Fallas de ciberseguridad, 4to riesgo global más importante

Actualmente, a las organizaciones les toma 277 días identificar y contener una violación de datos de acuerdo a informe de especialistas. Tan sólo para el cierre del 2023, se estima que las empresas invertirán 219,000 millones de dólares, lo que representa un incremento del 12.1% en comparación con 2022. En México, esta inversión se espera que sea un 14% más respecto al año pasado.

Pero **¿cómo proteger los activos digitales y garantizar la privacidad de los datos?** las tendencias como la Confianza Cero, DevSecOps y la automatización, son fundamentales para abordar los desafíos cibernéticos. Adoptar un enfoque centrado en datos y prepararse para el ransomware son pasos necesarios. **La conectividad 5G y la protección DDoS en la nube son áreas clave para la inversión en ciberseguridad.** Mantenerse al día en esta tecnología es crucial para garantizar un entorno seguro y resiliente.

Iniciativas de ciberseguridad

1. Enfoque de Confianza Cero:

La Confianza Cero es un enfoque revolucionario en ciberseguridad que plantea la premisa de que ninguna persona o dispositivo puede considerarse confiable por defecto. Este enfoque se basa en principios clave como la verificación constante de la identidad antes de otorgar acceso a recursos de red; acceso limitado; cifrado y autenticación.

2. Integración de la Seguridad en el Desarrollo:

DevSecOps representa una evolución en el desarrollo de software al integrar la seguridad en todas las etapas del ciclo de vida del producto. Algunos beneficios incluyen:

- Identificación temprana y respuesta rápida: La seguridad se considera desde el inicio del desarrollo, así las vulnerabilidades pueden abordarse en horas en lugar de semanas.
- Seguridad desde el diseño: Los productos se crean teniendo en cuenta la seguridad desde el principio.

3. Automatización en SecOps. Preparándose para la Detección Proactiva:

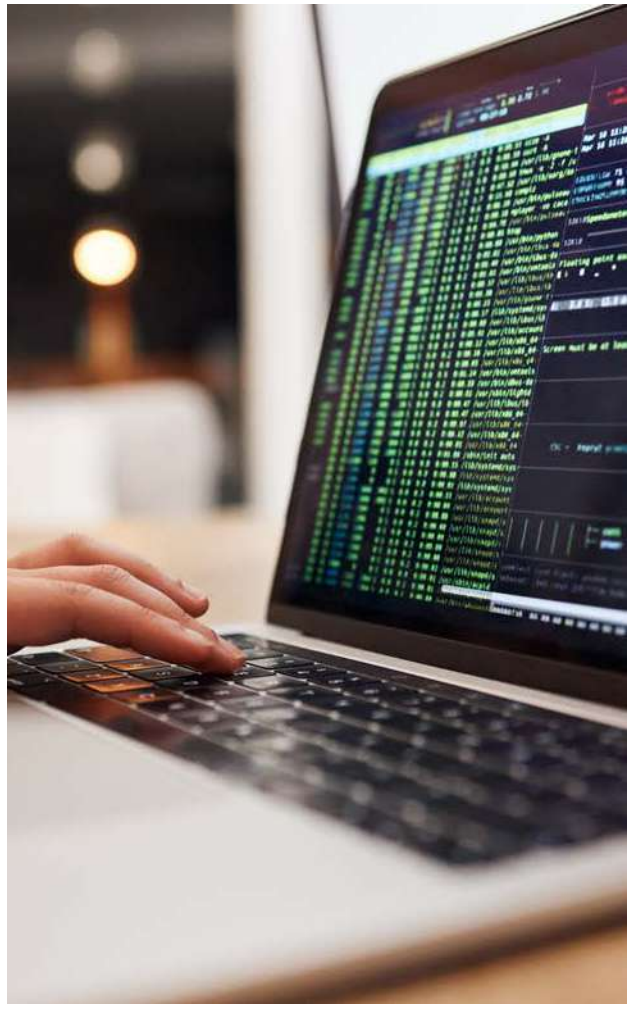
Las operaciones de seguridad deben invertir en automatización para mejorar la detección proactiva de amenazas. La automatización permite prestar atención a las tendencias de amenazas y mejorar la eficiencia. Reduciendo la complejidad y los costos de integración.

4. Seguridad centrada en datos:

Las organizaciones deben centrarse en proteger sus datos sin bloquear su accesibilidad. Algunas medidas incluyen evitar el acceso directo a los datos, utilizar la identidad para gestionar el acceso y simplificar la seguridad mediante soluciones integrales. Este enfoque es esencial en la banca para garantizar la seguridad de la información.

5. Preparación y Mitigación:

El ransomware operado por humanos representa una amenaza seria, por lo que se recomienda a las organizaciones realizar las siguientes acciones:



- Realice evaluaciones de riesgos para determinar la superficie de ataque, el estado actual de resiliencia y preparación de la seguridad en términos de herramientas, procesos y habilidades de defensa.
- Gobernanza del ransomware. Establezca procesos de cumplimiento que involucren a los tomadores de decisiones clave en la organización.
- Preparación operativa constante y planes de respuesta. Realice ejercicios y simulacros frecuentes para asegurarse de que los sistemas siempre puedan detectar ataques de ransomware y cree planes de respuesta.
- Costos de integración. Realice una copia de seguridad no solo de los datos, sino también de todas las aplicaciones no estándar y su infraestructura de TI de apoyo.
- Privilegio mínimo. Restrinja los permisos y deniegue el acceso no autorizado a los dispositivos. Bloquee la instalación de aplicaciones por parte de los usuarios estándar, reemplazándolos con una instalación de software administrada centralmente.
- Educar y capacitar. Los CISO y los líderes de seguridad pueden crear un programa de capacitación básico para todo el personal de la organización.

6. Ataques a Sistemas de Tecnología Operativa (OT):

Los ataques a sistemas OT, que controlan infraestructuras industriales, se están convirtiendo en un objetivo para los ciberdelincuentes. Para controlarlos es necesario la implementación de la API segura como una herramienta crítica.

7. Ciberseguridad para la conectividad 5G:

El principal de ellos es el riesgo de ciberseguridad, que se interpone en el camino de la confianza necesaria para integrar aplicaciones y redes de IoT. La solución radica en la combinación de cualquier elemento técnico, funcional o comercial del IoT con la ciberseguridad para formar un todo nuevo e integrado.

8. Gasto de seguridad en Cloud:

Los ataques DDoS pueden dejar los servicios fuera de línea durante períodos que van desde unos pocos segundos hasta semanas, y se espera que la demanda de soluciones de protección avanzada siga aumentando a medida que estos ataques se vuelvan más sofisticados. De hecho, en 2022, los ataques DDoS incrementaron en un 109%.

De acuerdo con el informe “Gasto Global en Seguridad de la Información” de Gartner, predijo **en 2022 que el gasto en seguridad en la nube aumentaría un 33,3% en comparación con 2021 y para este cierre de 2023 se espera que el gasto de seguridad en Cloud aumente un 27.8%;** con la creciente adopción de SaaS, es probable que se registren más ataques DDoS.

Para controlarlos se recomienda:

- Defensa contra la denegación de servicio. Aunque se producen ataques DDoS de varios terabits, la mayoría utiliza mucho menos ancho de banda, lo que significa que las soluciones on-premises son insuficientes. Se recomienda el uso de servicios de eliminación a nivel de proveedor contra DDoS para blindarse ante estos ataques.

- Operaciones de seguridad. Las defensas contra los ataques DDoS deben estar diseñadas para abordar ataques automatizados, así como los ataques específicos contra aplicaciones individuales.

En definitiva, en este contexto, donde la digitalización de las empresas ha aumentado el índice de los ataques, **las organizaciones deben ejecutar una estrategia amplia que cubra de manera específica cada punto de acceso de un activo informático,** lo que implica que los CISOs implementen una malla de ciberseguridad que impida a la delincuencia acceder a los datos digitales. **Además, es necesario actualizar de manera constante la tecnología con la que ya cuentan, y capacitar a todos los niveles de la empresa.**

Fuente de información: Canales TI