SENTRIS CIBERSEGURIDAD

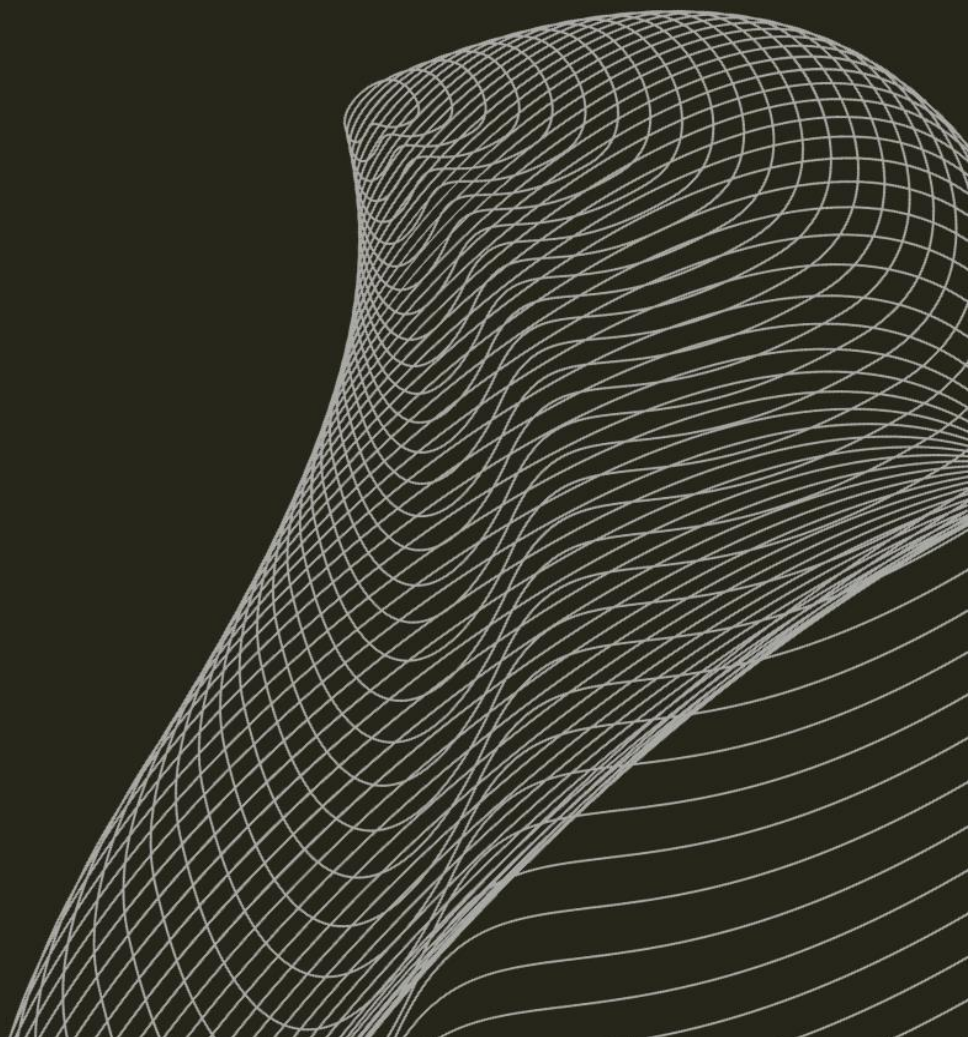
TRIMESTRAL
INFORME CIBERINTELIGENCIA
T3 2023

SENTRIS

+34 689 26 19 03

INFO@SENTRIS.ES

SENTRIS.ES



CONTENIDO

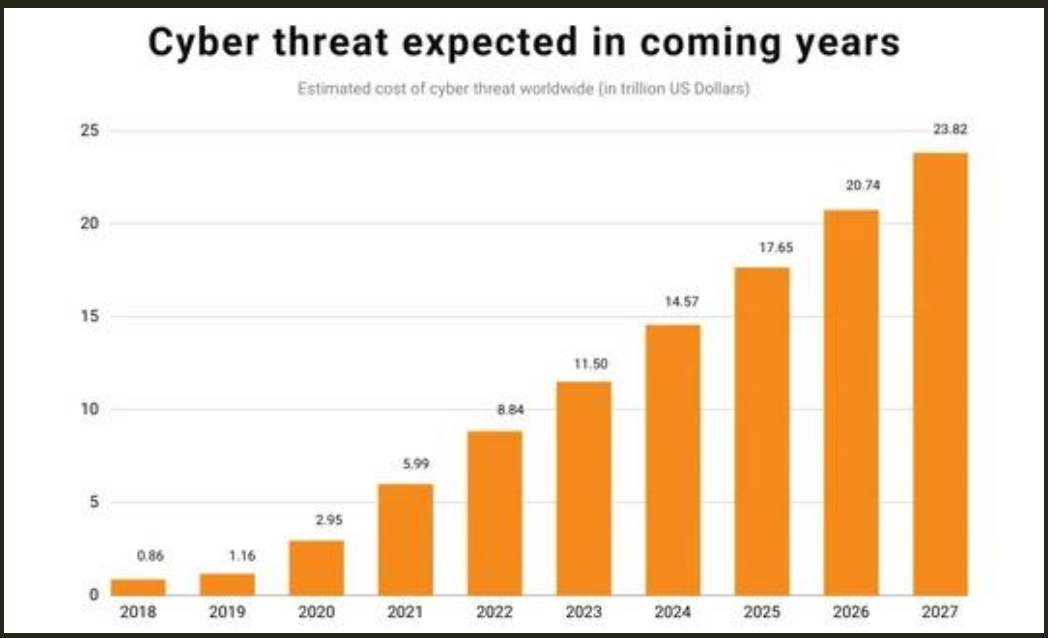
RESUMEN EJECUTIVO

LA ESCENA GLOBAL DEL MARCO DE CIBERSEGURIDAD.

El tercer trimestre de 2023 ha visto una evolución significativa en el panorama de las amenazas cibernéticas y este resumen ejecutivo proporciona una visión general de los hallazgos clave, las tendencias y las implicaciones basadas en los últimos datos.

En los hallazgos clave, observamos que el panorama de amenazas cibernéticas ha seguido evolucionando con nuevos actores de amenazas, técnicas de ataque sofisticadas y una escala de ataques sin precedentes. Los ataques de ransomware han aumentado, dirigidos tanto a organizaciones del sector público como privado. Ha habido un aumento en los ataques a la cadena de suministro, explotando vulnerabilidades en productos de software ampliamente utilizados. Las amenazas de criptomonedas, incluidos el cryptojacking y las estafas, también han aumentado debido al aumento de los precios de las criptomonedas.

En términos de tendencias, hemos visto la aparición de nuevas amenazas como la tecnología deepfake y la computación cuántica que plantean desafíos significativos para la ciberseguridad. El uso de la inteligencia artificial (IA) en operaciones de ciberseguridad ofensivas y defensivas ha aumentado. Los gobiernos de todo el mundo están implementando regulaciones de ciberseguridad más estrictas para proteger a los consumidores y la seguridad nacional.



Las implicaciones de estos hallazgos son profundas. Se espera que las organizaciones aumenten su inversión en medidas de ciberseguridad. Existe una creciente demanda de profesionales calificados en ciberseguridad para combatir estas amenazas en evolución. Educar a los usuarios sobre las amenazas cibernéticas y las prácticas seguras en línea es crucial.

En conclusión, el Informe de Ciberinteligencia Q3 2023 subraya la naturaleza dinámica del panorama de amenazas cibernéticas. Es imperativo que las organizaciones se mantengan informadas sobre estos desarrollos y mejoren proactivamente su postura de ciberseguridad.

PANORAMA DE AMENAZAS

EVOLUCIÓN DE LAS CIBERAMENAZAS Y SU IMPACTO EN EL PANORAMA GLOBAL, ESPAÑOL Y ESPECÍFICO DE LA INDUSTRIA

Descripción general de las amenazas globales

El panorama global de amenazas en el tercer trimestre de 2023 estuvo dominado por tres temas principales: ransomware, ataques a la cadena de suministro y seguridad en la nube.

El ransomware continuó siendo la forma más frecuente y disruptiva de ciberdelincuencia, afectando a organizaciones de todos los tamaños y sectores en todo el mundo. Según el Informe de amenazas cibernéticas de SonicWall 2023, el número de ataques de ransomware aumentó en un 62% en la primera mitad de 2023 en comparación con el mismo período en 2022, alcanzando un récord de 304,7 millones. El informe también señaló que el 71% de los ataques fueron libres de malware, lo que significa que los adversarios utilizaron herramientas y técnicas legítimas para comprometer los sistemas y redes de las víctimas.

Los ataques a la cadena de suministro, que implican comprometer a un proveedor externo o proveedor de servicios de confianza para obtener acceso a sus clientes o socios, también surgieron como un importante vector de amenazas en 2023. El ejemplo más notable de esto fue el ataque a la cadena de suministro MOVEit, que se descubrió en mayo de 2023 y afectó a más de 2,000 organizaciones en todo el mundo, incluidas varias agencias gubernamentales de los Estados Unidos y compañías Fortune 500. El ataque que involucró una inyección SQL permitió a los atacantes ejecutar comandos de forma remota, robar datos y moverse lateralmente dentro de las redes comprometidas. El alcance total y el impacto del incidente aún se están investigando, pero ha expuesto las vulnerabilidades y los riesgos de la cadena de suministro de software global.

La seguridad en la nube fue otro desafío clave para las organizaciones en 2023, ya que la adopción de servicios y aplicaciones en la nube aumentó debido a la pandemia de COVID-19, el cambio al trabajo remoto y la armonización de la computación en la nube en servicios como AWS, Azure o Google Cloud. Sin embargo, muchas organizaciones carecían de la visibilidad, el control y la protección de sus entornos en la nube, lo que las hacía vulnerables a diversas amenazas, como violaciones de datos, secuestro de cuentas, configuración incorrecta y ataques de denegación de servicio. Según el Informe de amenazas globales CrowdStrike 2023, la explotación de la nube creció un 95% en 2023, y

el número de actores de amenazas "conscientes de la nube" aumentó casi tres veces. El informe también destacó que la nube se utilizó como objetivo y vector para los ataques, ya que los adversarios aprovecharon los servicios y la infraestructura en la nube para lanzar y amplificar sus campañas.

Descripción general de amenazas regionales

EVOLUCIÓN DE LAS CIBERAMENAZAS Y SU IMPACTO EN EL PANORAMA GLOBAL, ESPAÑOL Y ESPECÍFICO DE LA INDUSTRIA

El panorama regional de amenazas en el tercer trimestre de 2023 varió según los factores geopolíticos y económicos, así como el nivel de madurez cibernética y resiliencia de cada región. El siguiente es un breve resumen de las principales tendencias y eventos que ocurrieron en cada región:

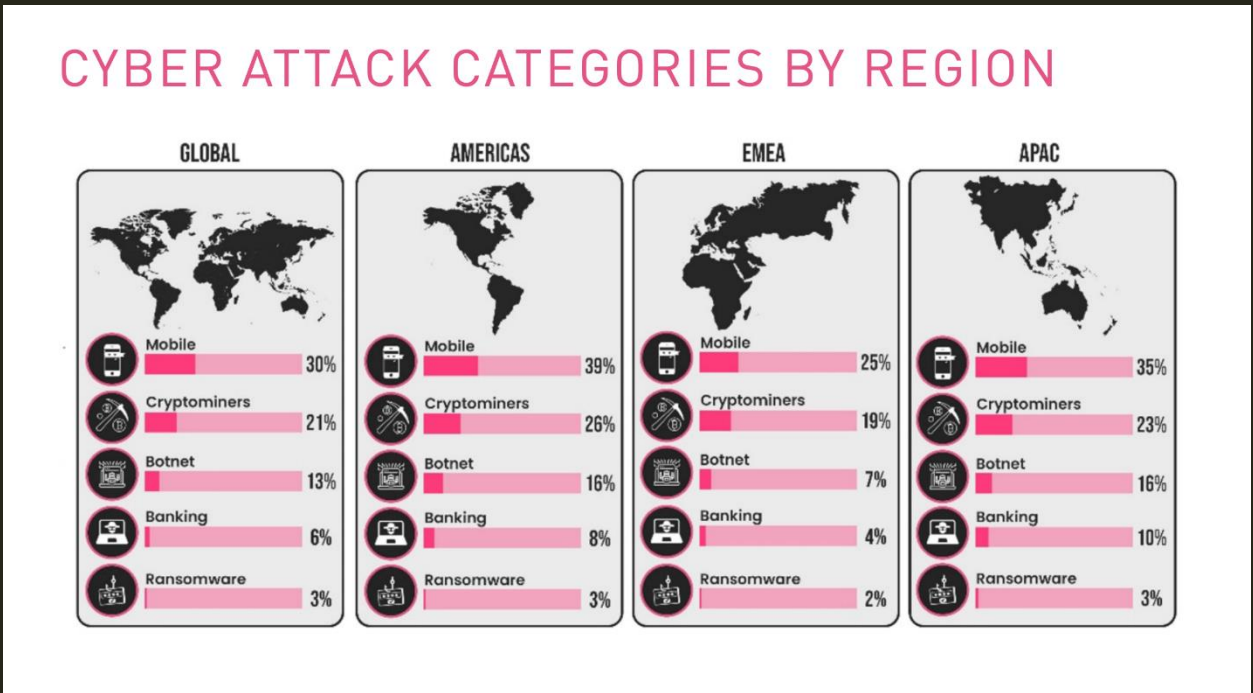
- **América del Norte**: América del Norte fue la región más atacada por las amenazas cibernéticas en el tercer trimestre de 2023, representando el 38% de los ataques globales, según el Informe de inteligencia de amenazas globales NTT 2023. La región enfrentó una oleada de ataques de ransomware, especialmente en los sectores de salud, educación y gobierno, que interrumpieron la prestación de servicios esenciales y causaron pérdidas financieras significativas. Además del ransomware, América del Norte también enfrentó amenazas persistentes de actores patrocinados por el estado, como China, Rusia, Irán y Corea del Norte, que apuntaron a los sectores críticos de infraestructura, gobierno, defensa y tecnología de la región para espionaje, sabotaje y operaciones de influencia.

- **Europa**: Europa fue la segunda región más atacada por las amenazas cibernéticas en el tercer trimestre de 2023, representando el 25% de los ataques globales, según el Informe de Inteligencia de Amenazas Global NTT 2023. La región se enfrentó a un entorno de amenazas complejo y dinámico, influenciado por la transición del Brexit, la cumbre de la OTAN, la cumbre UE-Estados Unidos y las tensiones con Rusia y Ucrania. El ransomware también fue una amenaza importante para Europa, afectando a varios sectores, como la salud, la fabricación, el transporte y la energía. Europa también enfrentó amenazas sofisticadas de actores patrocinados por el estado, como Rusia, China, Irán y Corea del Norte, que atacaron los sectores político, diplomático, militar e industrial de la región para espionaje, interrupción y operaciones de influencia.

- **Asia-Pacífico**: Asia-Pacífico fue la tercera región más atacada por las amenazas cibernéticas en el tercer trimestre de 2023, representando el 22% de los ataques globales, según el Informe de inteligencia de amenazas globales NTT 2023. La región enfrentó un panorama de amenazas diverso y en evolución, impulsado por la rápida transformación digital, la rivalidad geopolítica, la recuperación económica y el malestar social. El ransomware también fue una amenaza importante para Asia-

Pacífico, afectando a varios sectores, como la salud, la educación, las finanzas y el comercio minorista. Además del ransomware, Asia-Pacífico también enfrentó amenazas persistentes de actores patrocinados por el estado, como China, Rusia, Corea del Norte e Irán, que atacaron los sectores estratégico, económico y tecnológico de la región para espionaje, sabotaje y operaciones de influencia.

- **Medio Oriente y África**: Medio Oriente y África fueron la región menos atacada por las amenazas cibernéticas en el tercer trimestre de 2023, representando el 15% de los ataques globales, según el Informe de inteligencia de amenazas globales NTT 2023. Sin embargo, la región enfrentó un alto nivel de riesgo cibernético, debido a la inestabilidad política, los disturbios sociales, los desafíos económicos y la baja conciencia y preparación cibernética. El ransomware también fue una amenaza frecuente para Oriente Medio y África, afectando a varios sectores, como la salud, la educación, el gobierno y la energía. Además del ransomware, Oriente Medio y África también enfrentaron amenazas sofisticadas de actores patrocinados por el estado, como Irán, Israel, Rusia y China, que atacaron los sectores de seguridad, política y energética de la región para espionaje, sabotaje y operaciones de influencia.



Descripción general de amenazas del sector

La descripción general de amenazas específicas del sector en el tercer trimestre de 2023 proporciona un análisis detallado de las amenazas cibernéticas y las tendencias que afectaron a los sectores más específicos y vulnerables en el panorama global de amenazas. A continuación se presenta un breve resumen de las principales conclusiones y recomendaciones para cada sector:

- **Salud**: El sector de la salud fue el sector más atacado e impactado por las amenazas cibernéticas en el tercer trimestre de 2023, representando el 28% de los ataques globales, según el Informe de inteligencia de amenazas globales de NTT 2023. El sector se enfrentó a un aluvión de ataques de ransomware, que interrumpieron la prestación de servicios esenciales, pusieron en peligro la vida de los pacientes y expusieron datos confidenciales. Los principales desafíos y vulnerabilidades del sector fueron la falta de ciberhigiene, los sistemas heredados, la fuerza laboral remota y la compleja cadena de suministro. Las principales recomendaciones del sector fueron implementar una sólida estrategia de copia de seguridad y recuperación, actualizar y parchear los sistemas y aplicaciones, capacitar y educar al
personal sobre la conciencia cibernética y mejorar la visibilidad y el control de la red y los entornos en la
nube.

- **Educación**: El sector educativo fue el segundo sector más atacado e impactado por las amenazas cibernéticas en el tercer trimestre de 2023, representando el 16% de los ataques globales, según el Informe de inteligencia de amenazas globales de NTT 2023. El sector se enfrentó a una ola de ataques de ransomware, que interrumpieron las actividades de aprendizaje, dañaron la reputación y comprometieron los datos de los estudiantes, el personal y los ex alumnos. El sector también enfrentó amenazas de actores patrocinados por el estado, que buscaban robar propiedad intelectual, investigación e información personal. Los principales desafíos y vulnerabilidades del sector fueron la baja madurez cibernética, las restricciones presupuestarias, el aprendizaje remoto y la diversa base de usuarios. Las principales recomendaciones del sector fueron implementar una solución sólida de gestión de identidad y acceso, cifrar y proteger los datos en reposo y en tránsito, monitorear y asegurar los puntos finales y dispositivos.

ANÁLISIS DE INCIDENTES

EXAMINANDO EVENTOS CIBERNÉTICOS: DISECCIONANDO INCIDENTES Y DESCUBRIENDO TENDENCIAS

Incidentes relevantes

Incumplimiento de la Comisión Electoral

El 8 de agosto, la Comisión Electoral del Reino Unido emitió una notificación pública de un "ciberataque complejo" que ocurrió en octubre de 2022, pero que no se detectó hasta agosto de 2023. Los atacantes obtuvieron acceso a los servidores de la Comisión que contenían correos electrónicos, sistemas de control y copias de referencia de los registros electorales de los registrados para votar en el Reino Unido entre 2014 y 2022, así como de los votantes en el extranjero. Los registros electorales contienen los nombres de los votantes, las direcciones y la fecha en que alcanzan la edad para votar ese año.

La Comisión declaró que el ataque fue llevado a cabo por "actores hostiles" que explotaron una vulnerabilidad en el software utilizado por la Comisión para administrar los registros electorales. La Comisión no reveló la identidad o el motivo de los atacantes, pero dijo que estaba trabajando con el Centro Nacional de Seguridad Cibernética (NCSC) y la Oficina del Comisionado de Información (ICO) para investigar el incidente y evitar nuevas infracciones. La Comisión también aconsejó a los votantes afectados que vigilen sus informes crediticios y cuentas bancarias para detectar cualquier actividad sospechosa, y que denuncien cualquier caso de robo de identidad o fraude a las autoridades pertinentes.

El incidente de la Comisión Electoral es una de las violaciones de datos más grandes y graves en la historia del Reino Unido, ya que expuso la información personal de 40 millones de votantes, o aproximadamente el 60% de la población del Reino Unido, a un posible uso indebido y explotación por parte de actores maliciosos.

El incidente podría tener serias implicaciones para la democracia del Reino Unido, ya que los atacantes podrían usar los datos para manipular o influir en los votantes, o para interferir con el proceso electoral. El incidente también plantea preguntas sobre la seguridad e integridad del sistema electoral del Reino Unido, y la adecuación de las defensas cibernéticas y las capacidades de respuesta a incidentes de la Comisión.

Incidente de transferencia de MOVEit

El 29 de junio, Progress Software, la compañía de software con sede en Estados Unidos propietaria de MOVEit Transfer, un software de transferencia de archivos utilizado por muchas organizaciones para compartir datos confidenciales, reveló que había sufrido un incidente de seguridad que afectó a algunos de sus clientes. El incidente ocurrió el 23 de mayo, cuando un atacante desconocido explotó una vulnerabilidad en el software para

acceder y descargar archivos de algunos de los servidores de los clientes. La compañía dijo que parcheó la vulnerabilidad el 24 de mayo y notificó a los clientes afectados el 25 de mayo.

El incidente de MOVEit Transfer afectó a miles de organizaciones en varios sectores y regiones, incluyendo:

- El **Parlamento noruego** (Stortinget), que informó que el atacante accedió y descargó algunas de las cuentas de correo electrónico del parlamento, y que algunos de los datos se publicaron más tarde en línea.
- La **Agencia de Transporte de Nueva Zelanda** (NZTA), que informó que el atacante accedió y descargó algunos de los archivos de la agencia, incluida la información personal y comercial de algunos de sus clientes.
- La **Universidad de Colorado** informó que el atacante accedió y descargó algunos de los archivos de la universidad, incluida la información personal y de salud de algunos de sus estudiantes, profesores y personal.
- La **Universidad de California** informó que el atacante accedió y descargó algunos de los archivos de la universidad, incluida la información personal y financiera de algunos de sus estudiantes, profesores y personal.
- El **Instituto de Investigación Ocular de Singapur** (SERI), que informó que el atacante accedió y descargó algunos de los archivos del instituto, incluida la información personal y de salud de algunos de sus pacientes.
- La **Agencia Danesa para el Desarrollo y la Cooperación** (DANIDA), que informó que el atacante accedió y descargó algunos de los archivos de la agencia, incluida la información personal y del proyecto de algunos de sus socios y beneficiarios.

El incidente de MOVEit Transfer es una de las violaciones de datos más extendidas y diversas de 2023, ya que afectó a sectores y regiones críticas, y expuso datos confidenciales de millones de personas y entidades. El incidente ilustra el riesgo y el desafío de asegurar el software y los servicios de terceros, y los posibles efectos en cascada y transfronterizos de los ataques cibernéticos y cómo los grupos de ransomware, como Cl0p, pueden beneficiarse de las vulnerabilidades de 0day para propagar ransomware. El incidente también destaca la necesidad de una divulgación y notificación oportuna y transparente de los incidentes cibernéticos, y la importancia de parchear y actualizar el software y los sistemas.

Incidente de MGM Resorts

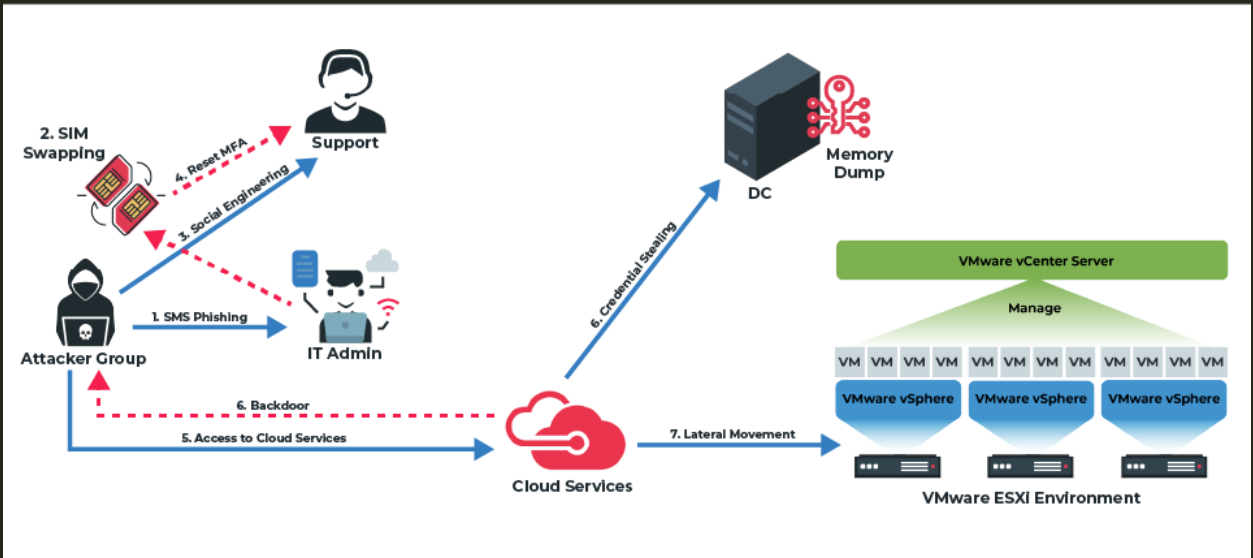
El 7 de septiembre de 2023, MGM Resorts International, una compañía global de hospitalidad y entretenimiento, reveló que había sufrido una violación significativa de datos. El incidente fue orquestado por piratas informáticos desconocidos que se hicieron pasar por un administrador de TI y obtuvieron credenciales de acceso. Esto llevó a un bloqueo de la red de MGM, interrumpiendo las operaciones durante diez días e impidiendo que los huéspedes del resort usaran sus tarjetas electrónicas de habitación, Wi-Fi,

quioscos de cajeros automáticos, dispositivos de juegos electrónicos y otros servicios del resort.

El incidente de MGM Resorts tuvo un impacto sustancial en las operaciones de la compañía y sus clientes. A pesar del anuncio de la compañía de que las operaciones habían vuelto a la normalidad, varios usuarios aún informaron problemas con su aplicación móvil. El incidente expuso potencialmente las direcciones de correo electrónico de los clientes, la información de la tarjeta de crédito y, para algunos miembros de lealtad, los números de seguro social. El alcance del incidente no se reveló de inmediato, incluido el tipo de información que puede haber sido comprometida y cuánto le costó a la compañía.

Este incidente subraya la importancia de medidas sólidas de ciberseguridad en la industria hotelera. También destaca el posible daño financiero y de reputación que puede resultar de tales infracciones.

A continuación una ilustración sobre el proceso de ataque a MGM.



Tendencias de incidentes

En esta sección, analizamos las tendencias y patrones de incidentes de ciberseguridad que ocurrieron en el tercer trimestre de 2023, en función de los datos recopilados de diversas fuentes, como resultados de búsqueda web, artículos de noticias y resultados de respuesta a preguntas. También proporcionamos algunas ideas y recomendaciones para que los líderes de seguridad y gestión de riesgos aborden las amenazas y desafíos emergentes.

Los principales hallazgos de nuestro análisis de incidentes son:

- Los ataques de ransomware continuaron siendo el tipo de ciberataque más frecuente y costoso, que afectó a varios sectores y regiones. Según un informe de Cybersecurity Ventures, se prevé que el ransomware cueste $ 265 mil millones anuales para 2031. Algunos de los incidentes de ransomware notables en Q3 2023 incluyen:
    - El Hospital for Sick Children (SickKids) en Toronto experimentó un ataque de ransomware el mismo día, que afectó sus operaciones clínicas y administrativas. Los atacantes afirmaron estar afiliados al Grupo LockBit, un proveedor de RaaS (ransomware como servicio), pero el grupo luego negó cualquier participación y se disculpó por el ataque. El grupo también proporcionó códigos de desbloqueo para los datos cifrados y se ofreció a ayudar al hospital a recuperarse del ataque.
    - La agencia francesa de desempleo Pôle emploi sufrió un ataque de ransomware en agosto de 2023, que expuso los datos personales y financieros de 10 millones de solicitantes de empleo y empleadores. Los atacantes utilizaron una vulnerabilidad en el software MOVEit Transfer, que también fue explotada en varias otras violaciones de datos en 2023. Los atacantes exigieron un rescate de 15 millones de euros (unos 17,5 millones de dólares) para eliminar los datos robados y restaurar los sistemas de la agencia.
- La creciente adopción de tecnologías emergentes, como la inteligencia artificial (IA), el aprendizaje automático (ML) y el metaverso, también planteó nuevos desafíos y oportunidades para la ciberseguridad. Según un informe de Gartner, los líderes de seguridad y gestión de riesgos deben repensar su equilibrio de inversiones en tecnología y elementos centrados en el ser humano al crear e implementar programas de ciberseguridad en línea con las nueve principales tendencias de la industria. Algunas de las tendencias e implicaciones clave para la ciberseguridad en el tercer trimestre de 2023 incluyen:

- Diseño de seguridad centrado en el ser humano, que prioriza el papel de la experiencia del empleado en todo el ciclo de vida de la gestión de controles. Para 2027, el 50% de los directores de seguridad de la información (CISO) de las grandes empresas habrán adoptado prácticas de diseño de seguridad centradas en el ser humano para minimizar la fricción inducida por la ciberseguridad y maximizar la adopción del control. Esta tendencia requiere que los CISO revisen los incidentes de ciberseguridad pasados para identificar las principales fuentes de fricción y aliviar la carga para los empleados a través de controles más fáciles de usar y efectivos.

- IA y ML, que proporcionan una mayor visibilidad y capacidad de respuesta en todo el ecosistema digital de la organización. Para 2025, el 75% de las herramientas de seguridad empresarial tendrán capacidades de IA / ML integradas o integradas, frente al 40% en 2022. Esta tendencia permite a los CISO aprovechar la IA / ML para diversos fines, como la detección, respuesta y prevención de amenazas, así como el análisis y la automatización de la seguridad. Sin embargo, esta tendencia también introduce nuevos riesgos, como ataques adversarios, prejuicios y ética, que requieren que los CISO establezcan mecanismos de gobernanza y supervisión para la IA / ML.

PERFILES DE ACTORES DE AMENAZAS

DETRÁS DE LAS PANTALLAS: PERFILANDO A LOS ADVERSARIOS EN EL CIBERESPACIO

Actores patrocinados por el estado

Los actores cibernéticos patrocinados por el estado han estado cada vez más activos en 2023. Por ejemplo, los actores cibernéticos vinculados a la República Popular China (RPC) conocidos como BlackTech han demostrado capacidades para modificar el firmware del enrutador sin detectar y explotar las relaciones de confianza de dominio de los enrutadores para pasar de subsidiarias internacionales a sedes en Japón y los Estados Unidos. Se han dirigido a los sectores gubernamental, industrial, tecnológico, de medios, electrónico y de telecomunicaciones, incluidas las entidades que apoyan a los militares de los Estados Unidos. y Japón.

Los grupos criminales notables incluyen NoName057 (16), un grupo hacktivista patriótico prorruso acreditado por ataques DDoS en varios sectores, y Mysterious Team Bangladesh (MTB), que llevó a cabo 846 ataques entre junio de 2022 y julio de 2023.

Grupos criminales

Los grupos cibercriminales se han vuelto más organizados, estructurados y sofisticados en 2023. Han pasado de ser unos pocos individuos aleatorios que llevan a cabo pequeños ataques DDoS o de desfiguración en sitios web de bajo nivel a organizaciones coordinadas con características distintas.

Es probable que prevalezcan tres categorías de delitos como servicio en el cuarto trimestre de 2023 y 2024: ransomware como servicio (RaaS), ladrón como servicio (SaaS) y víctimas como servicio (VaaS).

El aumento del ransomware como servicio (RaaS) ha permitido a los hackers menos calificados lanzar ataques costosos contra grandes organizaciones.

Grupos Hacktivistas

El hacktivismo ha visto un resurgimiento en Q3 2023. Grupos hacktivistas como Anonymous Sudan, Team Mysterious Bangladesh, Team Insane Pk, Hacktivist Indonesia, Ganosec team, Anonymous India, Indian Cyber Force, Kerala Cyber Xtractors han sido observados agravando los ataques DDoS y las desfiguraciones por sus creencias religiosas y
agendas políticas impulsadas por actores estatales o no estatales6. Otro grupo notable es Killnet, que atacó a miembros de la Familia Real en un ataque cibernético separado.

Este informe proporciona una instantánea del panorama de amenazas cibernéticas en el tercer trimestre de 2023. Es crucial que las organizaciones se mantengan informadas sobre estas amenazas e implementen medidas sólidas de ciberseguridad para proteger sus activos.

En conclusión, comprender estos perfiles de actores de amenazas es crucial para desarrollar estrategias efectivas de ciberseguridad. Al mantenerse informadas sobre sus tácticas y objetivos, las organizaciones pueden anticipar mejor las amenazas potenciales y tomar medidas proactivas para proteger sus activos digitales.

ANÁLISIS DE VULNERABILIDADES

DEBILIDADES SISTÉMICAS: IDENTIFICACIÓN Y EVALUACIÓN DE PUNTOS DÉBILES DIGITALES

Nuevas vulnerabilidades

En el ámbito de la ciberseguridad, constantemente se descubren e informan nuevas vulnerabilidades. Estas vulnerabilidades, si no se abordan, pueden proporcionar a los atacantes cibernéticos posibles puntos de entrada a los entornos objetivo.

Según el Informe de Seguridad Cibernética 2023 de Check Point Research, las nuevas vulnerabilidades, las reportadas en los últimos tres años, se utilizaron en el 24% de los intentos de explotación en 2022. Esta tendencia subraya la importancia de mantenerse al tanto de las nuevas vulnerabilidades e implementar medidas correctivas oportunas.

En el tercer trimestre de 2023, se informaron varias vulnerabilidades nuevas. Por ejemplo, CISA agregó tres nuevas vulnerabilidades a su Catálogo de Vulnerabilidades Explotadas Conocidas. Estos incluyen:

- CVE-2023-28432: Vulnerabilidad de divulgación de información en MinIO
- CVE-2023-27350: Vulnerabilidad de control de acceso incorrecto en PaperCut MF/NG
- CVE-2023-2136: Vulnerabilidad de Buffer Overflow en Google Chrome Skia

Vulnerabilidades explotadas

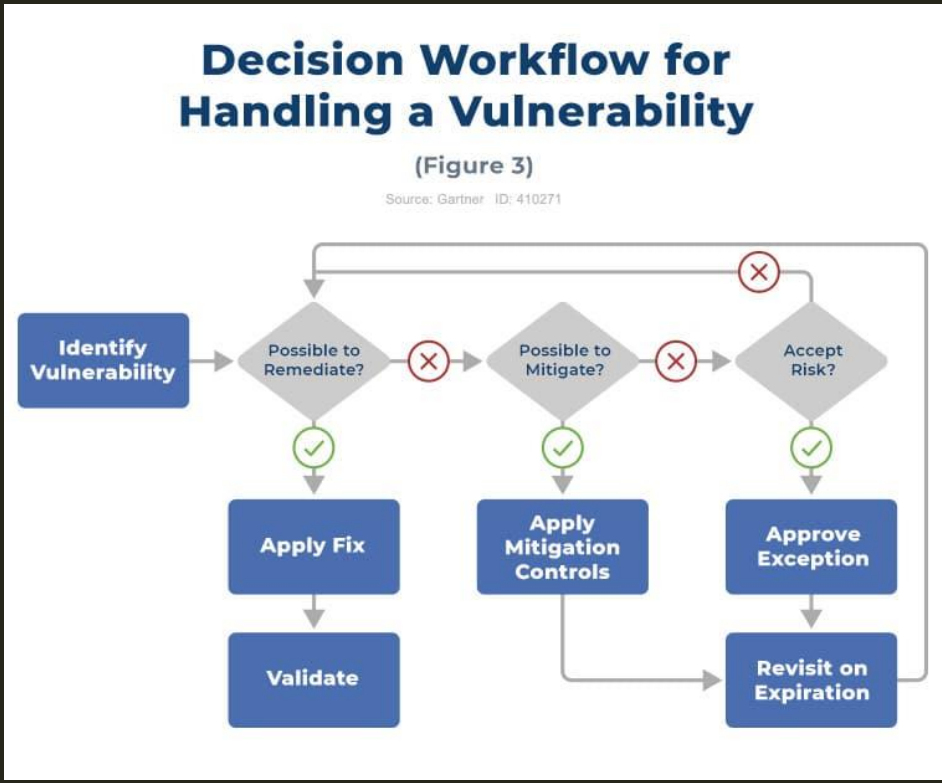
En términos de vulnerabilidades explotadas, la Agencia de Seguridad de Ciberseguridad e Infraestructura (CISA) ha agregado varias vulnerabilidades nuevas a su Catálogo de Vulnerabilidades Explotadas Conocidas basadas en evidencia de explotación activa.

Algunas de las vulnerabilidades notables incluyen:

- **CVE-2023-34362**: Vulnerabilidad de inyección SQL en Progress MOVEit Transfer
- **CVE-2023-0669**: Vulnerabilidad de ejecución remota de código (RCE) en Fortra GoAnywhere Managed File Transfer (MFT)
- **CVE-2023-41993**: Vulnerabilidad de ejecución de código en WebKit de varios productos de Apple
- **CVE-2023-22952**: Vulnerabilidad de ejecución remota de código en varios productos de SugarCRM
- **CVE-2022-41328**: Vulnerabilidad de Directory Traversal en Fortinet FortiOS

Estas vulnerabilidades plantean riesgos significativos, ya que son vectores de ataque frecuentes para los actores cibernéticos maliciosos.

Este informe subraya la importancia de mantenerse actualizado con las últimas vulnerabilidades y garantizar una corrección oportuna para reducir la exposición a los ataques cibernéticos.



MEDIDAS DEFENSIVAS

FORTALECIMIENTO DE LA FRONTERA DIGITAL: ESTRATEGIAS PARA MEJORAR LA RESILIENCIA CIBERNÉTICA

Prácticas recomendadas

Ante el aumento de las amenazas cibernéticas, es crucial que las organizaciones adopten estrategias sólidas de ciberseguridad para mantener la integridad y seguridad de nuestros activos digitales. Estas son algunas de las mejores prácticas que se han identificado para 2023:

1. **Implemente una política sólida de ciberseguridad**: realice una auditoría de ciberseguridad en su negocio para evaluar su situación actual. Desarrollar una estrategia de ciberseguridad centrada en las personas que proteja todo tipo de datos, pero especialmente la información confidencial y patentada.

2. **Asegure su perímetro y conexiones de IoT**: los perímetros de las organizaciones actuales se extienden mucho más allá de los firewalls y la DMZ.
3. **Emplee un enfoque de seguridad centrado en las personas**: todos los empleados, desde los ejecutivos hasta el personal de TI y el equipo de marketing, deben hacer su parte para proteger el negocio y sus datos de las amenazas y ataques de ciberseguridad.
4. **Controlar el acceso a datos confidenciales**: la implementación de controles de acceso puede evitar el acceso no autorizado a datos confidenciales. Esto incluye el uso de contraseñas seguras, la autenticación multifactor y la limitación del acceso según sea necesario.
5. **Gestione los riesgos de la cadena de suministro**: a medida que crece el número de terceros con los que se conecta e interactúa, también lo hace el potencial de los piratas informáticos para acceder a su infraestructura.
6. **Mejore su protección y administración de datos**: Proteja su infraestructura en la nube debido al mayor número de vectores de ataque, la complejidad de los entornos de nube y el reparto de responsabilidades de seguridad entre el cliente y el proveedor de servicios en la nube.

Casos de estudio

El ataque cibernético de The Guardian

El 20 de diciembre de 2022, el periódico The Guardian en el Reino Unido fue objeto de un ataque de ransomware. El efecto inmediato fue hacer que la empresa pidiera al personal que trabajara de forma remota mientras los sistemas internos estaban desconectados y clasificados. La organización empleada para investigar, KnowBe4, ha identificado que el phishing por correo electrónico fue el vector de ataque inicial.

Toronto SickKids

Además, el 20 de diciembre de 2022, el Hospital para Niños Enfermos (SickKids) en Toronto anunció un "código gris", lo que significaba que había experimentado una o más fallas del sistema. Esto resultó ser otro ataque de ransomware. Este ataque es único porque el proveedor de la infraestructura de ransomware como servicio, el Grupo LockBit, se ha disculpado públicamente por el ataque.

Estos estudios de caso destacan la importancia de implementar las mejores prácticas mencionadas anteriormente para protegerse contra tales ataques.

PANORAMA REGULATORIO

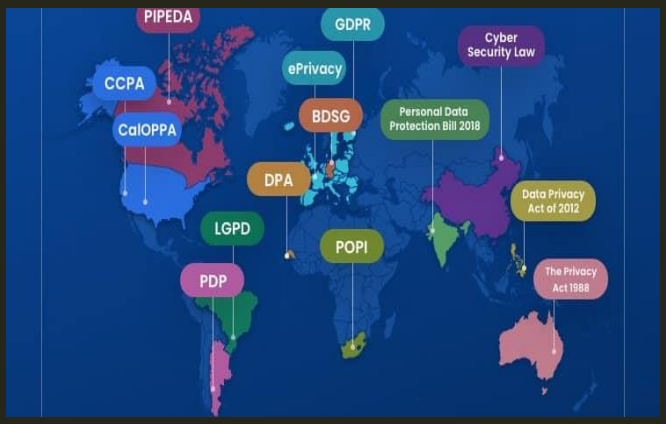
NAVEGANDO POR LA MATRIZ DE LA LEY CIBERNÉTICA: UNA MIRADA A LOS MARCOS REGULATORIOS EN EVOLUCIÓN

Regulaciones globales

En el panorama regulatorio global, el Global Cybersecurity Outlook 2023 del Foro Económico Mundial, en colaboración con Accenture, examina las tendencias de ciberseguridad que afectarán a nuestras economías y sociedades en el próximo año. El informe proporciona las últimas investigaciones sobre cómo el mundo está respondiendo a las amenazas cibernéticas y qué pueden hacer los líderes para proteger sus organizaciones.

Hallazgos clave

- La inestabilidad geopolítica, la rápida maduración y las tecnologías emergentes, la falta de talento disponible y el aumento de las expectativas de los accionistas y los reguladores representan algunos de los desafíos importantes que preocupan a los líderes cibernéticos y empresariales.
- Los mejores líderes se aprovechan de una amplia información y escuchan a todas sus partes interesadas, entienden su papel e impacto, y ejercen un buen juicio para lograr los resultados óptimos.



Regulaciones regionales

España

En España, existe un Código de Ley de Ciberseguridad publicado en el Boletín Oficial del Estado que contiene la normativa pertinente en materia de protección del ciberespacio. Además, en abril de 2023, España aprobó la Ley de Ciberseguridad 5G que

establece requisitos específicos de ciberseguridad para el despliegue y operación de redes 5G.

Europa

El Acta de Ciberseguridad de la UE refuerza ENISA (Agencia de la UE para la ciberseguridad) y establece un marco de certificación de ciberseguridad para productos y servicios3. El 18 de abril de 2023, se propuso una modificación específica para permitir la futura adopción de sistemas de certificación europeos para servicios de seguridad gestionados.

Además, desde el lanzamiento del Reglamento General de Protección de Datos (RGPD) en la Unión Europea, el número de multas a las empresas ha aumentado por infracciones especialmente graves, enumeradas en el art. 83 (5) GDPR, el marco de multas puede ser de hasta 20 millones de euros, o en el caso de una empresa, hasta el 4 % de su facturación global total del año fiscal anterior, lo que sea mayor.

Hallazgos clave

- La ciberseguridad está en el centro de atención más que nunca.
- El mayor interés de los gobiernos internacionales en la ciberseguridad generalmente conduce a una cosa, y eso es el aumento de las regulaciones.
- Simon Chassar, CRO de Claroty, dice que la infraestructura crítica será uno de los sectores bajo el mayor escrutinio y que muchas regulaciones y avisos de los Estados Unidos serán adoptados por otras naciones de todo el mundo en 2023.
- John Stevenson, Director Senior de Producto de Cyren, cree que los gobiernos buscarán introducir tolerancia al riesgo en Europa en lugar de una nueva legislación similar a la de los Estados Unidos.

Esto concluye la sección Panorama regulatorio del Informe de Inteligencia Cibernética para Q3 2023. La siguiente sección profundizará en las amenazas y tendencias cibernéticas específicas que se avecinan en el futuro.

PERSPECTIVAS FUTURAS

HORIZON SCANNING: ANTICIPANDO LOS DESAFÍOS CIBERNÉTICOS DEL MAÑANA

El Global Cybersecurity Outlook 2023 del Foro Económico Mundial, en colaboración con Accenture, ofrece una visión integral del futuro de la ciberseguridad. Este informe examina las tendencias de ciberseguridad que afectarán a nuestras economías y sociedades en el próximo año.

Hallazgos clave

- A medida que la inestabilidad económica y geopolítica se extiende al nuevo año, los expertos predicen que 2023 será un año consecuente para la ciberseguridad.
- La inestabilidad geopolítica, la rápida maduración y las tecnologías emergentes, la falta de talento disponible y el aumento de las expectativas de los accionistas y los reguladores representan algunos de los desafíos importantes que preocupan a los líderes cibernéticos y empresariales.
- Si los hallazgos de la Perspectiva Global de Ciberseguridad del año pasado reflejaron el impacto persistente de la pandemia y los efectos de la rápida digitalización, la Perspectiva Global de Ciberseguridad de este año revela preocupaciones sobre un mundo cada vez más fragmentado e impredecible.
- Construir resiliencia cibernética, a nivel mundial, ha sido una de las prioridades clave del Centro de Ciberseguridad del Foro Económico Mundial desde su creación.

Esto concluye la sección Perspectivas futuras del Informe de Inteligencia Cibernética para el tercer trimestre de 2023.

La siguiente sección profundizará en recomendaciones para todos, especialmente empresas, con respecto al Q4 2023 y los próximos años.

RECOMENDACIONES

HOJA DE RUTA HACIA LA RESILIENCIA: ESTRATEGIAS ADAPTADAS PARA LA MEJORA DE LA CIBERSEGURIDAD

Sobre la base de las tendencias y desafíos de ciberseguridad identificados en 2023, se proponen las siguientes recomendaciones para mejorar la postura de ciberseguridad de las organizaciones:

- **Confianza digital: una responsabilidad compartida**
  Las organizaciones deben trabajar para generar confianza digital con sus partes interesadas. Esto implica garantizar la seguridad y privacidad de los datos del usuario y ser transparente sobre las políticas de uso de datos.
- **La seguridad discreta impulsa comportamientos seguros**
  Las medidas de seguridad deben diseñarse de manera que no obstaculicen la experiencia del usuario. Esto puede alentar a los usuarios a seguir prácticas seguras sin sentirse agobiados.

- **Asegurar un futuro sin perímetro y centrado en los datos**
  Con la creciente adopción de servicios en la nube y el trabajo remoto, el concepto tradicional de un perímetro de seguridad se está volviendo obsoleto. Las organizaciones deben centrarse en proteger los datos en sí, independientemente de dónde residan.

- **Nuevas asociaciones, nuevos modelos**
  Las organizaciones deben considerar formar asociaciones y adoptar nuevos modelos de negocio para abordar los desafíos de ciberseguridad. Esto podría implicar colaborar con otras organizaciones o externalizar ciertas funciones de seguridad a proveedores de servicios especializados.

- **Confianza en la automatización**
  La automatización puede desempeñar un papel clave en la mejora de la ciberseguridad. Los sistemas automatizados pueden ayudar a detectar y responder a las amenazas de manera más rápida y eficiente.

- **Asegurar un mundo inteligente**
  Con la proliferación de dispositivos IoT, es crucial garantizar la seguridad de estos dispositivos. Las organizaciones deben implementar medidas de seguridad sólidas para los dispositivos IoT y educar a los usuarios sobre los riesgos potenciales.

- **Contrarrestar adversarios ágiles**
  Los ciberadversarios son cada vez más sofisticados y ágiles. Las organizaciones deben esforzarse por mantenerse un paso por delante actualizando continuamente sus medidas de seguridad y manteniéndose informadas sobre las últimas tendencias de amenazas.

- **Sea resiliente cuando y dónde importa**
  Las organizaciones deben centrarse en desarrollar resiliencia ante las amenazas cibernéticas. Esto implica contar con un plan sólido de respuesta a incidentes y estar preparado para recuperarse rápidamente en caso de una violación de seguridad.

APÉNDICE

DATOS SUPLEMENTARIOS: RECURSOS E INFORMACIÓN ADICIONALES

Glosario

- **Ciberseguridad**: La práctica de proteger sistemas, redes y programas de ataques digitales.
- **Confianza digital**: El nivel de confianza que los usuarios tienen en la capacidad de una organización para proteger y asegurar los datos y la privacidad de sus usuarios digitales.
- **Dispositivos IoT**: Los dispositivos de Internet de las cosas son dispositivos informáticos no estándar que se conectan de forma inalámbrica a una red y tienen la capacidad de transmitir datos.
- **Seguridad sin perímetro**: un enfoque de seguridad que asume que ningún tráfico dentro de la red de una organización es más confiable de forma predeterminada que el tráfico proveniente de fuera de la red.
- **Resiliencia**: La capacidad de prepararse y adaptarse a las condiciones cambiantes y resistir y recuperarse rápidamente de las interrupciones.

Referencias

Las referencias para este informe son las siguientes:

1. Perspectiva Global de Ciberseguridad 2023 del Foro Económico Mundial
2. Informe de Ciberresiliencia de Accenture
3. Las principales tendencias tecnológicas estratégicas de Gartner para 2023
4. Predicciones de Forrester 2023: Ciberseguridad
5. Predicciones mundiales de seguridad y confianza de IDC para 2023
6. Datos de 16 Honeypots propios distribuidos en EE. UU., UE, JP y ZA