cisco SECURE Partner

CONSTRUYA SU ESTRATEGIA DE RESILIENCIA CIBERNÉTICA

Ante un contexto en el que el cibercrimen crece cada año y las amenazas de agrupaciones de Ransomware como Conti se esparcen a otras latitudes, es hora de comprender que ya no se trata de si llegaremos a ser víctimas de un ataque cibernético sino de cuándo pasará. Las empresas deben construir una resiliencia cibernética que les brinde las capacidades para identificar, responder y recuperarse rápidamente de un incidente de seguridad. Para esto, necesitan trazar un plan que contemple:

Ciberseguridad como prioridad empresarial:

Los costos que tienen los ataques para las organizaciones deja claro que la ciberseguridad es un asunto de negocio y, por lo tanto, invertir en ella es justificado y esencial. Los líderes deben establecer la ciberseguridad como una prioridad operativa ante las juntas directivas y diseñar una estrategia acorde a sus vulnerabilidades con claridad de los riesgos existentes, cómo enfrentarlos, mitigarlos y tomar siguientes pasos.

Mantenerse actualizado sobre las nuevas amenazas cibernéticas:

El panorama cibernético evoluciona constantemente y las amenazas mutan hacia nuevas variantes. Formar parte de comunidades para darle seguimiento al comportamiento de los ataques es clave para identificar patrones, ver tendencias y prevenir incidentes futuros.

Invertir en soluciones de seguridad respaldadas por la industria:

Aún cuando la ciberseguridad sea prioridad, el presupuesto siempre va a ser finito. Para optimizar sus inversiones las empresas deben analizar a profundidad los desafíos que enfrentan y las herramientas necesarias para resolverlos. Es vital que esas herramientas puedan integrarse y operar en conjunto para ofrecer un mayor retorno de inversión.

Refinar la cultura interna:

Los usuarios suelen ser la mayor vulnerabilidad de una compañía a nivel de seguridad, por lo tanto, es vital concientizar y educar a los colaboradores en torno a la estrategia definida por la empresa, los riesgos a los que están expuestos, las prácticas seguras para evitar ataques y el plan de acción a seguir en caso de ser víctima de alguna trampa maliciosa. En este punto es vital contar con el respaldo de las juntas directivas o altos mandos, promoviendo así una cultura fuerte y de impacto para toda la organización.

A nivel de prioridades técnicas dentro de una estrategia de ciberseguridad, Cisco sugiere contemplar aspectos como:

- Seguridad del DNS
- Seguridad del correo electrónico
- Múltiple factor de autenticación y evaluación de postura
- Análisis anti-malware tanto en la red como en los dispositivos finales
- Detección y respuesta de red
- Investigación y respuesta de incidentes
- Inteligencia de amenazas
- Cumplimiento de políticas de uso adecuado para los usuarios internos y externos aunque estos estén fuera de la conexión VPN.

Cisco por décadas ha trabajado en generar conciencia sobre el rol de la seguridad en todo proceso de Transformación Digital. Es por eso que ha incorporado una arquitectura de seguridad integrada en todas sus soluciones que coloca a este elemento en el centro del negocio, de manera que cada uno de sus productos y servicios cuentan con el factor de ciberseguridad desde su conceptualización, de manera que contribuyen a la construcción de una verdadera **Resiliencia Cibernética.**

Al final del día, esa RESILIENCIA CIBERNETICA es lo que hará la diferencia a la hora de resistir a las amenazas impredecibles y emerger más fuertes como empresa.

boyra
comunica tus sueños

TELEFONOS: 57 6019156130, 57 350 6137478
DIAGONAL 61c Bis # 24-44 BOGOTA
WWW.BOYRA.COM