ELECTRO INDUSTRIA
Soluciones Tecnológicas para la Minería, Energía e Industria

Fecha: 28/08/2024 Audiencia: 0 Sección: ACTUALIDAD
Vpe: $491.372 Tirada: 0 Frecuencia: MENSUAL
Vpe pág: $661.122 Difusión: 0
Vpe portada: $661.122 Ocupación: 74,32%

"Zero Trust"

Asegurando la continuidad operativa del sector industrial

En la actualidad, se estima que el costo promedio de un ciberataque en entornos industriales es de alrededor de US$4,73 millones. Asimismo, se prevé que para 2025, los impactos globales lleguen a los 10,5 billones de dólares. Estas cifras resaltan la urgencia de que los distintos segmentos industriales enfrenten proactivamente una creciente ola de ciberamenazas.

Conforme el sector manufacturero avanza en su digitalización, las plantas industriales se han convertido en blancos prioritarios para los cibercriminales. Por ello, resulta fundamental fortalecer la seguridad de los sistemas IoT (del inglés "Internet of Things", Internet de las Cosas) y OT ("Operational Technology", Tecnología Operativa), implementando estrictos controles, acceso limitado y un monitoreo constante. En la actualidad, esto se puede lograr implementando soluciones como Zero Trust Network Access (ZTNA). Si reconocemos que diversos segmentos productivos están enfrentando a nivel mundial un incremento en ciberataques, es fácil ver la necesidad de adoptar soluciones de seguridad robustas y efectivas. De hecho, según el Foro Económico Mundial, el costo promedio por ciberataque es de US$4,73 millones en entornos industriales y una proyección de US$10,5 billones en impactos globales para 2025. Cifras que resaltan la urgencia de que los distintos segmentos industriales enfrenten proactivamente esta creciente ola de ciberamenazas. En este contexto, ZTNA ofrece una defensa integral que permite a las organizaciones manufactureras proteger sus activos críticos, garantizar la continuidad operativa y navegar con confianza en la era de la Industria 4.0.

"El desafío radica en que los sistemas de Control Industrial (ICS) y la Tecnología Operativa (OT), que son fundamentales para el funcionamiento de las fábricas, a menudo operan con tecnologías heredadas que carecen de medidas de seguridad adecuadas. Estas vulnerabilidades, junto con la convergencia de las redes de TI y OT, crean un entorno propicio para que los actores malintencionados exploten puntos débiles y accedan a sistemas críticos" , explica David López Agudelo, Vicepresidente de Ventas para USA/Latam de Appgate. "Frente a esta situación, la seguridad perimetral tradicional resulta insuficiente, y surge la necesidad de adoptar enfoques de ciberseguridad más avanzados".

Ventajas de ZTNA para la Ciberseguridad Industrial

Al ser los ciberataques cada vez más sofisticados, se ha vuelto fundamental en este tipo de industrias la adopción de medidas proactivas para proteger los diferentes sistemas. En este aspecto, ZTNA no sólo refuerza la seguridad, sino que también proporciona la agilidad necesaria para adaptarse a un panorama de amenazas en constante evolución, entregando los siguientes beneficios:

1. **Reducción de superficie de ataque:** ZTNA elimina la confianza implícita en usuarios y dispositivos, sin importar su ubicación, asegurando que el acceso a recursos críticos sólo se otorgue tras

ELECTRO INDUSTRIA
Soluciones Tecnológicas para la Minería, Energía e Industria

Fecha: 28/08/2024 Audiencia: 0 Sección: ACTUALIDAD
Vpe: $243.078 Tirada: 0 Frecuencia: MENSUAL
Vpe pág: $661.122 Difusión: 0
Vpe portada: $661.122 Ocupación: 36,77%

una verificación exhaustiva. Esto reduce la superficie de ataque y dificulta la actividad maliciosa.

2. **Integración modular y monitoreo avanzado:** Una solución modular de ZTNA facilita su integración incremental y ajustada a necesidades específicas. Ofrece monitoreo continuo y evaluación dinámica de riesgos, protegiendo los sistemas industriales contra amenazas emergentes y reduciendo el riesgo de movimientos laterales en la red.

3. **Seguridad moderna y sin interrupciones:** ZTNA moderniza la seguridad sin causar tiempos de inactividad, mediante túneles encriptados que protegen usuarios y recursos. Proporciona evaluaciones continuas de riesgo para ajustar permisos en tiempo real y bloquear amenazas proactivamente.

La seguridad industrial no es sólo una cuestión de proteger datos, sino de salvaguardar la innovación, la eficiencia y el crecimiento de la industria manufacturera. Adoptar este tipo de soluciones no es sólo una medida de protección, sino una inversión en el futuro resiliente y seguro del sector industrial.