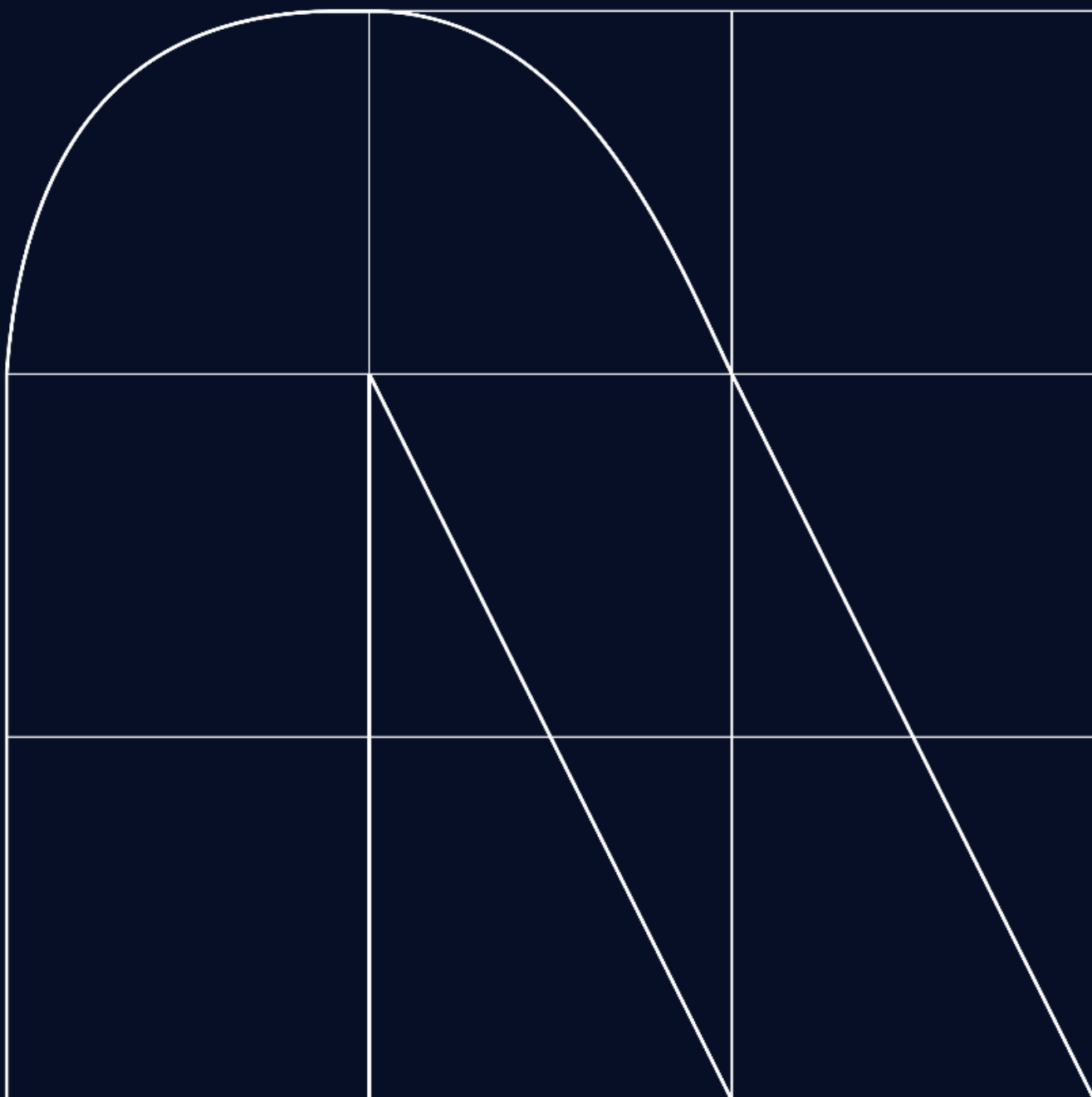
Número 89 | Abril 2024

NTT DATA

Radar

El magazine de ciberseguridad



Seguridad en aplicaciones e inteligencia artificial

Por Roberto Junior Ruiz Neyra

Mas del 50% de los malwares llegan a los usuarios a través de las aplicaciones en la nube. Muchos de ellos tienen origen geopolítico, mientras que otros se originaron por ciberdelincuentes como por ejemplo el grupo ruso Wizard Spider, TA505, FIN7. Entre las principales víctimas de estos ataques tenemos los servicios financieros y la atención sanitaria. La mayoría de estas situaciones sucede debido a las brechas de seguridad que presentan las aplicaciones donde los ciber atacantes aprovechan las vulnerabilidades para inyectar malwares y lograr su cometido.

¿Por qué sucede esto? Todo parte desde la seguridad en el diseño de estas aplicaciones hasta su propio desarrollo. Los últimos estudios han demostrado que más del 70% de las aplicaciones desarrolladas contiene brechas de seguridad, representando un riesgo importante en las organizaciones. Este riesgo es exponencial cuando las aplicaciones tienen un gran alcance comercial convirtiendo a varias empresas y países a la vez en víctimas potenciales. Un punto importante a tomar nota es que, a medida que la IA generativa viene ganando protagonismo en el desarrollo de software, aumenta el riesgo de vulnerabilidades si esta práctica no es controlada. Esto se debe a que el código es escrito por grandes modelos de lenguaje entrenados en fuentes de datos sin limpiar, como repositorios públicos de GitHub. Por eso, es super importante que se compruebe la seguridad de la nueva aplicación por medio de herramientas de escaneo de código estático (SAST) y herramientas de análisis de composición de software (SCA) manejados por especialistas de Ciberseguridad con la finalidad de maximizar la identificación de fallos o vulnerabilidades y corregirlos, permitiendo a los desarrolladores aprovechar al máximo las bondades de la IA sin comprometer la seguridad de las aplicaciones.

Afortunadamente, la era de la IA no viene únicamente a ganar terreno en el ámbito de desarrollo de software, sino también en el ámbito de seguridad en aplicaciones. Por ejemplo, dentro de la práctica de DevSecOps y Cloud Security están emergiendo nuevas soluciones que cubren casos de uso como interpretación de la vulnerabilidad y proponer scripts de remediación de dichas vulnerabilidades en tiempo real. Otro caso de uso interesante es el entrenamiento de la IA para realizar pruebas de seguridad mediante la simulación de ataques. Así como estos ejemplos, existen otros más donde podremos tener a la IA como aliado para asegurar el desarrollo y creación de las aplicaciones.
En NTT DATA estamos convencidos que la IA será clave para evolucionar e innovar la seguridad en las aplicaciones donde contribuimos con la agilidad en el “time to market”, no afectar la experiencia del usuario al momento de robustecer la seguridad y mantenernos firmes con el principio de “Confianza Cero”.

Roberto Junior Ruiz Neyra
Cybersecurity Manager

Cibercrónica

Por Christian Agreda

Comenzamos la ciber crónica de este mes, hablando de la Vulnerabilidad de día cero de SmartScreen de Windows Defender (CVE-2024-21412) descubierta.

Esta vulnerabilidad se debe a una falla al aplicar la " Marca de la Web " (MotW), una característica de seguridad utilizada por Windows para identificar archivos que se originan en fuentes potencialmente no confiables, como descargas de Internet, WebDAV y recursos compartidos SMB. En circunstancias normales, los archivos descargados de la web están etiquetados con MotW, lo que hace que Windows Defender SmartScreen emita alertas cuando dichos archivos intentan ejecutarse o cuando un usuario intenta ejecutarlos directamente. Este mecanismo actúa como una defensa crítica, evitando que se ejecute código malicioso o no autorizado sin el conocimiento o consentimiento del usuario.

Sin embargo, CVE-2024-21412 permitió a los atacantes eludir estas protecciones explotando una falla en el manejo de accesos directos a Internet (archivos .URL) y otros mecanismos [8]. A través de campañas de phishing diseñadas y el uso de sitios web comprometidos, los atacantes distribuyeron estos archivos .URL maliciosos. Cuando se ejecutaron, estos archivos no llevaban la etiqueta MotW, lo que cegó efectivamente a SmartScreen ante sus intenciones maliciosas. Este descuido permitió la ejecución del malware DarkMe sin activar las advertencias de seguridad habituales que alertarían a los usuarios sobre el peligro potencial.

Al eludir las defensas de SmartScreen, Water Hydra pudo ejecutar su cadena de ataque discretamente, infectando las máquinas de las víctimas sin ser detectado. El ataque aprovechó la confianza que Windows deposita en los archivos que carecen de la designación MotW, asumiendo que son seguros y se originan en una fuente confiable dentro del entorno del usuario. Esta explotación representa una importante violación de confianza en los mecanismos de seguridad diseñados para proteger a los usuarios del mismo tipo de ataque orquestado por Water Hydra.

Connectwise ha abordado dos vulnerabilidades críticas recientemente (CVE-2024-1709 y CVE-2024-1708) en todas las versiones locales de ScreenConnect anteriores a la 23.9.7 con un parche de seguridad urgente lanzado el 19 de febrero de 2024 [9]. CVE-2024-1709, vulnerabilidad de omisión de autenticación con una clasificación de gravedad crítica de 10/10, compromete ScreenConnect al permitir que usuarios no autorizados manipulen el acceso URL (exp. /SetupWizard.aspx/anygivenstring) al asistente de configuración, obteniendo potencialmente privilegios administrativos completos. y ejecutar código arbitrario.

Se descubrió una vulnerabilidad crítica, identificada como CVE-2023-22527, en Atlassian Confluence, que presenta un riesgo de seguridad grave con una puntuación CVSS de 10 [10]. Esta vulnerabilidad se debe a una falla de inyección de plantilla dentro del lenguaje de navegación de gráficos de objetos (OGNL), un componente ampliamente utilizado en aplicaciones web para crear plantillas del lado del servidor. El método de explotación implica que los atacantes se dirijan a archivos de plantilla .vm específicos dentro de Confluence, que manejan incorrectamente la entrada proporcionada por el usuario. Por ejemplo, la vulnerabilidad se identificó en el archivo /confluence/template/aui/text-inline.vm , donde los atacantes podían inyectar código malicioso a través de parámetros destinados a funciones legítimas de la página. Este archivo, entre otros, no logró desinfectar adecuadamente la entrada, lo que permitió a los atacantes ejecutar comandos de forma remota en el sistema afectado.

Para abordar esta vulnerabilidad, Atlassian ha lanzado actualizaciones para Confluence Data Center y Server, particularmente la versión 8.5.4 y posteriores , que incluyen parches para mitigar el riesgo de explotación. Estas actualizaciones corrigen la vulnerabilidad garantizando que la entrada del usuario se desinfecte adecuadamente y eliminando o protegiendo los archivos de plantilla afectados.

Acabamos nuestra cibercrónica del mes tratando una vulnerabilidad de Exchange. Es posible que los administradores de Exchange hayan disfrutado de un raro descanso de dos meses en la aplicación de parches, pero este mes se publica CVE-2024-21410 , una vulnerabilidad crítica de elevación de privilegios en Exchange. Microsoft explica que un atacante podría usar credenciales NTLM adquiridas previamente a través de otros medios para actuar como víctima en el servidor Exchange mediante un ataque de retransmisión NTLM. Una posible vía para esa adquisición de credenciales: una vulnerabilidad de fuga de credenciales NTLM en Outlook como CVE-2023-36761 , sobre la cual Rapid7 escribió en septiembre de 2023 .

Para agravar la preocupación de los defensores: Exchange 2016 figura como afectado, pero aún no figura ningún parche en el aviso CVE-2024-21410 . Los parches de Exchange 2019 están disponibles para CU13 y la nueva serie CU14. Según Microsoft, las instalaciones de Exchange donde la Protección extendida para la autenticación (EPA) ya está habilitada están protegidas, aunque Microsoft recomienda encarecidamente instalar la última actualización acumulativa. Se proporcionan más recursos en el aviso, incluida la guía genérica de Microsoft sobre cómo mitigar los ataques estilo Pass the Hash , así como el script Exchange Server Health Checker de Microsoft , que incluye una descripción general del estado de la EPA. La serie de actualizaciones Exchange 2019 CU14 habilita EPA de forma predeterminada.

Un día después de la publicación inicial, Microsoft actualizó el aviso de CVE-2024-21410 para indicar que, de hecho, ya habían tenido conocimiento de la explotación.

Christian Agreda Romero
Cybersecurity Lead Analyst

Integración de la seguridad de la información en las operaciones diarias de la Organización - El caso de DevSecOps

Por Notis Iliopoulos

La transición a la nueva realidad digital, liderada por grandes programas de transformación digital, junto con el rápido cambio y la adopción de la tecnología que la respalda, resalta la necesidad de implementar uno de los principios fundamentales de la seguridad de la información: integrar las responsabilidades de seguridad de la información en cada rol laboral. Este artículo se centra en incorporar los requisitos de seguridad de la información en el desarrollo de software/sistemas y las operaciones de sistemas de información, explorando cómo esto se puede lograr mediante la adopción e implementación práctica del enfoque DevSecOps.

DevOps ya ha sido adoptado como un proceso estándar con el objetivo de cerrar la brecha de colaboración entre los departamentos de desarrollo de software y los departamentos de operaciones de infraestructura de TI, para mejorar la fiabilidad del software, optimizar el ciclo de implementación de nuevas versiones (CI/CD) y reducir el tiempo de implementación. El proceso de DevOps, sirviendo como precursor de DevSecOps, fue rápidamente adoptado por empresas de desarrollo de software y organizaciones que dependen en gran medida de sistemas y aplicaciones de TI. Sin embargo, rápidamente se evidenció que los requisitos de seguridad de la información, el cumplimiento normativo, la protección de datos personales y la resistencia del software (colectivamente denominados seguridad de la información) deben ser parte del proceso de DevOps. En consecuencia, surgió la filosofía de DevSecOps, abarcando todos estos aspectos críticos.

La velocidad y frecuencia con la que se desarrollan y ponen a disposición nuevas versiones de software demuestran que los métodos tradicionales de gestión de la seguridad de la información, protección de la privacidad y cumplimiento normativo son ineficaces y obsoletos. La adopción del enfoque DevSecOps tiene como objetivo introducir un nuevo proceso que integre los requisitos de seguridad de la información en todo el ciclo de vida del desarrollo de software, considerando también las metodologías de desarrollo de software Agile más flexibles. Este proceso representa una evolución natural del proceso de DevOps y tiene como objetivo incorporar los requisitos de seguridad de la información en cada paso de las nuevas metodologías ágiles de desarrollo de software. Por lo tanto, los requisitos de seguridad de la información forman parte de cada ciclo de desarrollo de software (sprint) y no solo se abordan al final del proceso de desarrollo de software, como ocurre en los métodos tradicionales.

Un principio fundamental del proceso de DevSecOps es fomentar una cultura, seguida de una metodología de implementación relevante, donde los requisitos de seguridad de la información se integren sin problemas en los procesos de desarrollo, instalación y soporte de software. Por esto, las prácticas actuales y antiguas requieren ajustes o sustitución por un enfoque que se adapte fácilmente para garantizar la inclusión de todos los requisitos de seguridad de la información en un proceso repetible que se ajuste fácilmente al panorama tecnológico dinámico actual. Teniendo esto en cuenta, la seguridad de la información debe considerarse como un servicio que se proporciona a cada fase del ciclo de vida de desarrollo de nuevos productos de software o durante el proceso de CI/CD de aplicaciones de software existentes. Por lo tanto, la adaptación constante del proceso, su operación fluida y repetible y su automatización se convierten en un requisito esencial.

A continuación, se presentan los requisitos clave sobre seguridad de la información para cada fase del desarrollo de software que deben incluirse en el proceso de DevSecOps:

Diseño y Análisis: Durante la fase de diseño, el equipo de implementación identifica las necesidades de seguridad de la información para cada etapa del proyecto y asigna las responsabilidades pertinentes a ingenieros con las habilidades adecuadas. Al mismo tiempo, se lleva a cabo una evaluación inicial de amenazas y riesgos de seguridad de la información relacionados (perfilado de amenazas), con el objetivo de definir los requisitos y especificaciones de seguridad de la información para el entregable final (nuevo producto o nueva versión). Una forma efectiva de lograr esto es mediante la redacción y documentación del "Plan de Seguridad" del producto en desarrollo, que incluye las amenazas de seguridad de la información, posibles vulnerabilidades y medidas de protección propuestas. Además, el plan debe abordar los requisitos tanto para la protección de datos personales como para el cumplimiento normativo.

Diseño Arquitectónico del Producto: Adopción de la filosofía "Seguridad desde el Diseño", según la cual cada producto o cada nueva versión del producto se diseña desde el principio, teniendo en cuenta las mejores prácticas de seguridad de la información, que conciernen a cada componente del producto, desde el código fuente hasta la infraestructura en la que se instalará y operará. Durante el diseño arquitectónico, el mencionado "Plan de Seguridad" sirve como herramienta principal para diseñar las medidas de seguridad necesarias y considerar los requisitos de cumplimiento normativo relevantes.
Desarrollo y Revisión del Código Fuente: La preocupación principal es la mejora continua de la calidad, seguridad y resistencia del producto final a través del código fuente. Para ello, es necesario capacitar continuamente a los desarrolladores de prácticas de programación segura y resistente. Además de la capacitación, es necesario disponer de pautas documentadas sobre seguridad del código fuente, a las que los desarrolladores deben adherirse rigurosamente. A lo largo de la fase de desarrollo del código fuente, los principios mencionados deben ser conocidos e implementados por los ingenieros de software.

Revisión de Seguridad del Software: La revisión periódica del código fuente generado para identificar posibles vulnerabilidades de seguridad de la información y problemas de resistencia, debe considerarse como parte de las responsabilidades de los equipos de desarrollo de software. Esto se puede lograr mediante una combinación de herramientas automatizadas y verificaciones manuales, que debería ser parte de las prácticas regulares de inspección de software.

A diferencia de los métodos tradicionales, donde la revisión de seguridad del software se realiza al final de la fase de desarrollo por un equipo en particular, el proceso DevSecOps integra revisiones de seguridad a lo largo de la fase de desarrollo. Esto permite identificar y remediar tempranamente las vulnerabilidades de seguridad de la información. Además, las organizaciones que adoptan el proceso DevSecOps deben desarrollar y mejorar aún más los controles de seguridad de la información relacionados con el desarrollo de software, debido a la adopción de métodos ágiles de desarrollo de software que permiten la integración e implementación continua de nuevas versiones de software.
En un entorno así, es necesario incluir todos los controles requeridos para evaluar la seguridad del nuevo software o lanzamiento lo más temprano posible. Las evaluaciones deben detectar posibles vulnerabilidades de seguridad tanto en el flujo lógico del software como en la comunicación entre sus diferentes componentes, incluidas las interacciones a través de las interfaces de programación (APIs). Dichas evaluaciones pueden llevarse a cabo mediante el uso de herramientas automatizadas (análisis dinámico del código fuente) y ejercicios de pruebas de penetración. Además, estas evaluaciones deberían incorporarse en los escenarios de prueba predeterminados del entregable final, asegurando una gestión integral de las evaluaciones y pruebas realizadas en cada etapa.

Instalación: La implementación de la nueva versión de un producto de software en el entorno de producción se realiza mediante procesos automatizados, garantizando una implementación segura y confiable de la última versión. Además, es fundamental fortalecer el nivel de seguridad del entorno de producción donde se instala el producto, de acuerdo con la importancia de los datos alojados y las mejores prácticas aplicables.
Operación: Durante la fase operativa del nuevo software, se utilizan procesos automatizados para detectar vulnerabilidades técnicas de seguridad. Esto implica el uso de sistemas de monitoreo para detectar ataques maliciosos, sistemas de detección de intrusiones y sistemas de escaneo de vulnerabilidades de seguridad. De esta manera, se aumenta la efectividad de los controles contra posibles debilidades técnicas que los atacantes malintencionados podrían explotar. Al mismo tiempo, se recopila información en tiempo real para identificar posibles violaciones de seguridad en el entorno de producción, incluidas las violaciones relacionadas con el software. Cualquier defecto o vulnerabilidad identificada a través del monitoreo se informa a los ingenieros de operaciones del entorno de producción para que se resuelvan, asegurando una mejora continua, una mayor confiabilidad y seguridad del producto.

Trampas que necesitamos evitar
Adoptar la filosofía de DevSecOps es un proceso en sí mismo, que requiere una planificación cuidadosa y una implementación fluida. Para mejorar la efectividad del proceso y facilitar su integración en el entorno operativo existente, recomendamos evitar algunos obstáculos importantes:

Centrarse únicamente en cómo automatizar partes del proceso de DevSecOps: Para aprovechar plenamente las ventajas de DevSecOps, los requisitos de seguridad de la información deben ser parte de cada etapa del ciclo de vida del desarrollo de software. Como primer paso para adoptar DevSecOps, se recomienda formar un equipo interdepartamental de expertos que participen activamente y contribuyan en todas las fases del ciclo de vida del desarrollo de software, al mismo tiempo que optimicen el proceso agregando la automatización necesaria para respaldarlo.

Incapacidad para obtener el apoyo de la dirección: Para garantizar el apoyo de la dirección, es necesario resaltar las ventajas de adoptar el proceso de DevSecOps. Esto incluye enfatizar en la mayor efectividad del proceso general de desarrollo e implementación de software, así como en el nivel mejorado de seguridad y confiabilidad del producto o versión.

Aplicar las prácticas de DevSecOps solo al desarrollo de nuevos productos: La adopción del proceso de DevSecOps se facilita durante el desarrollo de nuevos productos de software, sin embargo, su valor inmediato para la organización se puede realizar aplicándolo a productos de software existentes, mostrando resultados inmediatos, como maximizar la flexibilidad, seguridad y confiabilidad del lanzamiento de nuevos productos. Por lo tanto, se debe entender el valor agregado del nuevo proceso y aplicarlo como una prioridad en las áreas que demuestren directamente su utilidad.
Incapacidad o fracaso para crear la cultura necesaria y las habilidades relevantes: La falta o el fracaso en establecer la cultura adecuada y desarrollar las habilidades pertinentes: La implementación del proceso de DevSecOps implica un cambio cultural, donde todos los implicados en el desarrollo del producto asumen la responsabilidad de la seguridad de la información, la fiabilidad y la resistencia, en lugar de delegarla en un equipo específico. Además, la formación y el desarrollo de las habilidades necesarias son cruciales para el éxito global de la adopción de DevSecOps.

Adopción efectiva y evolución del proceso DevSecOps
El principal cambio que impacta la manera actual de trabajar es establecer un equipo de trabajo interdepartamental horizontal. Este equipo estará formado por profesionales con diferentes habilidades que suelen trabajar en diferentes unidades organizativas, enfocados verticalmente en áreas específicas de experiencia. Esto implica la necesidad de eliminar los silos organizativos. Además, requiere desmantelar los silos organizativos que tradicionalmente separan a diferentes equipos y departamentos dentro de una organización. Es necesario crear una unidad organizativa permanente o un equipo virtual multifuncional de DevSecOps compuesto por profesionales con habilidades específicas de diferentes departamentos.

Claramente, el cambio más significativo que una organización debe experimentar es cultural. Esto abarca la operación, el nivel de agilidad y los servicios que el proceso DevSecOps pretende ofrecer. Por esto, la organización necesita identificar a aquellos que pueden contribuir y promover este cambio en términos de mentalidad y forma de trabajar, y designarlos como miembros clave del proceso DevSecOps. Esto llevará a la formación y operación de un equipo multifuncional, ya sea como una entidad completamente autónoma o una fuerza de tarea virtual. El objetivo principal es transferir todo el conocimiento adquirido en toda la organización, garantizando que la seguridad de la información se convierta en una parte integral del diseño y desarrollo de nuevos productos de software y nuevas versiones.

Los equipos DevSecOps, ya sean autónomos o virtuales, deben estar compuestos por ingenieros con habilidades diversas, capaces no solo en sus dominios de experiencia, sino también de enriquecer continuamente sus capacidades. Esto les permite ejecutar de manera efectiva una variedad de tareas interconectadas dentro del desarrollo de un nuevo producto o una nueva versión de software. Dichas tareas incluyen el desarrollo de software, la implementación y optimización de controles de seguridad de la información, y el mantenimiento y soporte de la infraestructura de TI. Cada miembro del equipo es responsable de la seguridad y confiabilidad del producto, ya sea para clientes externos o uso interno.

El proceso DevSecOps, desde su fase de inicio, debe servir como un marco robusto, ofreciendo servicios y creando metodologías, procedimientos y herramientas que se puedan utilizar con o sin la participación de los miembros del equipo DevSecOps. Al mismo tiempo, los miembros del equipo DevSecOps deben mejorar la efectividad de los servicios y herramientas que utilizan, así como capacitar y orientar a otros ingenieros sobre seguridad de la información, resistencia y confiabilidad del software.

Conclusión

DevSecOps se rige por una nueva filosofía que conduce a un nuevo enfoque en el desarrollo de nuevos productos y nuevas versiones de software. En la mayoría de los casos, no es necesario crear una unidad organizativa específica dedicada a las actividades de DevSecOps. La efectividad de la nueva filosofía/proceso se maximiza una vez que se convierte en una forma convencinal de trabajar y se integra como parte estándar de la cultura en cuanto al desarrollo de nuevos productos y lanzamientos de software.

Según las predicciones y tendencias recientes, hay una adopción más amplia de la filosofía que transformará DevSecOps en BizDevSecOps. Este es un nuevo enfoque para el desarrollo de productos de software que elimina las fronteras entre el mundo empresarial y los equipos técnicos, con el objetivo de capacitar a las empresas para construir productos de software más rápidos y confiables, adaptados a las necesidades del usuario final.

Notis Iliopoulos
Senior Manager
Cybersecurity EMEAL

Aplicaciones seguras en un sistema de gestión iam

Por Mijail Muñoz

En la securización de las aplicaciones, una línea clave es la Gestión de la Identidad y de los accesos. Uno de los focos de los atacantes es el robo de la identidad del usuario, para poder ejecutar operaciones fraudulentas. Contra esto, la concientización a todos los empleados debe ser una de las principales estrategias de la ciberseguridad en una organización.

Actualmente, existen diversos factores de ataque al usuario de una organización, por el cual se describirán algunos más conocidos como:

• Phishing: Ataque al usuario por médio de um correo electrónico.
• Ransomware: Software malicioso que inutiliza el dispositivo y encripta la información.
• Spyware: Programa que se instala en el ordenador y recopila la información del usuario.
• Troyano: Malware que puede ser el vehículo de transmisión de un virus con el que espiar, robar datos o tomar el control del dispositivo.
• Inyección SQL: Tipo de ciberataque afecta a los servidores de las empresas, los infecta y extrae información relevante, como datos de clientes, cuentas bancarias y contraseñas.
•Denegación de servicio (DoS): Su objetivo es sobrecargar el servidor de una página web para inutilizarla.

La implementación de aplicaciones seguras en un sistema IAM contribuye a fortalecer la seguridad, garantizar la conformidad con regulaciones y mejorar la eficiencia en la gestión de identidades y accesos. Es importante mantenerse actualizado con las mejores prácticas de seguridad y ajustar las políticas según evolucionen los riesgos y las necesidades organizativas.
Para garantizar la seguridad en un sistema de gestión IAM (Identity and Access Management), es importante utilizar aplicaciones que cumplan con las mejores prácticas de seguridad. En particual se debe asegurar que las aplicaciones cuenten con:

1. Provisionamiento y Desprovisionamiento Automatizado
Automatizar la creación, modificación y eliminación de cuentas de usuario ayuda a evitar errores humanos y garantiza la consistencia en la aplicación de políticas de seguridad.

2. Control de Acceso Basado en Roles (RBAC)
Utilizar modelos de RBAC garantiza que los usuarios solo tengan acceso a los recursos y datos necesarios para realizar sus funciones específicas. Esto minimiza los riesgos asociados con el acceso innecesario.

3. Monitoreo de Actividades del Usuario
Registrar y monitorear las actividades de los usuarios ayuda a detectar comportamientos inusuales o actividades maliciosas. Esto es crucial para cumplir con regulaciones de seguridad y responder rápidamente a amenazas.

4. Autenticación Multifactor (MFA)
Implementar MFA añade una capa adicional de seguridad al requerir más de una forma de autenticación. Esto reduce significativamente el riesgo de acceso no autorizado incluso si las credenciales de usuario se ven comprometidas.

5. Gestión de Contraseñas
Implementar políticas de contraseña fuertes y utilizar herramientas de gestión de contraseñas puede mejorar la seguridad sin sacrificar la usabilidad.

6. Federación de Identidad:
Permite a los usuarios acceder a múltiples sistemas y aplicaciones con una única identidad, reduciendo la necesidad de gestionar múltiples credenciales. Esto también puede mejorar la seguridad al centralizar la autenticación.

7. Auditorías y Reportes:
Realizar auditorías periódicas y generar informes detallados sobre las actividades de los usuarios y los cambios en los privilegios ayuda a cumplir con los requisitos de conformidad y a identificar posibles problemas de seguridad.

8. Gestión de Sesiones:
Monitorear y gestionar las sesiones de usuario puede prevenir el acceso no autorizado, especialmente en entornos sensibles. La implementación de cierre de sesión automático tras períodos de inactividad también es recomendable.

9. Automatización de Políticas de Acceso:
Automatizar la aplicación y actualización de políticas de acceso ayuda a garantizar que los cambios se realicen de manera consistente y oportuna, reduciendo el riesgo de configuraciones incorrectas.

10. Cifrado de Datos:
Implementar cifrado para proteger datos confidenciales, tanto en reposo como en tránsito, garantizando que solo los usuarios autorizados puedan acceder a la información sensible.

11. Gestión de Identidad en la Nube:
Si se utilizan servicios en la nube, es esencial gestionar de manera segura las identidades y accesos, adaptándose a los modelos de seguridad específicos de la nube.

La ciberseguridad es un campo en constante evolución, por lo que es fundamental estar al tanto de las últimas tendencias, amenazas y soluciones en IAM. Por esto, es recomendable que las empresas realicen un Assessment IAM de las Unidades Organizacionales o de las aplicaciones de manera periódica, con el propósito de encontrar puntos de mejora en los 06 dominios (Gestión de cuentas, Gestión de Autenticación, Gestión de Políticas y Procedimientos, Gestión de roles y permisos, Gestión del sistema IAM y Gestión de cuentas privilegiadas) y adaptar su sistema de control de accesos y de identidad tanto a nuevas amenazas como a evolución que haya tenido la organización desde el último assessment.

Mijail Muñoz
Cybersecurity IAM Leader

IA: Más allá de la industrialización de las labores de seguridad en el ciclo de vida del desarrollo del software.

La integración de la Inteligencia Artificial en la industria del desarrollo de software es una realidad que ha venido para quedarse. Actualmente, son muchos los proveedores que compiten por ser el primero en introducir la IA en la detección y corrección automática de vulnerabilidades en los ciclos de vida de desarrollo software de sus clientes.

La disrupción de la Inteligencia Artificial en el mercado del desarrollo de software está provocando un cambio en el modo en que las organizaciones tienden a industrializar sus pruebas de calidad y seguridad durante el ciclo de vida de desarrollo de software (en adelante SDLC).

Son muchos los usos que se están dando a la IA, con fines más o menos lícitos, por lo que se ha abierto el debate de la necesidad de regulación de esta recién nacida tecnología. En cualquier caso, la gran variedad de opciones que aportan las diferentes aplicaciones de la IA, se traduce en interesantes alternativas para la creación herramienta desde el punto de vista de la ciberseguridad.

Y es que, aunque hoy en día, la ciberseguridad depende en gran medida de los aportes humanos, gradualmente vemos que la tecnología se vuelve mejor que nosotros en tareas específicas, por eso se está empezando a integrar la IA con diferentes fines:

• Detección y alerta automática de ataques en tiempo real.
• Protección de datos en entornos híbridos (Legacy y/o Cloud)
• Clasificación automática de vulnerabilidades y asignación de riesgo mediante aprendizaje automático.
• Identificación de malas prácticas de seguridad en tiempo de desarrollo.
• Aportación de recomendaciones de seguridad para la resolución de vulnerabilidades o defectos.
• Identificación de requisitos de seguridad.
• Y otros tantos fines que se puedan imaginar.

En lo que compete al SDLC, las organizaciones están investigando diferentes vías que permitan automatizar las tareas en las diferentes fases:
1) Requisitos.
2) Diseño.
3) Implementación/desarrollo.
4) Testing y verificación.
5) Despliegue.
6) Operación.

Las alternativas que la IA nos proporciona a nivel de herramientas automáticas, está desencadenando un gran avance también los entornos SecDevOps, conduciéndonos a la evolución de lo que a día de hoy conocemos como herramientas AST (Application Security Testing). Estas herramientas están comenzando a sustituir sus motores de búsqueda por la IA, dotándolas de un mejor rendimiento cognitivo, con el objetivo de detectar defectos y vulnerabilidades en las diferentes fases del SSDLC.
Comienzan a ser muchos los proveedores de herramientas AST, que están desarrollando módulos de integración con ChatGPT o desarrollando su propia IA, aprovechando la potencia que esta tecnología ofrece. Gracias a la IA, no se necesita desarrollar motores de reglas y/o políticas que detecten patrones o flujos en el código, sino que la propia base de datos de la IA responderá a los defectos que pudiesen encontrarse en el código, en la aplicación en ejecución o en los entornos.
Por tanto, el camino que parece estar tomando la industria de la automatización parece estar orientándose hacia el desarrollo de módulos sencillos que hagan consultas a la IA, dejando a ésta las tareas complejas de decisión y potencia de cognitiva. Estos módulos funcionarán a modo de APIs, transformando las diferentes consultas a un lenguaje conocido por la IA que estemos usando. De esta forma seremos capaces de abarcar las pruebas de seguridad en todas las fases del SDLC, empleando:

• Módulos que consulten a la IA para el establecimiento de los requisitos de seguridad del software a diseñar en función de una serie de parámetros determinados por las necesidades a cumplir (tecnologías a usar, lenguajes, librerías, componentes, entornos, plataformas, integraciones, etc.)
• Integraciones con en el IDE para detectar defectos en tiempo de desarrollo, marcándolos en tiempo real y aportando a los desarrolladores alternativas para solventarlos.
• Módulos de Identificación de mejoras a implementar en el propio SDLC en función de los errores, vulnerabilidades, hallazgos o defectos más recurrentes.

• Iniciativas de concienciación y/o formación para desarrolladores en función de las tecnologías usadas y los defectos y vulnerabilidades encontradas.
• Desarrollo de herramientas para la consulta de vulnerabilidades en código, librerías o en tiempo de ejecución.
• Módulos de detección automática de firmas de malware y respuesta automática ante incidentes.
• Predicción de ataques en función de los comportamientos del software o sistemas.
• Automatización de la categorización de eventos, alertas y/o vulnerabilidades.
• Y otro sinfín de necesidades no cubiertas aún por las organizaciones y que se podrá abordar mediante el desarrollo de un simple módulo que realice la traducción de una consulta a la IA.

Estamos convencidos de que estas integraciones de las herramientas AST con la IA, traerá consigo un a mayor eficiencia de las tareas de revisión de la seguridad en el software suponiendo en última instancia un gran ahorro de costes. Observando su trayectoria, la IA reducirá muy probablemente los "Falsos Positivos o Falsos Negativos" en los hallazgos, así como la fatiga de alertas y eventos. Además, está permitiendo mejorar procesos de categorización y clasificación de dichos hallazgos de forma automática, lo cual vuelve a repercutir en la agilidad de las tareas de desarrollo seguro de Software.

Sin embargo, a pesar de la potencia que empieza a presentar la IA moderna, todavía no es capaz de interpretar los resultados con las mismas capacidades que un ser humano, por lo que no debemos dejar de revisar estos resultados en busca de posibles "Falsos Positivos o Falsos Negativos". En este sentido, los equipos de seguridad no deberíamos temer por ser sustituidos por una IA (al menos de momento), pues los equipos humanos seguirán siendo necesarios para la operación, revisión de resultados y o toma de decisiones "creativas". No obstante, y como es habitual en el campo de la ciberseguridad, el verdadero reto será continuar reciclándonos, invirtiendo en mantenernos actualizados en las nuevas tendencias del mercado y el futuro de tecnología. El sector necesita más expertos de ciberseguridad con especialidad en IA, capaces de innovar en la integración de ambos mundos y obtener el rendimiento diferencial que se espera de esta tecnología.

Desde NTT DATA estamos convencidos de que la integración de la IA en los entornos SecDevOps es una realidad que aún está tomando forma, ya que, aunque se está trabajando en la actualidad, la IA aún está por gobernar, es una herramienta muy potente pero que necesita estabilizase para marcar la confianza.

La IA también está madurando, estableciendo entornos de confianza, modelos cerrados que no comparten datos y permitirán una mayor privacidad y que conseguirán que la IA se haga adulta y podamos, ahora sí, incluirla en entornos productivos e industrializados

Caminamos por un sendero que se vislumbra emocionante, a la vez que motivante para los que trabajamos en compañías tecnológicas. En un momento en el que la evolución hacia el Cloud es primicia, junto con la automatización e industrialización, revolucionadas por la potencia cognitiva de la IA. Bajo este escenario, los equipos de seguridad tendremos que dar el 200% para abordar el nuevo paradigma, pero...¿quién dijo miedo?

Jose Carlos Moral Cuevas
Chief of Security Architecture
Area & Technical Manager

Incrementando la seguridad de las aplicaciones a través de Security Chaos Engineering

Tendencias

Es probable que todas las aplicaciones existentes en el mundo hayan sufrido algún tipo de fallo que haya puesto en apuros a más de uno. En 2011 Netflix introduce el concepto de caos en sus sistemas con el fin de probar su resiliencia; al apagar aleatoriamente instancias de EC2 en AWS lograron determinar que sus balanceadores de carga no funcionaban eficientemente. Hoy en día esta poderosa idea se ha trasladado a la ciberseguridad ofreciendo una perspectiva innovadora para descubrir vulnerabilidades en las aplicaciones.

Security Chaos Engineering consiste en introducir deliberadamente fallos de seguridad en las aplicaciones con el fin de analizar el comportamiento de sus componentes. Este concepto supone un cambio en la forma en que se audita la seguridad de un sistema, posibilitando la identificación de escenarios de riesgo que no son fácilmente detectables.
En la actualidad, la productividad del ciclo de vida del software se ha apalancado en prácticas DevOps, la construcción y entrega rápida de funcionalidades son fundamentales para garantizar transformación digital. Asimismo, la seguridad se ha mejorado al integrar herramientas de análisis estático y dinámico que permiten identificar vulnerabilidades rápidamente.

Sin embargo, una excesiva confianza en las herramientas puede llegar a ser contraproducente, en especial cuando los motores de escaneo no son lo suficientemente robustos o cuando los equipos de desarrollo pueden manipular las configuraciones, es allí donde el Hacking Ético sigue jugando un papel fundamental en el descubrimiento de aquellas brechas que no pueden ser identificadas mediante automatización.

Entonces, si existen herramientas automatizadas de seguridad y Hacking Ético para probar las aplicaciones ¿cuál es el aporte de Security Chaos Engineering? El poder de este concepto radica en su metodología, pues se basa en el descubrimiento de vulnerabilidades a través del método científico. Del mismo modo en que Pasteur descubrió la penicilina, a través de la observación de un evento, la formulación de una hipótesis y la ejecución de un experimento es posible descubrir nuevos escenarios de riesgo en las aplicaciones.

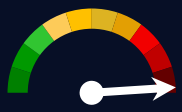
Imagine el siguiente escenario, la cuenta de un desarrollador de software ha sido comprometida por un adversario debido a credenciales débiles y la ausencia de múltiple factor de autenticación; El adversario se propone infectar los repositorios de las aplicaciones con código malicioso con el fin de ganar acceso a los servidores de la organización. ¿El ecosistema DevOps (procesos, herramientas y personas) tendrán la capacidad de detectar, prevenir y mitigar este tipo de vector de ataque?
SolarWinds asumía que sí, sin embargo, su herramienta de análisis estático no detectó el código malicioso, sus stakeholders no alertaron sobre desarrolladores auto-promoviendo código a las ramas principales, tampoco se detectaron las variaciones injustificadas en rendimiento de sus servidores, ni mucho menos el tráfico de paquetes no convencionales en su red, desencadenando el Supply Chain Attack con mayor impacto de las últimas décadas, afectando más de 20.000 empresas en todo el mundo.

Security Chaos Engineering brinda la posibilidad de inyectar fallos de seguridad en el código fuente, en librerías, servidores e incluso en la misma arquitectura de solución de un sistema con el fin de determinar si la organización se encuentra preparada ante ataques dirigidos. Por otro lado, Security Chaos Engineering promueve la automatización por lo que lo ideal es que las hipótesis, observabilidad y experimentos puedan ser automatizados a través de Scripting con el fin de ser puestos a prueba en diferentes aplicaciones y escenarios.
Con el auge de la transformación digital los ciberataques son cada vez más sofisticados y requieren nuevos mecanismos de protección y prevención, Security Chaos Engineering surge como un paradigma innovador que permite retar la seguridad de los sistemas y de este modo contribuir a mantener un ecosistema tecnológico resiliente y seguro.

Vulnerabilidades

Vulnerabilidad de inyección de código en PostgreSQL

Fecha: 06 de marzo de 2024
CVE: CVE-2024-27304



CVSS: 9.8

CRÍTICA

Descripción

Pgx es una librería para Go diseñada para interactuar con bases de datos PostgreSQL. El riesgo de seguridad identificado consiste en la posibilidad de inyección de código SQL cuando un atacante logra que una consulta o mensaje de enlace supere los 4 GB de tamaño.

Este problema se debe a un desbordamiento de enteros en el cálculo del tamaño, lo que permite que un mensaje de grandes dimensiones se divida en varios mensajes bajo el control del adversario.

El fabricante ha instado a los usuarios a actualizar a la versión más reciente para solucionar dicha vulnerabilidad. Además, se propone como medida temporal el rechazo de peticiones que sobrepasen un determinado tamaño.

Productos afectados

La vulnerabilidad afecta al producto PGX, en concreto a las siguientes versiones:

- Versiones anteriores a la 4.18.2.
- Versiones comprendidas entre la 5.0.0 y la 5.5.3 (ambas inclusive).

Solución

Se recomienda que los usuarios que actualicen a las versiones 4.18.2 o 5.5.4 para protegerse contra posibles ataques.

Además, también recomiendan que rechacen cualquier entrada del usuario que pueda resultar en una sola consulta o mensaje de enlace que exceda los 4 GB de tamaño, mitigando el riesgo de explotación de esta vulnerabilidad.

Referencias

- www.incibe.es
- nvd.nist.gov

Vulnerabilidad de escalada de privilegios en Microsoft AKS

Fecha: 12 de marzo de 2024
CVE: CVE-2024-21400

CVSS: 9

CRÍTICA

Descripción

Microsoft Azure Kurbenetes Service (AKS) se trata de un servicio de administración de Microsoft Azure que permite a los usuarios implementar, administrar y escalar fácilmente clústeres de contenedores basados en Kubernetes en la nube de Azure.

La vulnerabilidad CVE-2024-21400 consiste en una elevación de privilegios del contenedor oficial del servicio de Microsoft Azure Kubernetes. La vulnerabilidad descubierta permite a los atacantes obtener acceso no autorizado a recursos que se encuentran protegidos dentro de un clúster de Kubernetes. Esto podría conducir a la manipulación de datos confidenciales, interrupción del servicio o incluso compromiso total del clúster.

Productos afectados

La vulnerabilidad afecta al producto de Microsoft Azure Kubernetes Service, en concreto a las siguientes versiones:

- Versiones anteriores a la 0.3.3.
- Desde la versión 1.0.0, ésta incluida.

Solución

Se recomienda actualizar a la última versión para corregir errores.

Esta actualización se llevará a cabo mediante la actualización de la extensión *confcom* usando la siguiente interfaz de línea de comandos:

- `az extension update -n confcom`

Referencias

- www.incibe.es
- www.msrc.microsoft.com

Parches

CRÍTICA

Nuevo parche de seguridad para JetBrains TeamCity

Fecha: 4 de marzo de 2024
CVE: CVE-2024-27198 y 3 más

Descripción

JetBrains ha publicado una serie de actualizaciones de seguridad para solucionar varios problemas que afectan al producto TeamCity. La actualización corrige un total de 4 vulnerabilidades, una de ellas de severidad crítica, otra de criticidad alta y otras dos de severiad media.

La vulnerabilidad crítica (CVE-2024-27198) permite a los usuarios omitir el proceso de autenticación, lo que a su vez les otorgaba acceso no autorizado para realizar acciones de administración. Esta brecha de seguridad permitía que cualquier persona pudiera ejecutar tareas de administración sin la necesidad de estar autenticado.

El resto de las vulnerabilidades corregidas son:

- CVE-2024-27199 (alta): vulnerabilidad de *path traversal*.
- CVE-2024-28173 (media): vulnerabilidad en los campos de tipo *password*.
- CVE-2024-28174 (media): autorización incorrecta de URLs de acceso a S3.

Productos afectados

Esta vulnerabilidad afecta al producto TeamCity en las versiones anteriores a la 2023.11.4. JetBrains organiza sus versiones en función de la fecha, por lo que se podrá observar de manera intuitiva si se cuenta con una versión anterior a la requerida.

Solución

JetBrains recomienda actualizar a la versión 2023.11.4 del producto, que contiene los parches necesarios para mitigar las vulnerabilidades descritas.

Referencias

- nvd.nist.gov
- www.jetbrains.com

ALTA

Nuevos parches para los sistemas operativos de Apple

Fecha: 5 de marzo de 2024
CVE: CVE-2024-23225 y 1 más

Descripción

Apple ha lanzado actualizaciones de seguridad de emergencia que corrige dos vulnerabilidades de 0-day en iOS, identificadas como CVE-2024-23225 y CVE-2024-23296, las cuales fueron explotadas en ataques dirigidos a dispositivos iPhone.

CVE-2024-23225 y CVE-2024-23296 consisten en dos vulnerabilidades de corrupción de memoria que afectan a los sitemaas operativos iOS y iPadOS. La explotación de esta vulnerabilidad permitiría a un atacante, con capacidades arbitrarias de lectura y escritura en el kernel, evadir las protecciones de memoria de este.

De este modo, CVE-2024-23225 consiste en una falla de corrupción de memoria del kernel, mientras que CVE-2024-23296 es una falla de corrupción de memoria RTKit.

Productos afectados

Las vulnerabilidades afectan a los siguientes dispositivos:

- iPhone XS y posteriores.
- iPad Pro de 12,9 pulgadas de 2.ª generación y posteriores.
- iPad Pro de 10,5 pulgadas.
- iPad Pro de 11 pulgadas de 1.ª generación y posteriores.
- iPad Air de 3.ª generación y posteriores.
- iPad de 6.ª generación y posteriores.
- iPad mini de 5.ª generación y posteriores.

Solución

Apple recomienda actualizar sus dispositivos a la versión iOS 17.4, iPad 17.4, iOS 16.7.6 y iPad 16.7.6, solucionando un problema de corrupción de memoria mediante la mejora de la validación.

Referencias

- support.apple.com
- securityaffairs.com

Eventos

IV JORNADAS STIC & CONGRESO ROOTED_CON (10 al 12 ABRIL)

Los dos eventos de referencia del sector de la ciberseguridad en España, las Jornadas STIC y el Congreso RootedCON, han aunado esfuerzos para organizar conjuntamente un nuevo capítulo internacional de sus encuentros, en esta ocasión en Panamá, del 10 al 12 de abril de 2024. Ambas han escogido a la ciudad panameña como lugar estratégico para celebrar el mayor evento de ciberseguridad de Latinoamérica

Link

I JORNADA CIBERLEGAL (23 ABRIL)

Red Seguridad celebrará, en el Ilustre Colegio de Abogados de Madrid el 23 abril, la primera Jornada Ciberlegal. Un evento de lo más novedoso cuyo objetivo principal es conocer de primera mano los retos que la ciberseguridad impone tanto a la Administración de Justicia (jueces, fiscales...) y Fuerzas y Cuerpos de Seguridad como a los profesionales del ámbito del Derecho (abogados, procuradores, etcétera) y a los departamentos legales de las organizaciones.

Link

ASLAN 2024 (17-18 abril)

La 31º edición del Congreso & Expo Aslan 2024 ya está en marcha, bajo el reclamo «Un gran avance en digitalización». Organizado por la asociación @aslan, el congreso explorará la inteligencia artificial (IA) en los procesos de transformación digital de las organizaciones. Y tendrá lugar los próximos 17 y 18 de abril de 2024 en el Palacio Municipal de Congresos Ifema en Madrid.

Link

MUNDO HACKER 2024 (22 – ABRIL)

En Mundo Hacker Day más de 30 expertos abordarán los diferentes temas de relevancia en el mundo de la ciberseguridad, además, los asistentes tendrán la oportunidad no sólo de compartir conocimiento y experiencias, sino de fomentar el networking.

Link

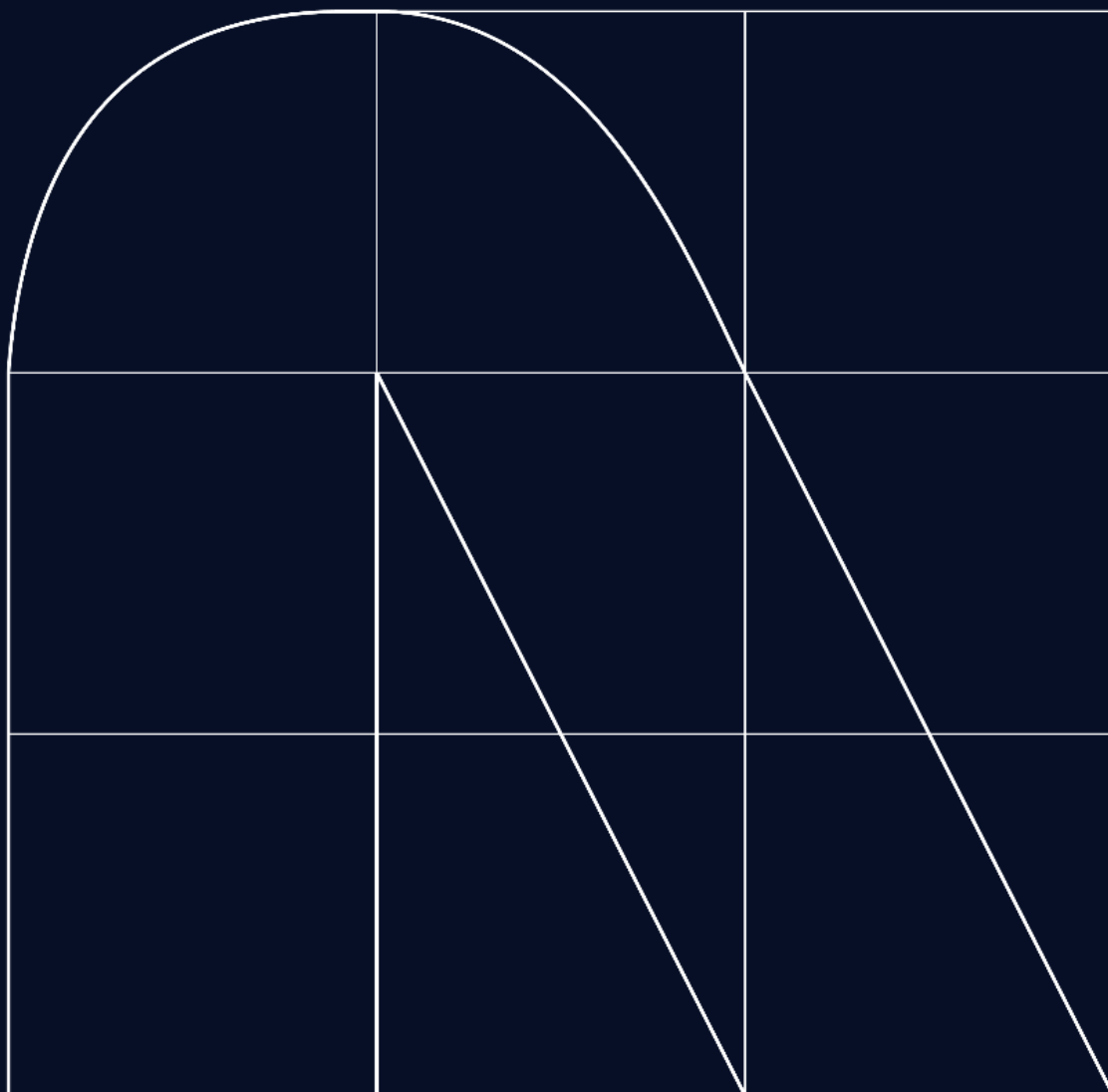
Recursos

Kali Linux 2024.1
La novedad más destacada de Kali Linux 2024.1 no está relacionada con el sistema operativo, sino con la infraestructura, ya que la distribución ha presentado la CDN Micro Mirror, la cual es “una red de espejos (mirrors) dedicados a servir Linux y Software Libre. A diferencia de los espejos tradicionales que albergan alrededor de 50TB de archivos de proyectos, los Micro Mirrors son máquinas con ‘solo’ unos pocos terabytes de almacenamiento que se centran en alojar solo los proyectos de mayor demanda.
Link

SORA
OpenAI, la empresa pionera en inteligencia artificial generativa, ha presentado Sora, un modelo revolucionario que convierte descripciones textuales en escenas de video realistas. Sora es capaz de crear escenas complejas con múltiples personajes y movimientos específicos, incluyendo detalles tanto del componente principal como del trasfondo. El modelo comprende cómo los objetos interactúan en el mundo físico y genera personajes convincentes que expresan emociones vibrantes.
Link

Tendencias de ciberseguridad 2024
Conoce las Tendencias en Ciberseguridad de mayor impacto para 2024 de varios analistas como Gartner, Google, Forrester, IDC y SealPath. Este artículo recoge las predicciones de futuro y pretende ayudarte a luchar contra las ciberamenazas en 2024 y a estar al tanto de lo último para mejorar tu capacidad de respuesta y adaptación.
Link

Ciber-Cluedo
El Centro Criptológico Nacional (CCN), adscrito al Centro Nacional de Inteligencia, ha desarrollado una nueva herramienta formativa para concienciar sobre el phishing. “Ciber-Cluedo” se incorpora ahora a la sección de gamificación de “Ángeles”. Su objetivo principal es fomentar el aprendizaje sobre amenazas de ciberseguridad, identificar los riesgos asociados a la suplantación de identidad, e implementar las medidas de seguridad adecuadas para una mejor protección ante este tipo de ataques.
Link



Powered by the cybersecurity NTT DATA team

es.nttdata.com