NÚMERO 80 | JULIO 2023

NTT DATA
Trusted Global Innovator

Radar

El magazine de ciberseguridad

LA ESCASEZ DE TALENTO Y LA ALTA ROTACIÓN: UNA PREOCUPACIÓN CRECIENTE EN LA ACTUALIDAD

Las organizaciones dependen cada día más de la tecnología, que evoluciona a alta velocidad, lo que se traduce en un incremento exponencial de las amenazas digitales cada vez más sofisticadas y con ataques difíciles de detectar y defender. Como consecuencia, hoy en día tenemos a nivel global una demanda de profesionales especializados en ciberseguridad que supera largamente la oferta disponible.

¿Y de qué tamaño es este GAP?

Algunos estudios revelan que a nivel mundial es de 3.4 millones de especialistas en seguridad (un 26% más que el pasado año), por ejemplo, en Latinoamérica es de 700.000 profesionales. Estos estudios revelan además que mientras la fuerza laboral crece, la demanda crece más rápidamente, mientras que la brecha entre la oferta y la demanda se amplía a mayor escala que la disponibilidad del talento.

A la búsqueda de profesionales especializados y mejor cualificados

Las competencias y experiencias críticas que requiere se pueden resumir en los siguientes elementos claves:

1. Experiencia laboral relevante en TI y en ciberseguridad.
2. Conocimiento de ciberseguridad avanzada.
3. Compresión de amenazas y vulnerabilidades.
4. Capacidad para resolver problemas.
5. Capacidad de influencia y articulación transversal en la organización.
6. Pensamiento estratégico y capacidad de reacción y decisión.

Entonces tenemos por un lado, a la tecnología y su evolución, que siempre se puede aprender,por el otro, encontramos capacidades como la **curiosidad**, la **resolución de problemas** y el **pensamiento crítico** que se valoran y consideran cada vez más imprescindibles para desempeñar esta especialidad. Con estas condiciones, la complejidad y desafío de identificar el talento para esta especialidad (función) se incrementan consistentemente.

¿Cómo se puede paliar el gap de talento?

Ante el desafío de la demanda de talento, las organizaciones deben reaccionar enfocándose en la formación en ciberseguridad, es decir por un lado con acciones de upskilling o la mejora de capacidades; y complementando con reskilling o adquisición de nuevas capacidades, ambas estrategias que resultan de mayor impacto. Encontramos que las organizaciones con iniciativas para formar talento interno por medio de asignaciones de trabajo rotativas, programas de mentoría y que alienten a los empleados de otras especialidades a unirse al campo de la ciberseguridad, son menos vulnerables a la falta de profesionales especializados en ciberseguridad.

Enrique Bernao

Manager de Ciberseguridad en NTT DATA Europe & Latam

CIBERCRÓNICA

En esta edición del RADAR hablaremos sobre la seguridad en usuarios finales. No es un mito que los humanos somos el eslabón más débil de la cadena. Recientemente se reportó un ataque sobre la ciudadanía que estaría afectando a infractores de tránsito. Si tienes multas de tráfico y tienes pendiente el pago tenmucho cuidado porque estafadores están engañando a incautos a través de ingeniería social.

Los timadores aprovechande la necesidad de los ciudadanos de tramitar la renovación de las licencias de conducción, ofreciéndoles supuestos descuentos para el pago de sus multas, cuando realmente los están robando.

Una de las víctimas de esta estafa menciona que recibió un correo electrónico que le indicaba que su licencia de conducción estaba a punto de vencer, y que podía acceder a descuentos en sus infracciones para que pudiese renovar su licencia.

> “Discord, el servicio de mensajería instantánea y VoIP, más utilizado por Gamers, Influencers y Streamers está notificando a sus usuarios que el pasado mes de mayo sufrieron un ataque informático que desencadenó en la exfiltración de datos de la plataforma.”

La víctima accedió a un enlace en donde un sitio web “exactamente igual al oficial” le mostró su historial de infracciones y la redirigió con un asesor vía WhatsApp. En esta conversación de WhatsApp, una supuesta asesora, quien además tenía datos exactos como: cantidad de multas, montos a pagar, fechas, direcciones y el documento depago, le pide a la víctima hacer una consignación. Todo para acceder a un supuesto descuento en la tarifa de la infracción.

A través de la denuncia de la ciudadanía se puso en alerta al comando cibernético de la policía y en pocas horas el sitio web se dio de baja, no obstante, no se tiene un registro exacto de las personas estafadas.

Si bien existe un factor humano fundamental para la materialización de este tipo de fraude, existen controles de seguridad que pueden ser implementados por los dueños de las aplicaciones para reducir la superficie ante este tipo de ataques sobre sus usuarios finales, por ejemplo, la de detección de clonación del sitio, autenticación para consulta de información, monitoreo de usabilidad, captcha, cuentas de asesor verificadas, entre otros.

Pasando a un ámbito global, Discord, el servicio de mensajería instantánea y VoIP, más utilizado por Gamers, Influencers y Streamers está notificando a sus usuarios que el pasado mes de mayo sufrieron un ataque informático que desencadenó en la exfiltración de datos de la plataforma. El ataque ocurrió después de que un encargado de soporte subcontratado fuese comprometido.

Al parecer el ataque expuso todos los tickets de soporte asignados al colaborador. Dentro de los datos exfiltrados se encontrarían: direcciones de correo electrónico, mensajes intercambiados, y los archivos adjuntos de soporte. El equipo de seguridad de Discord mencionó que una vez se detectó el incidente se deshabilitó la cuenta del colaborador y su máquina fue sometida a estrictas verificaciones antimalware.

“Debido a la naturaleza del incidente, es posible que su dirección de correo electrónico, el contenido de los mensajes de servicio al cliente y cualquier archivo adjunto enviado entre usted y Discord hayan sido expuestos a terceros”, fue el mensaje con que amanecieron cientos de usuarios al autenticarse en la plataforma. Asimismo, también mencionaron que están trabajando con su proveedor de soporte para implementar medidas eficientes para prevenir ataques similares en el futuro y recomendaron a sus usuarios tener estricta vigilancia ante ataques de Phishing dirigido.

De nuevo, colaboradores de las compañías son víctimas de ataques de ingeniería social con el objetivo de ganar acceso a los sistemas que gestionan. De allí la importancia de campañas de concientización efectivas que permitan a todos los colaboradores sin importar su área o experiencia técnica, detectar y reportar este tipo de ataques. También es importante que los usuarios finales de los servicios de soporte se abstengan de compartir información confidencial y sean muy concisos en los inconvenientes que presentan.

Continuamos con los ataques de denegación de servicio, Microsoft sufrió este tipo de ataque a principios del mes de junio. Los usuarios de Azure vieron afectado el acceso a la plataforma, por lo que se sospecha fue un ataque de denegación de servicio distribuido (DDoS). Según el sitio de monitoreo Downdetector, un 77% de los usuarios tuvieron problemas para acceder al sitio web de Azure, mientras que un 18% sufrió problemas para autenticarse.

El incidente llevó a la emisión de un comunicado por parte de Microsoft, en el cual reconocieron el problema y prometieron brindar una actualización en el transcurso de una hora o a medida que se desarrollaran los acontecimientos. El portal web quedó fuera de línea después de que un individuo que se identificara como Anonymous Suda y afirmara que estaba llevando a cabo un ataque DDoS. Sin embargo, Microsoft que es reconocido por contar con una sólida protección contra ataques de este tipo, argumenta que se ha logrado mitigar la afectación.

Este tipo de ataques sobre la infraestructura de Azure han sido recurrentes en lo que va del año, por ejemplo, entre enero y febrero, Microsoft reportó afectaciones en la disponibilidad de su servicio de WAF, Azure FrontDoor, provocando la caída de todos los sitios protegidos por el mismo, esto obligó a las compañías a deshabilitar esta protección y exponer sus servicios a internet durante más de 12 horas. Estos ataques sobre la nube de Microsoft demuestran que nadie se encuentra al margen de ataques cibernéticos, por lo que las organizaciones deben contar con modelos de defensa en profundidad, mecanismos de respaldo y planes de recuperación de desastres probados.

Finalizamos con el ataque la compañía Progress Software Corporation, reconocida por su oferta de software y servicios de TI, quienes han alertado a sus clientes sobre una preocupante vulnerabilidad en sus productos MOVEit Transfer y MOVEit Cloud. Esta vulnerabilidad, que fue catalogada como CVE-2023-34362 fue descubierta a comienzos del mes de junio y estaría afectando a cientos de miles de usuarios de diferentes compañías alrededor del mundo que utilizan estos servicios.

MOVEit Transfer es una solución cloud utilizada para almacenar y compartir archivos de manera segura en equipos, servidores, departamentos e incluso en cadenas de suministro. Su funcionalidad web permite una colaboración efectiva y transferencia automatizada de datos sensibles, todo ello sin necesidad de conocimientos de programación. Al parecer grupos cibercriminales rusos habrían explotado una inyección SQL en diferentes instancias de MOVEit logrando exfiltrar información de sus clientes, entre los cuales se encuentran la BBC, British Airways y Boots. Estos delincuentes estarían están reclamando una recompensa para no divulgar la información capturada.

En una serie de comunicados, Progress Software Corporation afirma que se encuentran trabajando activamente en solucionar esta vulnerabilidad, también aseguran estar comprometidos en mantener la confidencialidad y privacidad de sus clientes. Se espera que en los próximos días se brinden actualizaciones adicionales para abordar este problema y fortalecer aún más la seguridad de los productos MOVEit.

DATA SECURITY EN ENTORNOS MULTICLOUD Y REAL-TIME

Por: NTT DATA Europe & Latam

Los resultados favorables producto del uso del big data en cuanto a la optimización y eficiencia en las compañías no tienen precedentes. El crecimiento exponencial de la generación de datos tiene grandes desafíos en cuanto que son tecnologías que permiten el procesamiento de grandes cantidades de flujos de datos, en el menor tiempo posible y de la manera más económica. A ello se le suma que, para una mejor precisión en la toma de decisiones, es clave el procesamiento y uso de datos en tiempo real.

En este sentido, podemos citar al menos cuatro hitos claves en el desarrollo y crecimiento de la utilización de datos en tiempo real que son:

1) la cantidad de dispositivos a disposición para captar datos,

2) el internet de las cosas (IoT),

3) la nube y

4) el procesamiento in memory, el que se ha vuelto más accesible y popular en los últimos años.

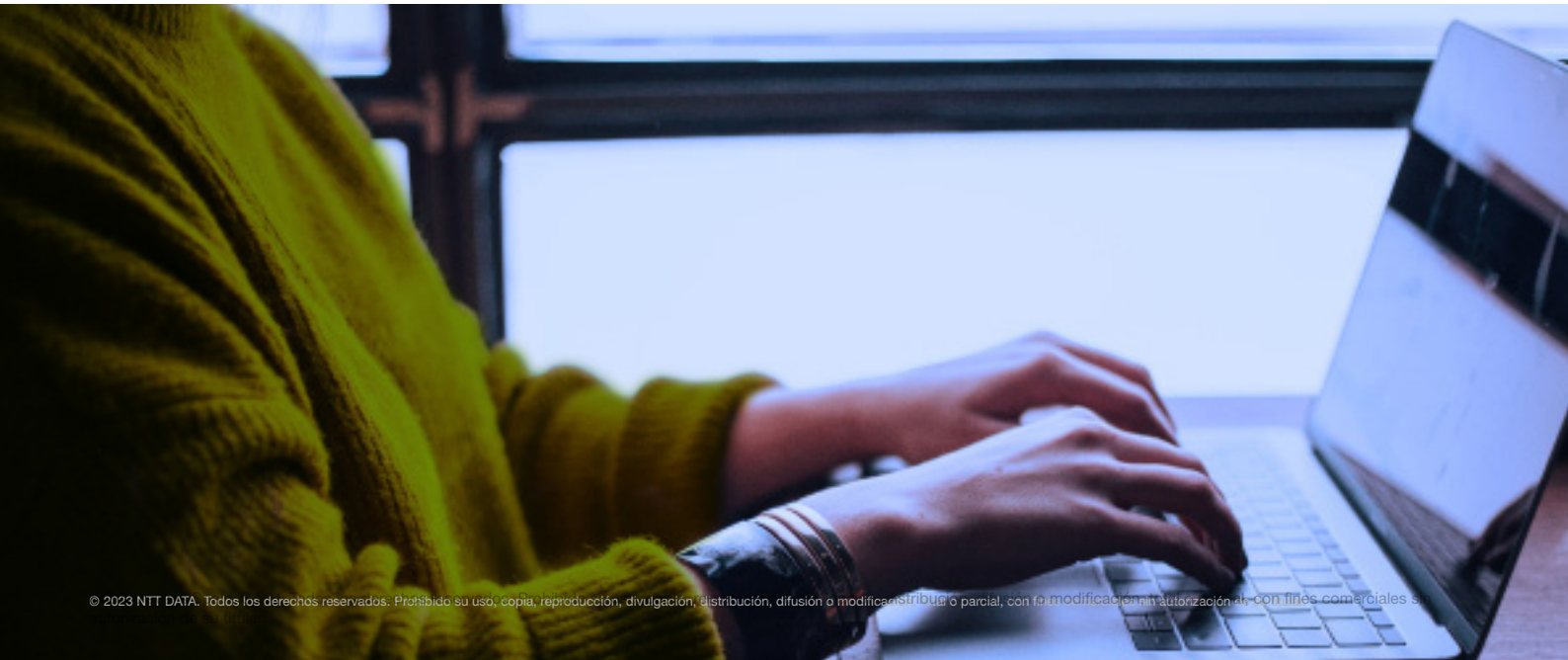
La implementación de todas estas herramientas y procesos tienen un gran desafío en común: la seguridad del dato end to end.

Siguiendo la conceptualización de Seguridad de Datos que desarrolla el DAMA-DMBOK , la misma incluye la planificación, el desarrollo y la ejecución de políticas y procedimientos de seguridad para proporcionar autenticación, autorización, acceso y auditoría adecuados de datos y activos de información.

Siendo el objetivo de las prácticas de seguridad de datos: proteger los activos de información en alineación con las normas de privacidad y confidencialidad, los acuerdos contractuales y los requisitos comerciales.

A pesar de ser imperante la implementación de este tipo de medidas, Confluent , en su reporte del año 2022, muestra que sólo el 27% de las empresas que entrevistaron cuenta con herramientas de seguridad para afrontar el procesamiento de datos en tiempo real, siendo su mayor desafío la implementación de seguridad y compliance en entornos multinube.

Algunos de los aspectos fundamentales a tener en cuenta en la implementación de medidas de seguridad en tratamiento de datos en tiempo real y multinube son:



- Identificación de amenazas en tiempo real: es fundamental contar con herramientas de monitoreo y análisis de datos que permitan detectar y prevenir posibles amenazas en tiempo real. Hoy en día existen diferentes desarrollos que aplican IA sobre los procesos para llevar adelante estas prácticas.
- Segmentación y seguridad en accesos: identificar y generar accesos en función de los permisos asociados, con autenticación adecuada, para evitar el riesgo de accesos no autorizados, garantizando que quienes se encuentran con autorización vigente tengan acceso a los datos.
- Protección de datos en tránsito: las organizaciones deben garantizar altos niveles de seguridad en torno a los datos en tránsito, implementando soluciones que permitan garantizar su integridad
- Respuesta rápida a incidentes de seguridad: es importante contar con planes de contingencia y respuesta a incidentes de seguridad para garantizar una respuesta rápida y efectiva en caso de que se produzca algún incidente de seguridad.
- Actualización constante: mantener actualizados los sistemas y herramientas de seguridad es clave para garantizar que se puedan identificar y prevenir nuevas amenazas de seguridad en tiempo real.
- Segmentación de red: la segmentación de red se utiliza para dividir una red en segmentos más pequeños y controlar el flujo de datos entre ellos. Esto ayuda a evitar que los atacantes se muevan lateralmente en la red y accedan a los datos confidenciales.
- Integración de herramientas de seguridad: En un entorno multinube, puede ser necesario integrar múltiples herramientas de seguridad de diferentes proveedores para garantizar una protección completa. Esto puede ser un desafío en términos de compatibilidad y configuración de herramientas.
- Cumplimiento normativo: realizar un plan de cumplimiento normativo, según las normas aplicables en cada país, sobre todo teniendo en cuenta las relativas a las transferencias internacionales de datos. Esto posee un alto grado de complejidad si pensamos en entornos multinube, toda vez que los datos y aplicaciones pueden estar distribuidos en múltiples proveedores de servicios en la nube con diferentes políticas de seguridad y herramientas de protección, las cuales deben unificarse.

Una de las tendencias más disruptivas en seguridad de datos, que ha cobrado relevancia en los últimos tiempos, es la adopción de tecnologías basadas en inteligencia artificial y aprendizaje automático para mejorar la detección de amenazas y la respuesta a incidentes de seguridad en tiempo real, algunas de ellas han sido mencionadas en nuestro RADAR del mes de marzo.

Respecto a los enfoques de seguridad, podemos mencionar el Zero Trust que desafía el modelo tradicional de confianza implícita y asume que todas las interacciones, tanto internas como externas, deben ser verificadas y autenticadas constantemente para reducir los riesgos de seguridad.

El modelo de seguridad Zero Trust actual se ha ampliado y sus principios se han implementado de muchas maneras, incluida la arquitectura Zero Trust, el acceso de red Zero Trust (ZTNA), la puerta de enlace web segura Zero Trust (SWG) y la microsegmentación. La seguridad Zero Trust también se denomina a veces seguridad sin perímetro.

De todas maneras, cabe resaltar que todas las implementaciones tecnológicas en materia de seguridad alcanzarán su éxito siempre y cuando las personas que trabajan en las empresas estén capacitadas en el tema y practiquen la seguridad a diario. Es por ello, que la concienciazión, alfabetización y educación en seguridad es el pilar esencial, sobre todo en empresas data driven que tengan como objetivo la democratización del dato.

En conclusión, la implementación de procesos y herramientas de seguridad del dato es imperante y debe tenerse en cuenta desde el inicio en la estrategia de datos que trace toda organización, debiendo ser uno de sus objetivos principales, toda vez que no sólo responde a necesidades del negocio en cuanto a la capacidad de tomar buenas decisiones, sino que su incumplimiento acarrea consecuencias legales y económicas las compañías.

GESTIÓN DE RIESGOS DE LA INTELIGENCIA ARTIFICIAL DESDE ENFOQUE DE NIST RMF Y NIST AI 100

Por: NTT DATA Europe & Latam

En la actualidad nos encontramos con que la Inteligencia Artificial (IA) ha transformado rápidamente nuestro mundo a través de la automatización de tareas, agilidad de procesar grandes cantidades de información, etc. Debido al gran avance de ésta, han surgido varias herramientas que incorporan la IA dentro de sus funcionalidades, ofreciendo software cada vez más avanzados. Esto a su vez, conlleva una serie de riesgos y amenazas que quizás no conocíamos antes o que actualmente estamos visualizando de una forma diferente.

El tema de la gestión de riesgos en la implementación de la IA es un asunto esencial, dado su creciente prevalencia en diversas actividades. Además, la adopción de sistemas de IA puede exacerbar ciertos riesgos dentro de una organización, especialmente en lo que respecta a la seguridad de la información y la privacidad. Es por eso que el debate sobre este tema se torna cada vez más relevante.

Algunos de estos riesgos son la discriminación, la pérdida de empleos y la privacidad de los datos, además de la falta de transparencia y explicabilidad de los algoritmos. También se han explorado los desafíos éticos y sociales relacionados con la IA, incluyendo el sesgo algorítmico, la criticidad de algunos datos personales y la seguridad cibernética.

Si bien la IA puede procesar grandes cantidades de datos en segundos, puede aumentar también significativamente el riesgo de violaciones de privacidad, por ejemplo.

Es importante mencionar que para afrontar y responder a los desafíos y complejidad de la gestión de riesgos en la IA existen frameworks, como la NIST RMF y la NIST AI 100, que pueden ser de gran ayuda para las organizaciones en la gestión de los riesgos asociados con la IA.

Estos marcos no solo proporcionan una guía para la identificación y evaluación de los riesgos, sino que también brindan un enfoque estructurado para la implementación de medidas de seguridad y para la monitorización y respuesta a los riesgos. Con la creciente importancia de la IA en nuestro mundo, la gestión efectiva de riesgos es esencial para proteger la privacidad y la seguridad de los datos, así como para garantizar la confianza en la tecnología de IA.

Al aplicar los marcos de seguridad adecuados en la implementación de la IA, las organizaciones pueden minimizar los riesgos asociados y maximizar los beneficios que la IA puede ofrecer.

Es por esto que la gestión de riesgos, desde un enfoque de GRC Governance, Risk and Compliance), se ha vuelto imprescindible para que la IA se desarrolle y utilice de manera segura y responsable en procesos dentro de una organización.

El NIST RMF y el NIST AI 100 son marcos complementarios que juntos pueden ayudar a las organizaciones a evaluar y gestionar los riesgos asociados con la implementación de la inteligencia artificial. El NIST RMF se compone de seis fases: categorización, selección de controles, implementación de controles, evaluación, autorización y monitoreo continuo. Al seguir este marco, las organizaciones pueden evaluar los riesgos asociados con los sistemas de información y tomar medidas para minimizar esos riesgos.

Por otro lado, el NIST AI 100 es un framework específico de inteligencia artificial que se puede aplicar al RMF para proporcionar pautas adicionales para la evaluación y gestión de riesgos en la implementación de la IA. Este marco se compone de cinco áreas clave: gobernanza, ciclo de vida de la IA, explicabilidad, privacidad y seguridad. Al combinar ambos marcos, las organizaciones pueden tener una comprensión más completa de los riesgos asociados con la implementación de la IA y tomar medidas para mitigar esos riesgos de manera más efectiva.

Aunque el uso de ambos framework no puede eliminar completamente los riesgos asociados con la IA, pueden ayudar a las organizaciones a evaluar y gestionar de manera efectiva estos.

De esta forma, es posible reducir la probabilidad de ocurrencia de las conductas que sean identificadas como riesgosas, como por ejemplo violaciones de seguridad.

Para garantizar una gestión adecuada de los riesgos asociados con la IA, el NIST AI 100 recomienda seguir una serie de 5 pasos clave:

El primer paso es la identificación de riesgos, que implica identificar los riesgos potenciales asociados con la implementación de la IA. En esta fase, se deben considerar tanto los riesgos de seguridad como los de privacidad, así como otros riesgos que puedan ser específicos del entorno de la organización.

El segundo paso es la evaluación de riesgos, que implica llevar a cabo una evaluación detallada de los riesgos identificados para determinar el impacto y la probabilidad de que se produzcan. Esta evaluación debe basarse en un análisis detallado de los riesgos y debe tener en cuenta tanto los aspectos técnicos como los de negocio.

Una vez que se han evaluado los riesgos, el tercer paso es la mitigación de riesgos, que implica implementar medidas de mitigación para reducir los riesgos identificados a un nivel aceptable. Estas medidas pueden incluir controles de seguridad adicionales, procedimientos de gestión de riesgos, políticas y prácticas de seguridad, entre otros.

El cuarto paso es la verificación y validación, que implica verificar que las medidas de mitigación implementadas funcionen correctamente y que los riesgos han sido mitigados a un nivel aceptable. Esto puede incluir pruebas de penetración, pruebas de seguridad, análisis de vulnerabilidades, entre otros.

Finalmente, el quinto paso es el monitoreo y mejora continua, que implica establecer un proceso de monitoreo y mejora continua para garantizar que las medidas de mitigación sigan siendo efectivas en el tiempo y que se mantengan actualizadas en respuesta a cambios en el entorno de la organización.

Incorporando un enfoque de Gobernanza, Riesgo y Cumplimiento (GRC), se puede desarrollar una estrategia integral para la gestión de la Inteligencia Artificial (IA). Este enfoque de GRC comprende aspectos críticos como la identificación de riesgos, el diseño e implementación de políticas y estándares claros, la selección minuciosa de proveedores, la implementación de controles de seguridad y la capacitación adecuada para los empleados. Este último factor es esencial para fomentar una cultura de cumplimiento dentro de la organización.

La adopción del enfoque de GRC no solo permite una gestión de riesgos más eficiente, sino que también ayuda a las empresas a garantizar el cumplimiento de los requerimientos regulatorios que puedan surgir. Esto se logra mediante la implementación de políticas y prácticas de seguridad adecuadas, lo que a su vez contribuye a la seguridad y eficacia de la implementación de la IA en la organización.

En resumen, la combinación del framework NIST AI 100, NIST RMF y el enfoque GRC puede ser una estrategia efectiva para mitigar los riesgos asociados con la implementación y uso de la inteligencia artificial en las empresas. La seguridad, privacidad y confiabilidad de los sistemas de inteligencia artificial son cruciales para el éxito de una organización, desde un enfoque integral y bien planificado para garantizar un entorno seguro y responsable.

TENDENCIAS

El uso de la biometría facial durante el proceso de onboarding como factor clave para adquirir más clientes

La constante evolución tecnológica ofrece infinitas oportunidades de negocio a las empresas que están dispuestas a embarcare en el journey de la transformación digital. Y cuando se trata de ofrecer experiencias de alto valor y con foco en el cliente, el onboarding digital contribuye significativamente.

Pero antes de seguir profundizando en la importancia del onboarding digital, se hace necesario comprender, ¿qué es onboarding digital? Una breve descripción podría ser un conjunto de instrucciones o interacciones que debe seguir un usuario con el fin de obtener un determinado producto y/o servicio.

El gran reto del onboarding digital

Esta definición de conjunto de instrucciones e interacciones se ha convertido en uno de los principales retos de las organizaciones en los próximos años. Si bien los usuarios demuestran su favoritismo para usar los canales digitales, la realidad es que alrededor del 70% de los usuarios abandonan los procesos de adquisición de productos y servicios, por una complicada y tediosa experiencia durante el proceso de onboarding (Financial Brands, 2022).

Razones de abandono de proceso de adquisición

Y no resulta un secreto que la primera interacción de un usuario con su producto y/o servicio es fundamental, y una mala experiencia puede impactar en incorporación de nuevos clientes o la retención de los actuales clientes. Por ello te dejamos, las 3 razones principales por las cuales los usuarios abandonan el proceso son:

1. Procesos largos: Indica que el proceso supera el tiempo esperado por el usuario.
2. No les aporta valor: No les generó la suficiente atención para iniciar y/o culminar el proceso de onboarding.
3. Demasiados requerimientos: El proceso pide demasiados requerimientos o estos son muy complejos de llevar a cabo.

Cómo las grandes empresas abordan este reto

Como respuesta a las principales razones de abandono, la identificación biométrica facial ofrece una experiencia de usuario fluida y segura que mejora las tasas de conversión durante el proceso de onboarding. Así mismo, dado que este tipo de soluciones son probabilísticas (a cierto nivel de % confirman la identidad de los usuarios) y con el fin de asegurar una mejora continua, es importante desarrollar ciertas capacidades como:

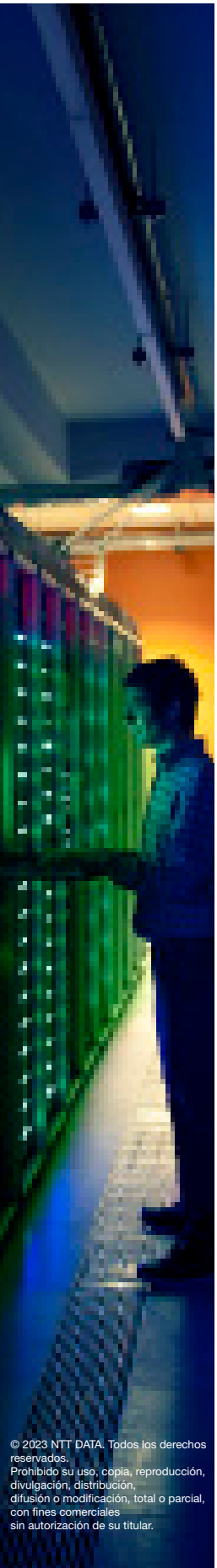
- Modelo seguro y escalable de desarrollo e integración.
- Modelo analítico a través de los pasos que recorre el usuario.
- Modelo preventivo de casos de suplantación

En Estados Unidos y Europa ya se pueden ver resultados positivos, como una reducción promedio del 20% en la tasa de abandono. Sin embargo, en el caso de Latinoamérica la adopción de soluciones de identificación biométrica facial sigue siendo menor.

Finalmente, las empresas que planean incrementar sus ratios de atracción y mantener a sus clientes mediante la innovación y transformación de sus canales digitales, no deben pasar por alto el papel crítico que conlleva la definición y gestión de sus procesos de onboarding. La incorporación de soluciones de identificación biométrica facial refuerza la seguridad de la información del cliente y ayuda a ofrecer una experiencia sin fricciones cada vez que un usuario interactúa con la marca.

VULNERABILIDADES

Reciba nuestro boletín completo de parches y vulnerabilidades suscribiéndose **aquí**.



Android

CVE-2023-21127;-21126;-21128;-21129;-21131;-21139;-21105;-21136;-21137;-21143
Fecha: 05/06/2023

Descripción. Se han descubierto múltiples vulnerabilidades en el sistema operativo Android de Google, la más grave de las cuales podría permitir la ejecución remota de código. Android es un sistema operativo desarrollado por Google para dispositivos móviles, incluidos, entre otros, teléfonos inteligentes, tabletas y relojes.

La explotación exitosa de la más grave de estas vulnerabilidades podría permitir una escalada de privilegios. Dependiendo de los privilegios asociados con el componente explotado, un atacante podría instalar programas; ver, cambiar o eliminar datos; o crear nuevas cuentas con todos los derechos.

Enlace: https://source.android.com/docs/security/bulletin/2023-06-01?hl=es-419
https://www.securityweek.com/androids-june-2023-security-update-patches-exploited-arm-gpu-vulnerability/

Productos afectados. Esta vulnerabilidad afecta a las siguientes versiones Android AOSP:
Versión 11, Versión 12, Versión 12L y Versión 13

Solución: La solución principal para solventar esta vulnerabilidad consiste en actualizar a las últimas versiones de Android.

Fortinet Fortigate

CVE-2023-27997
Fecha: 11/06/2023

Descripción. Fortinet publicó una actualización recientemente, luego del descubrimiento de una vulnerabilidad que podría permitir la ejecución remota de código no autenticado en los dispositivos. La falla, CVE-2023-27997, es un error de desbordamiento de búfer basado en montón. Este error, cuando se explota, puede permitir a usuarios no autenticados bloquear los dispositivos de forma remota y potencialmente ejecutar código.

En la actualidad, sigue siendo incierto si esta vulnerabilidad ha sido explotada activamente por atacantes. Sin embargo, el descubrimiento y la respuesta rápidos sirven como testimonio de la importancia de la vigilancia continua en la ciberseguridad.

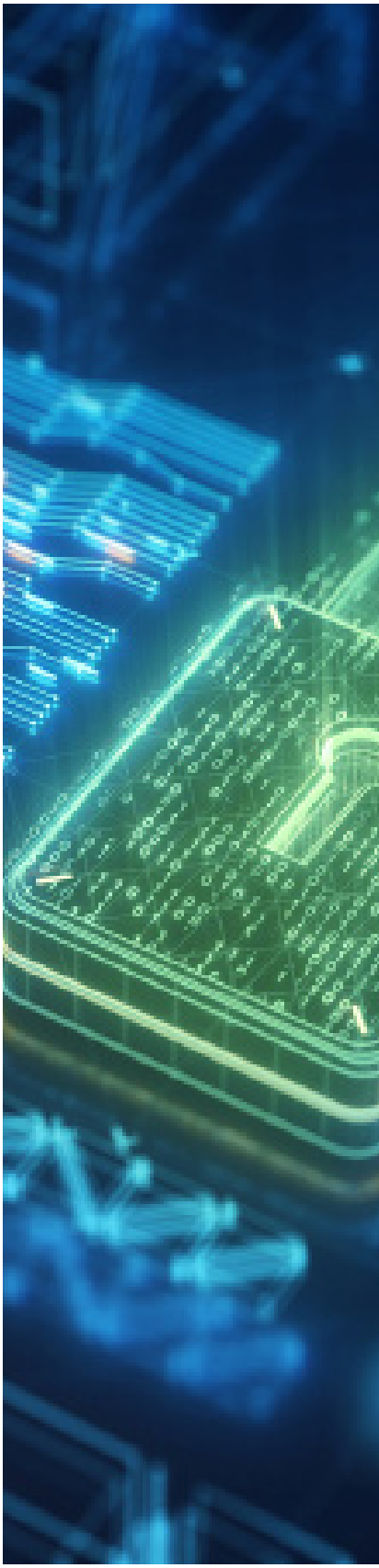
Enlace: https://securityonline.info/cve-2023-27997-fortinet-fortigate-pre-auth-rce-vulnerability/
https://www.bleepingcomputer.com/news/security/fortinet-fixes-critical-rce-flaw-in-fortigate-ssl-vpn-devices-patch-now/

Productos afectados.

- Los productos afectados corresponden a todas las versiones anteriores de FortiOS:
- 6.0.17
- 6.2.15
- 6.4.13
- 7.0.12
- 7.2.5

Solución: Actualizar los productos a las últimas versiones según corresponda previamente mencionadas.

PARCHES



MoveIT

Fecha: 02-06-2023

Descripción. La empresa propietaria del software MoveIT Transfer y MoveIT Cloud (Progress Software) ha publicado un parche de corrección para una vulnerabilidad crítica conocida como CVE-2023-34362.
Esta vulnerabilidad es de tipo inyección por SQL y permitiría permite a terceros tomar el control del panel de control de este software en un servidor. Una vez obtenido el acceso, se podría sustraer datos o realizar instalaciones como webshells (backdoors) y realizar modificaciones en el servidor comprometido.
Se tiene constancia que esta vulnerabilidad está siendo explotada desde finales del pasado mayo, además, se sabe que los atacantes que están explotando esta vulnerabilidad están creando backdoors en los servidores comprometidos con el nombre "human2.aspx".

Enlace:
https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2023-34362
https://news.sophos.com/es-es/2023/06/07/informacion-sobre-la-vulnerabilidad-cve-2023-34362-de-moveit-transfer-y-moveit-cloud/

Productos afectados:
Los productos afectados son:
- Move IT Transfer
- Move IT Cloud

Todas las versiones previas a la 13.0.6 resultan ser vulnerables.

Solución: Se recomienda actualizar los productos correspondientes a la última versión disponible (15.0.1)

Samsung

Fecha: 06-06-2023

Descripción. Samsung ha publicado su boletín de seguridad para revelar más información sobre el parche de seguridad de junio de 2023. Incluye 53 correcciones de Google para vulnerabilidades de seguridad que se encuentran en los teléfonos inteligentes y tabletas con Android. Tres de ellos están marcados como críticos, mientras que 50 están marcados como muy importantes. La actualización también incluye 11 correcciones para fallas de seguridad encontradas en dispositivos Samsung.

La firma surcoreana ha explicado tres de esas 11 vulnerabilidades (SVE o Samsung Vulnerabilities and Exposures). Las vulnerabilidades restantes no se revelarán hasta que todos los teléfonos y tabletas Galaxy reciban los parches de seguridad de junio de 2023 o posteriores.

Enlace: https://www.sammobile.com/news/samsung-june-2023-patch-detailed/
https://www.dealntech.com/samsung-june-2023-security-update-galaxy/

Productos afectados:
Versiones de Android 11, 12 y 13 previas a dicha actualización.

Solución: Para la corrección de estas vulnerabilidades es necesario la actualización al último parche de seguridad de junio 2023.

EVENTOS

Cyber Security Training at SANSFIRE

10 - 15 de julio de 2023 |

Aprende a combatir las últimas ciberamenazas del mundo con formación actualizada impartida por profesionales del mundo real. Conéctate con otros profesionales de la comunidad cibernética en uno de nuestros mayores eventos de 2023. Únete a nosotros en Washington, DC, o en vivo en línea para SANSFIRE 2023 (10 de julio - 15 de julio, EDT).

Enlace: https://www.sans.org/cyber-security-training-events/sansfire-2023/

Cyber Security Training at SANS Cloud Security

17 - 22 de julio de 2023 |

Aprende skills de ciberseguridad del mundo real de mano de los mejores expertos de la industria durante SANS Cloud Security San Francisco (del 17 al 22 de julio). Únete a nosotros en San Francisco, CA o en vivo en línea para experimentar la capacitación interactiva con laboratorios prácticos, practica tus habilidades durante uno de nuestros Torneos NetWars y establece contactos con otros profesionales en tiempo real. ¡Elige tu curso y regístrate ahora!

Enlace: https://www.sans.org/cyber-security-training-events/cloud-security-san-fran-2023/

Splunk Conf

17 - 20 de julio 2023 |

No es la típica conferencia de ciberseguridad, pero si eres un usuario de Splunk y estás en el campo de la ciberseguridad, este es un evento al que debes asistir. En Splunk Conf, serás capaz de aprender de los expertos de Splunk, sus compañeros y socios de Splunk acerca de cómo están abordando los retos de seguridad del mundo real. Podrás aprender con sesiones prácticas de los productos de seguridad Splunk y conocer las mejores prácticas para fortalecer tu postura de seguridad y mejorar tus habilidades.

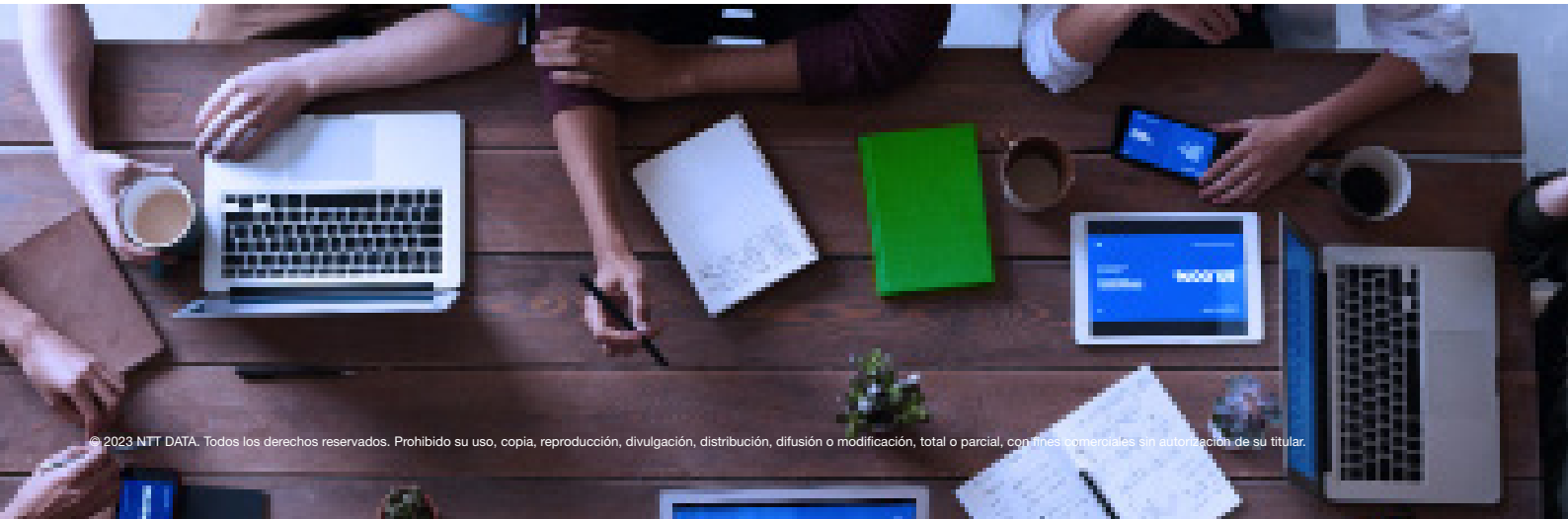
Enlace: https://conf.splunk.com/

Black Hat USA 2023

5 - 10 de abril de 2023 |

Las Black Hat Briefings son una serie de conferencias sobre seguridad de la información altamente técnicas que reúnen a líderes de opinión de todas las facetas del mundo de la infoseguridad, desde el sector empresarial y gubernamental hasta el académico, pasando por investigadores clandestinos. El entorno es estrictamente neutral en cuanto a proveedores y se centra en el intercambio de ideas prácticas y conocimientos oportunos y aplicables. Black Hat sigue siendo el mejor y mayor evento de su clase, único en su capacidad para definir el panorama de la seguridad de la información del mañana.

Enlace: https://www.blackhat.com/upcoming.html



RECURSOS

Google presenta nuevas funciones de ciberseguridad para ChromeOS

Google LLC ha anunciado un conjunto de nuevas funciones para ChromeOS destinadas a ayudar a las empresas a proteger los datos empresariales y los dispositivos de los empleados frente a los piratas informáticos. Las funciones se dieron a conocer en la conferencia anual RSA de Las Vegas.

Enlace: https://cloud.google.com/blog/products/chrome-enterprise/protect-business-data-chromeos-data-controls-and-new-security-integrations

2. Comprender los dos modelos de madurez de Zero Trust

Es una herramienta gratuita que puede ayudar a los defensores de la red a identificar posibles actividades maliciosas en los entornos de Microsoft Azure, Azure Active Directory y Microsoft 365. La herramienta proporciona nuevos métodos de autenticación y recopilación de datos para usar en el proceso de defensa de los mencionados entornos

Enlace: https://cloudsecurityalliance.org/artifacts/understanding-the-two-maturity-models-of-zero-trust/

CM Paquete legible por máquina (JSON/YAML/OSCAL)

CSA proporciona en un formato legible por máquina los Controles CCM, el Cuestionario de Seguridad CAIQ, las Directrices de Implementación (tanto JSON/YAML como OSCAL) y las Correspondencias (JSON/YAML) para apoyar a las organizaciones que deseen fomentar la automatización de CCM.

Enlace: https://cloudsecurityalliance.org/artifacts/ccm-machine-readable-bundle-json-yaml-oscal/

Palm2 de Google

PaLM 2 es la nueva versión del modelo de lenguaje de Google. Se trata del modelo que utilizará a partir de ahora Google Bard, y si Google aseguraba que PaLM era tres veces superior a GPT-3, es de esperar que esta nueva versión pueda enfrentarse directamente a GPT-4.

Enlace: https://ai.google/discover/palm2


NTT DATA
Trusted Global Innovator
powered by the
cybersecurity NTT DATA team
nttdata.com