31-01-2024

CYBEROMAX

NO.1

ENERO 2024
VERSIÓN NO 1

NOTICIAS

CIBERATAQUES MÁS RESALTANTES DEL 2023 Y ENERO 2024

ESTADÍSTICAS

SITUACIÓN ACTUAL CIBERSEGURIDAD

TENDENCIAS

LO QUE SE ESPERA EN CIBERSEGURIDAD EN EL 2024

CONTENIDO NO.1

NOTICIAS

Pág. 03

Top 5 incidentes de ciberseguridad 2023

Pág. 04 , 05, 06

Ciberataques Ene 2024

ESTADÍSTICAS

Pág. 07

Situación actual ciberseguridad

TENDENCIAS

Pág. 08, 09, 10, 11, 12

Lo que se espera en ciberseguridad en el 2024.

NOTICIAS

TOP 5 INCIDENTES DE CIBERSEGURIDAD 2023

01

Pentágono | Abr
Filtración de datos delicados de inteligencia militar, pone en riesgo la seguridad mundial.

02

MOVEit | May
Ataque zero day, compromete datos, Afectación: **2.600** Organizaciones, **83** millones de personas

03

DarkBeam |Sep
La mayor filtración de datos del 2023 **3.800** millones de datos expuestos.

04

MGM International/Cesars | Sep
Ataque de Ransomware costo estimado del ataque USD **100** millones.

05

23andMe | Oct
Ciberataque deja expuesto en darkWeb 20 millones de datos de ADN.

NOTICIAS

INCIDENTES DE CIBERSEGURIDAD ENERO 2024

Aerolínea Africana | 30-12-23
Ataque de Ransomware, grupo Ransomexx, la cual ha filtrado datos importantes de sus más de 4 millones de clientes en la DarkWeb.

Tigo Paraguay | 04-01-24
Ataque de Ransomware, grupo Balck Hunt afectando la prestación de servicios de teleco a más de 300 empresas, por lo cual "El DSIRT-MIL de la DIGETIC/FFAA" emiten alerta oficial.

LoanDepot | 04-01-24
Ataque de Ransomware, el cual ocasiono filtración de datos de 16,2 millones de clientes de la financiadora, la cual cerró algunos sistemas para evitar que la amenaza se propague.

Banco Nacional de Angola | 08-01-24
Ataque de Ransomware, Grupo Mitrelli, paralizó por más de 24 horas el Sistema de pagos en tiempo Real gestiona las operaciones interbancarias en todo el país.

ONG Water For People | 11-01-24
Ataque de Ransomware, grupo Medusa roba y filtra datos en la dark web producto que la ONG no paga rescate de USD 300 Mil.

Microsoft | 12-01-24
Ciberataque perpetrado por Midnight Blizzard el agente patrocinado por Rusia, quienes lograron ingresar a cuentas corporativas, sin embargo, no se registró ningúna afectación a sus clientes.

NOTICIAS

INCIDENTES DE CIBERSEGURIDAD ENERO 2024

Aeropuerto Internacional de Beirut | 12-01-24
Hackean el sistema de visualización de información de vuelo (FIDS) y también se vio afectado el sistema de inspección de equipaje del aeropuerto (BHS), ocasionando retrasos en los vuelos programados.

Pastelería Mozart |18-01-24
Filtración de datos en reconocida pastelería con más de medio siglo de operación en Chile, comprometiendo 10 millones de registro de sus clientes.

Foxsemicon |19-01-24
Ataque de Ransomware, grupo Balck Hunt afectando la prestación de servicios de teleco a más de 300 empresas, por lo cual "El DSIRT-MIL de la DIGETIC/FFAA" emiten alerta oficial.

TI Tietoevry | 20-01-24
Ataque de Ransomware a la empresa tecnológica de software, quien tuvo que detener alguno de sus sistemas para evitar la propagación, están trabajando en restaurar toda su operación, se desconoce atacantes.

Subway | 21-01-24
Ataque de Ransomware, grupo LockBit secuestra cientos de archivos financieros de la cadena de comida, solicitando pago de rescate hasta el 02 Feb.

Veolia | 23-01-24
Ataque de Ransomware a la empresa de suministro de agua en EE.UU y Canadá, quien tuvo que detener alguno de sus sistemas de facturación para evitar propagación, se desconoce aún datos comprometidos, se encuentran realizando un forense.

NOTICIAS

INCIDENTES DE CIBERSEGURIDAD ENERO 2024

Centro de Investigación Científica Espacial Rusa | 24-01-24
Hackers Ucranianos destruyen 280 servidores y unos 200 millones de gigabytes de información en un ciberataque contra una estación meteorológica rusa.

Ministerio de Relaciones Exteriores | 24-01-24
Violación de datos, la cual ha comprometido información personal de colaboradores y usuarios. Incidente se encuentra en investigación.

Empresa de Cosméticos | 25-01-24
Ataque de Ransomware, perpetrado por la banda Akira quienes robaron 110 GB de datos de la empresa de cosméticos Japonesa.

BuyGoods | 27-01-24
Filtración de datos por mala configuración en la nube deja accesible al público, pasaportes y detalles de tarjetas de los clientes.

Hackeo 263 periodistas Mexicanos | 29-01-24
Ex colaborador de la casa de gobierno mexicano vulnera un servidor del estado en donde se almacenaba información personal de periodistas.

ESTADÍSTICAS

Las estadísticas nos permiten contextualizar la situación actual de la ciberseguridad y permite a nuestros clientes y lectores identificar las amenazas y desafíos que enfrentan las empresas y las decisiones que deben tomar para proteger su ecosistema digital.

CHILE

N° 56 A nivel internacional en materia de ciberseguridad. *National Cyber Security Index*

N° 5 A nivel Regional en materia de ciberseguridad. *National Cyber Security Index*

27 Ataques digitales por minuto Ago 2022 – Ago 2023. *Kaspersky*

81%

de las organizaciones de América reconocen que tienen una brecha o vacío de disponibilidad *Fuente: Veam*

75%

de las organizaciones en América sufrieron al menos un ataque el año pasado *Fuente: Veam*

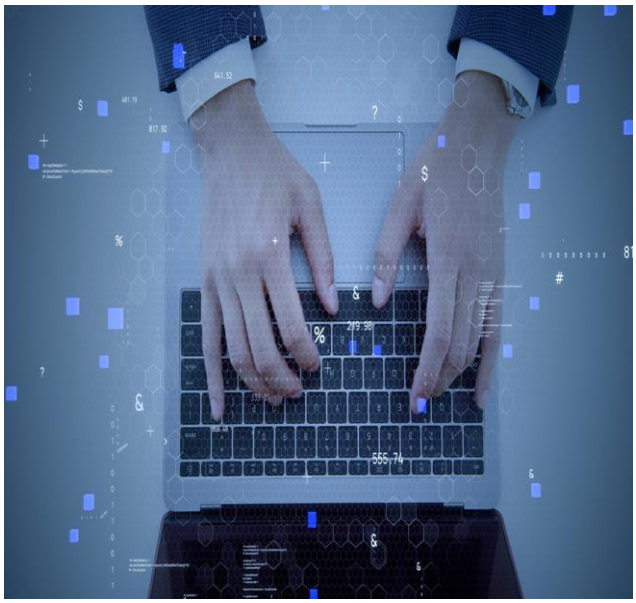
41%

de las organizaciones que sufrieron un material incidente en los últimos 12 meses dicen que fue causado por un tercero. *Fuente: WEF*

TENDENCIAS

LO QUE SE ESPERA EN CIBERSEGURIDAD EN EL 2024

El panorama de la ciberseguridad continuará evolucionando a un ritmo acelerado, eso ya es una realidad, debido a que existe un mayor número de tecnologías emergentes como la Inteligencia Artificial (IA), la nube y el Internet de las Cosas (seguridad IoT), por lo cual las empresas y las personas se enfrentan año tras año a desafíos de seguridad cada vez más complejo.



En RoMaX Techs desde el 2022 compartimos con nuestros clientes y seguidores las tendencias en ciberseguridad que se pronostican año tras año, brindando no solo una idea de las amenazas y desafíos actuales, sino también podamos ayudar a anticiparnos y prepararnos para el futuro.

A continuación, les compartimos que se espera en materia de ciberseguridad para el 2024:

Ciberseguridad en la estrategia empresarial:

La gestión de riesgos de ciberseguridad será una prioridad, en las empresas, quienes buscaran vincular los ciber riesgos a los riesgos estratégicos de la compañía.

PwC en su más reciente informe sobre tendencias de ciberseguridad reveló en su top 6 la preocupación por la mitigación de riesgos digitales y tecnológicos.

TENDENCIAS

Hoy hablamos de negocios digitales y ese temor es infundado al estar hoy en día conectados. Si bien, esto supone varios beneficios, como la simplificación de procesos y la creación de plataformas unificadas, también acarrea riesgos en toda una organización.

El World Economic Forum en su informe “Panorama Mundial de Ciberseguridad 2024” pone en evidencia las principales conclusiones en lo que sería la situación en 2024 y hace hincapié en la creciente desigualdad cibernética y el profundo impacto de las tecnologías emergentes, exigiendo una reflexión estratégica, una acción concertada y un compromiso firme con la ciber resiliencia y la gestión de los riesgos del ecosistema cibernético el cual es cada vez más problemático.

La IA generativa cómo apoyo a los equipos de ciberseguridad y factor de riesgo creciente:

La Inteligencia Artificial (IA), ha desempeñado un papel protagónico en las empresas que utilizan esta tecnología para combatir las amenazas e incidentes cibernéticos, ya que puede ayudar a reducir la desventaja en los equipos de ciberseguridad ante el creciente número y complejidad de ataques.

Existen plataformas que ya están licenciando sus modelos de lenguaje extenso (LLM) junto con sus soluciones de ciberseguridad. Por ejemplo, Microsoft Security Copilot ahora provee funciones de IA generativa para la gestión de la postura de seguridad, respuesta de incidentes y reportes de seguridad. Similarmente, Google anunció Security AI Workbench. El objetivo es ofrecer una suite integral de soluciones de ciberseguridad.

Algunos casos de uso de la IA generativa:

1. La IA generativa puede detectar proactivamente vulnerabilidades que los atacantes pueden explotar y analizar e identificar anomalías.
2. Con la ayuda de procesamiento de lenguaje natural (NLP), puede convertir datos técnicos en contenido comprensible.
3. Herramientas de IA generativas podrían recomendar y validar políticas de seguridad, además de automatizar controles creados con los objetivos y riesgos específicos de la empresa en mente.
4. Análisis del comportamiento de los usuarios.

TENDENCIAS

Son positivas la gran cantidad de tareas y apoyo que resulta adoptar herramientas basadas en IA, sin embargo, la rápida expansión de la IA generativa y otras nuevas tecnologías también pueden ser fácilmente utilizadas por ciberdelincuentes lo cual supone una grave amenaza tanto para las empresas como para la vida pública.

Los avances de la inteligencia artificial plantean más riesgos que “deepfakes o la desinformación”. El WEF plantea 6 principales riesgos, que afectan en general a la sociedad:

1. **Desinformación Organizada:** Las campañas que difunden información errónea a través de las redes sociales u otros canales pueden influir en la opinión pública.

2. **Deepfakes:** generados por IA como: vídeos o grabaciones de audio pueden utilizarse para difundir información falsa, manipular la percepción pública.

3. **Desinformación automatizada:** Los algoritmos de IA pueden emplearse para generar y difundir grandes volúmenes de desinformación, lo que dificulta su detección y combate.

4. **Publicidad dirigida:** Microtargeting basado en IA mediante anuncios personalizados puede utilizarse para manipular las opiniones o suprimir la participación social, en situaciones complejas.

5. **Protección de datos:** El procesamiento automatizado puede crear vías para la filtración de datos personales documentos de identidad, registros de residencia o de otros métodos que conectan con la información personal identificable (PII).

6. **Manipulación algorítmica de las redes sociales:** Los algoritmos de IA de las plataformas de medios sociales pueden manipularse para amplificar determinados mensajes políticos o suprimir otros, influyendo en la opinión pública.

TENDENCIAS

Seguridad en la nube:

Las empresas en los últimos años han migrado a soluciones en la nube y la seguridad en estos entornos se ha convertido en una preocupación. Si nos ponemos a pensar ¿Dónde está alojada gran parte de nuestra información?, la respuesta es fácil: ¡En la nube!

Es de gran importancia que los proveedores de servicios en la nube implementen medidas de seguridad robustas como, firewalls avanzados, sistemas de detección y respuesta a intrusiones y controles de acceso estrictos, asegurando así la protección integral de los datos empresariales en la nube, pero no todo está en manos de nuestros proveedores de servicios, la ciberseguridad debe ser predictiva y anticipada, en ese caso, el uso de una nube local con elementos de autenticación que vaya más allá de las contraseñas como las huellas digitales, y el pentesting son otras tecnologías que contribuyen a evitar y combatir a la ciberdelincuencia.

Las compañías deben acostumbrarse a controlar absolutamente todo: identidad y acceso (IAM), movimiento lateral, cuentas de correo, portales web, aplicaciones, información propietaria, interacciones con el cliente, sistemas operativos, dispositivos conectados, etc.

Simplificación de las herramientas tecnológicas:

De acuerdo a una encuesta realizada por PwC a finales del 2023, el 49% de los líderes de áreas de ciberseguridad eligió la optimización y modernización de las tecnologías v/s a la cifra del 2022 donde tan solo el 32% estaba ya optando por esa estrategia.

La operación en silos que involucra tecnologías, software y proveedores que no trabajan en conjunto, ni bajo procesos claros, puede entorpecer el tiempo de gestión requerida para gestionar los riesgos de ciberseguridad e impedir la visión integral. Una suite de soluciones de ciberseguridad integrada y con procesos claros, documentados e implementados puede ayudar a evitar grandes y costosas brechas de ciberseguridad.

TENDENCIAS

Las Regulaciones incentivan la gestión de la ciberseguridad:

La gestión de ciberseguridad está siendo cada vez más tomada enserio, ya no se trata de un entorno donde grandes compañías son reguladas y se esfuerzan por cumplir con las normativas, año tras año se suman nuevas invenciones y con ello nuevas regulaciones, que no solo deben cumplir grandes empresas sino también pymes.

Las regulaciones pueden verse limitantes. Sin embargo, también pueden dar a las organizaciones confianza para explorar, experimentar, inventar y competir.

En chile el año 2023 fue de grandes desafíos (aprobación Ley Marco de ciberseguridad, actualización de la política nacional de ciberseguridad) donde los entes reguladores incentivaron el cumplimiento para proteger nuestro ecosistema digital.

El año de los ciberseguros:

Desde el 2020 los ciberataques han ido en aumento ocasionando que año tras año más empresas estén optando por contratar un ciberseguro, en el 2022 casi un 70% de las empresas americanas solicitaron un ciberseguro. *Estudio, titulado "Cyber Insurance - If You Get It, Be Ready to Use It", Censuswide.*

Entre las principales razones para solicitarlo, como razón principal se encuentra la reducción de riesgos, exigencias de la dirección ejecutiva, otro punto importante que ha hecho a las empresas tomar la decisión, los incidentes de ransomware cada vez más organizados y letales.

En 2024, los tipos más comunes de ataques a las pymes incluyen malware, phishing, ataques basados en web, ransomware y denegación de servicio distribuido (DDoS). Incidentes bastante complejos que para las buenas prácticas puede resultar insuficientes dado el avance de las amenazas, en ese sentido nadie está del todo protegido de un ciberataque. Ante este escenario, optar por un ciberseguro puede ser la opción que más se evidencie durante el 2024.

RoMaX Technologies

Empresa consultora de Seguridad de la Información y Ciberseguridad especializada en abordar sus servicios, asesorías y soluciones desde una mirada estratégica formada por expertos en ciberseguridad con +27 años de experiencia, calidad y excelencia comprobada.

#JuntosTransformamosLaCiberseguridad

Contacto@romaxtechs.com

2024