Tendencias en Ciberseguridad para el 2024

Para el año 2024, se espera que el 30% de las empresas adopten capacidades como Secure Web Gateway (SWG), Cloud Access Security Brokers (CASB), Zero Trust Network Access (ZTNA) y Firewall As A Service (FWaaS).

Gartner también predice que para 2025, casi la mitad de los líderes de seguridad cibernética cambiarán de trabajo, y el 25% de ellos pasarán a desempeñar roles diferentes. Además, el 50% de los directores de seguridad de la información (CISO) adoptarán un diseño centrado en el ser humano para reducir las fricciones operativas de la seguridad cibernética. Las grandes empresas se centrarán en implementar programas de "Zero Trust" y la mitad de los líderes de seguridad cibernética intentarán utilizar la cuantificación del riesgo cibernético para impulsar la toma de decisiones corporativas.

Balance 2023

Mientras tanto la ciberseguridad sigue siendo un tema crítico en todo el mundo, con una creciente preocupación por los ataques cibernéticos, la protección de datos y la privacidad en línea.

Algunas tendencias y desafíos comunes en ciberseguridad han incluido:

- **Aumento de ataques de ransomware:** Los ataques de ransomware, en los que los ciberdelincuentes cifran datos y exigen un rescate para su liberación, eran cada vez más comunes y sofisticados.
- **Ataques de ingeniería social:** Los ciberdelincuentes utilizan tácticas de ingeniería social para engañar a las personas y obtener información confidencial o acceso a sistemas.
- **Falta de conciencia y formación en ciberseguridad:** Muchas organizaciones y usuarios individuales todavía carecen de una comprensión completa de las mejores prácticas de seguridad en línea.
- **Preocupaciones sobre la privacidad y protección de datos:** La recopilación y el manejo de datos personales siguen siendo un tema candente, especialmente con la implementación de regulaciones como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea.
- **Desarrollo de tecnologías emergentes y la ciberseguridad:** La adopción de tecnologías como el Internet de las cosas (IoT), la inteligencia artificial (IA) y la computación en la nube plantea nuevos desafíos en términos de seguridad.
- **Regulaciones y cumplimiento normativo:** Los gobiernos y organismos reguladores están implementando normativas más estrictas para garantizar la seguridad y privacidad en línea.

Tendencias para 2024

Algunas tendencias en ciberseguridad que se esperan para el 2024 serán:

Ataques basados en Inteligencia Artificial (IA): Se espera una proliferación de ataques basados en IA, especialmente la IA generativa y el aprendizaje automático. Estas tecnologías están aumentando la frecuencia y complejidad de los ataques cibernéticos. Pueden permitir a los ciberdelincuentes lanzar ataques sofisticados y sigilosos, como los "*deepfakes*" o desarrollar un malware que evoluciona automáticamente.

Ciberseguros y paneles de control de amenazas en tiempo real serán métodos esenciales para mejorar la resiliencia cibernética frente a las amenazas generativas de la IA.

Cibercrimen en aplicaciones de mensajería: Se prevé un aumento en el cibercrimen a través de aplicaciones de mensajería.

Protección de datos en entornos de nube híbrida: Se espera que la IA y el aprendizaje automático se utilicen de manera generalizada para proteger datos en estos entornos.

Ataques de Ransomware Potenciados por IA: Se espera que estos programas avanzados de ransomware burlen fácilmente los mecanismos de defensa tradicionales, adaptándose a diversos entornos y haciendo su detección y mitigación cada vez más difícil.

Internet de las Cosas (IoT) y Dispositivos Conectados: Con la proliferación de dispositivos IoT, se espera un aumento en los ataques dirigidos a estos dispositivos debido a sus potenciales vulnerabilidades.

Qué deberíamos considerar para mitigar esas tendencias

Algunas tendencias en ciberseguridad que podrían ser relevantes en 2024 y están basadas en las tendencias observadas durante los últimos años.

Ciberseguridad en la Nube: Con la adopción continua de soluciones en la nube, se espera un enfoque renovado en la seguridad de los servicios y la infraestructura en la nube.

Privacidad y Cumplimiento Normativo: Las regulaciones de privacidad y protección de datos, como el GDPR, seguirán siendo importantes. Se espera una mayor presión para el cumplimiento de estas regulaciones.

La Gestión de Riesgo y Cumplimiento (GRC): es una actividad que recorre los procesos, activos (recursos que materializan actividades de los procesos) y esquemas de cumplimiento, de forma organizada, integrando los componentes y facilitando los procesos de gestión de riesgo, análisis de impacto y verificación de cumplimiento de las expectativas internas y externas de una organización.

El propósito de una GRC es garantizar la visibilidad de los riesgos e impactos de los procesos de la organización para mejorar los controles internos, su capacidad de resiliencia y la mejora continua.

Inteligencia Artificial en Ciberseguridad: Se espera una mayor adopción de IA y machine learning en la detección y respuesta a amenazas.

Desarrollo de Amenazas APT (Amenazas Persistentes Avanzadas): Se prevé que las APT sigan evolucionando, utilizando tácticas más avanzadas y personalizadas para eludir la detección.

Educación y Sensibilización en Ciberseguridad: A medida que las amenazas evolucionan, la educación y concienciación de los usuarios finales se volverán aún más críticas.

Es importante tener en cuenta que estas tendencias están basadas en la evolución histórica de la ciberseguridad y las tecnologías emergentes hasta la fecha. La situación real en 2024 podría ser diferente por lo que se recomienda mantenerse actualizado con fuentes confiables de noticias, expertos en ciberseguridad y en Riesgos de Tecnología Informática desarrollando planes actualizados y probados como el RIA (Risk Impact Análysis), DRP (Disaster Recovery Plan), PCN (Plan de Continuidad del Negocio, etc.

Héctor M. Amodeo

Socio

Gerente Comercial