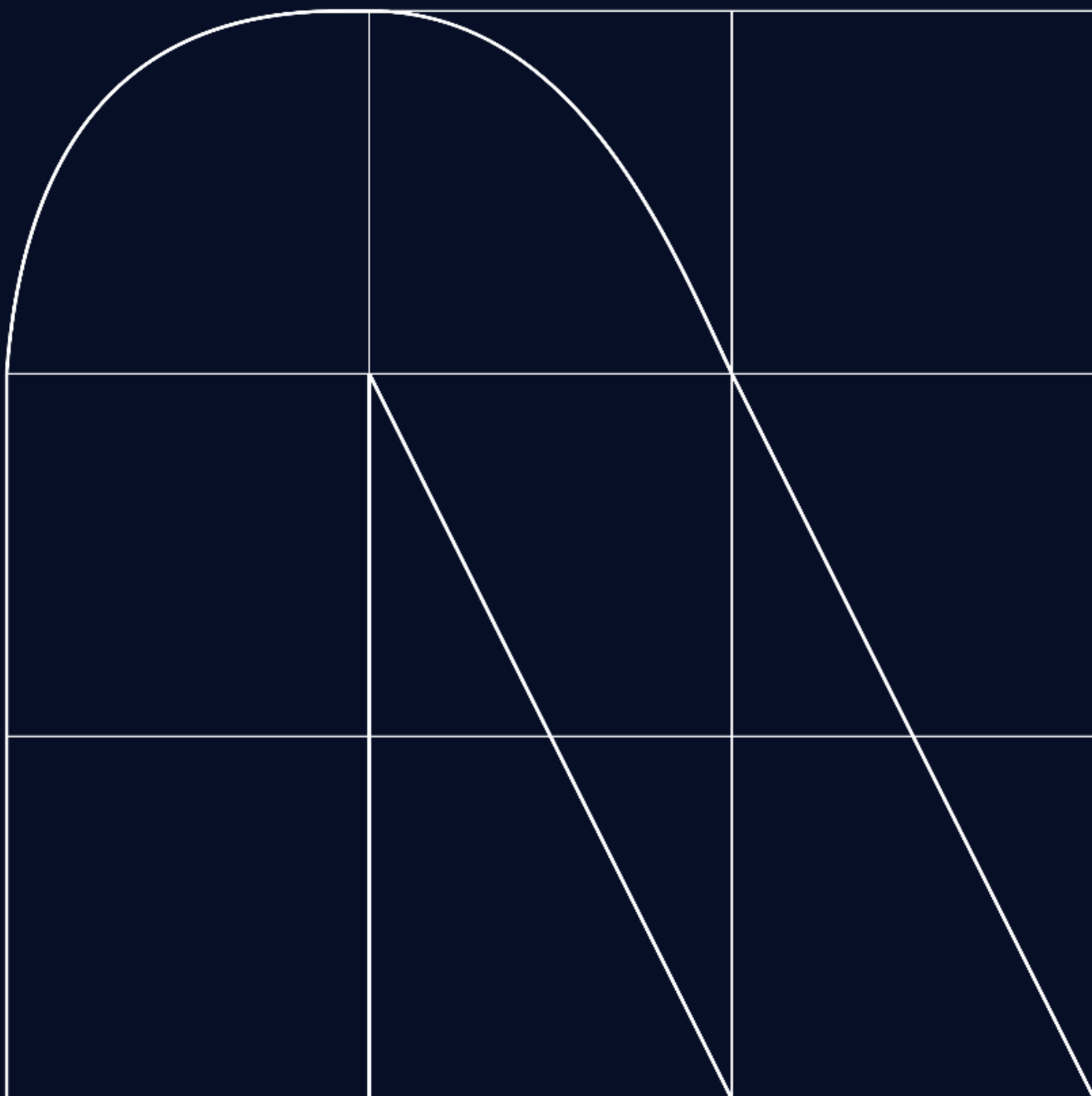
Número 85 | Diciembre 2023

NTT DATA

Radar

El magazine de ciberseguridad



El largo camino hacia la ciberseguridad evolutiva

Por: Conrad López

La política de seguridad de la información de una organización determina, en gran medida, cuáles son los objetivos de esta en ese terreno, asociados a la misión, visión y valores de dicha organización. La estrategia de ciberseguridad es el instrumento que permite a la dirección de la organización establecer el camino a seguir para alcanzar dichos objetivos a lo largo del tiempo, adaptándose a los cambios que la propia evolución de la compañía sufre como respuesta a las necesidades y requisitos determinados por el entorno cambiante en que se desenvuelve.

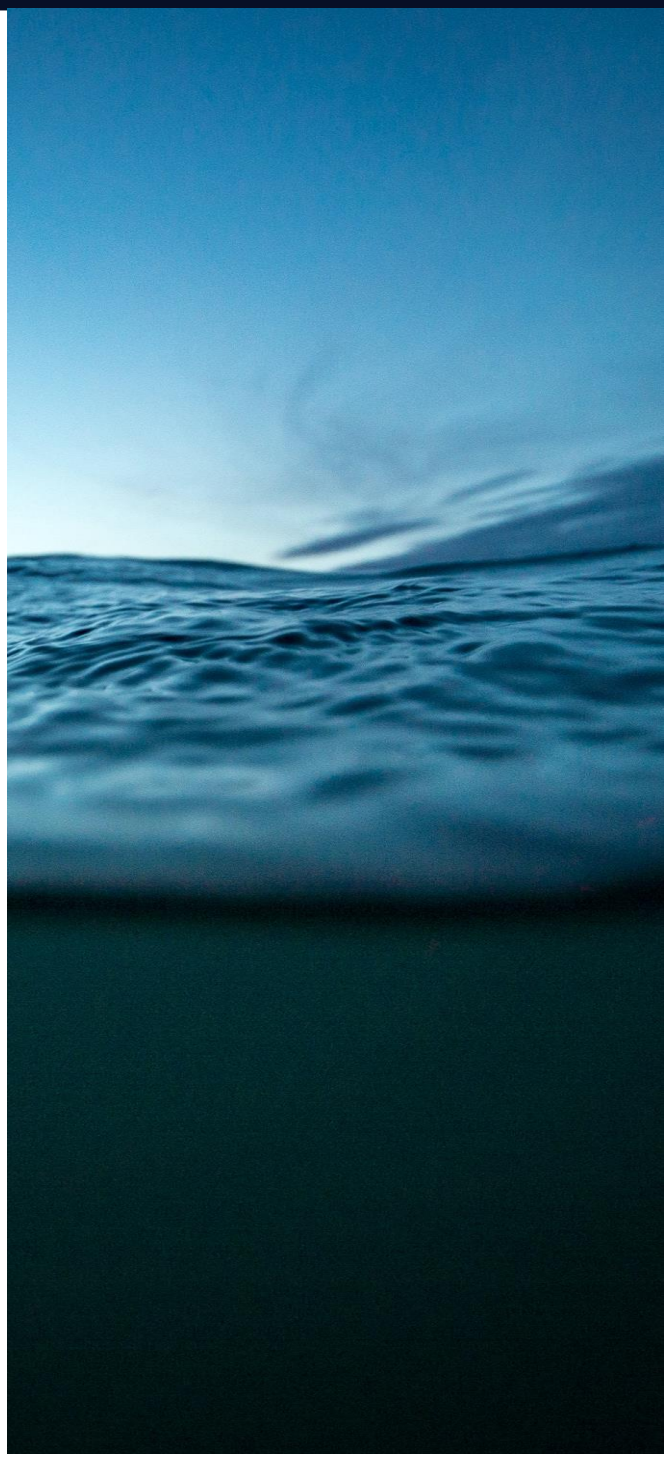
La alineación de la estrategia de ciberseguridad con la estrategia de negocio es un proceso continuo que requiere una colaboración estrecha entre la función de ciberseguridad y la dirección de la organización. Cuando se logra esta alineación, la ciberseguridad se convierte en un habilitador de los objetivos comerciales al proteger los activos y la reputación de la organización. Pero ¿cómo conseguir ese alineamiento estratégico? Algunos factores clave son:

Comprensión e involucración por parte de la dirección: es fundamental que los líderes de negocio comprendan la importancia de la ciberseguridad y como está intrínsecamente relacionada con el éxito de la organización. Esto se puede lograr a través de sesiones de concienciación y capacitación específicas para los líderes. En definitiva, la función de ciberseguridad debe estar involucrada en la planificación estratégica para asegurar que se tengan en cuenta los riesgos y las oportunidades de seguridad.

Integración en los procesos de negocio: la ciberseguridad debe estar "incrustada" de forma natural en los procesos de negocio de manera que sea un componente irrenunciable de la operación diaria. Esto incluye la identificación de activos críticos, la gestión de riesgos, la gestión segura de la cadena de suministro, la gestión de proyectos y la toma de decisiones.

Evaluación de riesgos tecnológicos y empresariales: no se trata solo de evaluar riesgos tecnológicos, sino también riesgos comerciales. Es necesaria una adecuada comprensión de cómo los riesgos cibernéticos pueden impactar en la continuidad del negocio, la reputación de la empresa y el cumplimiento normativo. En cualquier caso, el riesgo tecnológico es componente esencial del riesgo operativo de las organizaciones en su transformación digital.

Comunicación efectiva: es crucial establecer una comunicación constante entre la función de ciberseguridad y la dirección de la organización, manteniendo a los responsables informados sobre amenazas cibernéticas, vulnerabilidades y logros en la mitigación de riesgos.



Objetivos de ciberseguridad alineados: es necesario alinear los objetivos de ciberseguridad con los objetivos de desarrollo del negocio y de evolución tecnológica de la compañía. Para ello es necesario comprender e internalizar multitud de aspectos como:

Identificación del escenario de riesgo al que está sometida la organización, desarrollando una adecuada estrategia de inteligencia de amenazas y la respuesta necesaria, tanto de forma proactiva como reactiva.

Implicaciones normativas y requisitos tecnológicos impuestos por la presencia de la organización en diferentes ámbitos geográficos.

Necesidades de cumplimiento de la regulación existente en el sector de mercado en que se desenvuelve la organización

Nuevos retos de seguridad impuestos por la evolución tecnológica planeada para la organización para soportar su estrategia de negocio.

Mejora de la cultura de ciberseguridad de la organización, manteniendo una concienciación adecuada de empleados, colaboradores y dirección de esta.

Medición correcta de la efectividad en los procesos de gestión de ciberseguridad definidos en el modelo de gobierno de seguridad de la organización, facilitando la toma de decisiones que permitan garantizar el alineamiento con los objetivos trazados y facilitando, en la medida de lo posible, evaluar el retorno de la inversión en ciberseguridad.

Asignación de recursos: es necesario alinear los recursos de ciberseguridad con las prioridades del negocio. Esto puede implicar asignar presupuesto y personal en función de las necesidades de ciberseguridad identificadas, y en particular facilitar la independencia y capacidad del responsable de ciberseguridad (CISO) en el desarrollo de su función.

Además, la constante evolución del entorno tecnológico, social, comercial, político y empresarial requiere la capacidad de evaluar la situación de seguridad de la organización (conciencia situacional), adaptando con flexibilidad la estrategia de ciberseguridad a medida que cambian las amenazas y los objetivos comerciales. Para ello es necesario realizar evaluaciones periódicas (auditorías normativas, auditorías técnicas, análisis de madurez de la función de ciberseguridad, reevaluaciones del marco de control existente, etc.) y ajustar la estrategia según sea necesario.

Definitivamente, un elenco de aspectos complejos que requieren un conocimiento y dedicación que, teniendo en cuenta los resultados que arrojan múltiples estudios de analistas sobre la situación de la ciberseguridad en España, hacen que para la mayoría de las organizaciones sea, cada día, más necesario contar con el apoyo de colaboradores expertos en la materia que faciliten el aseguramiento en la consecución de los objetivos y la propia estrategia de ciberseguridad de estas. Datos como que el número de organizaciones con 5 o menos empleados dedicados a la función de ciberseguridad en España, independientemente del volumen de facturación de la compañía, supera el 50% (y, entre ellos, el 30% con facturaciones superiores a 100M€ (ISMS Forum, III Indicador de madurez en ciberseguridad) parecerían corroborar esta afirmación.

Conrad López
Cybersecurity Technical Manager

Cibercrónica: La complejidad de la gestión de la información sensible en la tormenta cibernética

Por: NTT DATA Europe & Latam

En la era de la información digital, la seguridad en el manejo de datos supone un desafío crucial. Nos encontramos inmersos en un escenario donde la integridad y confidencialidad de nuestra información personal pende de un hilo, constantemente amenazada por ciberdelincuentes.

En las últimas semanas, una conocida aerolínea se encuentra en el epicentro de las noticias relacionadas con la ciberseguridad tras haber dejado información sensible de miles de sus clientes a manos de ciberdelincuentes. El ataque, descubierto el 10 de octubre de este mismo año, ha llevado a la aerolínea a emitir una alerta urgente a sus clientes, solicitándoles que cancelen sus tarjetas de crédito como medida preventiva ante la gravedad de la situación.

La organización no ha publicado aún el número oficial de personas afectadas, pero según diferentes medios que se han hecho eco de la noticia, se habla de más de 100.000 clientes. No es la primera vez que les ocurre, ya que hace unos años, la AEPD (Agencia Española de Protección de Datos) les impuso una multa de 600.000€ por no aplicar las medidas de seguridad exigidas por ley. La compañía no ha aportado más datos, pero según expertos en ciberseguridad, se especula que el robo de datos donde se incluyen algunos de los más sensibles como el CVV de las tarjetas, se ha realizado a través de otros medios.

> La rápida evolución de las tácticas de los ciberdelincuentes exige una actitud vigilante por parte de las organizaciones

Dicha compañía dispone desde 2020 de la certificación PCI-DSS, que implica que su compañía ha pasado diferentes auditorías independientes que certifican que utilizan la información sensible de sus clientes de una manera adecuada y segura. Por lo que primeros indicios apuntan a una posible inyección de código llamada web skimming, donde los atacantes aprovechan esta modificación en el código fuente de la aerolínea para enviarse dicha información sensible a un servidor externo.

El ciberataque subraya no solo la importancia de la adopción de prácticas de seguridad robustas como pueden ser a través de certificaciones, sino que también es esencial que las empresas inviertan en la formación continua de su personal, asegurándose de que estén actualizados sobre las últimas amenazas y técnicas de seguridad.

También es clave la implementación de tecnologías avanzadas como sistemas de detección de intrusiones, herramientas cruciales que permiten identificar y responder rápidamente a posibles amenazas. No obstante, la tecnología por sí sola no es suficiente; la conciencia constante y la vigilancia proactiva son fundamentales.

La rápida evolución de las tácticas de los ciberdelincuentes exige una actitud vigilante por parte de las organizaciones, que deben estar al tanto de las amenazas emergentes y en continuo desarrollo para adaptar así sus estrategias de seguridad en consecuencia.

Por tanto, este incidente subraya la importancia de combinar certificaciones, capacitación continua, tecnologías avanzadas y una mentalidad proactiva para salvaguardar la integridad y la confianza de la información de los clientes.

De DevOps a SecDevOps: Fusionando seguridad y agilidad

ANÁLISIS

DevOps: Development + Operations. Fusionar los procesos propios de desarrollo del software con aquellos pertenecientes a la integración y despliegue de dichos desarrollos. Suena difícil, y, de hecho, lo es. Si sumamos a la ecuación la ciberseguridad, se complica. A partir de ese momento pasamos a hablar de DevSecOps, o incluso de SecDevOps, dependiendo de lo presente que esté la seguridad en todo el proceso.

Las sinergias entre ciberseguridad y DevOps

Inicialmente DevOps surge de la necesidad de construir y entregar software de forma continua y automática lo más rápido posible. Un equipo de desarrolladores termina de implementar una nueva funcionalidad en una aplicación web, e interesa que esa funcionalidad sea probada, integrada y desplegada lo antes posible en los entornos productivos con el objetivo de disponibilizarla cuanto antes al usuario final.

Los conceptos clave aquí son “colaboración” y “acelerar”. Necesitamos colaborar para conseguir la agilidad en la entrega de software a la que aspiramos. Esto presenta una serie de desafíos, mayormente el cambio de mentalidad y que la necesidad de comunicación entre departamentos a veces se demuestra que no es fácil. Un rol de operaciones no se puede meter en la mente de un desarrollador y viceversa. Sin embargo, el cambio tampoco tiene por qué ser inmediato y se pueden ir incorporando procesos/tecnologías poco a poco.

La preocupación de las empresas en torno a la ciberseguridad ha ido aumentando en estos últimos años, a medida que fueron creciendo tanto el número de ataques como la gravedad de las consecuencias. Se hizo patente que era necesario desarrollar software poniendo especial atención a la seguridad de este.

Tenemos un escenario en el que necesitamos construir y entregar software de forma ágil (DevOps), pero a la vez garantizando su robustez ante ciberataques (Sec). Así nace el DevSecOps. De nuevo, esto presenta sus desafíos, ya que ahora no es sólo una colaboración entre Devs y Ops, sino que también se integran el equipo de ciberseguridad. Además, la inclusión de herramientas y procesos de seguridad al final puede repercutir en la rapidez con la que un desarrollo sale a un entorno productivo. Esto se debe a que el hecho de incluir los análisis necesarios para verificar la seguridad de dicho desarrollo puede ralentizar el proceso global, sobre todo si es necesario incluir un filtrado de falsos positivos. Sin embargo, debemos decidir qué es lo importante: que los desarrollos salgan lo más rápido posible a entornos productivos independientemente de las vulnerabilidades que puedan contener, o que, a pesar de una menor rapidez en este despliegue, nuestros desarrollos cuenten con un grado suficiente de seguridad.

De la teoría a la práctica: herramientas para hacer seguro el desarrollo

Hoy en día existe un amplio abanico de herramientas que nos ayudan a aportar seguridad a los desarrollos incluidos en un entorno DevSecOps. Dependiendo del tipo de tarea que lleven a cabo y del momento en que se ejecuten, podemos diferenciar los siguientes tipos:

- SAST: Static Application Security Testing. En esta clasificación encontramos aquellas herramientas que analizan el código fuente de los desarrollos en busca de posibles defectos que puedan provocar vulnerabilidades de seguridad. Ejemplos de tecnologías SAST son: Veracode, Fortify o Coverity.
- SCA: Software Composition Analysis. Este tipo de software se encarga de detectar si existen vulnerabilidades de seguridad conocidas en las dependencias externas utilizadas en los desarrollos. Ejemplos de herramientas SCA son: Snyk, Black Duck o XRay.
- DAST: Dynamic Application Security Testing. Similar al SAST, pero con la diferencia de que en vez de analizar el código fuente de los desarrollos, analiza el comportamiento de estos una vez desplegados. Realiza pruebas automáticas en busca de comportamientos que podrían fallos de seguridad, como fugas de información o indisponibilidad de los servicios. Ejemplos de herramientas DAST son: Burp Suite, Nessus, Acunetix.
- RASP: Runtime application self-protection. Similar a la tecnología de los WAF (Web Application Firewall). Se encarga de detectar y bloquear posibles intentos de ataque sobre aplicaciones desplegadas. A diferencias de los WAF, que funcionan a nivel de red, los RASP se ejecutan a nivel de aplicación. Cuentan con cierta información sobre la funcionalidad e infraestructura interna de las aplicaciones que protegen y, por lo tanto, son más precisos a la hora de detectar posibles ataques. Ejemplos de RASP son: Imperva, Hdiv y OpenRASP.

DevSecOps vs SecDevOps

Hoy en día, ambos términos se utilizan indistintamente como sinónimos y la diferencia es bastante difusa. Sin embargo, hay algunos matices que los diferencian.

- DevSecOps es un entorno de DevOps al que se le han incluido añadidos de seguridad: Herramientas SAST/SCA para analizar el código y las dependencias, tal vez un RASP para monitorizar y proteger los desarrollos ya desplegados... En definitiva, la seguridad existe en el entorno DevOps como un añadido necesario, pero sin que afecte a todas y cada uno de los procesos que se ejecutan.
- SecDevOps es un entorno de DevOps en el que se prioriza la seguridad y se pone un foco consciente en que cada uno de los procesos existentes se lleven a cabo teniéndola en cuenta. Los desarrolladores tienen disponibles herramientas de análisis SAST en sus IDEs; existe una batería de pruebas de seguridad actualizada periódicamente que se ejecuta cada vez que se sube código a los repositorios; se ejecutan análisis completos SAST, SCA, DAST y/o IAST con security gates que evitan que se despliegen desarrollos vulnerables, y se monitorizan y protegen los desarrollos desplegados mediante herramientas RASP y/o SIEM.

Mientras que en DevSecOps la seguridad es contemplada y se tiene en cuenta, en SecDevOps se prioriza y se considera el elemento que tiene que abarcar al resto.

Como nota final, nuestro objetivo es construir software, no sólo de forma ágil, sino también con las mayores garantías de seguridad posible. Por lo tanto, deberíamos apuntar siempre a contar con un entorno SecDevOps. Sin embargo, lo más probable es que intentar pasar directamente de un entorno DevOps a uno SecDevOps sea contraproducente, ya que todos los usuarios implicados se verán sobrepasados con tal volumen de nuevas herramientas y procesos. La mejor estrategia consistirá en ir implementando poco a poco dichas herramientas y, al mismo tiempo, ir formando a los usuarios en el uso de las mismas.

Miguel Otero
Cybersecurity Lead Architect
NTT DATA Europe & Latam

Antonio Gallego
Cybersecurity Analyst
NTT DATA Europe & Latam

SBOM en Ciberseguridad: La Clave para una defensa efectiva.

TENDENCIAS

Con la creciente amenaza de ciberataques sofisticados, las organizaciones buscan constantemente formas innovadoras de proteger sus activos digitales. En este contexto, el SBOM (Software Bill of Materials) emerge como una herramienta crucial para fortalecer las defensas cibernéticas.

El SBOM es esencialmente una lista detallada de todos los componentes de software utilizados en una aplicación o sistema. Esta lista proporciona información vital sobre las bibliotecas, frameworks y módulos que conforman el software. En el contexto de la ciberseguridad, el SBOM se convierte en una herramienta invaluable, ya que brinda una visión completa de la superficie de ataque potencial.

Al incorporar SBOM en la estrategia de ciberseguridad, las organizaciones ganan una transparencia sin precedentes en su cadena de suministro de software. Esto significa que cada componente utilizado en el desarrollo de software se documenta y puede rastrearse fácilmente.

La visibilidad en la cadena de suministro es crucial para identificar posibles vulnerabilidades y riesgos de seguridad. La capacidad de conocer y comprender cada elemento de software utilizado permite a las organizaciones tomar medidas proactivas para mitigar riesgos y fortalecer sus defensas. Uno de los mayores beneficios del SBOM en el ámbito de la ciberseguridad es su capacidad para facilitar la gestión de vulnerabilidades y parches. Al conocer todos los componentes de software y sus versiones, las organizaciones pueden identificar rápidamente las vulnerabilidades conocidas y aplicar los parches correspondientes de manera eficiente.

Esta capacidad de respuesta rápida es esencial para contrarrestar las amenazas emergentes. Los ciberdelincuentes a menudo aprovechan vulnerabilidades conocidas en software desactualizado para llevar a cabo ataques. El SBOM permite a las organizaciones cerrar estas brechas de seguridad de manera oportuna, reduciendo significativamente el riesgo de explotación.

En un entorno regulado, el SBOM se convierte en un aliado clave para garantizar el cumplimiento normativo. Las regulaciones de ciberseguridad cada vez más estrictas requieren un enfoque proactivo para gestionar riesgos.

El SBOM proporciona una documentación detallada que facilita la demostración de la conformidad con las normativas vigentes.

Además, facilita las auditorías de seguridad. Los equipos de seguridad pueden revisar exhaustivamente la lista de componentes de software, verificar la presencia de parches y evaluar la postura general de seguridad de la organización. Esto no solo cumple con los requisitos normativos, sino que también fortalece la postura de seguridad de la organización.

La incorporación del SBOM en las prácticas de desarrollo seguro es esencial para maximizar su eficacia. Integrar el SBOM en el ciclo de vida del desarrollo de software desde el principio garantiza que la transparencia y la gestión de riesgos sean parte integral de todo el proceso. Los equipos de desarrollo pueden utilizar el SBOM para tomar decisiones informadas sobre la selección de componentes de software, evaluando la seguridad de cada elemento antes de su implementación.

Esta práctica proactiva contribuye a la creación de software más seguro desde el inicio, reduciendo la necesidad de correcciones costosas en etapas posteriores.

En resumen, el SBOM se ha convertido en una herramienta esencial en la ciberseguridad moderna. Proporciona transparencia, visibilidad y eficiencia en la gestión de vulnerabilidades, lo que es crucial en un entorno digital cada vez más amenazante. Integrar el SBOM en la estrategia de ciberseguridad no solo fortalece las defensas de una organización, sino que también contribuye al cumplimiento normativo y al desarrollo seguro de software.

En última instancia, el SBOM no es simplemente una lista de componentes de software, sino una herramienta estratégica para construir un futuro digital más seguro.

Vulnerabilidades

Vulnerabilidad en Confluence Data Center and Server

Fecha: 31 de octubre de 2023
CVE: CVE-2023-22518

CRÍTICA

CVSS: 10

Descripción

Desde Atlassian se ha publicado una vulnerabilidad de severidad crítica que afecta a sus productos Confluence Data Center y Confluence Data Server. Dicha vulnerabilidad afecta a todas las versiones de ambos productos.

Mediante esta falla de seguridad, un atacante no autenticado podría beneficiarse de una autorización incorrecta, lo cual podría permitirle reiniciar la instancia de Confluence y crear una cuenta de administrador.

Una vez conseguidos los privilegios de administrador, el atacante podría realizar todo tipo de acciones en la instancia de Confluence, lo que supone una pérdida completa de la confidencialidad, integridad y disponibilidad.

Enlaces:
https://confluence.atlassian.com/security/cve-2023-22518-improper-authorization-vulnerability-in-confluence-data-center-and-server-1311473907.html
https://jira.atlassian.com/browse/CONFSERVER-93142
https://nvd.nist.gov/vuln/detail/CVE-2023-22518

Productos afectados:
La vulnerabilidad afecta a todas las versiones de los siguientes productos:

- Confluence Data Center
- Confluence Data Server

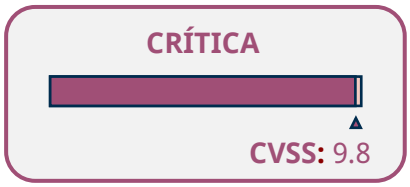
Resolución:
El fabricante ha recomendado actualizar lo antes posible a una de las siguientes versiones:

- 7.19.16
- 8.3.4
- 8.4.4
- 8.5.3
- 8.6.1

Vulnerabilidades

Múltiples vulnerabilidades en productos QNAP

Fecha: 3 de noviembre de 2023
CVE: CVE-2023-23368



Descripción

El pasado 4 de noviembre QNAP publicó una vulnerabilidad crítica que afecta a varios de sus productos (QTS, QuTS hero y QuTScloud).

Esta vulnerabilidad de inyección de comandos podría permitir a los atacantes ejecutar comandos de manera remota.

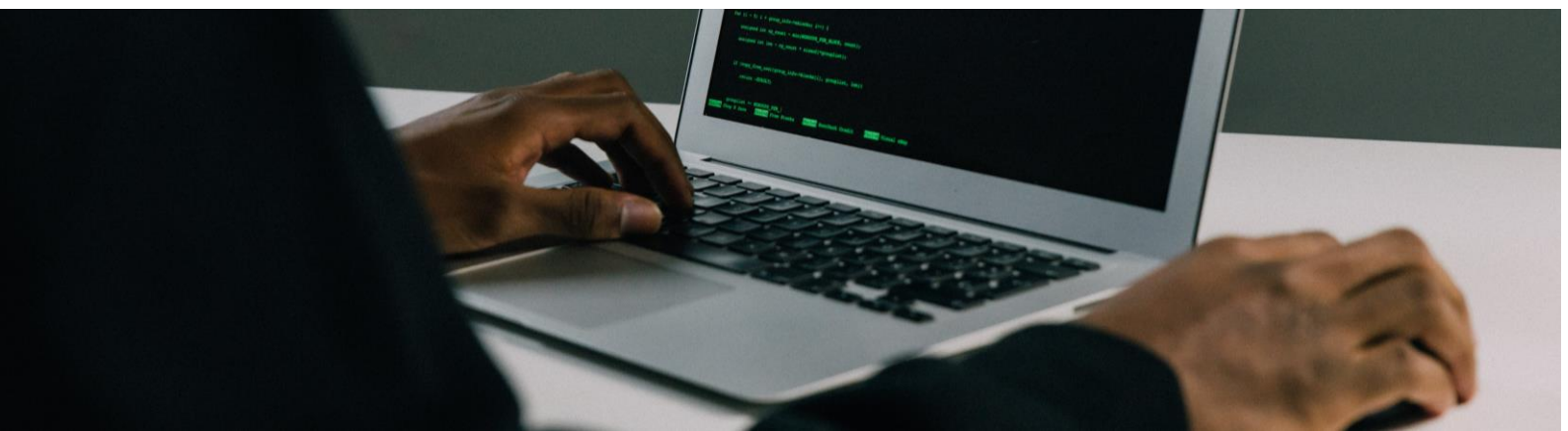
Desde QNAP se informa que el problema ha sido solucionado y se recomienda actualizar los sistemas a la última versión lo antes posible para evitar la explotación de dicha vulnerabilidad por parte de atacantes externos.

Enlaces:
https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2023-23368
https://www.qnap.com/en/security-advisory/qsa-23-31
https://nvd.nist.gov/vuln/detail/CVE-2023-23368

Productos afectados:
Los diferentes productos afectados por la vulnerabilidad son los siguientes:

- QTS (versiones 5.0.x)
- QTS (versiones 4.5.x)
- QuTS hero (versiones h5.0.x)
- QuTS hero (versiones h4.5.x)
- QuTScloud (versiones c5.0.x)

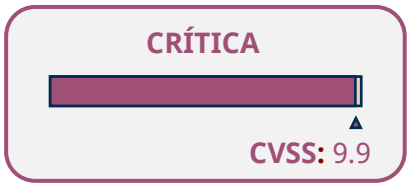
Resolución:
El fabricante ha publicado una serie de actualizaciones con el fin de solucionar dicha vulnerabilidad. Se recomienda la instalación de dichos parches lo antes posible.



Parches

Múltiples parches para vulnerabilidades en Veeam

Fecha: 6 de noviembre de 2023
CVEs: CVE-2023-38547, CVE-2023-38548, CVE-2023-38549 y CVE-2023-41723



Descripción

Veeam ha publicado una serie de parches de seguridad que corrijen un total de 4 vulnerabilidades, dos de ellas de severidad crítica y otras dos de severidad media:

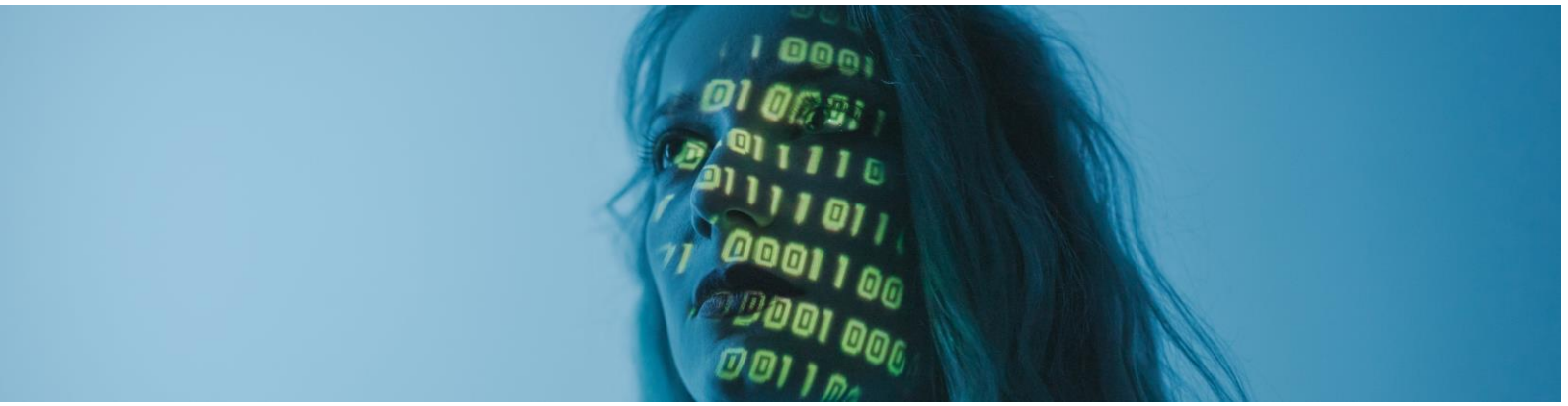
- **CVE-2023-38547**: vulnerabilidad crítica que permite a un atacante no autenticado la ejecución remota de código en servidores SQL.
- **CVE-2023-38548**: vulnerabilidad de severidad crítica que permitiría a un usuario sin privilegios con acceso a Veeam ONE Web Client, la obtención de *hashes* NTLM de cuentas usadas por Veeam.
- **CVE-2023-38549:** vulnerabilidad XSS de severidad media que permite la escalada de privilegios de usuario "Power User" a "Administrator".
- **CVE-2023-41723**: vulnerabilidad de severidad media que permite a un usuario con privilegios de "Read-Only" consultar información del apartado "Dashboard Schedule".

Desde Veeam se recomienda parar inmediatamente los servicios de Veeam ONE en caso de usar versiones afectadas, aplicar los parches y reiniciar dichos servicios.

Enlaces:
https://www.veeam.com/kb4508
https://thehackernews.com/2023/11/critical-flaws-discovered-in-veeam-one.html

Productos afectados:
Dichas vulnerabilidades afectan a las siguientes versiones de Veeam ONE:
- Veeam ONE 11
- Veeam ONE 11a
- Veeam ONE 12

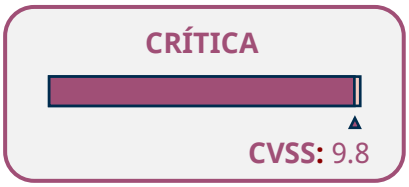
Actualización:
La solución propuesta por el fabricante consiste en la actualización a las siguientes versiones:
- Veeam ONE 11 (11.0.0.1379)
- Veeam ONE 11a (11.0.1.1880)
- Veeam ONE 12 P20230314 (12.0.1.2591)



Parches

Múltiples parches de seguridad para productos Microsoft

Fecha: 14 de noviembre de 2023
CVEs: CVE-2023-36025, CVE-2023-36033, CVE-2023-36036, CVE-2023-36038, CVE-2023-36413, CVE-2023-36028, CVE-2023-36397



Descripción

Microsoft ha publicado su boletín de seguridad mensual para corregir un total de 63 vulnerabilidades en sus productos. Entre ellas, existen un total de 5 vulnerabilidades 0-day:

- **CVE-2023-36025 (CVSS: 8.8):** vulnerabilidad en Windows SmartScreen Security Feature que permite evadir algunas medidas de seguridad.
- **CVE-2023-36033 (CVSS: 7.8):** vulnerabilidad de elevación de privilegios en Windows DWM Core Library.
- **CVE-2023-36036 (CVSS: 7.8):** vulnerabilidad de escalada de privilegios en Windows Cloud Files Mini Filter Driver.
- **CVE-2023-36038 (CVSS: 8.2):** vulnerabilidad DoS en ASP.NET Core.
- **CVE-2023-36413 (CVSS: 6.5):** vulnerabilidad en Microsoft Office que permite evadir ciertas características de seguridad.

Además, se han corregido dos vulnerabilidades de severidad crítica:

- **CVE-2023-36028 (CVSS: 9.8):** vulnerabilidad de ejecución de código remoto en Microsoft Protected Extensible Protocol (PEAP).
- **CVE-2023-36397 (CVSS: 9.8):** vulnerabilidad de ejecución de código remoto en Windows Pragmatic General Multicast (PGM).

Microsoft recomienda la instalación de todos los parches de seguridad en los productos afectados, ya que algunos de ellos están siendo activamente explotados.

Enlaces:
https://msrc.microsoft.com/update-guide/releaseNote/2023-Nov
https://thehackernews.com/2023/11/alert-microsoft-releases-patch-updates.html

Productos afectados:
Dichas vulnerabilidades abarcan un gran número de productos Microsoft. Dichos productos pueden consultarse en: https://msrc.microsoft.com/update-guide/releaseNote/2023-Nov

Actualización:
Aplicar el parche de seguridad correspondiente en los productos afectados.

Eventos

XV JORNADAS STIC CCN-CERT
30 noviembre – 3 diciembre

Las Jornadas STIC CCN-CERT, en su decimoquinta edición del 30 de noviembre al 3 de diciembre, son un evento clave de ciberseguridad en España que ha evolucionado durante quince años, reuniendo a profesionales, entidades públicas, empresas y universidades. A pesar de los desafíos de la COVID-19, la última edición se adaptó con éxito. Este año, bajo el lema "Ciberseguridad 360º. Identidad y Control de Datos", el evento será híbrido, con actividades presenciales y en línea, ofreciendo una visión integral del sector a nivel nacional e internacional

Enlace

LA ÚLTIMA CENA DE OSINT
2 – diciembre

En respuesta a la creciente importancia del ciberespacio y la ciberseguridad en la geopolítica global, QuantiKa14 organiza un evento efímero único: La Última Cena OSINT en Sevilla. Este encuentro excepcional ofrecerá discusiones de vanguardia sobre ciberinteligencia, con distinguidos ponentes y patrocinadores. La velada incluirá tres ponencias, una pausa para café y networking, seguida de una cena donde la conversación será tan deliciosa como los platos. Sevilla se convertirá en el epicentro de esta conversación vital en un momento crucial para mantenerse informado y conectado en este ámbito clave.

Enlace

BLACK HAT EUROPE 2023
4 – 7 diciembre

Black Hat es un destacado evento de seguridad informática que reúne a expertos de la industria para explorar las últimas investigaciones y tendencias. Durante cuatro días, ofrece formaciones técnicas prácticas seguidas de dos días de presentaciones sobre vulnerabilidades. Black Hat Europe será presencial en Londres del 4 al 7 de diciembre, seguido de una experiencia virtual a partir del 13 de diciembre con grabaciones de todas las sesiones. Este año, se presenta el programa "Certified Pentester", un examen práctico de un día centrado en pentesting

Enlace

CIBER1C MX
7 diciembre

Ciberilatam, en colaboración con el Centro Criptológico Nacional de España y la Fundación Borredá, organiza el I Congreso de Ciberseguridad en Infraestructuras Críticas y Servicios Esenciales de México (CIBER1C MX) el 7 de diciembre en el Club de los Periodistas. Este evento, respaldado también por Segurilatam, reunirá a profesionales para explorar estrategias de ciberseguridad en la protección de infraestructuras críticas y servicios gubernamentales esenciales, abordando desafíos, amenazas en ciberseguridad para el gobierno corporativo y discutiendo el futuro del sector, entre otros temas relevantes.

Enlace

Recursos

Flipper zero desafía la seguridad de los iphones

El Flipper Zero, reconocido como el "tamagotchi" para hackers, ha ganado notoriedad por su versatilidad y capacidad para realizar experimentos de hacking. Recientemente se ha revelado que este dispositivo multifuncional puede desafiar la seguridad de los iPhones, en particular aquellos que ejecutan iOS 17. Con un precio de aproximadamente 250 euros, el Flipper Zero puede interceptar y reproducir señales inalámbricas, pero su capacidad para enviar iPhones a bucles de denegación de servicio (DoS) mediante una avalancha de mensajes a través de Bluetooth ha planteado preocupaciones significativas. Aunque aún no hay una solución definitiva para prevenir estos ataques, la situación destaca la importancia de la regulación y la ética en el campo de la ciberseguridad a medida que las avanzan y son usadas de forma maliciosa.

Enlace

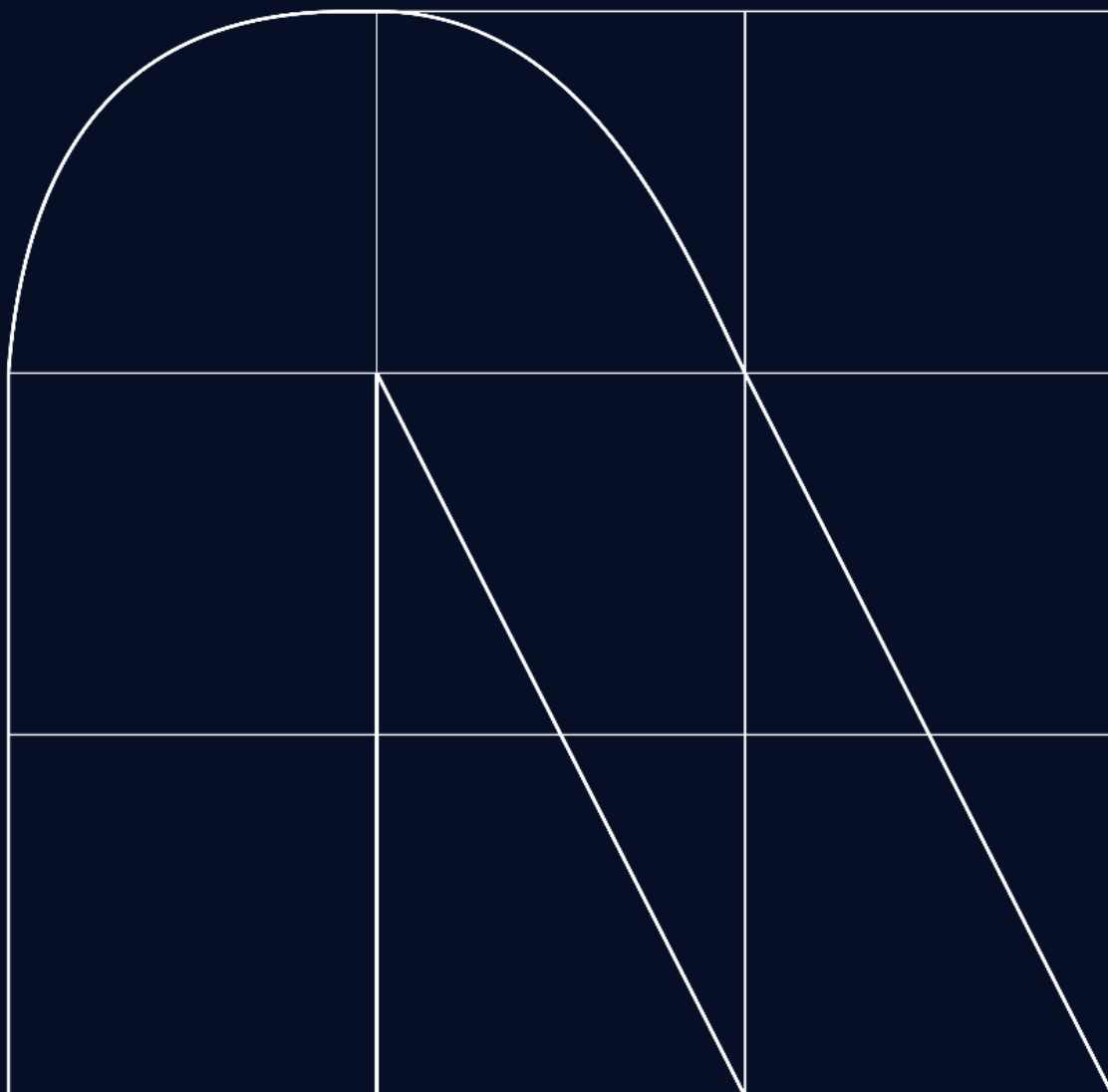
Microsoft ofrece nuevas herramientas de ia para afrontar ataques cibernéticos

Microsoft ha anunciado su compromiso de mejorar en el ámbito de la ciberseguridad, ampliando las capacidades de sus herramientas y técnicas para detectar amenazas. La compañía planea poner estas capacidades directamente a disposición de sus clientes, proporcionándoles herramientas de inteligencia artificial (IA) con el objetivo de fortalecer la defensa contra ataques cibernéticos. Este enfoque refleja la iniciativa de Microsoft para empoderar a los usuarios con soluciones avanzadas en la lucha contra las amenazas digitales.
Enlace

La estafa del falso hijo (whatsapp, bizum...)

La Policía Nacional ha emitido una advertencia a los ciudadanos sobre la estafa del falso hijo, que ha llevado al arresto de 17 personas en Cataluña por estafar 60.000 euros con este método. La estafa implica que los estafadores se hacen pasar por hijos o hijas a través de mensajes de WhatsApp, solicitando dinero para emergencias ficticias. Las víctimas, generalmente madres preocupadas, transfieren dinero a cuentas bancarias o identificadores de Bizum proporcionados por los estafadores. La policía aconseja desconfiar de mensajes inesperados, verificar la autenticidad de las solicitudes de dinero urgente, contactar directamente a los familiares supuestamente afectados y abstenerse de realizar transferencias a cuentas desconocidas para evitar caer en este tipo de estafa.

Enlace



Powered by the cybersecurity NTT DATA team

es.nttdata.com