

Marzo 2024



Radar

Powered by women



La adopción de la IA en las áreas de ciberseguridad

Por [Maria Pilar Torres](#)

Seguro que todos los lectores de esta revista se han preguntado varias veces los últimos meses hasta donde podrá aportar la IA y la IA generativa a nuestras áreas de ciberseguridad. Estamos viendo como esta tecnología avanza con paso seguro en otras áreas de las organizaciones, hecho constatado en el reciente estudio hecho por NTT DATA y el MIT sobre adopción de IA y con alcance Latinoamérica. En nuestra área tenemos déficit de talento experto y hay muchas tareas repetitivas donde parece que esta tecnología podría hacer un buen papel.

Para adentrarnos un poco más en este punto, hemos querido hacer un ejercicio para entender cómo se está usando la IA en las áreas de ciberseguridad, para el cual se ha lanzado una sencilla encuesta. Además de todo el detalle que podrán leer en el informe con los resultados quisiera compartir varios outputs:

Materialización del valor invertido en IA en ciberseguridad.

“Más del 95% de las organizaciones cree que la IA tendrá un impacto medio o alto en las áreas de ciberseguridad”

La IA está generando alta expectativa en ciberseguridad, y esto se traduce en presupuesto invertido y en apoyo de la organización. Esto supone que los CISOs deben materializar y cuantificar el valor invertido en IA en su área, demostrando que se han logrado alguno de los beneficios esperados. Especial importancia tiene este reto en las organizaciones que declaran llevar usando IA en las áreas de ciberseguridad más de 3 años.

Definición de casos de uso concretos de IA en ciberseguridad

“El SOC se percibe como el área donde más puede apoyar la IA, y si nos vamos a los dominios de la NIST, hay una opinión muy general de que los dominios identificar proteger, detectar, responder se pueden ver muy beneficiados con la IA”

La definición de casos de uso permitirá explicar cómo se está adoptando la IA en ciberseguridad, a la vez que limita el alcance a valorar y cuantificar. Actualmente se puede comenzar por la definición de casos de uso de SOC para ir extendiéndolo a dominios del NIST y otros ámbitos como gobierno o riesgos.

Cuidado del talento en IA & Ciberseguridad

“El talento, o más bien, la falta de él es la principal barrera de adopción de la IA”

Las organizaciones deben pensar qué carrera van a dar a los profesionales expertos en IA y ciberseguridad. Estas personas buscan nuevos retos y si no los encuentran en una organización, cambiarán a otra. Buscar la resiliencia en la rotación de este personal clave debe ser también parte de la estrategia de adopción de la IA.

Del informe se desprende que es un hecho la presencia de la IA en las áreas de ciberseguridad, en algunas desde hace varios años. Toca por lo tanto madurar el papel de la IA y maximizar su valor.



Las nuevas regulaciones de ciberseguridad de 2024

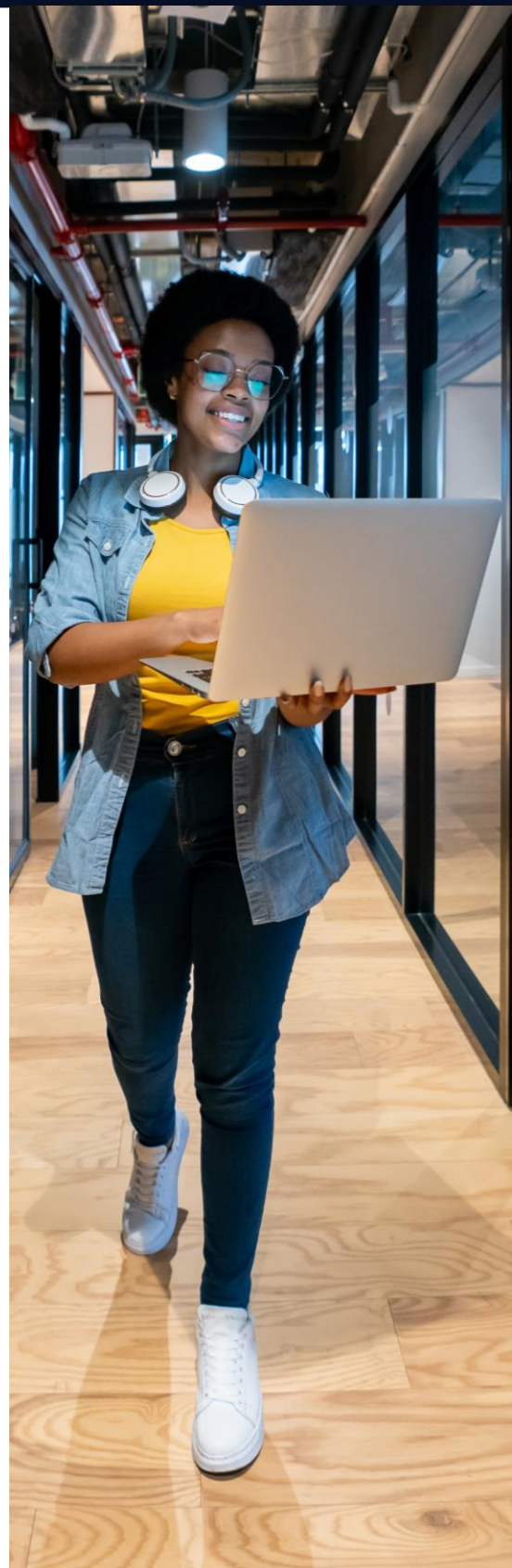
Por [Marta Fernández](#)

Son muchos los retos de ciberseguridad para 2024, desde la IA, la seguridad en la nube, la falta de talento, la concienciación de empleados y la sociedad hasta la preparación para la era cuántica, pero este año tenemos que decir que estamos ante unas regulaciones que entrarán en vigor y, por tanto, el cumplimiento normativo y la correcta gestión del riesgo serán una de las materias presentes en las agendas de muchos CISOS y profesionales de la ciberseguridad.

Durante el año 2024, entrarán en vigor, se actualizarán o revisarán varias regulaciones. Por ejemplo, el RGPD puede dar lugar a refuerzos estrictos en 2024, se presentará el primer paquete de normas técnicas sobre la Ley de Resiliencia Operacional Digital (DORA) que entrará en vigor en las entidades financieras de toda la UE en enero de 2025. Adicionalmente, encontraremos novedades con la nueva regulación NIS2, la entrada en vigor de WP.29 y se podrá votar la Ley de IA de la UE. Por tanto, es importante conocer el alcance e impacto en cada organización de cada una de estas regulaciones de 2024 y adelantarse, ya que su incumplimiento podría tener graves consecuencias legales, financieras y de reputación. En este artículo vamos a profundizar en el cambiante mundo de las legislaciones y regulaciones de ciberseguridad nuevas que entrarán en juego este año.

La Unión Europea da algunos pasos firmes en lo que concierne a materia de seguridad. Este año entra en vigor la directiva NIS2, adoptada el 14 de diciembre, cuyas medidas deben implementarse antes del 17 de octubre. La nueva NIS2 rompe con las limitaciones de su predecesora NIS1 (UE 2016/1148) permitiendo establecer un nivel alto y común en toda la Unión. Pone especial foco en la resiliencia de terceros y proveedores de servicios de infraestructuras críticas. Tiene un enfoque claro a la gestión del riesgo, incluyéndose disposiciones específicas para notificación de incidentes de ciberseguridad. Con ello se fomenta el intercambio de información y la cooperación público -estratégica para la gestión de crisis cibernéticas y divulgación de vulnerabilidades. En ese enfoque de riesgos, aborda también especialmente la seguridad en la Cadena de Suministro. La regulación también trae con ella medidas que conducen a la monitorización y supervisión del cumplimiento para evitar sanciones. Por tanto, es recomendable que las organizaciones obligadas al cumplimiento de esta regulación comiencen a definir un plan de ciberseguridad para abordar los nuevos requisitos que trae esta regulación. que toman como punto de partida el Threat Intelligence.

Por otra parte, una normativa que tendrá más impacto y transcendencia es la legislación y regulación sobre inteligencia artificial (IA). Se espera que la ley sea ratificada durante el primer trimestre de 2024 y su aplicación total está prevista para 2026. Aunque las tecnologías de IA no son nuevas, vivimos una creciente adopción y uso acompañada de desafíos técnicos, comerciales y de seguridad. Estos desafíos tienen un alcance global, tanto para organizaciones como para la ciudadanía o la sociedad. Se abrieron muchos debates para responder a cómo se monitorizará el uso de la IA y cómo regularizará los datos que se comparten a través de la IA, en definitiva, cómo controlará el cumplimiento de un uso bajo requisitos legales e incluso éticos.



La prioridad del Parlamento con la publicación de esta regulación es garantizar que los sistemas de IA utilizados en la UE sean seguros, transparentes, trazables, no discriminatorios y respetuosos con el medio ambiente. En definitiva, la ley de Inteligencia artificial es la primera regulación sobre la IA a nivel mundial, cuyo objetivo es regular la inteligencia artificial (IA) para garantizar mejores condiciones de desarrollo y uso de esta tecnología innovadora.

En abril de 2021, la Comisión propuso el primer marco regulador de la UE para la IA. La ley también basa su enfoque en el riesgo, pudiendo ser Mínimo, Alto e Inaceptable. Se establece una evaluación en la categorizando los sistemas IA, los cuales pueden ser modelos funcionales, modelos altamente capaces y modelos con propósitos generales. Esta regulación establece las prohibiciones para uso de la IA y vela por los derechos de los usuarios, que deberán informarse cuando existe tratamiento por parte de la IA. El objetivo es alcanzar un acuerdo a finales de este año. En función del nivel de riesgo, la nueva normativa establece obligaciones para proveedores y usuarios. Analicemos los diferentes niveles, empezando por el de mayor exposición al riesgo:

- **Los sistemas de IA de riesgo inaceptable** son los que se consideran una amenaza para las personas y serán prohibidos. Aquí se incluyen los que pueden llegar a la manipulación cognitiva, clasificación de las personas, la biometría y el reconocimiento facial.
- **Sistemas de IA de alto riesgo** son los que afecten negativamente a la seguridad o a los derechos. Se incluyen los sistemas de IA que se utilicen en productos sujetos a la legislación de la UE sobre seguridad de los productos y lo sujetos a los ámbito específico de : identificación biométrica y categorización de personas físicas, gestión y explotación de infraestructuras críticas, educación y formación profesional, empleo, gestión de trabajadores y acceso al autoempleo, acceso y disfrute de servicios privados esenciales y servicios y prestaciones públicas, aplicación de la ley, gestión de la migración, el asilo y el control de fronteras y asistencia en la interpretación jurídica y aplicación de la ley.
- **Sistemas de IA de riesgo limitado**, limitado deben cumplir unos requisitos mínimos de transparencia

La IA está transformando la ciberseguridad con sistemas de detección y respuesta automatizados, pero también preocupa a potenciales ataques automatizados y a atacantes que IA desarrollan ataques más sofisticados y difíciles de detectar. Avanzarse a los nuevos ataques y ganar capacidades de detección y respuesta es otro de los grandes desafíos.

La ciberseguridad también se aplica sobre productos como los coches, los cuales cada vez incluyen mayores funcionalidades basadas en Software y conectividad. Es por ello que, desde el pasado julio de 2022, todos los fabricantes de automóviles deben cumplir con el nuevo reglamento WP.29 UN R155/R156 para obtener la homologación del vehículo. WP.29 es como se conoce al Foro Mundial para la Armonización de la Reglamentación sobre Vehículos, que pertenece a la Comisión Económica de las Naciones Unidas para Europa (UNECE).

A partir de julio de 2024, el requisito de homologación bajo esta regulación se obligado para todos los vehículos nuevos vendidos en la Unión Europea, independientemente de cuándo haya obtenido el fabricante la homologación de tipo del vehículo. De hecho, es posible que para cumplir con el reglamento algunos modelos más antiguos que se sigan fabricando, deban introducir cambios para ser homologados de nuevo. El objetivo de esta regulación es asegurar que existe un margo de gestión de seguridad sobre los coches. A partir de este año, los coches deberán ir certificados en esta regulación, lo cual garantiza que son seguros ante la posibilidad de una amenaza cibernética o de un posible ataque a través de vulnerabilidades del Software del vehículo, sensores o cualquier otro servicio que esté conectado

En resumen, las regulaciones pretenden dar el marco normativo para estandarizar, establecer requisitos mínimos que velen siempre por la seguridad de los datos y de las personas. Estamos viviendo un momento de transformación, con nuevas tecnologías, productos, y elementos de la cadena de suministro entre otros. El control y mitigación del riesgo de seguridad que acompaña esta transformación se hace crucial para evitar catástrofes y grandes pérdidas, así como la resiliencia a posibles amenazas. Las regulaciones son un marco excelente y guía para llevar a cabo esta misión.

Hackeo extremo

Por [M^a Ángeles Gutiérrez](#)

Primero fue el mundo IT, al conectarlo a internet lo volvimos vulnerable y susceptible de ser hackeado, después conectamos el OT, las fábricas, los cajeros, hace unos años también el IoT, y ahora, a nosotros mismos, hace unos días nos anunciaban que se había implantado con éxito un chip cerebral que permitirá entre otras muchas cosas, controlar el teléfono o el ordenador, y a través de ellos casi cualquier dispositivo, con sólo pensar...

Es cierto que llevamos años incorporando diferentes dispositivos en nuestro cuerpo, estamos hablando de; marcapasos, implantes cocleares (estimulación directa del nervio auditivo), neuro estimuladores (para tratar la epilepsia o el dolor crónico mediante estimulación directa de áreas del cerebro o nervios periféricos), monitores de glucosa implantables, implantes retinales oculares (restauran parcialmente la visión al estimular la retina con señales eléctricas), chips RFID subcutáneos (dispositivos de identificación por radiofrecuencia), prótesis neuro controladas, sensores de presión (utilizados para monitorizar la presión intracraneal), biomarcadores implantables (detectan y monitorizan biomarcadores específicos en el cuerpo para proporcionar información sobre la salud en general), pero los últimos anuncios como el de *neura link* van un poco más allá..., conectamos nuestro propio cerebro, somos un terminal más ¿Conectado a la red? ¿Expuestos como cualquier dispositivo a ser hackeado?

La convergencia entre tecnología y cuerpo humano, desde luego, plantea nuevos retos, la creciente integración de dispositivos electrónicos en el cuerpo humano conocida como cuerpo conectado o cuerpo cibernético trae desafíos significativos.

La recopilación constante sobre datos biométricos y de salud que permiten estos dispositivos preocupa la privacidad individual, incorpora nuevas vulnerabilidades, los dispositivos implantables pueden ser susceptibles a ataques cibernéticos comprometiendo la integridad y confidencialidad de los datos médicos, incluso poniendo en riesgo la salud del individuo con nuevas infecciones y manipulaciones, mantener estos dispositivos seguros durante el tiempo mediante actualizaciones es un desafío técnico aún no resuelto, faltan estándares universales comunes que dificultan la interoperabilidad y la adopción masiva, no se integran con seguridad y eficientemente con el sistema biológico sin efectos secundarios.

Por otro lado, está todavía pendiente de analizar la aceptación de estas tecnologías por parte de la población y como afecta a la percepción de la identidad y la autonomía individual, así como impacto en la autoestima, la presión por conformarse a estándares de belleza o rendimiento pueden crear una cultura de inseguridad y disconformidad con el cuerpo natural, así como a la intensificación de las desigualdades creando brechas entre aquellos que tengan o no acceso a las mismas, como impactarán en las relaciones interpersonales es otra incógnita, además la dependencia excesiva de estos dispositivos podría afectar gravemente a la capacidad del cuerpo para funcionar de forma natural, y la obsolescencia tecnológica podría dejar a las personas en situaciones de riesgo si los dispositivos fallan o se vuelven incompatibles con las nuevas tecnologías.

En resumen, todo aquello que esté conectado a la red, o tenga un sistema inalámbrico es susceptible de ser hackeado, así que para no renunciar a los beneficios que seguro nos traerá el "cuerpo conectado" (para miles de personas parapléjicas, con ELA, pérdida de visión, afasia,...

Sin duda será una gran oportunidad) y prevenir y evitar la gran tentación que casi seguro supondrá el intentar acceder a la información de nuestra salud incluso puede que directamente a nuestros pensamientos y manipularlos, para evitar ese "hackeo extremo" pongamos a disposición de estos nuevos usos, todo lo aprendido sobre seguridad, tanto desde el punto de vista técnico como normativo y regulatorio, y no volvamos a cometer el error, de hacer despliegues masivos, de tecnologías inmaduras desde el punto de vista de la ciberseguridad, nos va mucho en ello, en este caso la salud y la hasta la vida.

Gobierno de identidades

Por [Andea Muñoz](#)

Desde la era de la revolución industrial las empresas han evolucionado y con ello se han adaptado a las necesidades de un mercado cambiante, en base a los nuevos descubrimientos y requerimientos de la industria. Sin embargo, desde la llegada de la internet esta evolución ha dado un giro mucho mayor e inicio una aceleración exponencial, lo que ha obligado a las empresas a adaptarse más rápidamente al cambio. Uno de los pilares de esta evolución es la transformación digital, la cual se podría resumir como la adopción de la tecnología en todos los procesos del negocio.

En 2020 con la covid-19, esta transformación se forzó y las empresas se vieron obligadas a adaptarse, ¿pero implica tener una empresa en el mundo digital?, ¿que implica para las empresas no controlar los datos y la información que se mueve por ella?, todos estos desafíos se empezaron a volver preguntas que requerían respuesta inmediata. Antes de la transformación digital todos los datos e información de las empresas estaban físicamente en ellas, por lo que los esfuerzos estaban hacia proteger el perímetro y prevenir la fuga de información. Pero con la transformación digital, la necesidad de movimiento, trabajo remoto y la adopción de la nube, el perímetro se expande volviéndose imposible de controlar, dejando a las empresas sin borde; La identidad de las personas y los sistemas de autenticación se vuelven relevantes para la protección de los datos de las empresas ahora descentralizadas.

Otro punto que ha generado nuevas brechas de seguridad y preocupaciones entre las áreas de seguridad pero que sin embargo es una tendencia mundial y que facilita el trabajo de las empresas es el movimiento a la nube.

A lo anteriormente mencionado se suma el cambio de generaciones que se vuelve por un lado la fuerza laboral más importante y el área de consumo más fuerte, las generaciones Milenians y Centenials ya representan el 59% de la fuerza laboral de las empresas, y estas generaciones tienen un pensamiento al que las empresas se deben adaptar, es un pensamiento que requiere agilidad y atención inmediata a sus necesidades ya que son generaciones que crecieron con la tecnología como parte fundamental de sus vidas.

A estas generaciones la necesidad de mayor tiempo libre, flexibilidad de trabajo y posibilidad de teletrabajo, son unos de los puntos claves para mantener el talento, estas generaciones también tienen orientaciones a que los procesos se hagan de una manera rápida y en general vía aplicaciones, sin filas sin contacto y mejorando la experiencia de usuario. Todo esto lleva a las empresas a la necesidad de transformarse para seguir vigente en el mercado. Un claro ejemplo de esto es el ver que las empresas más grandes y con mayor crecimiento actualmente son empresas de tecnología.

Por todo lo antes expuesto y con el aumento de las amenazas cibernéticas, cada vez más empresas priorizan la seguridad de la identidad como un punto clave en sus estrategias de seguridad, de esta forma mitigar riesgos y proteger sus activos digitales. Esto se ve reflejado en el aumento de adquisiciones de tecnologías como IAM (Identity and Access Management), PAM (Privileged Access Management) y MFA (Multifactor Authentication), así como en recomendaciones de entidades como Gartner que ponen a algunas de estas tecnologías como claves en la estrategia de las empresas y resaltan su importancia.



Las cuentas privilegiadas traen consigo otros problemas que se deben tomar en consideración, dependiendo del sistema que se maneje; Muchas contraseñas están escritas en el código del sistema, esta es una mala práctica, aunque más común de lo pensado, sin embargo, se la realiza para proteger la disponibilidad de los sistemas, esto puede traer que existan claves que no son cambiadas por años, con mayor medida la brecha de seguridad se abre si hablamos de ex empleados.

A todo lo anterior hay que sumar los posibles errores humanos, los humanos somos la parte fundamental de las organizaciones sin embargo en el recurso humano se generan varias brechas de seguridad, entre los errores más comunes, en la mayoría de los casos por falta de capacitación en tecnología de información, es el guardar contraseñas en lugares no apropiados como en un Excel, compartir las contraseñas, dejar sesiones abiertas, todo ello aumenta la probabilidad de ser atacados.

¿Qué es y que abarca el gobierno de identidades?

El Gobierno de Identidades IDG (Identity Governance), hace referencia al conjunto de procesos, tecnologías y políticas que se utilizan para gestionar la identidad digital dentro de una organización. Esto es la definición de roles de las identidades (a que sistemas, cómo y con qué privilegios y autorizaciones puede acceder una identidad) y garantizar el manejo adecuado de estas asignaciones. Una identidad digital puede ser tanto una persona que forma parte de la organización, como un proveedor o un sistema que tenga identidad digital. El gobierno de identidades incluye el aprovisionamiento y desaprovisionamiento de las identidades, así como la gestión de los accesos de la misma.

¿Que tomar en cuenta para un buen gobierno de identidades?

Para que una empresa pueda adoptar su gobierno de identidades de una forma efectiva debería tomar en cuenta las siguientes recomendaciones:

Identificar las identidades, el alcance de estas identidades tanto internas como de sus aliados estratégicos y proveedores, y los riesgos asociados a su manejo. De igual manera se debe identificar los usuarios con altos privilegios y las cuentas a las que tienen acceso. Para esto se recomienda una consultoría de gobierno de identidades.

Desarrollar políticas y procedimientos que permitan determinar de forma clara la gestión de las identidades en la empresa, como se crearán los usuarios, como se darán de baja, con que autorizaciones y bajo esquema y procedimiento, que debe alinearse a las mejores prácticas de seguridad y privacidad de datos.

Analizar e implementar las tecnologías adecuadas tanto de IAM como de PAM, para esto se recomienda hacer una matriz de necesidades a cubrir, cantidad de usuarios que tendrán acceso a la tecnología, y que alcance se quiere abarcar a nivel de casos de negocios y tecnologías de la empresa a las que se deben integrar. Este análisis previo es clave para el éxito de la adopción de la tecnología, permitirá a la empresa poder explotar adecuadamente lo adquirido y no tener tecnologías subutilizadas.

Para el punto anterior es muy importante contar con un aliado estratégico para la consultoría, implementación y despliegue de la tecnología. Contar con un partner adecuado con experiencia y conocimiento, para el gobierno de identidades, así como para los demás aspectos de seguridad es clave para el éxito.

Involucrar y educar a los usuarios que forman parte de la organización, sobre cómo mantener sus claves y accesos protegidos, así como la importancia de la adopción tecnológica, hará que el camino sea más sencillo y que exista menos resistencia al cambio.

Monitorear y revisar de forma continua el cumplimiento de las políticas de gestión de identidades, la congruencia de los datos manejados y la efectividad de los controles aplicados, para esto se pueden realizar auditorías y análisis constante del manejo de las identidades.

Otra buena práctica es la integración de las soluciones de IAM y PAM con otras herramientas de seguridad para la detección y respuesta oportuna de incidentes de seguridad.

Por último, se debe tomar en cuenta el cumplimiento normativo que rige según la industria y el país donde se encuentre tomando aspectos como la ley de datos personales y estándares de seguridad como la ISO27001.

Maximizando la resiliencia cibernética

Por [Almudena Abolafia](#)

En el siempre dinámico panorama de la ciberseguridad, la prevención proactiva y la preparación son esenciales.

En este artículo, exploraremos cómo la integración estratégica de Cyber Threat Intelligence (Inteligencia de Amenazas o CTI, por sus siglas en inglés) y la Simulación de Adversarios puede potenciar la resiliencia cibernética de las organizaciones. Estas dos disciplinas, si se combinan de manera efectiva, ofrecen un enfoque holístico para identificar, evaluar y mitigar las principales amenazas cibernéticas.

Cuando hablamos de CTI no hablamos sólo de recopilar datos; es mucho más. Se trata de un proceso dinámico y continuo de recolección de datos, análisis exhaustivo y aplicación de información específica sobre amenazas, actores maliciosos o threat actors, como son más comúnmente conocidos, y sus motivaciones. Esta inteligencia puede provenir de fuentes externas como, por ejemplo, feeds de amenazas e IOCs publicados, así como de fuentes internas como, por ejemplo, registros de eventos de seguridad identificados por los equipos de Blue Team o actividades de threat hunting sobre la red interna de una organización para identificar indicios de actividad maliciosa o no autorizada. Al comprender las tácticas, técnicas y procedimientos (TTPs) de los adversarios, las organizaciones pueden anticiparse y prevenir estos ataques mediante la generación de reglas de detección (detection rules) basadas en estas TTPs, y contrarrestar las ciberamenazas de manera más efectiva.

Por otra parte, la Simulación de Adversarios, frecuentemente confundida con “ejercicio de Red Team”, va más allá del clásico pentesting o test de intrusión, donde el foco está en identificar vulnerabilidades. En este caso, estamos hablando de emular threat actors y replicar, en la medida de lo posible, las TTPs que utilizan en sus ataques, lo que permite evaluar la resiliencia de la postura de seguridad de una organización y proporciona una visión realista de su capacidad de detección y respuesta ante las posibles vulnerabilidades y debilidades a las que se enfrentarían en un ciberataque real. La principal diferencia entre un ejercicio de Simulación de Adversarios y un ejercicio de Red Team radica precisamente en la necesidad de colaboración entre el equipo de CTI y el de Red Team durante la fase de preparación del ejercicio.

¿Cómo enriquece un equipo de CTI a un equipo de Red Team?

La sinergia entre el equipo de CTI y el de Red Team es crucial para una postura de ciberseguridad efectiva. La Inteligencia de Amenazas (CTI) informa y personaliza los escenarios de simulación de adversarios, mejorando significativamente la capacidad del equipo de Red Team de diseñar un escenario de ataque adaptado a las principales amenazas a las que deba enfrentarse la organización. Por ejemplo, la identificación por parte del equipo de CTI de APT38 como un actor malintencionado que se centra en instituciones financieras, permite a un equipo de Red Team que preste servicio a un banco, modelar ataques específicos basados en las mismas TTPs y artefactos que utiliza este threat actor, ayudando a la organización a identificar sus principales puntos de fallo e incrementar su nivel de madurez en materia de ciberseguridad mediante la mejora de su capacidad de detección y de respuesta ante ciberataques.



Para que esta sinergia sea exitosa se deben realizar las siguientes actividades:

Identificación de los principales threat actors que operan en el sector de la organización objetivo y/o han afectado recientemente a sus competidores, proporcionando contexto sobre las TTPs utilizadas y objetivos del ataque. Este ejercicio es realizado por el equipo de inteligencia de amenazas (CTI) durante la denominada “fase de preparación” de un ciber ejercicio o ciberataque.

Modelado de ataques basado en la información de CTI previamente obtenida, lo que permitirá diseñar escenarios de ataque realistas.

Personalización de los escenarios de ataque, teniendo en cuenta las herramientas (artefactos) y técnicas específicas usadas por los grupos de threat actors que se van a emular contra la organización objetivo.

Análisis de las vulnerabilidades que serán objetivo de explotación durante el ejercicio. Comprenderlas, permitirá a las organizaciones identificar dónde deben poner foco para una detección proactiva y respuesta rápida que mejore su postura de seguridad y minimice el impacto de posibles brechas de seguridad.

Al alinear las simulaciones de Red Team con amenazas específicas, las organizaciones pueden maximizar la eficiencia de sus recursos de seguridad, focalizándolos en las áreas más críticas. Además, la retroalimentación constante entre el equipo de CTI y el Red Team garantiza una mejora continua del servicio, adaptando la postura de seguridad de la organización a las amenazas emergentes.

En NTT DATA creemos que la integración profunda de los servicios de Threat Intelligence y Simulación de Adversarios representa un hito crucial en la evolución de las estrategias de ciberseguridad. Por ello, dentro de nuestro catálogo de servicios impulsamos la realización de estos ejercicios ya que, al unir estas dos disciplinas, las organizaciones se beneficiarán de defenderse contra amenazas actuales y se posicionarán estratégicamente para enfrentar desafíos emergentes que puedan afectar a su sector. La resiliencia cibernética y la ciberseguridad efectiva van más allá de la protección; son fruto de una mentalidad proactiva y evolutiva.

La sinergia entre Threat Intelligence y la Simulación de Adversarios es el camino hacia una postura de seguridad más sólida y adaptativa, maximizando la resiliencia cibernética de cualquier organización. .



Inteligencia Artificial: Navegando la frontera entre la defensa y el ataque

Por [Mafalda Maciel Querido](#)

Hemos comprobado que la Inteligencia Artificial no es solo una nueva palabra de moda o una tendencia "sexy" en el mundo de las tecnologías. De hecho, la Inteligencia Artificial incorpora campos que ya conocemos desde hace mucho, como el Aprendizaje Automático (Machine Learning) y el Aprendizaje Profundo (Deep Learning), con pruebas demostradas, y ahora tiene un nuevo enfoque y su uso se ha democratizado. Sin embargo, su rápida evolución y uso por parte de la sociedad, como ya han demostrado varios estudios, nos preocupa a los profesionales de la ciberseguridad. Más aún, diría que la sociedad tendrá inevitablemente que enfrentar.

Podemos ver el problema desde dos perspectivas. Por un lado, sabemos que esta tecnología cambiará la forma en que trabajamos, acelerará procesos lentos, permitirá aumentar la productividad y combatir la falta de profesionales en este campo. Las organizaciones que no se suban al tren de la innovación, inevitablemente quedarán rezagadas, como ya hemos visto históricamente. Por otro lado, sabemos que la línea que separa los aspectos positivos de los peligros inminentes que nos trae la Inteligencia Artificial es delgada, y que, por lo general, los atacantes siempre intentan estar un paso adelante. Como cualquier héroe, la Inteligencia Artificial también tendrá su villano.

Son innegables los impactos positivos que la Inteligencia Artificial aporta a la ciberseguridad: una mayor y mejor automatización en la detección y respuesta a amenazas, con la posibilidad de analizar volúmenes masivos de datos a velocidades sin precedentes y, por lo tanto, identificar anomalías de manera más rápida, lo que permite a los equipos de seguridad anticipar riesgos y amenazas de manera más efectiva, y también ayudar en esta crisis de recursos humanos especializados que estamos experimentando; un análisis de patrones y comportamientos más rápido; sistemas adaptativos que evolucionan para hacer frente a nuevas amenazas; aumento de la previsibilidad y de la capacidad y velocidad de la toma de decisiones basada en datos e información concreta. En resumen, la Inteligencia Artificial puede y debe ser utilizada como una herramienta aliada, que nos ayuda en términos de productividad, análisis de información y rapidez de respuesta en este entorno de rápida transformación en el que vivimos.

Sin embargo, como cualquier tecnología, también trae nuevos riesgos y, para la ciberseguridad, representa un nuevo factor de rapidez, sofisticación y alcance de los ataques. A medida que las barreras de defensa evolucionan, también lo hacen las tácticas utilizadas por agentes maliciosos. La automatización lleva a la explotación de vulnerabilidades a gran escala que, beneficiándose también de la adaptabilidad de los sistemas, aprenden nuevas formas de sortear las barreras de seguridad a medida que las encuentran; tácticas de engaño y evasión que imitan el comportamiento humano legítimo, dificultando su detección; el reconocimiento orientado por Inteligencia Artificial que permite un análisis exhaustivo y más rápido de posibles objetivos, identificando vulnerabilidades y puntos de entrada en la infraestructura de una organización; la capacidad de crear mensajes de phishing, smishing y vishing altamente dirigidos y convincentes, que junto con el uso de deepfake, eleva todo el campo de la ingeniería social a un nivel más sofisticado, impredecible y difícil de detectar, y trae una nueva disrupción en lo que respecta a las precauciones y mecanismos de defensa con los que debemos dotar a nuestros colaboradores.

Además del conflicto moral y ético que surge del uso de la Inteligencia Artificial Generativa -sobre la cual cada vez más instituciones, estatales y no estatales, están investigando- y de los peligros relacionados con la compartición no intencionada de datos personales e información sensible, ya sea por desconocimiento, falta de medidas tecnológicas para su prevención, o incluso descuido, surge una exposición aumentada de lo que muchos consideran el eslabón más débil, y para otros, la primera línea de defensa de las organizaciones: el elemento humano.

El uso masivo de esta nueva tecnología acaba de comenzar, y ya tiene un alcance mayor que cualquier otra tecnología o plataforma vista anteriormente, y las consecuencias ya se están sintiendo. Aunque aún no existen estudios de gran alcance sobre el impacto que la Inteligencia Artificial tendrá en la seguridad de la información y la ciberseguridad desde el punto de vista del riesgo humano, ni análisis estadísticos muy concretos, ya están surgiendo los primeros casos de ataques perpetrados con base en tecnologías de Inteligencia Artificial Generativa.

La concienciación de los colaboradores y de la sociedad en general en materia de Seguridad de la Información sigue siendo uno de los puntos menos evidentes y de mayor dificultad de ejecución. Aún tenemos el desafío de preparar y alertar a los colaboradores de las organizaciones sobre los riesgos y la importancia de la seguridad, y hacerlo eficazmente y que dé resultados, resultados difíciles de medir, porque las variables son muchas y difíciles de cuantificar y calificar.

Entonces, ¿cómo debemos proceder frente a estas nuevas y mejoradas amenazas? ¿Cómo enseñamos a detectar ataques cada vez más creíbles, a simple vista? ¿Cómo detectamos comportamientos anómalos cuando cada vez se asemejan más a los nuestros? ¿Tendremos que reinventarnos, y reinventar la forma en que concienciamos a nuestros colaboradores? En este momento, surgen dudas para las cuales, por ahora, tenemos pocas respuestas concretas.

Los equipos de seguridad deben repensar su enfoque, adoptando una postura proactiva y adaptándose a la nueva realidad generada por la implementación de tecnologías defensivas avanzadas, con un enfoque central en la maximización de la automatización, la detección de amenazas, la agilidad operativa y la mejora de la toma de decisiones. La necesidad apremiante de superar las limitaciones de recursos es, sin lugar a duda, un área donde la Inteligencia Artificial emerge como una aliada esencial.

La dependencia de la IA no solo como una solución para la falta de recursos, sino como un enfoque estratégico para enfrentar riesgos y amenazas en constante evolución, es imperativa. En este sentido, la reorganización de los equipos de seguridad debe incorporar no solo la implementación de tecnologías avanzadas, sino también la exploración continua de nuevas metodologías que estén alineadas con los desafíos emergentes.

La construcción de una cultura de seguridad sólida es crucial para la eficacia a largo plazo, involucrando no solo la capacitación de los colaboradores con conocimientos actualizados, sino también la promoción de una mentalidad vigilante en las actividades diarias, tanto profesionales como personales. Debemos fomentar el análisis crítico, la desconfianza constructiva y la aplicación de buenas prácticas en todos los aspectos de la vida cotidiana, estableciendo así una línea de defensa sólida.

En última instancia, la convergencia de la tecnología y la ciberseguridad es un área desafiante que requiere la unión estratégica de la Inteligencia Artificial con las capacidades humanas. Reconocer la inevitabilidad de esta batalla tecnológica de titanes y abrazar la Inteligencia Artificial como un aliado indispensable es la clave para fortalecer las organizaciones contra las amenazas emergentes.



Panorama de amenazas en el sector minero

[Por Julissa Emily Calderon](#)

La evolución tecnológica en el sector minero, la digitalización y la adopción de tecnologías avanzadas para optimizar sus procesos productivos, como los perforadores y camiones autónomos, los gemelos digitales, entre otros, dejan un entorno operativo cada vez más conectado, el cual ha introducido nuevos riesgos y ampliado la superficie amenazas cibernéticas a las que deben enfrentarse las compañías de este rubro.

Ciberspionaje

La mayoría de las minas a nivel mundial son atacadas para recopilar información de inteligencia del negocio. Los delincuentes informáticos pueden estar patrocinados por grupos de interés que ven a las empresas mineras como un “tesoro” o incluso estados nacionales que lanzan campañas de espionaje, dado que la minería es un sector de relevancia económica para cualquier país.

Información sobre la exploración geológica, el valor de los recursos naturales, estrategias corporativas de precios y patentes tecnológicas de exploración, extracción y procesamiento, contienen datos confidenciales y de propiedad intelectual atractivos para estos atacantes.

Terceros con acceso

La minería es una compañía con muchos proveedores externos que laboran en toda la cadena productiva, que muchas veces no siguen buenas prácticas de seguridad que pueden comprometer de sobremanera las operaciones.

Los incidentes relacionados a ataques de cadena de suministro es una modalidad que crece y que supone un gran riesgo, ya que los ciberdelincuentes buscan llegar al objetivo a través de los proveedores de confianza quienes son parte clave de la cadena de valor y procesos críticos de las compañías. La falta de establecimiento de reglas y permisos con el mínimo privilegio en su conexión a las redes, deja “sin llave” las puertas de acceso y al libre albedrío a vulnerabilidades como malware, podrían infectar la red e incluso tener llegada a los sistemas de control industrial, considerando que aun muchas compañías no tienen segmentada sus redes IT/OT con controles de seguridad perimetral robustos. Recientemente, se ha conocido que los ataques APTs en compañías industriales han utilizado a los proveedores como una ventana de acceso sigiloso que ha comprometido la continuidad operativa.

Campañas de Phishing:

Las campañas de phishing tienen como meta personal de minería, no sólo considerando a altos ejecutivos sino también a superintendentes de operaciones, supervisores de sistemas de control, técnicos de instrumentación y operadores.

Un ataque público fue el que tuvo la empresa minera Canadiense Goldcorp, que por esa amenaza perdió 16GB aproximadamente de información confidencial que incluía información de identificaciones, credenciales de empleados y documentos presupuestarios.

Es por esto que tener un programa de concientización que vaya dirigido a empleados según su rol y funciones en la compañía, quienes comprendan su participación y su papel en la ciberseguridad de la compañía se torna importante. No todo el personal está expuesto de la misma forma o tendrá un vector de ataque en común, por lo cual deben ser importantes programas especializados para cada perfil, a fin de lograr que estén preparados para cualquier situación de peligro.

Las amenazas en el sector vienen evolucionando a un ritmo creciente para la industria minera, por lo cual es importante que los responsables de la operación comprendan el panorama actual de los riesgos a los cuales están enfrentándose continuamente. Se tiene un desafío importante al definir acciones que permitan a las compañías gestionar los riesgos que puedan afectar y comprometer las operaciones industriales, por lo cual deben tener claro lo crucial que es estar preparados para proteger sus principales activos en orden de prevenir amenazas en tiempo real y bloquear ataques emergentes, aplicando controles y políticas “zero trust” que los blinden ante cualquier ataque.

Navegando por la privacidad de un mundo interconectado

Por [Emily Pereda](#)

En la era de la hiperconectividad, nuestra vida cotidiana se ha visto profundamente transformada por la tecnología, ofreciendo comodidades y eficiencias que eran inimaginables hace apenas unas décadas. Dispositivos IoT, sistemas de domótica, y vehículos conectados han convertido lo que antes eran conceptos futuristas en componentes integrales de nuestra realidad diaria; sin embargo, esta transformación digital viene acompañada de crecientes preocupaciones sobre la privacidad y seguridad de los datos personales. Como profesional en ciberseguridad, y más recientemente, como madre, mi percepción sobre la tecnología ha evolucionado hacia una reflexión más crítica sobre cómo estas innovaciones afectan la privacidad y seguridad de nuestras familias.

IoT y Domótica: ¿Comodidad a Costo de la Privacidad?

La promesa de un hogar inteligente se ha materializado a través de dispositivos IoT y sistemas de domótica, brindándonos control remoto sobre iluminación, climatización, y seguridad; sin embargo, la conveniencia de estos dispositivos viene con riesgos inherentes. Cada dispositivo conectado representa un vector potencial de ataque para los ciberdelincuentes, quienes podrían acceder a datos personales sensibles o manipular la funcionalidad de los sistemas domésticos. Por ejemplo, un ataque dirigido podría comprometer cámaras de seguridad, revelando detalles íntimos de nuestra vida cotidiana o permitiendo a los intrusos monitorear nuestros movimientos.

¿Cuántas veces nos hemos topado con historias o videos sobre niños que desarrollan un temor hacia las cámaras de vigilancia? Estas herramientas, instaladas por nosotros para brindarnos tranquilidad al poder observar a los pequeños mientras nos ocupamos en otras tareas o incluso para monitorearlos a distancia mientras estamos en el trabajo, se supone que deberían ser un recurso seguro y confiable. Sin embargo, la realidad puede ser diferente. El miedo en los niños surge cuando su espacio, que debería ser de seguridad y confort, es violado. Los incidentes documentados muestran cómo personas no autorizadas logran acceder a estas cámaras, interactuando con los niños y transformando un entorno de protección en uno de vulnerabilidad y miedo.

Esta intrusión no solo rompe la barrera física de seguridad que intentamos mantener alrededor de nuestros hijos, sino que también infringe la confianza y la sensación de seguridad que estos dispositivos están destinados a ofrecer. Cuando un niño se siente amenazado en su propio hogar, el daño va más allá de un simple acto de invasión de la privacidad; se convierte en una cuestión de seguridad emocional y psicológica. La pregunta que surge entonces es crucial: ¿Cómo podemos asegurarnos de que la tecnología diseñada para proteger a nuestros seres queridos no se convierta en una fuente de ansiedad y miedo para ellos?

Responder a esta preocupante pregunta implica abordar el problema desde múltiples ángulos, priorizando tanto la seguridad tecnológica como la comunicación abierta y la educación. En primera instancia, es fundamental seleccionar dispositivos de vigilancia de marcas reconocidas que ofrezcan altos niveles de seguridad, incluyendo cifrado avanzado y autenticación de dos factores, para dificultar el acceso no autorizado. Además, mantener el software de estos dispositivos constantemente actualizado asegura que cualquier vulnerabilidad conocida sea rápidamente corregida.

Por otro lado, la educación y la comunicación juegan un rol clave. Es esencial enseñar a los niños sobre la tecnología de una manera apropiada para su edad, explicándoles cómo funcionan estas cámaras y el propósito que cumplen, reforzando la idea de que están diseñadas para mantenerlos seguros. Asimismo, es importante escuchar y validar sus sentimientos si expresan miedo o inquietud, asegurándoles que están protegidos y que las medidas de seguridad están en lugar para su bienestar. Con medidas de seguridad tecnológica robustas con comunicación efectiva y empática, podemos utilizar la tecnología de vigilancia para maximizar la seguridad sin comprometer la sensación de seguridad y confort de los niños en sus hogares.

En el caso de los niños más pequeños, que aún no pueden hablar o expresarse de manera clara, la situación es más desafiante, ya que no pueden comunicar directamente lo que les sucede. Aquí la configuración que hagamos juega un papel fundamental para abordar estas dificultades.

La evolución continua: más allá de la biometría

Por [Nelvys Pamela Porras](#)

Con el avance implacable de la tecnología, la inteligencia artificial (IA) emerge como un actor clave en la transformación de la gestión de accesos. La capacidad de la IA para analizar y adaptarse a los patrones de comportamiento del usuario ofrece una capa adicional de seguridad. Los sistemas basados en aprendizaje automático pueden identificar actividades anómalas y detectar posibles amenazas antes de que se materialicen, proporcionando una respuesta proactiva en lugar de reactiva.

La búsqueda de nuevas formas de autenticación no se detiene en la biometría y la autenticación multifactorial. La autenticación basada en el comportamiento surge en el horizonte como una posible frontera futurista. Este enfoque implica analizar cómo un usuario interactúa con dispositivos y plataformas, evaluando patrones de comportamiento únicos. A medida que los algoritmos mejoran, esta forma de autenticación promete ser más resistente a las amenazas y menos invasiva para la experiencia del usuario.

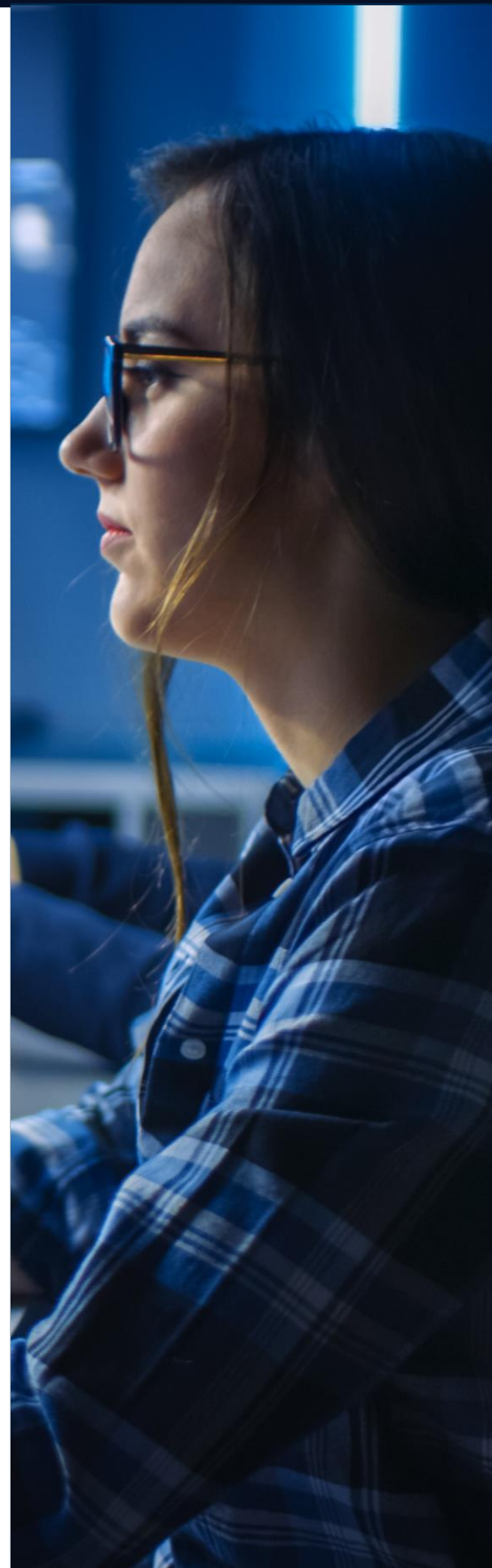
Las contraseñas tradicionales siguen siendo un punto débil en la seguridad digital. Las amenazas de ataques de fuerza bruta evolucionan constantemente, aprovechando la creciente potencia de cómputo y la sofisticación de las técnicas; hoy día se observan cómo estas amenazas emergentes desafían la integridad de las contraseñas y cómo la industria responde a estos desafíos en constante evolución.

Entendiendo un poco se deben contemplar las tendencias de los usuarios, los factores que contribuyen a la elección de contraseñas débiles y la tendencia a la reutilización. Entender estos aspectos proporciona una visión más profunda sobre cómo las prácticas de seguridad pueden adaptarse para abordar no solo las amenazas tecnológicas sino también los comportamientos humanos que ponen en riesgo la seguridad.

Si bien las huellas dactilares y el reconocimiento facial han sido pioneros en la adopción de la biometría, se pueden observar mejoras recientes. Tecnologías como el escaneo de retina, la voz y la dinámica de escritura están ganando terreno, brindando un abanico más amplio de opciones biométricas, estas tecnologías avanzadas abordan los desafíos de seguridad y privacidad asociados con la biometría.

La biometría no se limita solo al desbloqueo de teléfonos o a la gestión de fotos, la biometría se está integrando en sectores como la banca, la atención médica, transporte; transformando la manera en que interactuamos con servicios esenciales y garantizando una autenticación más segura en múltiples escenarios.

La preocupación por la privacidad y la seguridad de los datos biométricos sigue siendo un tema central; para poder abordar estas preocupaciones, se observan soluciones innovadoras, como la descentralización de datos y el uso de blockchain, que buscan abordar estas inquietudes; así mismo las regulaciones gubernamentales y los estándares de la industria están evolucionando para salvaguardar la integridad de los datos biométricos.



Se evidencian avances tecnológicos que están fortaleciendo la biometría, desde la mejora en la precisión de los sensores hasta la integración de la inteligencia artificial para la detección de intentos de suplantación. Estos desarrollos buscan abordar desafíos previos y mejorar la aceptación general de la biometría como método seguro y confiable.

La eliminación de contraseñas y la adopción de la biometría buscan mejorar la experiencia del usuario; el diseño centrado en el usuario da forma a interfaces intuitivas y procesos de autenticación seguros, accesibles y amigables para todos, independientemente de su nivel de experiencia tecnológica.

Analizar la resistencia al cambio en la adopción de nuevas tecnologías de autenticación; así como comprender la psicología detrás de la resistencia al cambio permitirá desarrollar estrategias efectivas para la transición hacia métodos de autenticación más seguros y avanzados.

Más allá de la biometría y la autenticación multifactorial, examinar las nuevas formas de autenticación que podrían surgir en el futuro; desde la autenticación cerebral hasta la autenticación basada en ADN, se vuelve relevante determinar los límites de la innovación, y cómo podrían revolucionar aún más la seguridad digital.

La transformación constante en el ámbito tecnológico conlleva desafíos inesperados; anticiparse a posibles dilemas éticos, de seguridad y de privacidad que podrían surgir con nuevas tecnologías de autenticación; Identificar estos desafíos permitirá a la industria prepararse y mitigar riesgos potenciales.

La eliminación de contraseñas y la adopción de la biometría no solo representan un cambio en la gestión de accesos, sino el comienzo de una revolución más amplia en la seguridad digital; los hitos alcanzados hasta ahora destacan cómo la industria está liderando la vanguardia de la innovación y delineando las perspectivas para un futuro digital seguro, eficiente y centrado en el usuario.

Radar

Powered by women

Suscríbete



Awareness en tu día a día ... ¿Por qué no?

Por Stephanie A. Ramos

Cuando pensamos en awareness siempre viene a la mente si los usuarios en las empresas entienden y tienen conocimiento de lo que esta palabra, actividad o acción conlleva y la realidad es que si volteamos en la mayoría de las empresas sigue siendo un tema poco gestionado. Ahora bien, si pensamos como individuos en la vida diaria ¿quién realmente lleva a cabo temas de awareness con cotidianeidad?... Muy pocos.

Si este tema tan importante lo compartiéramos con la importancia que conlleva seguro evitaríamos muchos incidentes de seguridad, no solo en la vida laboral, sino también en el día a día daríamos menos oportunidades a formas de extorsión, nos expondríamos a las empresas donde laboramos, colegas de trabajo y seres queridos.

Te has preguntado ¿cómo iniciarías una estrategia desde tu trinchera personal? ¿qué dejarías de hacer? ¿cómo le comunicarías esto a tus familiares y amigos? Sabemos que estando en un mundo de ciberseguridad el tema puede ser un poco más sencillo puesto que tenemos el contexto a la mano y no solo por un tema laboral nosotros en ciberseguridad entendemos y somos conscientes del contexto global, es el colmo que teniendo este contexto y toda esa información de primera mano no estemos haciendo nada, seguimos subiendo fotos personales y sin el cuidado debido de lo que mostramos en la misma, registrándonos en sitios que no tenemos certeza de la seguridad, seguimos aceptando avisos de privacidad que nunca leemos por completo, seguimos atendiendo mensajes de texto y what's app de cosas que no nos explicamos cómo llegaron a nosotros, y cuándo hacemos retrospectiva del ¿cómo? Y ¿cuándo? Caemos en esa pequeña línea que nos vuelve tan vulnerables.

¿Qué es awareness?, si lo googleamos la traducción literal el “conciencia”.

awareness o concienciación en ciberseguridad hace referencia a una formación sobre la importancia de la ciberseguridad, capacitando a los usuarios a través de simulaciones automatizadas y personalizadas de ataques de phishing y programa maligno, disminuyendo el número exitoso de ciberataques en las compañías.

Ahora, ¿realmente tenemos “Conciencia de la seguridad”? ¿Qué tan conscientes somos de lo que hacemos en nuestro día a día?, si nosotros tuviéramos esa información siempre presente de lo que no debemos exponer y a su vez lo aplicáramos y comentáramos con nuestro núcleo familiar ya sería mucho más fácil hacer esa red de buenas prácticas, si, sería mucho más fácil ya que compartiríamos estas buenas prácticas de una forma natural, con un simple, No subas fotos de la casa, oye elimina el dato de tus redes de donde trabajas, para eso hay plataformas específicas, oye hija/o cuida las imágenes que compartes de tu cole, oye cuida las contraseñas de la cuenta... entre otras.

Bien siendo conscientes todo lo que nos comparten en los trabajos de buenas prácticas, todo lo que ponemos en acción en nuestro día a día laboral, ¿cumplimos en tiempo con las capacitaciones?, ¿entendemos realmente los lineamientos? Como podremos estar actualizados si no estamos haciendo caso a la información de primera mano la cual tiene la mejor intención de hacernos esa conciencia sobre la seguridad.



Muchas preguntas pocas respuestas, bien... hagamos que valga la pena tener buenas prácticas de awareness en nuestro día a día. Las recomendaciones realmente son sencillas:

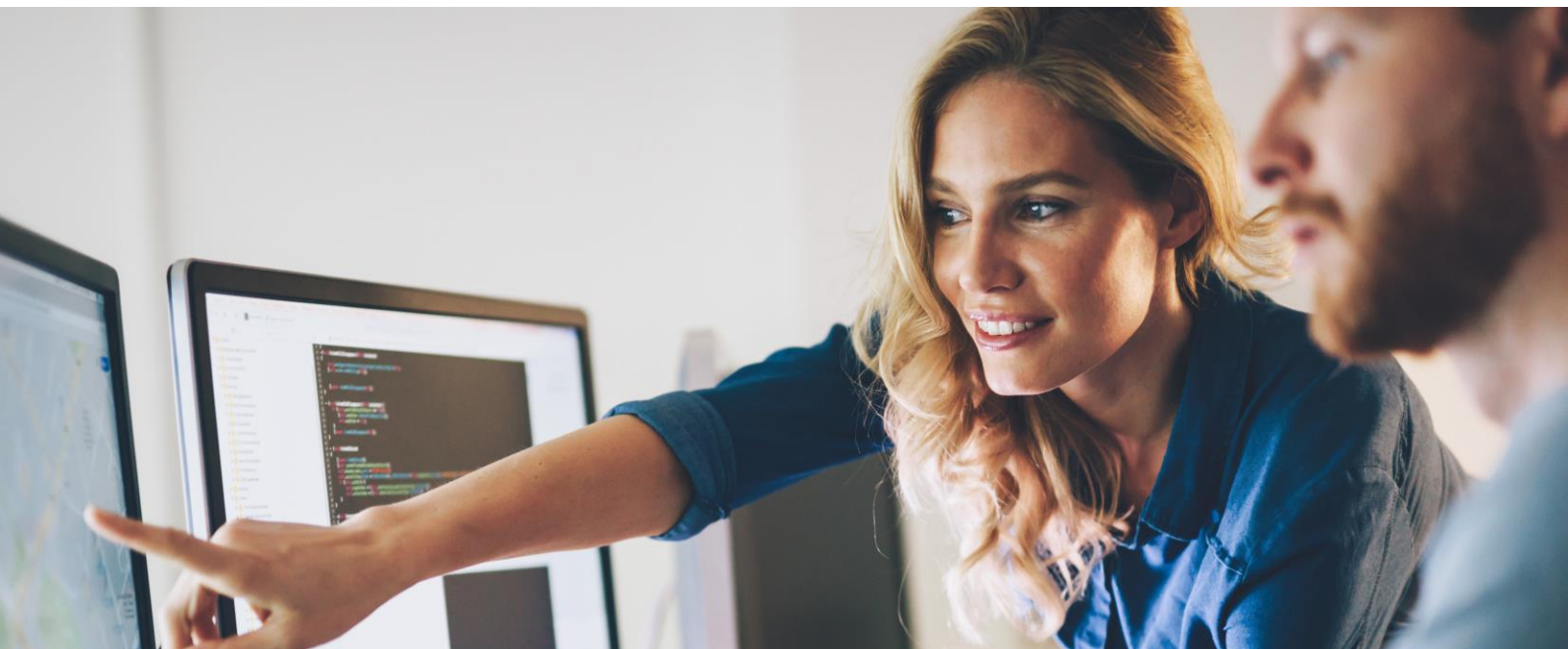
No comparta tu información en cualquier plataforma.

- Asegúrate que los códigos QR, que parecen tan inocentes y prácticos sean los del lugar al que quieres entrar.
- Los correos entrantes desconocidos, ¡No los abras por curiosidad! ... nada es gratis y lo más lógico puede ser lo más ilógico.
- Seamos desconfiados al recibir mensajes o llamadas de desconocidos y sobre todo si son de "conocidos" pero nos cuestiona temas o solicita algo que no lo vemos cotidiano ¿por qué no?, preguntar o cuestionar, al final... si es un conocido o familiar por supuesto hay esa confianza y tranquilidad. Y si es un compañero bueno con más razón.
- Si sabemos que en la compañía usamos un MFA o ¿cómo podríamos llamarlo más coloquialmente? Ese doble chequeo de acceso a una app, sistema, cuenta, etc, y ¿por qué no? pedirles a nuestros familiares cercanos que lo apliquen en sus actividades con una conversación casual de 5 minutos lo podemos explicar en casa...
- En contraseñas, muchas personas suelen confiar en su nombre, fecha de cumpleaños, de la mascota, pongámosle ingenio, amor a nuestra seguridad, piensa que si le ponen contraseña a algo es porque seguro guardas información importante para ti.
- Que hay de los tickets que tiramos indiscriminadamente, no tenemos esa precaución de revisar si traen algún dato que cualquier curioso o interesado en nosotros pueda recolectar y seguro piensas "no" eso solo pasa en las películas pues sí, pero ya pensaste que las películas terminan volviéndose una realidad.

Por qué usar los equipos personales para temas laborales podemos perfectamente hacerlo de una manera segura y como bien es el tema awareness y es conciencia y en este caso nuestro tema es conciencia en ciberseguridad y haciendo mucho uso de estos términos en este artículo de estas dos palabras ¿por qué? olvidamos ser conscientes del cuidado de la información que manejamos en nuestros móviles, es sencillo temas de la compañía no los descargo, no los comparto por medios no permitidos y listo. Ah, pero que tal comparto el estado de cuenta como si fuera cualquier documento, o el famoso pack, yo se lee y da risa, pero eres si lo piensas es una realidad.

Podría seguir con algunos puntos más, sin embargo, es bien importante que, al finalizar la lectura de este, te lleves en mente como vives los temas de awareness día a día en la oficina y en casa y con los amigos y con la sociedad y que no les hagamos tan fácil el trabajo a los que quieren nuestra información o que nos ven como un acceso a datos que ni siquiera nos corresponde o pertenece.

Hagamos de estas prácticas algo nuestro, compartámoslo, creemos esa red o esa estrategia desde nuestra trinchera. Y Compliquemos la accesibilidad a nuestras privacidades.



Comenzamos la cibercrónica de este mes con la noticia de un informe realizado por la compañía de ciberseguridad ESET que relata el panorama de las amenazas en España y el mundo. En el informe, España destaca como uno de los países con más detecciones de amenazas, quedando solo por detrás de Japón y Estados Unidos.

La amenaza detectada como más popular sigue siendo el phishing, siendo esta, casi la tercera parte de todas las amenazas detectadas. El informe advierte sobre un aumento en las técnicas utilizadas por los ciberdelincuentes, siendo cada vez más prominente el uso de la inteligencia artificial. Estas técnicas aportan una capa de sofisticación a los ataques generando contenidos falsos, fotomontajes, deepfakes, o suplantaciones de identidad de personas relevantes. Se prevé que la tendencia en este tipo de intentos de ataque vaya en aumento dada la rapidez de crecimiento de este tipo de herramientas y su cada vez más fácil acceso, de hecho, es algo que ya está pasando y que nos lleva a otros términos, como el smishing y el vishing.

Este tipo de phishing mediante sms sigue una estructura muy parecida a la que siguen en los correos electrónicos. Se trata de enviar de forma masiva anzuelos, esperando que los usuarios piquen en el engaño. Las dos formas de operar más comunes son: la suplantación de empresas de servicios de envíos, empresas telefónicas o bancos, y suplantación de familiares o conocidos.

En cuanto al vishing, la Guardia Civil recientemente ha alertado sobre el aumento de este tipo de fraudes y ha indicado a la población que sea cauta y tenga precaución al respecto, dado que con los avances tecnológicos de la inteligencia artificial hace que cada día la suplantación de personas mediante videollamada pueda ser cada vez más real.

Esto nos lleva a hablar de la profesionalización del fraude, la cual está en incremento estos últimos años. Existen reportes de empresas en el extranjero que se dedican expresamente a montar call centers que se hagan pasar por el equipo de soporte de diferentes servicios con la intención de estafar a los posibles usuarios a través de la utilización de su información. El usuario de youtube conocido como Savitar (el cual divulga contenido relacionado con el hacking ético y la ciberseguridad), hace unas semanas, relató en uno de sus videos como un hacker que se dedica a desatapar estafas de este tipo. La metodología que utilizaba era recopilar información de estos centros de llamada tras infectar todos sus equipos, para posteriormente ponerse en contacto con las autoridades para que entrasen en el centro a detener la actividad. La oficina desde la que operaban parecía bastante profesionalizada, siendo posible incluso que algunas de las personas que trabajaban en esta actividad no estuviesen al corriente de la ilegalidad de esta.

Para recalcar esto, una noticia del portal ITUser nos relata cómo el cibercrimen funciona ya como cualquier otra empresa y sus objetivos son equivalentes a estas (reducción de costes, mejora de la eficiencia y obtención de ingresos), alcanzando estas actividades un valor cercano al 1,5% del PIB mundial. Paradójicamente, la percepción de la población con respecto a su vulnerabilidad ante los ciberataques no progresa acorde a su impacto y popularidad. Según recalca el Centro de Coordinación Nacional del INCIBE: "En general, año tras año, los usuarios piensan que son menos atacados. Pero, sin embargo, la tendencia real es creciente. De hecho, el porcentaje de usuarios que declaran tener malware en sus equipos es muy bajo, sobre todo, si lo comparamos con la realidad"

Para cerrar la cibercrónica de este mes, hay que recalcar que, dado el incremento de esta situación en la cual el ciberfraude mejora día a día ante la no percepción de la población, es necesario prestar atención en especial a las nuevas tecnologías que cada vez se integran más en nuestras vidas. Según diversas fuentes, el vector de ataque más común hasta el momento sigue siendo el correo electrónico, a través del cual se pueden infectar los ordenadores o dispositivos móviles. Sin embargo, esta situación puede ser muy diferente en un futuro no muy lejano.

Recientemente hemos visto noticias en las cuales empresas como Apple sacaba al mercado sus nuevas gafas de realidad aumentada, o incluso como la empresa Neuralink estaba realizando pruebas con un chip cerebral. Creemos que la industria del fraude todavía está lejos de acercarse a estos dispositivos, pero según la oferta y el uso de este tipo de tecnologías vaya en aumento, la industria los tomará como nuevos vectores de ataque.

Durante los últimos años, se ha discutido ampliamente acerca del posible impacto a nivel mundial que podría generar el acceso de gran parte de la sociedad a la tecnología cuántica. Dado que cada vez su funcionamiento y rendimiento está cobrando mayor relevancia, institutos internacionales de ciberseguridad han iniciado acciones para intentar instaurar medidas preventivas frente a la eventual revolución que esta nueva tecnología podría ocasionar.

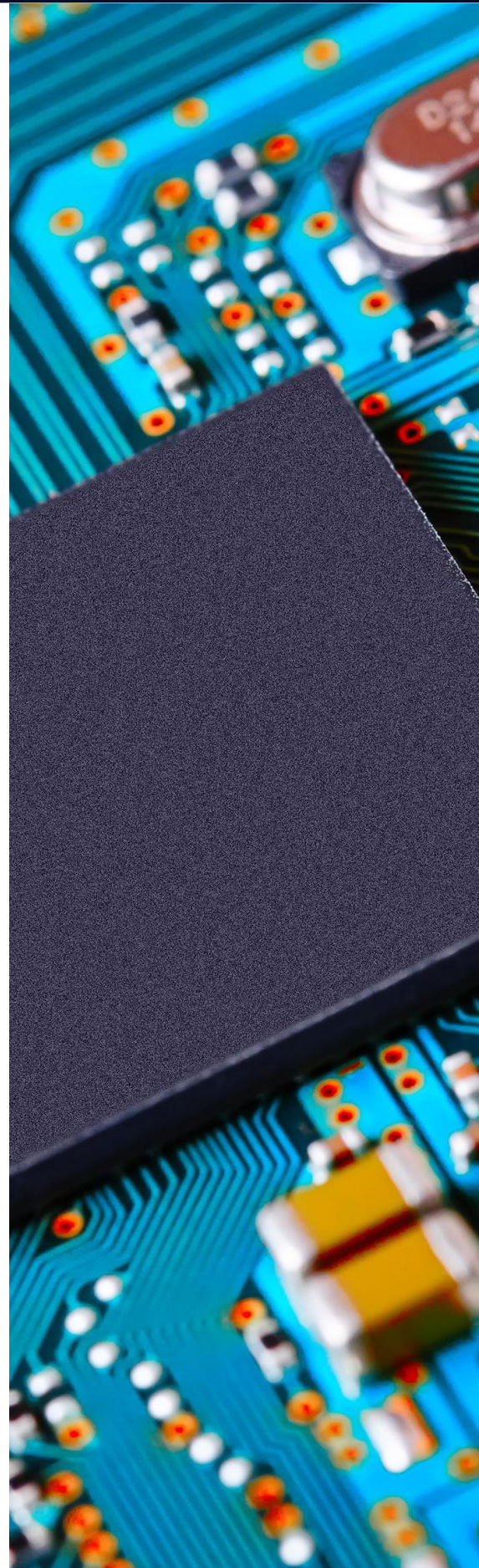
A diferencia de los ordenadores clásicos que se utilizan hoy en día, donde se usan bits para representar información como 0 o 1, los ordenadores cuánticos utilizan qubits, que no solo representan los bits clásicos, sino que además incorporan un estado adicional donde representa ambos al mismo tiempo mediante un fenómeno llamado superposición. Esto proporciona una capacidad para realizar cálculos exponencialmente mayores que un ordenador convencional, suponiendo una amenaza ante los sistemas criptográficos actuales que se basan en la dificultad computacional para resolverlos. Por este motivo, ha surgido un creciente interés en el desarrollo de algoritmos criptográficos cuántico-resistentes.

Hasta la fecha, los protocolos de seguridad utilizados para la protección de la integridad y confidencialidad de los datos se basan primordialmente en los cifrados RSA y ECC. Según múltiples estudios realizados por el "World Economic Forum", además de los cronogramas establecidos por la CNSA, los ordenadores cuánticos presentan una amenaza para estos cifrados de seguridad, ya que pasarían a considerarse vulnerables debido a la capacidad de cómputo que presenta esta nueva tecnología. Se estima que esta brecha de seguridad a nivel mundial pueda ocurrir tan pronto como a principios de 2030. Por esto mismo, los sistemas clásicos se consideran vulnerables al "Harvest now, decrypt later" (HNDL: Roba ahora, descifra después), donde actores maliciosos roban y almacenan datos para poder descifrarlos más adelante en caso de que obtengan la oportunidad de acceso a ordenadores cuánticos.

Tanto IBM como Pablo Alto han comenzado a expresar sus planes de acción para prevenir y contrarrestar esta futura problemática, especialmente tras el mensaje publicado por el Instituto Nacional de Normas y Tecnología (NIST), donde anuncia que comenzará a lo largo de este año a desarrollar y establecer estándares criptográficos seguros contra la computación cuántica. Con los cuatro cifrados "post-quantum" (PQC) escogidos en 2022 tras 6 años de investigación internacional y el anuncio de NIST en agosto de 2023 sobre sus planes de estandarización de 3 de los cifrados ganadores, se espera que su aprobación e implementación transcurra a lo largo de 2024. Dichos cifrados son: "Crystals Kyber", "Crystals-Dilithium" y "SPHINC+".

Con el continuo avance del desarrollo de la computación cuántica de la mano de empresas como IBM, Google, D-Wave y IonQ entre muchas, la aportación de NIST supone un inmenso soporte para movilizar a todos los sectores dependientes de la seguridad de los cifrados clásicos.

La tendencia observada en los últimos meses sugiere que el año 2024 marca el inicio de significativos cambios en los protocolos de seguridad. Este movimiento refleja la creciente conciencia sobre la necesidad de adaptarse a la era cuántica, destacando la importancia de desarrollar y adoptar algoritmos cuántico-resistentes para continuar con la securización de la integridad y confidencialidad de los datos.



Vulnerabilidades

Vulnerabilidad de código remoto en productos de Cisco

Fecha: 24 de enero de 2024
CVE: CVE-2024-20253



Múltiples vulnerabilidades en productos de Fortinet

Fecha: 8 de febrero de 2024
CVEs: CVE-2024-23113 y 1 más



Descripción

Desde Cisco se ha reportado una vulnerabilidad crítica que afecta a un gran número de sus productos.

Se trata de una vulnerabilidad de ejecución de código remoto, debida al inadecuado procesamiento de los datos de entrada proporcionados por el usuario. Un atacante podría explotar la vulnerabilidad mediante el envío de un mensaje especialmente diseñado a un puerto de escucha del dispositivo afectado.

Mediante su explotación, un atacante podría ejecutar comandos arbitrarios en el sistema operativo del dispositivo con privilegios de usuario del servicio web. Además, con acceso al sistema operativo, el atacante podría establecer permisos de acceso *root* en el sistema.

Productos afectados

La vulnerabilidad afecta a los siguientes productos:

- Unified Communications Manager (Unified CM)
- Unified Communications Manager IM & Presence Service (Unified CM IM&P).
- Unified Communications Manager Session Management Edition (Unified CM SME).
- Unified Contact Center Express (UCCX).
- Unity Connection.
- Virtualized Voice Browser (VVB).

Solución

El fabricante ha publicado actualizaciones para los productos afectados.

Referencias

- www.incibe.es
- sec.cloudapps.cisco.com

Descripción

Desde Fortinet han informado el pasado viernes de dos vulnerabilidades críticas en su sistema operativo FortiOS.

La vulnerabilidad más crítica, CVE-2024-23113, es una vulnerabilidad de cadena de formato controlada externamente (CWE-134), como puede ser a través de la entrada de un usuario, en el demonio *fgfmd* de FortiOS.

La segunda vulnerabilidad, CVE-2024-21762, es una vulnerabilidad de escritura fuera de límites (CWE-787).

La explotación de alguna de estas vulnerabilidades podría permitir a un atacante remoto no autenticado ejecutar código arbitrario o comandos mediante solicitudes especialmente diseñadas.

Productos afectados

Las vulnerabilidades mencionadas afectan a las siguientes versiones del sistema operativo FortiOS:

- FortiOS 7.4 de la versión 7.4.0 a la 7.4.2
- FortiOS 7.2 de la versión 7.2.0 a la 7.2.6
- FortiOS 7.0 de la versión 7.0.0 a la 7.0.13
- FortiOS 6.4 de la versión 6.4.0 a la 6.4.14
- FortiOS 6.2 de la versión 6.2.0 a la 6.2.15
- FortiOS 6.0

Para ver el resto de productos afectados puede consultar los enlaces de referencia.

Solución

Fortinet recomienda desactivar SSL VPN como *workaround* y actualizar FortiOS a las siguientes versiones o superiores: 7.4.3; 7.2.7; 7.0.14; 6.4.15; 6.2.16.

Referencias

- www.incibe.es
- www.fortiguard.com
- www.fortiguard.com

CRÍTICA

Nuevos parches de seguridad para GitLab CE/EE

Fecha: 25 de enero de 2024
CVE: CVE-2024-0402 y 4 más

Descripción

GitLab ha lanzado el pasado 26 de enero una serie de parches de seguridad para solventar un conjunto de 5 vulnerabilidades, de las cuales una está categorizada como crítica y el resto cuenta con una categorización de severidad media.

La vulnerabilidad crítica, CVE-2024-0402, podría permitir que un usuario autenticado escriba archivos en ubicaciones arbitrarias dentro del servidor de GitLab al momento de crear un espacio de trabajo. Esta brecha de seguridad podría conllevar la distribución de *malware*.

El resto de las vulnerabilidades corregidas en este parche de seguridad podrían permitir las siguientes acciones:

- Desencadenar un ataque de DoS (CVE-2023-6159).
- Acceso o exposición de datos confidenciales (CVE-2023-5933 y CVE-2023-5612).
- Asignar cualquier usuario sin restricciones a las solicitudes de fusión (MR) que han sido creadas dentro de un proyecto en GitLab (CVE-2024-0456).

Productos afectados

Las versiones de GitLab afectadas son las siguientes:

- 12.7 anterior a 16.6.6;
- 13.7 anterior a 16.6.6;
- 14.0 anterior a 16.6.6;
- 16.0 anterior a 16.5.8;
- 16.6 anterior a 16.6.6;
- Todas las anteriores a 16.6.6;
- 16.7 anterior a 16.7.4;
- 16.8 anterior a 16.8.1.

Solución

Actualizar a las versiones 16.5.8, 16.6.6 y 16.7.4 de GitLab CE/EE. La versión 16.8.1 únicamente contiene el parche para la vulnerabilidad CVE-2024-0402.

Referencias

- about.gitlab.com
- www.helpnetsecurity.com

CRÍTICA

Nuevos parches de seguridad para dispositivos Android

Fecha: 5 de febrero de 2024
CVE: CVE-2024-0031

Descripción

Android ha publicado un nuevo boletín de seguridad que corrige una vulnerabilidad crítica y 45 vulnerabilidades de severidad alta.

La vulnerabilidad crítica consiste en un fallo de escritura fuera de límite presente en la función "attp_build_read_by_type_value_cmd", que de ser explotada permitiría al atacante ejecutar código de forma remota en el sistema operativo del dispositivo, sin necesidad de privilegios de ejecución *system*. Esta vulnerabilidad ha sido identificada como CVE-2024-0031.

Las vulnerabilidades corregidas en el parche afectan tanto al sistema operativo como a componentes del sistema como Arm, MediaTek, Qualcomm, o Unisoc.

Productos afectados

Los productos afectados por dicha vulnerabilidad son los siguientes:

- Android Open Source Project (AOSP): versiones 11, 12, 12L, 13 y 14
- Componentes de Arm, MediaTek, Unisoc y Qualcomm

Solución

Android recomienda comprobar que el fabricante del dispositivo haya publicado un parche de seguridad y aplicar la actualización correspondiente.

Referencias

- www.incibe.es
- source.android.com

Eventos

Innovate Cybersecurity Summit

Este evento de tres días reúne a ejecutivos y CISOs de ciberseguridad de todo EE.UU. para discutir y aprender, dentro de un marco de asistencia exclusivo. Este año se ha realizado organizado en Nashville, Tennessee, en los días del 25 al 27 de febrero.

Las personas que acuden a esta experiencia tienen acceso a paneles y sesiones formativas de CISOs que tratan las mejores prácticas y retos actuales, mostrando en paralelo las oportunidades y últimas soluciones tecnológicas en cuanto a ciberseguridad.

Se trata de un evento único del cual se puede aprender información valiosa para posicionar tu organización en un buen estado a nivel de protección y respuesta frente a amenazas en este campo.

[Link](#)

Cyber Security World Madrid 2024

Evento que tendrá lugar en la capital española los días 16 y 17 de octubre, en el pabellón 9 de Ifema Madrid. En él se reunirán profesionales de la ciberseguridad tanto corporativa como empresarial e institucional de las principales compañías de la ciberseguridad a nivel mundial para tratar el incremento actual de ciberataques, sus tipologías y las inversiones en este campo para poder así proteger el dato y la actividad de las organizaciones.

Este año se preveen alrededor de 400 empresas que expondrán sus soluciones cloud, y más de 350 ponentes que expondrán las novedades actuales dentro del sector.

[Link](#)

Infosecurity Europe 2024

Esta feria tendrá lugar del 4 al 6 de junio en el ExCeL London, en Reino Unido. Reunirá a profesionales y empresas del ámbito de la ciberseguridad para tratar las últimas novedades del campo y compartir experiencias, a través de conferencias y eventos dentro de la misma donde poder ampliar conocimientos y la red de networking.

Se considera una de las ferias europeas más importantes en cuanto a ciberseguridad, ya que reúne a gran número de proveedores de soluciones.

[Link](#)

Infosecurity México 2024

Evento organizado en el Centro Citibanamex de la Ciudad de México para entrar en materia de ciberseguridad, sobre todo en relación con las últimas tendencias y métodos de seguridad de la información.

Se podrá establecer contacto con expertos importantes dentro de la industria de la seguridad de la información, lo cual puede permitir mejorar la protección de las empresas encontrando soluciones que se adapten a los nuevos tiempos.

Por tanto, la temática principal que se dará durante los días 22 y 23 de octubre será la normativa, así como las ciberamenazas y la protección, tanto particulares como empresas e instituciones públicas.

[Link](#)



Recursos

Materiales de formación y entrenamiento para especialistas en ciberseguridad de ENISA (European Union Agency for Cybersecurity)

ENISA lleva introduciendo desde 2008 material de ciberseguridad para la formación de cualquiera al que le interesa ampliar sus conocimientos. En su web incluyen información para docentes y estudiantes, para complementar una parte más práctica.

La formación se compone de cuatro áreas principales: Técnica (análisis forense, honeypots o detección proactiva son algunos de los temas), Operacional (redacción de avisos de seguridad o manejo de incidentes en la nube), Cooperación y Legal (identificación, gestión de rastros de ciberdelitos, cooperación con las fuerzas del orden) y Configuración de una CSIRT (es decir, formarse para poder responder de manera efectiva a un incidente de seguridad informática).

[Link](#)

Revolucionando la gestión de identidades: cómo Web3 descentraliza y protege los sistemas IAM

En el siguiente enlace, DataVeritas explica el novedoso campo de Web3 y su relación con el concepto de la identidad descentralizada. Esta idea revolucionaria busca que el usuario tenga control total sobre su identidad digital, reduciendo el número de vulnerabilidades provocadas por otros tipos de gestión y las limitaciones del individuo al usarlo. Todo ello se nutre de campos como el blockchain y otro tipo de tecnologías IAM actuales e innovadoras.

Web3 es por tanto una buena elección para una gestión descentralizada de la identidad de una manera más segura, superando ciertos desafíos actuales en materia IAM. Se trata de una solución que ha podido ya probarse con éxito en sectores como el bancario o el sanitario.

[Link](#)

NIST Cybersecurity Framework (CSF) 2.0

Se trata de un marco de Ciberseguridad publicado por el instituto estadounidense NIST (National Institute of Standards and Technology). Su origen se remonta a 2014, cuando se publicó con el objetivo de servir apoyo a la Ley de Mejora de la Ciberseguridad de EEUU. El objetivo de esta guía es la de gestionar y reducir riesgos, así como fortalecer las medidas de ciberseguridad.

Centrándonos en la herramienta en sí, NIST Cybersecurity Framework (CSF) 2.0 Reference Tool permitiría estudiar el borrador CSF 2.0 Core. Este incluye funciones, categorías, subcategorías y ejemplos de su implementación, ofreciendo versiones legibles por humanos y máquinas en JSON y Excel, así como permitiendo el uso de búsqueda por palabras y términos clave. Dentro de la herramienta se podrán encontrar las siguientes funciones:

- GOBIERNO (GV): establecer y monitorear la estrategia, expectativas y política de gestión de riesgos de ciberseguridad de la organización.
- IDENTIFICAR (ID): ayudar a determinar el riesgo de ciberseguridad actual para la organización.
- PROTECT (PR): utilizar salvaguardas para prevenir o reducir el riesgo de ciberseguridad
- DETECT (DE): encontrar y analizar posibles ataques y compromisos de ciberseguridad
- RESPONDER (RS): tomar medidas ante un incidente de ciberseguridad detectado
- RECUPERAR (RC): restaurar activos y operaciones que se vieron afectados por un incidente de ciberseguridad,

Es una herramienta en desarrollo y que se prevé que finalice en 2024, lo que permitirá unir CSF con marcos, estándares, guías y recursos relacionados con la ciberseguridad. En versiones futuras, se espera poder permitir a los usuarios generar su propia versión de CSF 2.0 Core al poder seleccionar otra información y recursos como referencia.

[Link](#)





Ma Pilar Torres
Directora Ciberseguridad



Marta Fernández
Cibersecurity Manager



Ma Angeles Gutiérrez
Cybersecurity Manager



Andrea Muñoz
Cibersecurity Manager



Almudena Abolafia
Cybersecurity Manager



Julissa E. Calderón
Cybersecurity Project Leader



Emily J. Pereda
Cybersecurity Lead Consultant



Mafalda Maciel Querido
Senior Lead Analyst Cybersecurity



Nelvys P. Porras
Cybersecurity Expert Analyst



Stephanie A. Ramos
Lead Analyst Cyber

Radar

Powered by women



Powered by the
cybersecurity
NTT DATA team

es.nttdata.com