y facilita la ingeniería inversa de algoritmos.
- **Vulnerabilidades expuestas:** modelos de IA identifican debilidades en cifrados modernos y permiten ataques de canal lateral más sofisticados.
- **Adaptándose a la IA:** la IA también se utiliza para descifrar sistemas criptográficos basados en IA, creando una carrera entre el desarrollo de cifrados y las herramientas para romperlos.

La IA y la computación cuántica

La convergencia de la inteligencia artificial y la computación cuántica está abriendo un capítulo sin precedentes en el criptoanálisis. La capacidad de la IA para aprender, optimizar y reconocer patrones complejos se convierte en una herramienta crucial para descifrar la seguridad de la información en la era cuántica.

La IA optimiza algoritmos cuánticos específicos, como el algoritmo de Shor, mediante la determinación de parámetros óptimos y la mitigación de errores. En el algoritmo de Grover, esta tecnología guía la búsqueda de claves y analiza patrones para revelar información oculta.

¿Qué vulnerabilidades se pueden deducir de la futura computación cuántica?

La computación cuántica, con su potencial disruptivo, plantea un riesgo significativo para la criptografía actual.

Si bien aún se encuentra en desarrollo, la capacidad de las computadoras cuánticas para romper los algoritmos criptográficos actuales es una amenaza real que podría tener consecuencias con un alto impacto.

Impacto Potencial:

- **Pérdida de Confidencialidad:** información sensible como datos financieros, registros médicos y secretos gubernamentales podría verse expuesta.
- **Pérdida de Integridad:** la manipulación de datos y la falsificación de firmas digitales podrían socavar la confianza en los sistemas digitales.
- **Pérdida de Confianza:** el impacto en el comercio electrónico, las comunicaciones en línea y otras actividades que dependen de la criptografía podría ser severo.

La probabilidad de que las computadoras cuánticas rompan los algoritmos criptográficos aumenta con el tiempo. A corto plazo, el riesgo es de nivel bajo a medio, pero a largo plazo, la probabilidad se vuelve significativa. Estas probabilidades pueden cambiar en función de la evolución de las computadoras cuánticas.

¿Qué acciones se pueden tomar?

La inminente llegada de la computación cuántica representa una amenaza sin precedentes para la criptografía actual. Para salvaguardar la información a largo plazo, la adopción de la criptografía post-cuántica (PQC) se vuelve imperativa. Sin embargo, esta transición no es trivial y requiere una planificación y ejecución meticulosas.

La implementación de PQC no es un evento único, sino un proceso continuo que demanda planificación, implementación y monitoreo constantes.

La estandarización de algoritmos es crucial para garantizar la compatibilidad entre sistemas y comunicaciones. Se debe tener en consideración, que, a día de hoy, ya existen estándares candidatos por parte de NIST para tener un marco estándar para la PQC.

La adopción de la criptografía post-cuántica (PQC) requiere un proceso que puede distribuirse de la siguiente manera:

1. **Inventario y evaluación:** identificar sistemas, evaluar vulnerabilidades y priorizar la migración.
2. **Investigación y selección:** seguir la estandarización, evaluar algoritmos y seleccionar los adecuados.
3. **Pruebas e implementación:** realizar pruebas, planificar la migración e implementarla gradualmente.
4. **Monitorización y adaptación:** monitorizar el rendimiento y adaptarse a los cambios en la seguridad cuántica.

César Huanayque Vilca
Cybersecurity Expert Architect

La gestión de Identidades y Accesos: Desafíos y soluciones innovadoras

Artículo por Alicia Lara Herrera

En el entorno corporativo actual, la gestión de identidades y accesos se ha convertido en un eje central para la seguridad organizacional. Con la transformación digital y la creciente movilidad laboral, las empresas enfrentan desafíos significativos para proteger sus recursos y garantizar el cumplimiento normativo. A continuación, se profundiza en los principales aspectos de este complejo panorama.

Seguridad de Credenciales y Autenticación Multifactor

Las credenciales de usuario son la primera línea de defensa contra accesos no autorizados. Tradicionalmente, las contraseñas han sido el método más común de autenticación. Sin embargo, debido a la facilidad con la que pueden ser comprometidas, las organizaciones están adoptando tecnologías de autenticación multifactor (MFA). MFA requiere múltiples formas de verificación, como algo que el usuario sabe (contraseña), algo que el usuario tiene (un dispositivo móvil), y algo que el usuario es (huella dactilar o reconocimiento facial).

Ventajas y Desafíos de MFA:

- **Ventajas:** aumenta considerablemente la dificultad para que actores malintencionados accedan a sistemas, ya que necesitarían comprometer múltiples factores de autenticación.
- **Desafíos:** la implementación de MFA puede enfrentar resistencia por parte de los usuarios debido a la percepción de complejidad adicional. Además, existen problemas de accesibilidad en contextos donde los usuarios no pueden acceder fácilmente a dispositivos secundarios.

Gestión de Identidades Privilegiadas (PIM)

La gestión de identidades privilegiadas se centra en controlar y proteger el acceso a cuentas que poseen permisos elevados. Estas cuentas son objetivos atractivos para los atacantes debido a su capacidad de acceso a sistemas críticos.

Importancia y Estrategias de PIM:

- **Importancia:** prevenir el abuso de privilegios es crucial para evitar la exposición de datos sensibles y la interrupción de operaciones críticas.
- **Estrategias:** las empresas deben implementar controles de acceso estrictos, auditorías regulares y monitorización continua de actividades para detectar y responder a posibles abusos de privilegios.

Zero Trust: Un Nuevo Paradigma

El modelo de seguridad Zero Trust se basa en el principio de que ninguna entidad, interna o externa, debe ser de confianza por defecto. Cada acceso debe ser verificado y cada acción monitorizada.

Implementación de Zero Trust:

- **Verificación Continua:** Requiere autenticación y autorización continuas para cada solicitud de acceso.

- **Monitorización constante:** las organizaciones deben implementar herramientas de monitorización en tiempo real para detectar comportamientos anómalos y responder rápidamente a amenazas potenciales.

Identidad digital basada en *blockchain*

El *blockchain* ofrece un enfoque innovador para la gestión de identidades proporcionando un registro inmutable de identidades que es verificable y seguro.

Beneficios y limitaciones:

- **Beneficios:** la naturaleza descentralizada de *blockchain* reduce el riesgo de manipulación de datos y proporciona una trazabilidad clara de las transacciones de identidad.
- **Limitaciones:** la falta de estandarización y la necesidad de infraestructura específica limitan su adopción masiva.

Gestión de Identidad como Servicio (IDaaS)

- IDaaS ofrece una solución en la nube para la gestión de identidades, facilitando la implementación y administración mediante plataformas escalables y flexibles.

Aspectos Críticos de IDaaS:

- **Facilidad de Implementación:** permite a las organizaciones externalizar la gestión de identidades, reduciendo la carga interna sobre los equipos de TI.
- **Riesgos Asociados:** la dependencia de proveedores externos puede presentar riesgos de seguridad y problemas de integración con sistemas internos existentes.

Autenticación Biométrica

La autenticación biométrica, que utiliza características físicas únicas como huellas digitales y reconocimiento facial, ofrece un nivel de seguridad superior a los métodos tradicionales.

Ventajas y retos:

- **Ventajas:** reduce significativamente el riesgo de robo de identidad al basarse en características inherentes al individuo.
- **Retos:** las preocupaciones sobre privacidad y el almacenamiento seguro de datos biométricos deben ser abordadas para asegurar la confianza del usuario.

Cumplimiento normativo y protección de identidad

Normativas como el GDPR y la LGPD exigen un manejo riguroso de los datos personales, imponiendo sanciones severas por incumplimiento.

Requisitos de cumplimiento:

- **Manejo de datos personales:** las organizaciones deben implementar políticas de protección de datos que garanticen la privacidad y seguridad de la información personal.
- **Auditorías y reportes:** es crucial mantener registros detallados de accesos y actividades para demostrar el cumplimiento y responder a auditorías regulatorias.

Inteligencia Artificial y Aprendizaje Automático

La inteligencia artificial (IA) y el aprendizaje automático (ML) son herramientas poderosas en la detección de fraudes y comportamientos sospechosos.

Aplicaciones en seguridad:

- **Análisis de patrones:** estas tecnologías permiten analizar grandes volúmenes de datos para identificar patrones y anomalías que podrían indicar amenazas.
- **Respuesta proactiva:** al detectar comportamientos inusuales, los sistemas pueden activar alertas y respuestas automáticas para mitigar riesgos antes de que se materialicen.

En resumen, la gestión de identidades y accesos en el entorno corporativo moderno requiere un enfoque multifacético que incorpore tecnologías avanzadas y mejores prácticas. Al abordar estos desafíos con soluciones innovadoras, las organizaciones pueden proteger efectivamente sus activos y garantizar el cumplimiento normativo, asegurando así su continuidad y reputación en un mundo cada vez más digital.

Alicia Lara Herrera
Cybersecurity Expert Engineer

Algunos desafíos cuánticos

Espacio cuántico
por María Gutiérrez

Desde el equipo de Cuántica de NTT DATA queremos contribuir a la divulgación del conocimiento de la tecnología cuántica. Para ello, y como parte de nuestras a actividades, estamos preparando un curso sobre esta materia que tiene los siguientes objetivos:

- **Comprender los fundamentos de la computación cuántica:** explicar los principios básicos, la diferencia con la computación clásica y su evolución histórica.
- **Familiarizarse con herramientas y simuladores cuánticos:** introducir entornos y plataformas cuánticas permitiendo la experimentación con circuitos cuánticos básicos.
- **Explorar algoritmos cuánticos y sus aplicaciones:** presentar algoritmos clave como Shor, Grover analizando su impacto en optimización y criptografía.
- **Identificar retos y oportunidades en el campo cuántico:** analizar desafíos tecnológicos, limitaciones actuales y tendencias futuras en la adopción y escalabilidad de la computación cuántica.

A continuación, os comparto algunos de los contenidos del curso que nos permitirán ir aproximándonos a los principios fundamentales de la tecnología y la computación cuántica y que iremos comentando en los números de la revista RADAR de este año. Para comprender el potencial de esta tecnología, es esencial conocer cuatro principios fundamentales:

- **Cúbits:** son la unidad básica de información cuántica y pueden representar tanto 0 como 1 al mismo tiempo debido a la superposición.
- **Superposición:** un cúbit puede estar en múltiples estados simultáneamente, lo que otorga a los computadores cuánticos su gran capacidad de paralelización de cálculos.

- **Entrelazamiento:** es un fenómeno donde dos o más cúbits están correlacionados de tal forma que el estado de uno depende del otro, independientemente de la distancia que los separe.
- **Interferencia Cuántica:** se refiere a cómo los estados cuánticos pueden combinarse y cancelarse, lo que permite dirigir la computación hacia las soluciones correctas en algoritmos específicos.

A pesar del enorme valor de la tecnología cuántica para revolucionar múltiples industrias, su desarrollo y adopción enfrentan diversos desafíos tecnológicos, arquitectónicos y de infraestructura. La transición de los modelos computacionales clásicos hacia un paradigma cuántico no es trivial y requiere superar barreras fundamentales en *hardware*, *software* y modelos de implementación.

¿Dónde están los principales desafíos?

1. Hardware cuántico:

El hardware cuántico es uno de los aspectos más críticos en la evolución de la computación cuántica, los principales retos incluyen:

- **Escalabilidad de los cúbits:** actualmente, la cantidad de cúbits disponibles en *hardware* cuántico varía significativamente entre los diferentes enfoques tecnológicos. Mientras que IBM y Google trabajan en superconductores, D-Wave ha desarrollado *annealers* con miles de cúbits, aunque con limitaciones en su aplicabilidad.
- **Tiempo de coherencia:** Los cúbits pierden su estado cuántico debido a la decoherencia en tiempos muy cortos. Esto limita la cantidad de operaciones que se pueden realizar antes de que la información se degrade.

2. Infraestructura y adopción:

La integración de la computación cuántica en el ecosistema tecnológico actual requiere superar varios desafíos:

- **Limitaciones en la conectividad de los cúbits:** las conexiones entre cúbits no son perfectas. En arquitecturas como la de D-Wave, los cúbits deben encadenarse para representar variables, lo que genera problemas de estabilidad y precisión.
- **Escalabilidad comercial:** la computación cuántica todavía está en una etapa de desarrollo. Si bien algunos problemas pueden resolverse con *hardware* NISQ (Noisy Intermediate-Scale Quantum), la verdadera ventaja cuántica requerirá *hardware* de corrección de errores, lo cual aún está lejos de ser una realidad

Arquitecturas y modelos computacionales

Los modelos de computación cuántica también presentan retos importantes:

- **Ruido y errores en la ejecución:** la ejecución de algoritmos cuánticos en *hardware* real introduce ruido que puede afectar la precisión de los resultados. Las estrategias de mitigación de errores, como la extrapolación de “ruido cero” (Zero Noise Extrapolation), están en desarrollo, pero aún no se han resuelto completamente.
- **Codificación y mapeo de problemas:** a diferencia de la computación clásica, los problemas deben representarse en términos de puertas cuánticas y conectividad limitada de cúbits. Esto añade un nivel adicional de complejidad en el diseño de algoritmos.

En el próximo número hablaremos de los principales problemas que ya se están beneficiando de la aplicación de la tecnología cuántica.

Ciberseguridad del mañana: Innovaciones que nos protegen hoy

Tendencias por José Cárdenas Camacho

En la era digital, la velocidad a la que evolucionan las amenazas de ciberseguridad exige que las empresas adopten soluciones innovadoras para proteger sus activos y mantener la continuidad operativa. Las recientes estadísticas indican que el gasto global en ciberseguridad superó los 150 mil millones de dólares en 2024, con proyecciones de un crecimiento anual del 12% en los próximos años. Este panorama impulsa la búsqueda constante de tecnologías disruptivas que transformen la defensa digital.

Nuevos Paradigmas en la Protección Digital

El modelo tradicional de defensa ya no es suficiente ante la sofisticación de los ataques actuales. Organizaciones de renombre han empezado a adoptar arquitecturas *Zero Trust*, que asumen que ninguna entidad, ya sea interna o externa, es de confianza por defecto. Según Gartner, se estima que el 70% de las empresas implementarán este enfoque antes de 2026, lo que refleja una tendencia irreversible hacia una verificación continua de identidades y accesos.

Tecnologías emergentes y aplicaciones en la defensa contra ciberataques

Inteligencia Artificial y *Machine Learning*:

El análisis predictivo basado en inteligencia artificial permite identificar patrones anómalos en tiempo real. Algoritmos de *machine learning* están siendo entrenados para detectar comportamientos inusuales, logrando reducir los tiempos de respuesta ante incidentes críticos. Estudios de IDC pronostican un crecimiento anual del 28% en inversiones dirigidas a estas tecnologías, subrayando su impacto en la detección temprana de amenazas.

Blockchain y seguridad de datos

La tecnología *blockchain* ofrece una trazabilidad inmutable que resulta esencial para garantizar la integridad de la información. En sectores sensibles como el financiero y el sanitario, su aplicación ha permitido disminuir significativamente los riesgos de fraude y alteración de datos, consolidándose como un pilar en la validación de transacciones digitales.

Criptografía cuántica

Ante la inminente era de la computación cuántica, la criptografía cuántica emerge como una solución revolucionaria para proteger la confidencialidad de la información. Esta técnica utiliza principios de la física cuántica para generar claves de cifrado prácticamente inviolables, ofreciendo una barrera robusta frente a la capacidad de procesamiento de los futuros atacantes.

Automatización y orquestación de respuestas

La integración de sistemas de automatización y orquestación permite una respuesta coordinada ante incidentes. Estas herramientas facilitan la contención y mitigación de ataques al aislar sistemas comprometidos y desplegar parches de seguridad de manera instantánea, lo que puede reducir hasta en un 50% el tiempo de reacción ante amenazas emergentes.

Impacto y proyecciones en el sector

La convergencia de estas tecnologías no solo mejora la seguridad, sino que también redefine el mercado. Se proyecta que el sector de innovaciones en ciberseguridad alcanzará un valor superior a los 300 mil millones de dólares para 2027, impulsado por la creciente demanda de soluciones adaptativas en un entorno de amenazas en constante evolución. La inversión en I+D, junto con alianzas estratégicas entre el sector privado y organismos gubernamentales, está acelerando la transformación digital de la defensa cibernética.

Conclusión

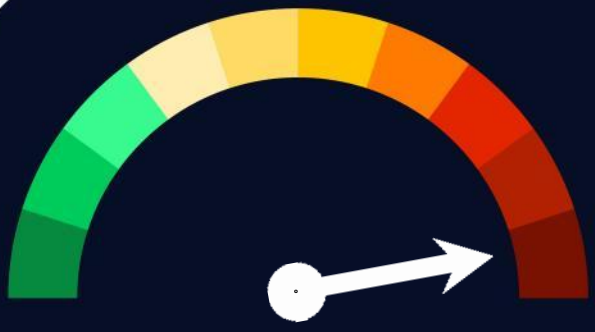
El futuro de la ciberseguridad está marcado por la integración de soluciones que combinan inteligencia artificial, *blockchain*, criptografía cuántica y automatización. Estas innovaciones, lejos de ser modas pasajeras, representan el camino hacia entornos digitales resilientes y adaptativos. En un contexto de amenazas crecientes, la apuesta por la innovación no es solo estratégica, sino esencial para garantizar la protección integral de las organizaciones en la era digital.

José Cárdenas Camacho
Cybersecurity Analyst

Vulnerabilidades

Vulnerabilidad crítica en productos VMware

Fecha: 4 de marzo de 2025
CVE: CVE-2025-22224



CVSS: 9.3

CRÍTICA

Descripción

La vulnerabilidad crítica CVE-2025-22224, que afecta a productos VMware, ha sido identificada y reportada por Broadcom Inc. Es un fallo de tipo TOCTOU (*Time-of-Check Time-of-Use*), que provoca una escritura fuera de límites. Si se explota con éxito esta vulnerabilidad, un atacante con privilegios administrativos en una máquina virtual podría ejecutar código en el *host*, como el proceso VMX.

Además, se ha clasificado otra vulnerabilidad de alto riesgo (CVE-2025-22225), directamente relacionada con la primera. Esta permite una escritura arbitraria en el *kernel*, lo que podría provocar un escape del entorno protegido dentro del proceso VMX.

Solución

VMware ha publicado actualizaciones de seguridad para proveer una solución para estas vulnerabilidades. Dichos parches se encuentran disponibles en el portal oficial del fabricante.

Se recomienda actualizar los productos afectado a la versión más reciente lo antes posible.

Productos afectados

Esta vulnerabilidad afecta a los siguientes productos de WMware:

- ESXi 7.0 y 8.0
- Fusion 13.x.
- Workstation 17.x.
- Cloud Foundation 4.5.x y 5.x.
- Telco Cloud Platform: 5.x, 4.x, 3.x y 2.x.
- Telco Cloud Infrastructure: 3.x y 2.x.

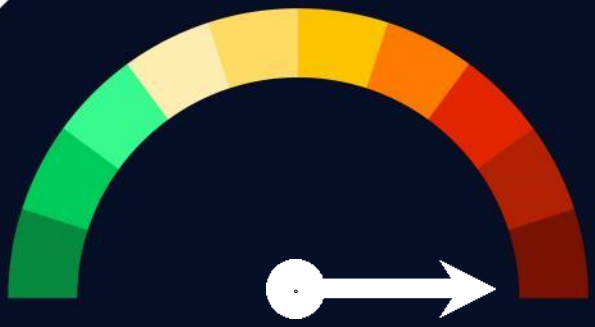
Referencias

- cert.europa.eu
- broadcom.com

Vulnerabilidades

Vulnerabilidad crítica en Kibana

Fecha: 5 de marzo de 2025
CVE: CVE-2025-25015



CVSS: 9.9

CRÍTICA

Descripción

Se ha identificado una vulnerabilidad crítica en Kibana (CVE-2025-25015), la cual está relacionada con "Prototype Pollution", lo que permite a un atacante ejecutar código arbitrario mediante la carga de archivos manipulados, así como solicitudes HTTP especialmente diseñadas. Se le ha asignado una puntuación CVSS de 9.9, lo que la convierte en una amenaza crítica para los sistemas afectados.

Este tipo de ataque podría permitir la toma de control del servidor Kibana, acceso a datos confidenciales y despliegue de cargas adicionales para comprometer aún más el entorno.

Solución

Para mitigar los riesgos asociados con esta vulnerabilidad, se recomienda:

- Actualizar inmediatamente a Kibana versión 8.17.3, donde el problema ha sido corregido.

Si la actualización no se puede llevar a cabo de inmediato, se recomienda una mitigación temporal deshabilitando la funcionalidad "Integration Assistant" en el archivo de configuración kibana.yml. Para ello, es necesario agregar la siguiente línea:

```
xpack.integration_assistant.enabled: false
```

Productos afectados

Las versiones afectadas son las siguientes:

- V8.15.0 a V8.17.0: cualquier usuario con el rol "Viewer" puede explotar la vulnerabilidad.
- V8.17.1 y V8.17.2: solo es vulnerable si se poseen todos los siguientes permisos: *fleet-all, integrations-all, actions:execute-advanced-connectors*.

Referencias

- nvd.nist.gov
- discuss.elastic.co
- thehackernews.com

TLP:WHITE

Boletín de seguridad de marzo de Android

Fecha: 3 de marzo de 2025
CVE: CVE-2024-43093 y 43 más

Crítica

Descripción

El boletín de seguridad de Android de marzo de 2025 aborda un total de 44 vulnerabilidades, incluidas diez críticas. La más grave de estas es una vulnerabilidad en el componente de sistema que, sin necesidad de privilegios de ejecución adicionales, puede llevar a la ejecución remota de código.

También han publicado parches para dos vulnerabilidades de gravedad alta que han sido explotadas activamente:

- CVE-2024-43093: vulnerabilidad de escalada local de privilegios, permitiendo acceso no autorizado a los directorios críticos del sistema.
- CVE-2024-50302: vulnerabilidad que, debido a una falla de escalada de privilegios, podría provocar una fuga de memoria del *kernel.*

Productos afectados

Los componentes afectados por estas vulnerabilidades son:

- Framework
- Sistema
- Kernel
- Componentes de Terceros:
  - MediaTek
  - Qualcomm

Además, es posible que los dispositivos con Android 10 y versiones posteriores también reciban actualizaciones de seguridad.

Solución

Se han publicado varios parches de seguridad en este boletín, por lo que se recomienda a todos los usuarios de Android actualizar a la versión más reciente para solucionar las vulnerabilidades.

Referencias

- thehackernews.com
- android.com

TLP:WHITE

Actualización de seguridad para productos Microsoft

Fecha: 11 de marzo de 2025
CVE: CVE-2025-24983 y 56 más

Crítica

Descripción

Microsoft ha publicado actualizaciones de seguridad para 57 vulnerabilidades, incluyendo 6 críticas y 7 *zero-days* (seis explotadas activamente y una divulgada públicamente). Entre las vulnerabilidades corregidas, hay de elevación de privilegios, evasión de características de seguridad, ejecución remota de código, divulgación de información, denegación de servicio y suplantación de identidad.

Entre las vulnerabilidades más importantes se encuentran las siguientes *zero-days*:

- CVE-2025-24983 (SYSTEM): elevación de privilegios SYSTEM explotando una condición de carrera.
- CVE-2025-24984 (NTFS): permite leer fragmentos de memoria mediante USBs maliciosos.
- CVE-2025-24985 (FAT): permite la ejecución remota de código a través de imágenes VHD maliciosas.
- CVE-2025-24991 (NTFS): divulgación de información a través de VHDs manipulados.
- CVE-2025-24993 (NTFS): ejecución remota de código por desbordamiento de búfer en NTFS.
- CVE-2025-26633: evasión de seguridad permitiendo ejecutar archivos .msc maliciosos.

Productos afectados

Algunos de los productos afectados son:

- Windows 11: Versiones 22H2 y 24H2.
- Windows 10: Versiones 21H2 y 22H2.
- Windows Server 2022, 2019, 2016, 2012 R2.
- Microsoft Office 2016, 2019 y 2021.
- SharePoint 2013, 2016 y 2019.
- Visual Studio 2019 y 2022

Solución

Desde Microsoft recomiendan la actualización inmediata a la última versión disponible de cada sistema y aplicación.

Referencias

- www.bleepingcomputer.com
- answers.microsoft.com

Eventos

Forum InCyber Europe 2025
1 – 3 de abril

El Forum InCyber Europe 2025 se llevará a cabo el 1 al 3 de abril en el Lille Grand Palais, Francia, consolidándose como uno de los eventos más relevantes en el ámbito de la ciberseguridad y la confianza digital en Europa. Bajo el lema “Más allá del Zero Trust, confianza para todos”, esta edición explorará estrategias innovadoras para fortalecer la seguridad en un entorno digital cada vez más complejo. El evento reunirá expertos, líderes del sector y organizaciones clave en una combinación de conferencias, mesas redondas y demostraciones técnicas, abordando temas como gestión de riesgos, soberanía digital y lucha contra el crimen cibernético.

Enlace

Black Hat Asia 2025
1 – 4 de abril

Del 1 al 4 de abril de 2025, el Marina Bay Sands Expo & Convention Centre en Singapur será el epicentro de la ciberseguridad con el Black Hat Asia 2025. Este evento reunirá a expertos globales para discutir las amenazas emergentes, con un enfoque especial en inteligencia artificial, ciberseguridad en servicios financieros y nuevas vulnerabilidades en dispositivos móviles. El programa incluirá capacitaciones avanzadas, conferencias técnicas y presentaciones de herramientas innovadoras, además de oportunidades exclusivas de *networking* en su sala de negocios.

Enlace

Gartner Security & Risk Management Summit
7 – 8 de abril

El Gartner Security & Risk Management Summit 2025 se llevará a cabo del 7 al 8 de abril de 2025 en el Conrad Dubai, situado en Emiratos Árabes Unidos. Este evento está diseñado para líderes de seguridad y gestión de riesgos en Oriente Medio, ofreciendo una plataforma para descubrir las últimas perspectivas y soluciones en ciberseguridad. Los asistentes tendrán la oportunidad de participar en sesiones centradas en temas clave como inteligencia artificial en ciberseguridad, seguridad en la nube, seguridad de aplicaciones, y gestión de riesgos y cumplimiento.

Enlace

RSA Conference
28 de abril – 1 de mayo

La RSA Conference 2025 se celebrará del 28 de abril al 1 de mayo de 2025 en el Moscone Center de San Francisco, California. Bajo el lema “Muchas veces, una comunidad”, el evento reunirá a profesionales de la ciberseguridad para abordar temas críticos como inteligencia artificial, seguridad en la nube y gestión de riesgos. El programa incluirá conferencias magistrales, sesiones interactivas y oportunidades de *networking*, ofreciendo una plataforma para compartir conocimientos y explorar soluciones innovadoras en el ámbito de la seguridad digital.

Enlace

Recursos

➢ ENISA NIS360

El informe ENISA NIS360, publicado por la Agencia de la Unión Europea para la Ciberseguridad (ENISA), evalúa la madurez y criticidad de los sectores cubiertos por la Directiva NIS2, proporcionando un análisis detallado del estado de ciberseguridad en sectores clave como energía, transporte, finanzas, salud y entre otros. Basado en datos de autoridades nacionales, empresas del sector y fuentes de la UE como Eurostat, este informe es crucial para ayudar a los Estados Miembros a identificar brechas, priorizar recursos y fortalecer la resiliencia cibernética en la Unión Europea.

Enlace

➢ NIST SP 800-226, Guidelines for evaluating differential privacy guarantees

El NIST Special Publication 800-226, emitido por el Instituto Nacional de Estándares y Tecnología (NIST), proporciona directrices para evaluar las garantías de privacidad diferencial, una técnica matemática clave para proteger la información personal en el análisis de datos. Este documento es fundamental para ayudar a las organizaciones gubernamentales y empresas a comprender y aplicar la privacidad diferencial de manera efectiva, identificando factores críticos y riesgos communes en su implementación.

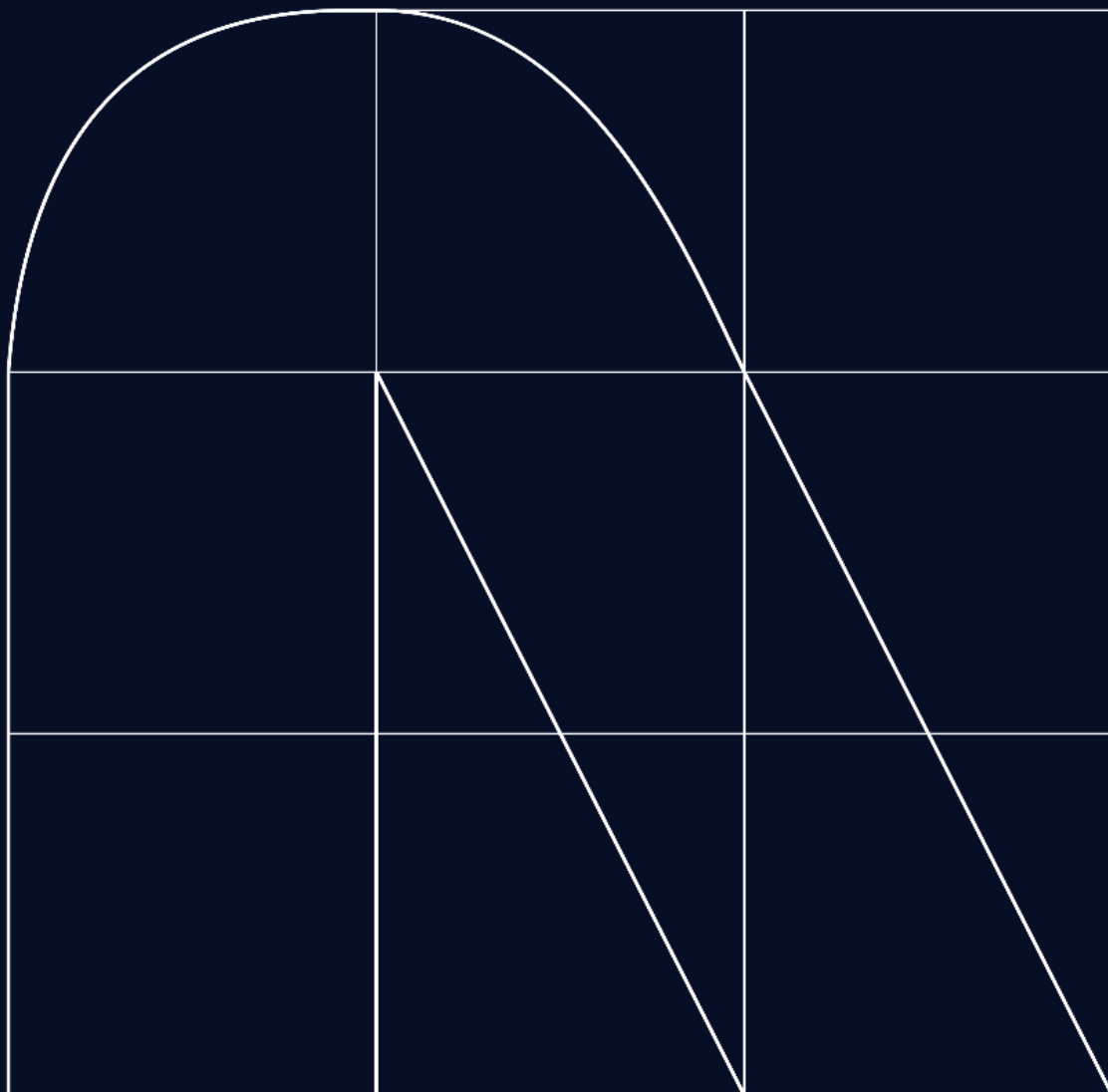
Enlace

➢ Entrada en vigor de ciertos artículos de la Ley 21.663

Recientemente, entraron en vigor ciertos artículos de la Ley 21.663, conocida como Ley Marco de Ciberseguridad en Chile. Esta legislación establece un nuevo modelo de gobernanza que promueve la implementación de estándares de ciberseguridad en los sectores público y privado del país. La Ley crea la Agencia Nacional de Ciberseguridad (ANCI) y define obligaciones específicas para los Operadores de Importancia Vital (OIV), incluyendo la implementación de sistemas de gestión de seguridad de la información y planes de continuidad operacional.

Enlace

Suscríbete a RADAR
up.nttdata.com/suscribetearadar



Powered by the cybersecurity NTT DATA team

es.nttdata.com