MARSH

Lessons learned from Cyber Incident Response

La ponencia muestra por qué una estrategia centrada en evitar brechas ya no es realista. Para la alta dirección, la prioridad es preparar a la organización para resistir, responder y recuperarse con rapidez: gobierno de crisis, activos críticos identificados, continuidad, respaldos protegidos, escenarios probados y decisiones preaprobadas.

Latinoamérica: objetivo de ataques

La región se ha convertido en un objetivo atractivo para grupos sofisticados. Los ataques de ransomware en LAC pasaron de 302 en 2023 a 432 en 2025. Brasil concentra un 32%, México el 17% y Argentina el 12%.

Ransomware: prioridad ejecutiva

Los ataques de ransomware fueron catalogados como la principal preocupación para CISOs en 2026. La pérdida promedio global alcanza USD 1,53 millones, sin considerar pagos de extorsión, y 49% de empresas afectadas pagó la extorsión.

Recuperación: el reto crítico

Solo 16% de las organizaciones logra recuperarse de un ataque de ransomware en menos de un día. Los RTO/RPO deben validarse frente a escenarios catastróficos, no solo frente a interrupciones operativas convencionales.

Errores que elevan el impacto

Los fallos más críticos incluyen planes no probados, respaldos sin monitoreo, ausencia de continuidad, desconocimiento de la superficie externa, inventario tecnológico incompleto y falta de preaprobación para acciones de alto impacto.

Respuesta como ciclo integral

La preparación debe cubrir prevención, prueba, respuesta y post-incidente: evaluación de capacidades, planes y protocolos, simulaciones de crisis, pruebas de Red Team, análisis forense, gestión de reclamos y lecciones aprendidas.