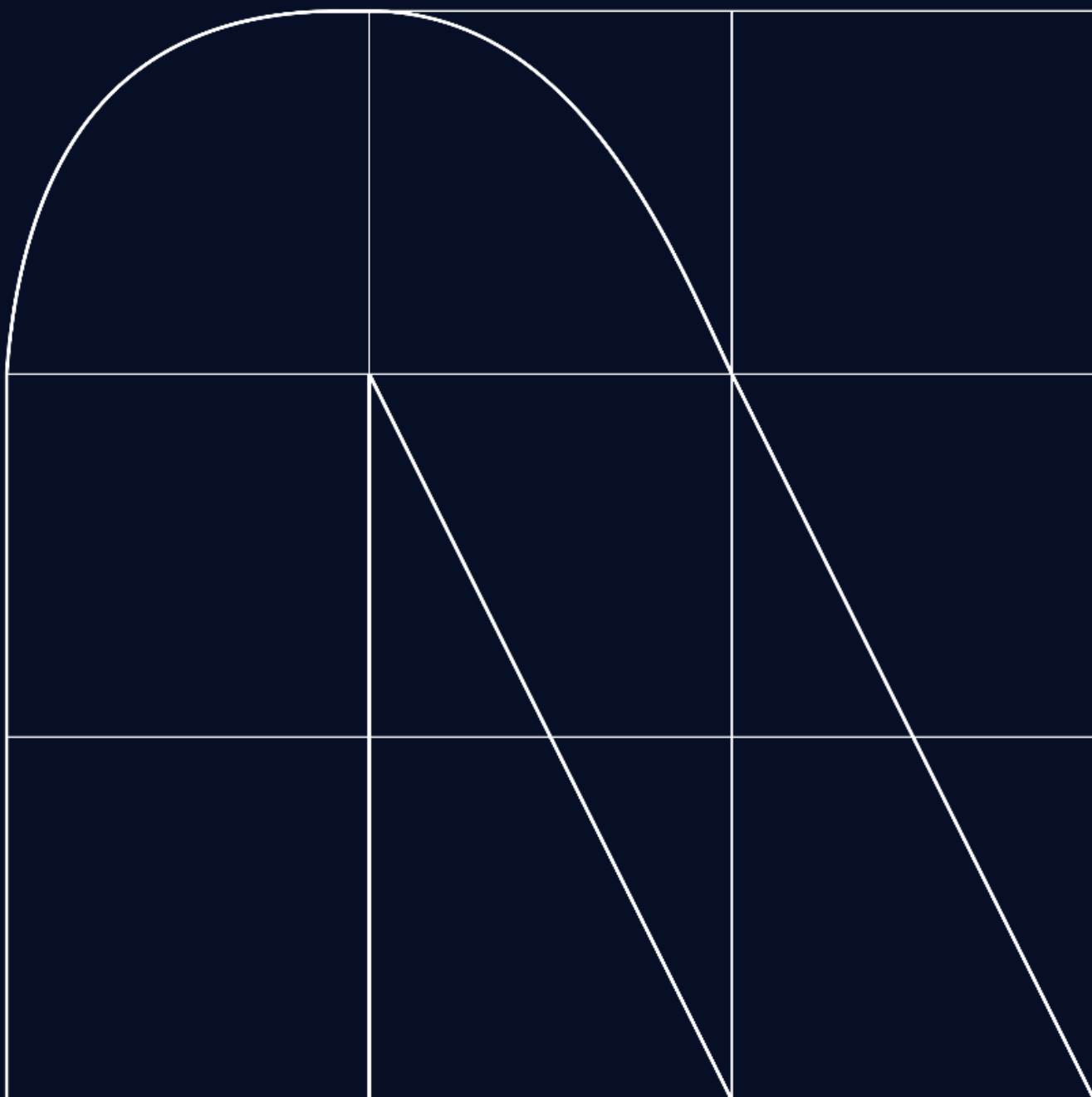
Número 90 | Mayo 2024

NTT DATA

Radar

El magazine de ciberseguridad



Integración de la IA y ML en la Detección y Respuesta ante Amenazas

Por Ángel Pérez y Diego Martín

En un mundo cada vez más digitalizado, la ciberseguridad se ha convertido en una preocupación primordial para empresas, gobiernos y usuarios individuales. Con el aumento constante de las amenazas cibernéticas, la necesidad de soluciones innovadoras se hace más evidente que nunca. En este contexto, la Inteligencia Artificial (IA) y el Aprendizaje Automático (Machine Learning) emergen como herramientas cruciales en la defensa contra estas amenazas

Estas tecnologías ofrecen un enfoque proactivo y adaptable para abordar los desafíos cibernéticos. Al analizar grandes volúmenes de datos en tiempo real, la IA y el ML pueden detectar patrones y comportamientos anómalos, anticipándose y neutralizando las amenazas antes de que causen daño. Esta capacidad predictiva es esencial en un entorno donde las amenazas evolucionan constantemente y donde la detección temprana puede marcar la diferencia entre un ataque exitoso y una defensa efectiva.

Desde la detección de amenazas hasta la respuesta a incidentes, las aplicaciones de la IA y el ML en ciberseguridad son diversas y efectivas. Estas tecnologías permiten a los equipos de seguridad responder de manera rápida y eficiente ante posibles ataques, reduciendo el error humano y mejorando la eficiencia operativa. A pesar de los beneficios, la implementación de la IA y el ML en ciberseguridad también enfrenta desafíos, como la disponibilidad de datos de entrenamiento adecuados y la vulnerabilidad a ataques adversarios.

A pesar de los desafíos, numerosas empresas han tenido éxito en la aplicación de la IA y el ML en ciberseguridad. IBM, Darktrace, Cylance y Fortinet son solo algunos ejemplos de empresas que han desarrollado soluciones innovadoras que utilizan estas tecnologías para detectar y prevenir amenazas de manera eficiente. Estos casos de éxito demuestran el potencial de la IA y el ML para fortalecer las defensas cibernéticas y proteger los activos digitales en un entorno cada vez más hostil y complejo. En última instancia, la integración de la IA y el ML en la ciberseguridad ofrece oportunidades significativas para fortalecer la protección contra las amenazas digitales, pero su éxito dependerá de cómo se implementen y utilicen de manera responsable y ética.

Por ejemplo, Symantec hace uso de inteligencia artificial en varios de los servicios que ofertan. En su servicio de “Análisis de reputación de archivos” mediante el análisis de miles de millones de enlaces, sitios web y archivos determina si un archivo es confiable o inseguro, asignándole así una puntuación antes de que llegue los equipos.

Otro ejemplo de Symantec es su servicio de seguridad “Email Security Cloud”, el cual filtra los mensajes no deseados del correo electrónico en la nube, y protege los buzones de correo de ataques dirigidos. Este servicio tiene capacidades de autoaprendizaje e inteligencia de Symantec para brindar una seguridad de correo electrónico efectiva y precisa, y es compatible con los proveedores de correo más famosos.

Por otro lado, hacen uso de un aprendizaje automático avanzado para determinar la confiabilidad de un archivo al reconocer atributos maliciosos y definir reglas para realizar detecciones. Este aprendizaje automático permite bloquear nuevas variantes de malware mediante el análisis de miles de millones de ejemplos de archivos maliciosos y no maliciosos que están contenidos en la red de inteligencia global.

Otra de las grandes empresas que ya hacen uso de la inteligencia artificial es IBM, en su suite “QRADAR”, siendo esta una solución modernizada de detección y respuesta ante amenazas. La cartera incluye IA y automatización de nivel empresarial para aumentar drásticamente la productividad de los analistas, ayudando así mayoritariamente a los equipos con recursos limitados.

Para finalizar, una de las otras soluciones de IBM que implementa inteligencia artificial es “IBM Security Verify”. Esta solución implementa un contexto profundo impulsado por inteligencia artificial para la gestión de accesos tanto de los consumidores como del personal, protegiendo así a los usuarios y aplicaciones dentro y fuera de la empresa con un enfoque de software como servicio.

Cibercrónica

Por Álvaro Ceruelo y Cayetano Valero

La Unión Europea prevé un aumento de campañas de desinformación centradas en las elecciones europeas de junio, provenientes de agentes externos, especialmente los relacionados con el gobierno ruso, con el objetivo de interferir en los procesos electorales. Estas campañas de desinformación se han ido adaptando a las restricciones surgidas a raíz de la invasión rusa de Ucrania, con un uso mayoritario de Internet y servicios de mensajería instantánea como medios de distribución de las campañas, frente a otros más tradicionales como la televisión, que quedaron censurados en Europa.

La identificación de desinformación se ha vuelto cada vez más compleja, por una parte debido al uso de los medios de distribución mencionados, así como por la propia naturaleza de la desinformación, que aprovecha los avances en tecnologías como la Inteligencia Artificial (IA), para producir resultados cada vez más sofisticados con menos esfuerzo. Los avances en este campo han quedado reflejados en estudios recientes, que han documentado el uso de IA generativa para la producción de texto, vídeos e imágenes relacionadas con campañas de desinformación en al menos 16 países durante el año 2023.

Phishing en la campaña de declaración de la renta

En paralelo, con la campaña de declaraciones de la renta en pleno auge, los ciberdelincuentes están aprovechando la oportunidad para engañar a las personas a través de correos y mensajes masivos con engaños en los que intentan que alguien caiga en la trampa. Para ello están lanzando campañas, de phishing, en las cuales envían mensajes masivamente, con la esperanza de que alguien caiga en la trampa.

En estos correos, los ciberdelincuentes utilizan tácticas engañosas, a menudo afirmando que la Agencia Tributaria te va a devolver dinero. Además, pueden incluir enlaces a páginas web fraudulentas que parecen oficiales, pero que están diseñadas para robar información personal, como números de tarjetas y códigos de seguridad. Estas páginas web son falsificaciones que utilizan logos y tipografías de la Agencia Tributaria para parecer una web oficial.

Es recomendable buscar la web de la Agencia Tributaria o donde se quiera acceder, entrar en la página oficial y autenticarse desde ahí para buscar posibles notificaciones. En resumen, la seguridad en línea sigue siendo una preocupación constante. Con la temporada de impuestos en marcha, es importante tener precaución y estar atentos a los correos y mensajes que recibimos, ya que muchos de ellos pueden ser fraudulentos.

Vulnerabilidades destacadas

Recientemente, se ha descubierto un problema de seguridad en la herramienta XZ Utils (CVE-2024-3094), comúnmente utilizada en sistemas operativos Linux. Esta herramienta se utiliza para comprimir y descomprimir datos en formato XZ. Andrés Freund, un desarrollador de Microsoft, detectó código malicioso oculto en esta herramienta mientras investigaba problemas de rendimiento en SSH. El código malicioso modifica funciones dentro del paquete liblzma, e interfiere con los datos utilizados por la herramienta y, en ciertas condiciones, podría permitir a un atacante obtener acceso a un sistema afectado. Sin embargo, este código malicioso no se encuentra en la distribución Git de la herramienta, sólo en el paquete de descarga completo.

Adicionalmente, Fortinet ha publicado detalles acerca de una vulnerabilidad crítica de tipo SQL Injection, presente en las versiones 7.2.0 a 7.2.2 y 7.0.1 a 7.0.10 de FortiClient Enterprise Management Server, que permite a un atacante ejecutar comandos o código de forma remota a través de peticiones específicamente diseñadas, pudiendo obtener acceso como administrador al servidor donde se ejecuta el software.

Las estrategias de cumplimiento normativo

Por Soledad Romero

En un mundo cada vez más globalizado, las organizaciones encaran el cumplimiento normativo de manera muy diversa. Hacerlo de forma efectiva y rentable requiere la definición de una estrategia sólida que implique a los diferentes actores e interesados que han de participar en ella. La complejidad del cumplimiento normativo en un mundo globalizado.

Todas las organizaciones se enfrentan actualmente a un complejo panorama normativo cada vez más cambiante y globalizado. La proliferación de leyes y regulaciones en diferentes ámbitos y jurisdicciones presenta desafíos significativos para las entidades que buscan operar dentro de los límites de la legalidad.
Siendo conscientes del hecho de que cumplir con las leyes es fundamental para mantener la integridad y la confianza en las instituciones y mercados (locales, regionales, nacionales o internacionales), cada organización busca adherirse a las regulaciones que le son aplicables y pertinentes no solo para ahorrar costes, evitar incidentes de ciberseguridad o sanciones, sino también con el objetivo de prever por dónde van las tendencias, fortalecer su reputación y las relaciones con los stakeholders.

En un entorno tan dinámico como el actual, prepararse para responder eficazmente es todo un desafío. Por lo tanto, resulta crucial planificar y establecer una estrategia de cumplimiento sólida y bien estructurada. Esto no solo implica identificar el nivel de madurez de cumplimiento dentro de la organización, sino también evaluar si se tiene un conocimiento y entendimiento profundo de la regulación. Además, es importante alcanzar la flexibilidad y la capacidad para anticipar y adaptarse rápidamente a cualquier nuevo requisito legal que pueda surgir. En resumen, el cumplimiento normativo es un aspecto crítico que requiere atención constante y una estrategia proactiva para asegurar el éxito y la sostenibilidad a largo plazo de cualquier organización. Esta estrategia o enfoque proactivo exige desde el inicio una actitud consciente y diligente entre los actores clave que suelen intervenir desde su planificación y sus funciones, a saber:

- Oficial de Cumplimiento: Es el responsable de planificar y ejecutar el plan de cumplimiento y de comunicar las medidas a seguir a toda la organización.
- Alta Dirección: Debe estar comprometida con la cultura de cumplimiento y garantizar que se asignen los recursos necesarios.
- Departamento Legal: Asesora sobre las implicaciones legales y ayuda a interpretar la normativa aplicable.
- Departamento de TI: Implementa y mantiene las soluciones tecnológicas para apoyar el cumplimiento.
- Recursos Humanos: Se encarga de la formación y sensibilización del personal en materia de cumplimiento.
- Auditores Internos y Externos: Verifican el cumplimiento y la efectividad de las políticas y procedimientos.
- Empleados: Todos los miembros de la organización deben estar informados y seguir las políticas de cumplimiento.

Entre las recomendaciones y buenas prácticas más habituales a la hora de establecer la estrategia podemos considerar las siguientes:

1. Establecer una línea de base: partiendo de la realización de una auditoría para conocer el estado actual de cumplimiento y las regulaciones aplicables.
2. Elaboración de procedimientos: que sean accesibles y fácilmente aplicables dentro de la organización y revisados periódicamente.
3. Seguimiento y monitorización: en orden a asegurar el cumplimiento continuo y actualizar conforme a las necesidades de la entidad.
4. Implicación de la alta dirección: como hemos comentado más arriba en relación con los actores clave.
5. Capacitación continua: Los empleados deben estar bien informados sobre las normativas y cómo estas afectan sus roles. En este sentido un plan de formación ad hoc debería ser regular y adaptable a los cambios que se produzcan en la legislación.

Por último, medir el éxito de una estrategia de cumplimiento implica evaluar cómo las actividades de la organización se alinean con las regulaciones y leyes aplicables. La medición a través KPIs específicos, las encuestas, los análisis de riesgos o los análisis de riesgos, son entre otros los elementos que nos proporcionan una visión cuantitativa y cualitativa del rendimiento de la estrategia de cumplimiento y ayudan a las organizaciones a ajustar sus prácticas para mejorar continuamente.

Soledad Romero
Expert Consultant in Cybersecurity GRC at NTT DATA

Tenemos que normatizar la Inteligencia Artificial

Por Carlos Chavarria

El uso de la inteligencia artificial en la UE estará regulado por la Ley de Inteligencia Artificial, la primera ley integral sobre Inteligencia Artificial, de aquí en adelante IA, del mundo. La prioridad del Parlamento es garantizar que los sistemas de IA utilizados en la UE sean seguros, transparentes, trazables, no discriminatorios y respetuosos con el medio ambiente. Los sistemas de IA deben ser supervisados por personas, en lugar de por la automatización, para evitar resultados perjudiciales. El Parlamento también quiere establecer una definición uniforme y tecnológicamente neutra de la IA que pueda aplicarse a futuros sistemas de IA.

Por todo ello, el Parlamento Europeo y sus países miembros han comenzado a realizar borradores, normativas y leyes para delimitar la IA. El Parlamento Europeo concretamente tiene pendiente de aprobar el "REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO POR EL QUE SE ESTABLECEN NORMAS ARMONIZADAS EN MATERIA DE INTELIGENCIA ARTIFICIAL (LEY DE INTELIGENCIA ARTIFICIAL) Y SE MODIFICAN DETERMINADOS ACTOS LEGISLATIVOS DE LA UNIÓN".

Dentro de los estados miembros, España está desmarcándose como uno de los principales líderes tras la aprobación el 22 de agosto de 2023 del RD 729/2023 por el que se el que se aprueba el Estatuto de la Agencia Española de Supervisión de Inteligencia Artificial. Además, la AEPD ha elaborado dos guías sobre IA. La primera de ellas en febrero de 2020 para adecuar al RGPD los tratamientos de IA y una segunda en enero de 2021 sobre los Requisitos para Auditorías de Tratamientos que incluyan IA.

En este contexto político, la Comisión Europea ha propuesto un marco reglamentario sobre inteligencia artificial con los siguientes objetivos específicos:

- Garantizar que los sistemas de IA introducidos y usados en el mercado de la UE sean seguros y respeten la legislación vigente en materia de derechos fundamentales y valores de la Unión;
- Garantizar la seguridad jurídica para facilitar la inversión e innovación en IA;
- Mejorar la gobernanza y la aplicación efectiva de la legislación vigente en materia de derechos fundamentales y los requisitos de seguridad aplicables a los sistemas de IA;
- Facilitar el desarrollo de un mercado único para hacer un uso legal, seguro y fiable de las aplicaciones de IA y evitar la fragmentación del mercado.

¿Qué problemas resuelven la aplicación de estas normativas?

En este contexto, la IA presenta una serie de problemas y riesgos que han de ser mitigados en la medida de lo posible a través de la legislación de la UE.

Por la creciente utilización de la IA tanto a nivel empresarial como cotidiano es necesario su regularización por las razones que exponemos a continuación:

- Ética y derechos individuales: La IA puede tener un impacto significativo en la vida de las personas, desde la toma de decisiones automatizadas hasta la recopilación y el uso de datos personales. La normatización ayuda a garantizar que se respeten los derechos individuales y se eviten prácticas discriminatorias o injustas.
- Privacidad y seguridad: La falta de regulación puede llevar a vulnerabilidades de seguridad y a la explotación de sistemas de IA. Las normas pueden establecer estándares de seguridad y privacidad para proteger a las personas y las organizaciones.
- Transparencia y responsabilidad: Las regulaciones pueden requerir la transparencia en los algoritmos y los procesos de toma de decisiones de la IA. Además, pueden establecer responsabilidad legal en caso de errores o daños causados por sistemas de IA.
- Sesgo algorítmico: La regulación puede abordar el sesgo en los sistemas de IA y garantizar que no se tomen decisiones injustas o discriminatorias basadas en la raza, género u otros factores.
- Competencia justa: Puede prevenir prácticas anticompetitivas y promover la innovación justa en el mercado de la IA.
- Seguridad pública: Las regulaciones pueden abordar la seguridad en aplicaciones críticas, como vehículos autónomos y sistemas de atención médica, para evitar riesgos para la vida y la salud.
- Mitigación de riesgos: La IA plantea riesgos significativos, como el desempleo tecnológico, la falta de privacidad y el sesgo algorítmico. La normatización puede ayudar a abordar estos problemas y mitigar los riesgos.
- Confianza pública: Fomenta la confianza del público en la tecnología de IA, lo que puede ser crucial para su adopción generalizada.
- Coherencia global: La regulación puede ayudar a establecer estándares comunes en un mundo cada vez más interconectado, facilitando la cooperación internacional y el comercio de tecnología de IA.

La normatización de la inteligencia artificial es esencial para garantizar que esta tecnología se desarrolle y se utilice de manera ética, segura y responsable, beneficiando a la sociedad en general y minimizando riesgos.

¿Cuándo entrarán en vigor las normativas?

El principal problema que hay a la hora de legislar este ámbito es que la innovación tecnológica es mucho más rápida que lo que tardamos en crear, desarrollar y aprobar las leyes. Pese a la creciente utilización de la IA aún no hay una fecha definida de aprobación de la Ley de Inteligencia Artificial de la UE. El 14 de junio de 2023 en el PE se aprobaron una serie de enmiendas. Han comenzado las conversaciones sobre la forma final de la ley en el Consejo, junto a los países de la UE. El objetivo es alcanzar un acuerdo a finales de este año.

¿Qué requisitos de Auditoría deberemos cumplir?

En cuanto a la Ley de IA de la UE, cómo aún no está aprobado y está abierta a modificaciones, es pronto para poder determinar que requisitos serán de obligado cumplimiento.

Con respecto a España, la AEPD ha publicado dos guías sobre IA, de las cuales destacamos "Requisitos para Auditorías de Tratamientos que incluyan IA". En ella, se realiza una aproximación a un conjunto de controles que podrían incorporarse a las auditorías de tratamientos de datos personales que hacen uso de componentes basados en IA. Es importante destacar que todos los controles incluidos están concebidos para realizar un análisis de la adecuación del tratamiento desde una perspectiva de protección de datos. Además, se añaden algunas notas metodológicas que pueden resultar propias y características de este tipo de auditorías.

A muy alto nivel se deberá:

- Identificación y transparencia del componente
- Propósito del componente IA
- Fundamentos del componente IA
- Gestión de los datos
- Verificación y validación

¿Qué organizaciones se verán afectadas por las normativas de IA?

Se verán afectadas todas las organizaciones que desarrollen, comercialicen o utilicen servicios de IA, pero también aplicarán estas normativas a las estructuras que utilicen servicios de IA de un tercero o tengan contrato con un proveedor que utilice servicios de IA para los servicios que les presta.

Pero adicionalmente, cuando las organizaciones consideran elegir un proveedor de servicios de inteligencia artificial (IA) externo en el futuro, deben tener en cuenta algunos factores como, por ejemplo:

- Experiencia y especialización:
- Transparencia y ética
- Cumplimiento normativo
- Escalabilidad y flexibilidad
- Seguridad y privacidad
- Facilidad de integración

En definitiva, tenemos que prepararnos para cumplir con las normativas de IA y garantizar que nuestras organizaciones estén alineadas con las regulaciones y estándares relevantes y esto se conseguirá realizando un proceso continuo que requerirá un compromiso constante con la ética, la seguridad en el desarrollo y la implementación de tecnologías de IA.

Mantenerse actualizado sobre los cambios de las futuras y actuales normativas puede ayudar de una manera muy notoria de cualquier organización tenga un cumplimiento constante y evitar así sanciones futuras.

Ley de Resiliencia Operativa Digital: Fortaleciendo la Ciberseguridad en la Unión Europea

Por David Miguel Campos

La Ley de Resiliencia Operativa Digital (DORA, por sus siglas en inglés) representa un hito regulatorio significativo para el sector financiero de la Unión Europea, con el objetivo de fortalecer la resiliencia operativa digital de las entidades financieras. Introducida en enero de 2023 y prevista para ser aplicada en enero de 2025, DORA busca armonizar las regulaciones existentes, centrándose en la gestión de riesgos de tecnologías de la información y comunicación (TIC) y la resiliencia ante graves interrupciones operativas. Esta regulación es especialmente relevante en el contexto bancario y de seguros, donde la dependencia de servicios de TIC de terceros es considerable y los riesgos asociados pueden tener importantes implicaciones transfronterizas.

El marco de DORA se construye sobre cinco pilares principales: gestión de riesgos de TIC, respuesta e informe de incidentes, pruebas de resiliencia operativa digital, gestión de riesgos de terceros e intercambio de información e inteligencia. Estos pilares están diseñados para garantizar que las entidades financieras puedan encontrar, proteger, detectar, responder y recuperarse eficazmente de las amenazas cibernéticas. Además, DORA establece requisitos estrictos para los contratos con proveedores de servicios de TIC, incluyendo cláusulas sobre derechos de auditoría, subcontratación y mecanismos de terminación.

¿Cuáles son los desafíos principales de DORA?

La implementación de DORA presenta varios desafíos para las entidades financieras en la Unión Europea. En primer lugar, la necesidad de una alineación integral con los requisitos de gestión de riesgos de TIC puede requerir una revisión significativa de las prácticas actuales. Las entidades deberán establecer un marco de gestión de riesgos robusto y adaptable que aborde todos los aspectos de la resiliencia operativa digital, desde la prevención de incidentes hasta la recuperación.

Otro desafío es la gestión de riesgos de terceros, especialmente en un entorno donde muchas operaciones dependen de servicios de TIC proporcionados por entidades externas. Las entidades financieras deberán asegurarse de que los contratos con los proveedores incluyan disposiciones rigurosas sobre ciberseguridad y mecanismos de respuesta a incidentes, lo que puede ser complejo de negociar e implementar.

Además, DORA requiere que las entidades financieras realicen pruebas de resiliencia operativa digital, lo que implica desarrollar y ejecutar una serie de pruebas avanzadas para evaluar la capacidad de resistir y recuperarse de graves interrupciones operativas. Esto requiere inversiones en tecnología y experiencia, así como la creación de procesos internos para llevar a cabo estas pruebas regularmente. La notificación de incidentes relacionados con TIC también es un aspecto crítico de esta ley. Las entidades deben ser capaces de detectar e informar sobre incidentes significativos a las autoridades relevantes en un breve período, lo que requiere sistemas de detección y comunicación eficientes y confiables.

El intercambio de información e inteligencia sobre amenazas cibernéticas es otro requisito de DORA que puede ser desafiante, ya que requiere la implementación de canales seguros y efectivos para el intercambio de información entre entidades financieras y autoridades, así como entre entidades financieras y sus pares o partes interesadas relevantes, respetando la confidencialidad y la protección de datos.

Finalmente, esta regulación establece un marco de supervisión para proveedores críticos de TIC, lo que significa que las entidades financieras deberán adaptarse a un nuevo nivel de escrutinio y cumplimiento por parte de las autoridades regulatorias. Esto puede implicar ajustes significativos a las operaciones y gobernanza de TIC para cumplir con los estándares establecidos.

¿Cómo superar los desafíos planteados por Dora?

Para superar los desafíos planteados por la implementación de la Ley de Resiliencia Operativa Digital (DORA), las entidades financieras pueden adoptar una variedad de estrategias efectivas. En primer lugar, es crucial desarrollar una comprensión profunda de los requisitos de DORA, lo que puede lograrse a través de programas de capacitación y concientización interna. Esto incluye familiarizarse con los cinco pilares de DORA: gestión de riesgos de TIC, respuesta e informe de incidentes, pruebas de resiliencia operativa digital, gestión de riesgos de terceros e intercambio de información e inteligencia.

Un enfoque proactivo para la gestión de riesgos de TIC es esencial, lo que significa encontrar, evaluar y mitigar riesgos. Las entidades deben establecer un marco de gestión de riesgos robusto que esté integrado en toda la organización, asegurando que las medidas de ciberseguridad estén alineadas con los objetivos comerciales y la tolerancia al riesgo de la entidad.

La colaboración con proveedores de servicios de TIC es otro aspecto crítico. Las entidades financieras deben asegurarse de que los contratos con terceros incluyan cláusulas detalladas sobre ciberseguridad, derechos de auditoría y mecanismos de respuesta a incidentes. Además, es importante llevar a cabo una diligencia debida rigurosa y monitoreo continuo de los proveedores para asegurar que también cumplan con DORA.

Las pruebas de resiliencia operativa digital son críticas para evaluar la capacidad de resistir y recuperarse de interrupciones operativas. Las entidades deben implementar un programa de pruebas integral que incluya pruebas básicas y avanzadas para identificar vulnerabilidades y mejorar las estrategias de respuesta.

La notificación rápida de incidentes relacionados con TIC a las autoridades competentes es un requisito de DORA. Para lograr esto, las instituciones financieras necesitan sistemas eficientes de detección e informe de incidentes para poder responder rápidamente y de manera apropiada.

El intercambio de información sobre amenazas cibernéticas es vital para la resiliencia operativa digital. Las entidades deben establecer canales seguros y efectivos para el intercambio de información e inteligencia sobre amenazas cibernéticas, tanto internamente como con otras entidades regulatorias y autoridades.

Finalmente, las entidades financieras deben estar preparadas para el nuevo marco de supervisión para proveedores críticos de TIC establecido por DORA. Esto puede requerir ajustes a las operaciones y gobernanza de TIC para cumplir con los estándares de supervisión.

Conclusión

En resumen, cumplir con DORA es un proceso complejo que requiere un enfoque estratégico y un compromiso continuo con la mejora de la resiliencia operativa digital. Superar sus desafíos requiere un enfoque holístico y estratégico, que implique inversión en tecnología, procesos y capital humano. El cumplimiento de DORA no es solo un problema regulatorio, sino también una oportunidad para que las entidades financieras fortalezcan su resiliencia operativa digital y protejan sus operaciones y clientes de interrupciones y amenazas cibernéticas. La colaboración y el compromiso continuo con la mejora de la resiliencia operativa serán fundamentales para el éxito en este camino.

Para las entidades que ya tienen certificación ISO 27001, un estándar internacional para sistemas de gestión de seguridad de la información, o que han implementado marcos como NIST, el camino hacia el cumplimiento de DORA puede ser más sencillo. ISO 27001 proporciona un marco que se alinea con los principios de gestión de riesgos de DORA, mientras que NIST ofrece una guía para encontrar, proteger, detectar, responder y recuperarse de amenazas cibernéticas. Sin embargo, la certificación ISO 27001 o la implementación de NIST no equivalen a un cumplimiento automático de DORA. Es esencial que las entidades realicen un análisis de brechas para encontrar áreas donde las prácticas existentes puedan necesitar ajustes para cumplir con los requisitos específicos de esta ley.

Parches

CRÍTICA Actualizaciones de seguridad críticas para Google Chrome

Fecha: 2 de abril de 2024
CVE: CVE-2024-3156 y 2 más

Descripción
Google ha publicado una serie de actualizaciones de seguridad para solucionar varios problemas que afectan al producto Google Chrome. La actualización corrige un total de 3 vulnerabilidades, todas ellas de severidad crítica.

La vulnerabilidad CVE-2024-3156 de tipo implementación inapropiada en el motor JavaScript V8 de Google Chrome podría ser explotada para ejecutar código arbitrario o acceder a información sensible en el sistema.

La vulnerabilidad CVE-2024-3158 ocurre cuando un programa accede a un área de memoria después de que ha sido liberada, lo que podría resultar en un comportamiento impredecible o en la ejecución de código no autorizado.

La vulnerabilidad CVE-2024-3159 afecta también al motor de JavaScript V8 por a un acceso incorrecto a memoria *out-of-bounds*, lo que puede ocasionar comportamientos impredecibles mediante manipulaciones específicas de JavaScript o incluso permitir la ejecución de código malicioso.

Productos afectados
Las versiones de Google Chrome afectadas por esta vulnerabilidad son:

- Versiones anteriores a 123.0.63.12.105 123.0.63.12.106 y 123.0.63.12.107 para Windows y Mac.
- Versiones anteriores a 123.0.63.12.105 para Linux.

Solución
Actualizar Google Chrome a la última versión disponible para Windows, Mac y Linux desde la página oficial.

Referencias
- chromereleases.googleblog.com
- www.bleepingcomputer.com

CRÍTICA Actualización de seguridad de abril de Android Pixel/Nexus

Fecha: 2 de abril de 2024
CVE: CVE-2024-29740 y 2 más

Descripción
El boletín de seguridad de Android del 2 de abril de 2024 destaca varias vulnerabilidades de seguridad detectadas en dispositivos Android Pixel/Nexus de gravedad crítica y alta.

De entre todas las vulnerabilidades detectadas, cabe destacar 1 de severidad crítica y 2 de severidad alta (de carácter *zero-day*), que se detallan a continuación:

- CVE-2024-29740 (crítica): vulnerabilidad de escalada de privilegios en los citados dispositivos Pixel.
- CVE-2024-29745 (alta): vulnerabilidad que puede conllevar divulgación de información confidencial.
- CVE-2024-29748 (alta): vulnerabilidad de escalada de privilegios.

Productos afectados
Se puede consultar la lista completa de los productos afectados, que afectan a los dispositivos Pixel compatibles, en el siguiente enlace: support.google.com

Solución
La solución a estas vulnerabilidades implica la aplicación de parches de seguridad a nivel de plataforma proporcionados por el Proyecto de Código Abierto de Android (AOSP).

Los teléfonos Pixel reciben actualizaciones para solucionar los problemas de seguridad que se detallan en los boletines públicos de seguridad de Android. Se recomienda comprobar y actualizar a la última versión de Android Pixel según se indica en la página oficial.

Referencias
- cybersecuritynews.com
- bleepingcomputer.com

Vulnerabilidades

Vulnerabilidad crítica en la librería XZ Utils

Fecha: 1 de abril de 2024
CVE: CVE-2024-3094

CVSS: 10

CRÍTICA

Descripción

Se descubrió código malicioso en los *tarballs* de XZ Utils, comenzando con la versión 5.6.0. A través de una serie de ofuscaciones complejas, el proceso de construcción de liblzma extrae un archivo de objeto precompilado de un archivo de prueba disfrazado en el código fuente, que luego se utiliza para modificar funciones específicas en el código de liblzma.

Esto resulta en una biblioteca liblzma modificada que cualquier software vinculado a esta biblioteca puede usar, interceptando y modificando la interacción de datos con esta biblioteca .

Productos afectados

Se ha indicado que los paquetes afectados están presentes solo en Fedora 41 y Fedora Rawhide dentro del ecosistema comunitario de Red Hat. Ninguna versión de Red Hat Enterprise Linux (RHEL) está afectada.

Solución

Se recomienda a los usuarios afectados que actualicen a las versiones que no incluyen el código malicioso.

Las versiones comprometidas de las bibliotecas XZ Utils son 5.6.0 y 5.6.1, solo incluidas en el paquete de descarga de *tarballs*.

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

Referencias

- nvd.nist.gov
- www.tarlogic.com

Vulnerabilidad en dispositivos NAS D-Link

Fecha: 3 de abril de 2024
CVE: CVE-2024-3272 y 1 más

CVSS: 9.8

CRÍTICA

Descripción

Las vulnerabilidades identificadas como CVE-2024-3272 y CVE-2024-3273 tienen severidades crítica y alta, respectivamente.

La vulnerabilidad crítica se encuentra en la URI nas_sharing.cgi de los dispositivos NAS D-Link.

Actualmente, existe un *exploit* para la vulnerabilidad crítica, que podría permitir la obtención de credenciales mediante la manipulación de argumentos. Además, el ataque puede ser iniciado de manera remota.

Productos afectados

Los modelos afectados por esta vulnerabilidad son aquellos que han alcanzado su fin de vida (EOL) y, por tanto, ya no reciben actualizaciones de *firmware*. Estos incluyen:

- DNS-340L
- DNS-320L
- DNS-327L
- DNS-325

D-Link ha confirmado que estos modelos están expuestos a ser explotados debido a la vulnerabilidad y recomienda retirarlos.

Solución

Dado que D-Link no planea lanzar una actualización de firmware para estos modelos EOL, la recomendación oficial es retirar y reemplazar estos dispositivos vulnerables. Se aconseja a los usuarios que, si continúan utilizando estos dispositivos contra la recomendación de D-Link, aseguren tener el *firmware* más reciente disponible en el sitio web de legado de D-Link, actualicen regularmente la contraseña única del dispositivo para acceder a su configuración web y mantengan la encriptación Wi-Fi activada con una contraseña única.

Referencias

- nvd.nist.gov
- nvd.nist.gov
- thehackernews.com

Eventos

RSA CONFERENCE 2024 SAN FRANCISCO (6 mayo – 9 mayo)

La RSA Conference, fundada en 1991 por RSA Security, se ha destacado como una de las conferencias más importantes en el ámbito de la ciberseguridad a nivel global. Este evento emblemático reúne a expertos, líderes de la industria y profesionales de TI para abordar los desafíos actuales y emergentes en seguridad informática. A través de presentaciones, paneles, talleres y demostraciones, la conferencia ofrece un espacio vital para explorar nuevas soluciones y mejores prácticas en protección de datos, amenazas cibernéticas, seguridad en la nube, inteligencia artificial aplicada a la seguridad, cumplimiento normativo y otros temas clave en la protección de la información. La RSA Conference se ha convertido en una plataforma esencial para la colaboración, el aprendizaje y la innovación en un mundo digital cada vez más interconectado.
Enlace

OSINTOMÁTICO CONFERENCE 2024 (17 mayo – 18 mayo)

La conferencia Osintomático 2024 reúne a profesionales de la seguridad, investigadores y entusiastas para compartir conocimientos sobre técnicas de inteligencia de código abierto (OSINT) e ingeniería social. El programa incluye ponencias, talleres, mesas redondas y demostraciones prácticas sobre temas como la recopilación de información de fuentes abiertas, análisis de datos de redes sociales, investigación de antecedentes y ciberseguridad. Los ponentes son expertos reconocidos en sus campos, y la conferencia es una excelente oportunidad para aprender y establecer contactos con otros profesionales del sector.
Enlace

45TH IEEE SYMPOSIUM ON SECURITY AND PRIVACY (22 mayo – 24 mayo)

Desde 1980, el Simposio de Seguridad y Privacidad del IEEE ha sido el principal foro para presentar avances en seguridad informática y privacidad electrónica, y para reunir a investigadores y profesionales en el campo. El Simposio de 2024 marcará el 45º encuentro anual de esta conferencia emblemática. El Simposio se llevará a cabo del 20 al 22 de mayo de 2024, y los Talleres de Seguridad y Privacidad se llevarán a cabo el 23 de mayo de 2024. Ambos eventos tendrán lugar en San Francisco, California, en el Hilton San Francisco Union Square.
Enlace

XIII FORO DE CIBERSEGURIDAD (XIII FORO DE CIBERSEGURIDAD 14 mayo)

El XIII Foro de Ciberseguridad, organizado por ISMS Forum Spain y su grupo de trabajo Cyber Security Centre (CSC), se celebrará en Madrid el día 14 de mayo de 2024. El evento abordará las últimas tendencias y desafíos en materia de seguridad informática, con un enfoque especial en la protección de datos, la gestión de riesgos y la respuesta a incidentes. El programa incluye ponencias de expertos, mesas redondas y casos prácticos, convirtiéndose en una cita ineludible para aquellos que deseen conocer las últimas tendencias y solución en materia de ciberseguirdad.
Enlace

BARCELONA CYBERSECURITY CONGRESS (21 mayo – 23 mayo)

El Barcelona Cybersecurity Congress, en su edición de 2024, se establece como un evento fundamental en el ámbito de la seguridad digital en España. Bajo el lema "Ciberseguridad en la Era Digital: Protección Integral y Resiliencia", este congreso proporcionará una plataforma tanto presencial como virtual para abordar los desafíos actuales y futuros en el ámbito de la ciberseguridad. Con un enfoque integral, se explorarán temas cruciales como la identidad digital, la protección de datos y la gestión de riesgos en un entorno cada vez más interconectado. .
Enlace

IX JORNADAS NACIONALES DE INVESTIGACIÓN EN CIBERSEGURIDAD (27 mayo – 29 mayo)

JNIC es un congreso científico que promueve el contacto, intercambio y discusión de ideas, conocimientos y experiencias entre la red académica y de investigación por una parte, y profesionales y empresas por otra. Sirve de escaparate de los últimos avances científicos en la materia y materializa un foro de debate en el que presentar perspectivas y enfoques innovadores en ciberseguridad, posibilitando la conexión entre la acción investigadora e innovadora y el desarrollo de productos y servicios de valor para la sociedad. Investigadores y profesionales de diferentes puntos de la geografía nacional presentarán el resultado de sus investigaciones científicas desde diversas perspectivas con un nexo común: la ciberseguridad. Las Jornadas se centrarán en tres ejes: Investigación, Transferencia y Formación en Ciberseguridad
Enlace

Recursos

EVOLUCIÓN DE LAS AMENAZAS A LOS DATOS EN 2024
En esta era digital, los datos se han convertido en uno de los recursos más valiosos para empresas, gobiernos e individuos por igual. Sin embargo, de igual forma que aumenta nuestra dependencia de los datos, también lo han hecho las amenazas y riesgos asociados a ellos. En este año 2024 se presentarán una serie de nuevos desafíos en la frontera de la seguridad de los datos, y los ciberataques se volverán más avanzados complejos y graves.
Enlace

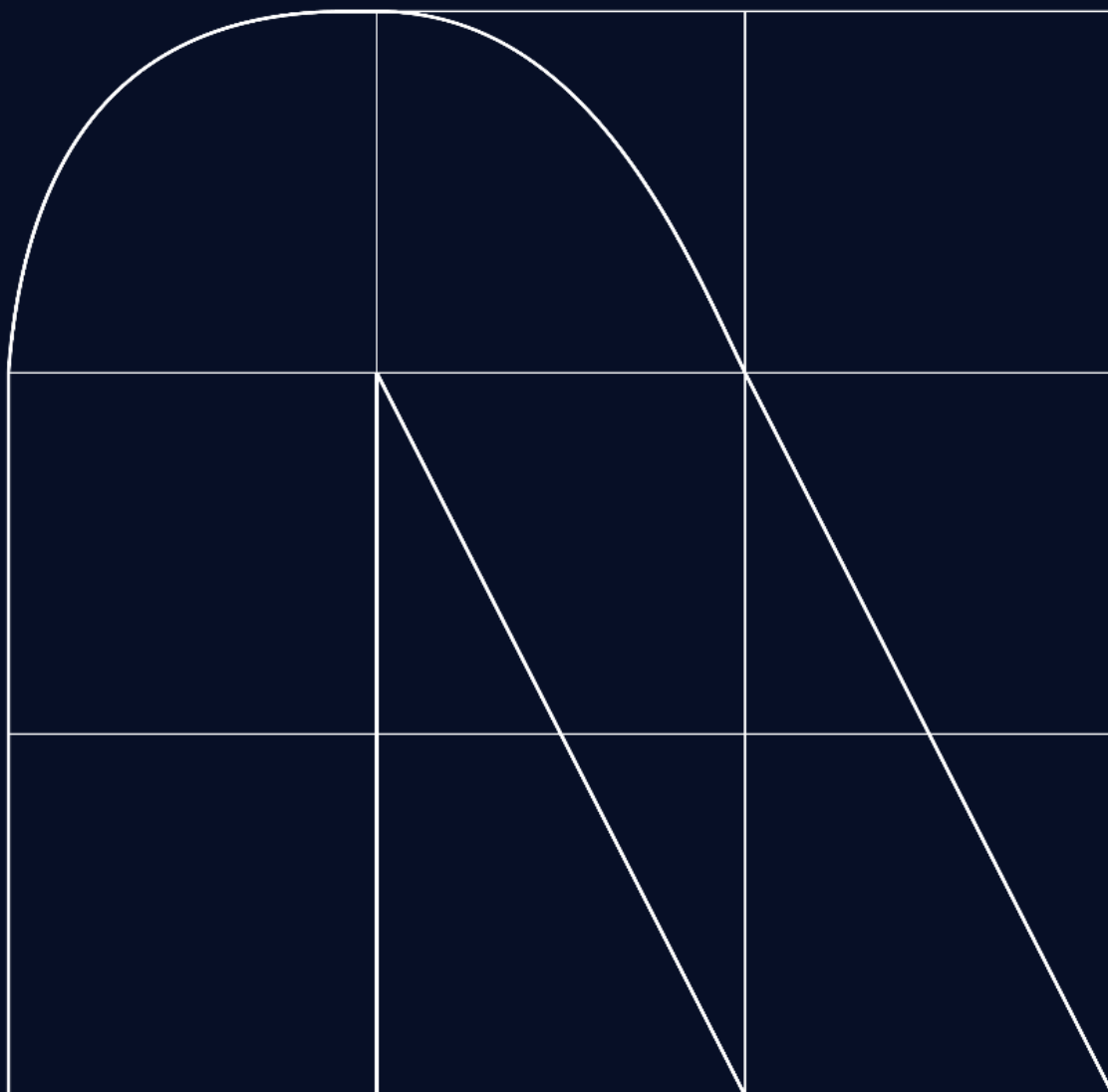
¿ESTÁ PREPARADO EL SECTOR DE LA CIBERSEGURIDAD PARA LA IA?
En los últimos años, se ha incrementado notablemente el interés en torno a la crucial función de la inteligencia artificial en la protección contra las ciberamenazas, así como en los notables beneficios que proporciona a la estrategia empresarial de ciberseguridad. No obstante, en este artículo, se aborda la pregunta fundamental de si el sector de la ciberseguridad está debidamente preparado para hacer frente a todas las complejidades inherentes a la IA, más allá de sus beneficios evidentes
Enlace

CONJUNTO DE MEDIDAS SOBRE CIBERSEGURIDAD
Con el fin de reforzar la solidaridad de la UE y sus capacidades para detectar amenazas e incidentes de ciberseguridad, preparase para ellos y responder cuando se produzcan, así como para mejorar su ciberresiliencia, la Presidencia del Consejo y los negociadores del Parlamento Europeo han alcanzado un acuerdo provisional acerca del llamado Reglamento de Cibersolidaridad y de una modificación específica del Reglamento sobre la Ciberseguridad
Enlace

THUNDERSTRIKE: EJECUTANDO APLICACIONES MALICIOSAS DESAPERCIBIDAS ANTE SOLUCIONES ANTIMALWARE MODERNAS

El compromiso de NTT DATA con la innovación se intensifica con cada paso que damos. En el reciente Congreso RootedCON, uno de los eventos más destacados en el ámbito hispanohablante, nuestros compañeros Antonio Pérez Sánchez y Marcos González Hermida presentaron Thunderstrike, una herramienta innovadora.

Thunderstrike es una herramienta de post-explotación con técnicas avanzadas de evasión que permite la carga y ejecución de aplicaciones .NET, como Seatbelt y Rubeus, entre otras. Esta herramienta es capaz de hacerlo sin ser detectado por los sistemas antimalware modernos: los sistemas Endpoint Detection and Response (EDR).



Powered by the cybersecurity NTT DATA team

es.nttdata.com