LITORALPRESS

Fecha: 28-07-2025
Medio: Revista Channel News
Supl. : Revista Channel News
Tipo: Noticia general
Título: Riesgo en servicios básicos aumenta para los altos cargos ejecutivos en Latinoamérica

Pág. : 39
Cm2: 413,1

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida

Informe de Fortinet

Riesgo en servicios básicos aumenta para los altos cargos ejecutivos en Latinoamérica

47% de los encuestados en la Región reportó por lo menos una brecha de ciberseguridad en su infraestructura de servicios básicos (también conocidos como OT) el año pasado, con un 27% reportando más de tres brechas. Mientras que otras regiones reportaron que el regreso al servicio después de un ataque suele durar horas, la mitad de los encuestados latinoamericanos informaron tiempos más largos para volver a operar, incluso varios días.

Fortinet anunció los hallazgos de su reporte global sobre el estado de tecnología operacional y ciberseguridad de 2025. Estos resultados representan el estado actual de la seguridad para OT y destacan las oportunidades de mejora continua para que las organizaciones se protejan contra un panorama de amenazas de IT/OT en constante expansión.

Aunque la madurez de la seguridad de OT ha logrado avances notables, el informe revela que el 47% de los encuestados latinoamericanos reportaron al menos una intrusión de ciberseguridad en el último año, y el 27% reportó más de tres intrusiones. Los tiempos de recuperación después de un ataque son más largos en la región, según los encuestados, con un 46% reportando que necesitan varios días para regresar al servicio.

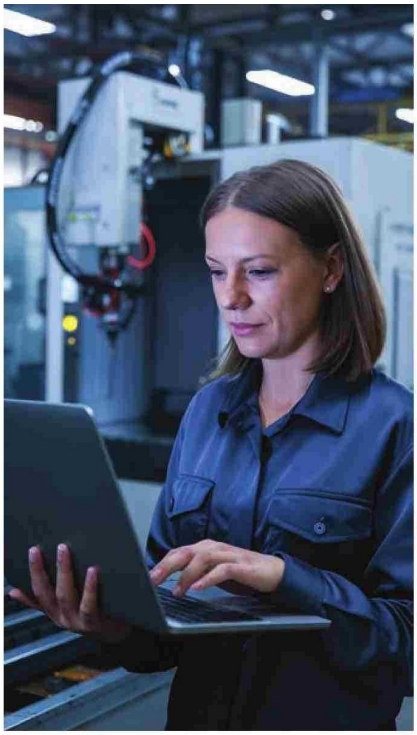
LITORALPRESS

Fecha: 28-07-2025
Medio: Revista Channel News
Supl. : Revista Channel News
Tipo: Noticia general
Título: Riesgo en servicios básicos aumenta para los altos cargos ejecutivos en Latinoamérica

Pág. : 40
Cm2: 419,8

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida

> CIBERSEGURIDAD



Hallazgos clave en América Latina

● **La madurez de la ciberseguridad para OT está afectando al impacto de las intrusiones:** En el nivel básico 1, el 26% de las organizaciones afirman haber establecido visibilidad e implementado la segmentación, frente al 20% del año anterior. La mayoría de las organizaciones afirma que su madurez en materia de seguridad se encuentra en la fase de acceso y perfilado nivel 2.

El informe también encontró una correlación entre la madurez y los ataques. Las organizaciones que se consideran más maduras (niveles 0-4) sufren menos ataques o indican que están mejor preparadas para hacer frente a tácticas menos sofisticadas, como la suplantación de identidad. Sin embargo, algunas tácticas, como las amenazas persistentes avanzadas (APT) y el malware OT, son difíciles de detectar, y es posible que las organizaciones menos maduras no cuenten con las soluciones de seguridad necesarias para determinar su existencia.

● **La responsabilidad de la seguridad OT sigue aumentando entre los altos ejecutivos:** Se ha producido un aumento significativo en la tendencia global de las empresas que planean integrar la ciberseguridad bajo la responsabilidad del CISO u otros ejecutivos. A medida que la responsabilidad sigue recayendo en los altos cargos ejecutivos, la seguridad OT se convierte en una cuestión prioritaria para los consejos de dirección. Los principales líderes internos que influyen en las decisiones de ciberseguridad de OT son ahora, con un margen cada vez mayor, los CISO o CSO. Ahora, más de la mitad (52%) de las organizaciones afirman que el CISO/CSO es responsable de la infraestructura OT, frente al 16% en 2022.

● **La adopción de las mejores prácticas en materia de ciberseguridad está teniendo un impacto positivo:** Además de los niveles de madurez que afectan al impacto de las intrusiones, parece que la adopción de buenas prácticas, como la implementación de medidas básicas de ciberhigiene y una mejor formación y concienciación, está teniendo un impacto real, incluida una reducción significativa de los casos de compromiso del correo electrónico empresarial. Otras prácticas recomendadas incluyen la incorporación de inteligencia de amenazas, que se disparó (49%) desde 2024.

Además, se observó una disminución significativa en el número de proveedores de dispositivos OT, lo que es un signo de madurez y eficiencia operativa. Más organizaciones (78%) utilizan ahora solo entre uno y cuatro proveedores de OT, lo que indica que muchas de estas organizaciones están consolidando proveedores como parte de sus mejores prácticas. Las redes y la seguridad unificadas en sitios OT remotos mejoraron la visibilidad y redujeron los riesgos cibernéticos, lo que condujo a una reducción del 93% en los incidentes cibernéticos en comparación con una red plana. Las soluciones simplificadas de Fortinet permitieron también multiplicar 7x el rendimiento gracias a la reducción de clasificación y configuración.

Mejores prácticas

De igual modo, el reporte global de Fortinet ofrece información útil para que las organizaciones refuercen su postura de seguridad. Las organizaciones pueden abordar los desafíos de seguridad de OT, adoptando las siguientes mejores prácticas.

● Establecer controles de visibilidad y compensación para los activos OT. Las organizaciones deben poder ver y comprender todo lo que hay en la red OT. Una vez que se establece la visibilidad, las organizaciones deben proteger cualquier dispositivo que parezca ser vulnerable, lo que requiere controles compensatorios de protección diseñados específicamente para dispositivos sensibles de OT. Capacidades como políticas de red conscientes del protocolo, análisis de interacción de sistema a sistema y monitoreo de endpoint pueden detectar y prevenir el compromiso de activos vulnerables.

● Implementar la segmentación. Reducir las intrusiones requiere un entorno OT reforzado con controles sólidos de políticas de red en todos los puntos de acceso. Este tipo de arquitectura para OT comienza con la creación de zonas o segmentos de red. Normas como la ISA/IEC 62443 exigen específicamente la segmentación para reforzar los controles entre las redes OT e IT y entre los sistemas OT. Los equipos también deben evaluar la complejidad general de la administración de una solución y considerar los beneficios de un enfoque integrado o basado en la plataforma con capacidades de administración centralizadas.

● Integrar OT en las operaciones de seguridad (SecOps) y la planificación de respuesta a incidentes. Las organizaciones deben estar madurando hacia SecOps para IT-OT. Para lograrlo, OT debe ser una consideración específica para los planes de SecOps y respuesta a incidentes, en gran parte debido a algunas de las diferencias entre los entornos OT e IT, desde los tipos de dispositivos únicos hasta las consecuencias más amplias de una brecha de OT que afecte operaciones críticas.

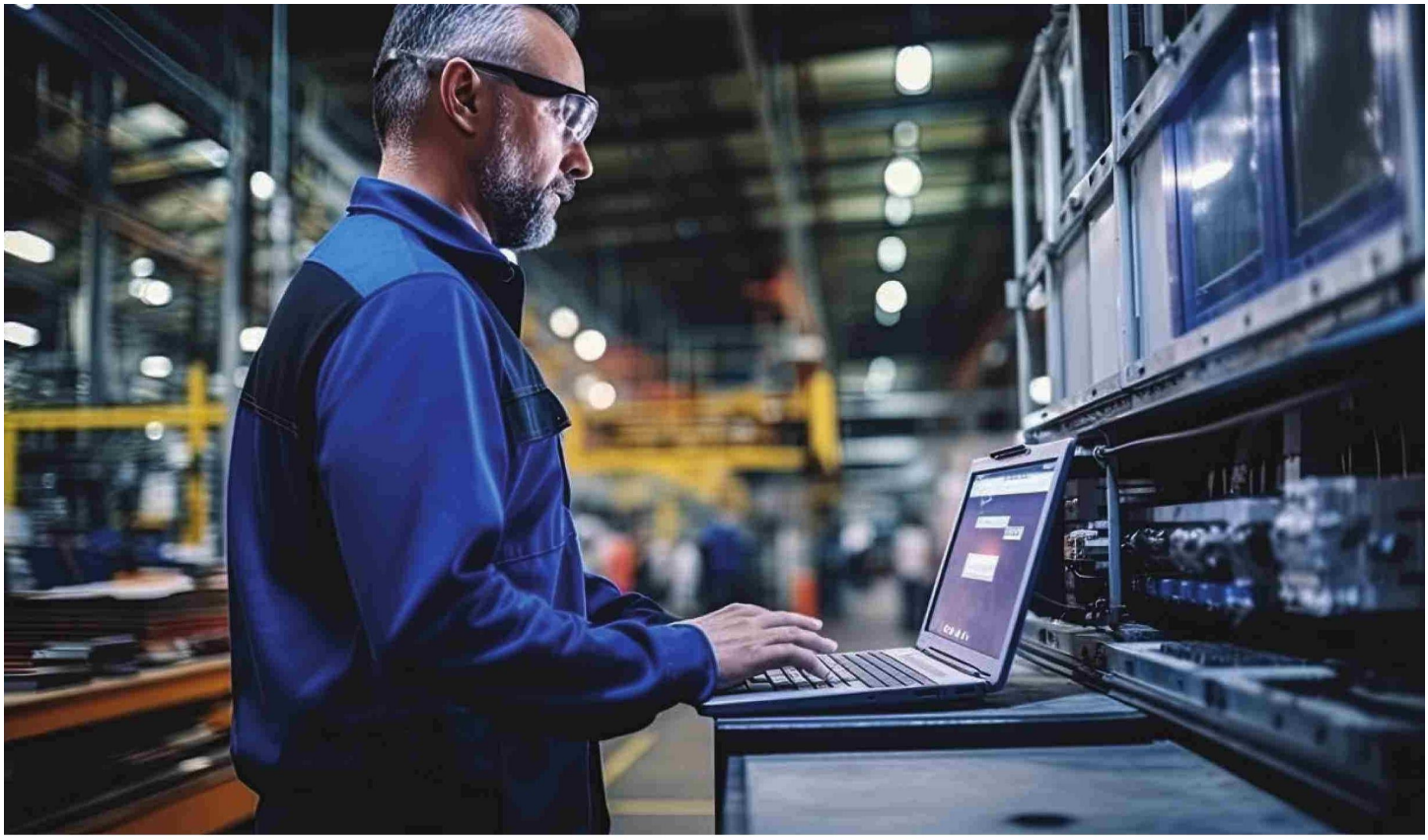
Un paso que los equipos pueden dar para avanzar en esta dirección es crear manuales de estrategias que incorporen el entorno de OT de la organización. Este

LITORALPRESS

Fecha: 28-07-2025
Medio: Revista Channel News
Supl. : Revista Channel News
Tipo: Noticia general
Título: Riesgo en servicios básicos aumenta para los altos cargos ejecutivos en Latinoamérica

Pág. : 41
Cm2: 462,2

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida



tipo de preparación avanzada fomentará una mejor colaboración entre los equipos de IT, OT y producción para evaluar adecuadamente los riesgos cibernéticos y de producción. También puede garantizar que el CISO tenga el conocimiento, la priorización, el presupuesto y la asignación de personal adecuados.

- Considerar un enfoque de plataforma para su arquitectura de seguridad. Para abordar las amenazas de OT en rápida evolución y una superficie de ataque en expansión, muchas organizaciones utilizan una amplia gama de soluciones de seguridad de diferentes proveedores, lo que da como resultado una arquitectura de seguridad demasiado compleja. Esto ha dado lugar a una arquitectura de seguridad excesivamente compleja que dificulta la visibilidad y supone una carga adicional para los limitados recursos del equipo de seguridad. Un enfoque de seguridad basado en plataformas puede ayudar a las organizaciones a consolidar proveedores y simplificar su arquitectura. Una plataforma de seguridad sólida diseñada específicamente para proteger las redes de IT y los entornos de OT puede proporcionar integración de soluciones para mejorar la eficacia de la seguridad mientras permite que la administración centralizada mejore la eficiencia. La integración puede proporcionar también una base para respuestas automáticas a las amenazas.
- Adopción de Inteligencia contra amenazas y servicios de seguridad específicos para OT. La seguridad de OT depende de la concientización oportuna y la información analítica precisa sobre los riesgos inminentes. Una arquitectura de seguridad basada en plataformas también debe aplicar inteligencia de amenazas impulsada por IA para ofrecer protección casi en tiempo real contra las últimas amenazas, variantes de ataques y exposiciones. Las organizaciones deben asegurarse de que sus fuentes de inteligencia contra amenazas y contenido incluyan información sólida y específica de OT en sus fuentes y servicios.

Todos, desde los altos directivos hasta los empleados de base, deben comprometerse a proteger los sistemas OT sensibles y asignar los recursos necesarios para garantizar la seguridad de sus operaciones críticas.

Una responsabilidad de todos

A juicio de Nirav Shah, Vicepresidente Senior de Productos y Soluciones de Fortinet, esta edición del informe muestra que las organizaciones se están tomando más en serio la seguridad de OT. "Vemos esta tendencia reflejada en un notable aumento de la asignación de la responsabilidad del riesgo de OT a la alta dirección, junto con un repunte en las organizaciones que informan de un aumento en las tasas de madurez de la seguridad para OT", explicó. "Junto a estas tendencias, estamos observando una disminución del impacto de las intrusiones en las organizaciones que dan prioridad a la seguridad para OT. Todos, desde los altos directivos hasta los empleados de base, deben comprometerse a proteger los sistemas OT sensibles y asignar los recursos necesarios para garantizar la seguridad de sus operaciones críticas". ChN

Artículo gentileza de Fortinet.
https://www.fortinet.com