Cómo mantener el buen funcionamiento de las operaciones mediante la aplicación de los modelos Zero-Trust para entornos OT

Los activos OT conectados exponen las redes empresariales a un amplio, avanzado y lucrativo panorama de ciberamenazas que los cibercriminales suelen aprovechar. La aplicación de los modelos Zero-Trust en los entornos OT garantiza una mayor automatización, fiabilidad y seguridad en sus operaciones.

¿Cuál de las siguientes afirmaciones sobre el modelo Zero-Trust es cierta para su organización?

- La adopción de principios Zero-Trust es una prioridad absoluta para nosotros
- Sabemos que el modelo Zero-Trust es beneficioso para nuestra organización y lo aplicamos en avances e iniciativas
- Estudiamos la aplicación Zero-Trust en cada caso, cuando las circunstancias lo requieren, pero no es una prioridad para nosotros
- No estoy seguro/no lo sé

Fuente: Encuesta de IDC sobre seguridad, 2022 (n = 700)

¿Cómo protege las implementaciones IIoT de su organización?

64 %	52 %	47 %	43 %	42 %	40 %	33 %	29 %	1 %
Seguridad de dispositivos	Gateaway de seguridad perimetral	Control de acceso a la red (NAC)	PKI u otras soluciones de identidad de dispositivos	Firewall industrial	Seguridad integrada en el dispositivo/ sensor	Arquitectura Zero-Trust	Detección y prevención de intrusiones	Otros (especifique)

Fuente: Encuesta de IDC sobre seguridad, 2022 (n = 233)

Zero-Trust es un asunto prioritario en materia de seguridad. El 41 % de las organizaciones da prioridad, con una estrategia y unos objetivos definidos, a los principios Zero-Trust. Además, cuentan con el apoyo de la alta dirección para nuevas inversiones e iniciativas en este contexto. Sin embargo, Zero-Trust no es un producto, una solución o una red específica que simplemente se adquiere. Constituye un enfoque estratégico en materia de seguridad y esto la convierte en una arquitectura difícil de implementar. Solo un tercio de las organizaciones utiliza actualmente el modelo Zero-Trust para proteger sus implementaciones de IIoT.

Zero-Trust

La arquitectura Zero-Trust se basa en el principio de denegar todas las solicitudes de acceso a la red de forma predeterminada. Este enfoque requiere una supervisión constante de las amenazas que sufre la empresa y un mantenimiento continuo del entorno. Además, puesto que se trata de un modelo y no se limita a una solución técnica, es necesario que se satisfagan los requisitos de cumplimiento y de control.

La iniciativa Zero-Trust se está convirtiendo en una de las más importantes para la mayoría de las organizaciones, a medida que avanzan con las iniciativas DX y sus modelos de negocio cambian. Se trata de una estrategia que se adopta en todos los niveles de la empresa con el objetivo de reducir el riesgo general en todas las actividades. Cada vez hay más aplicaciones empresariales que migran a la nube y más dispositivos conectados a la red (los activos de IoT y OT), por lo que la eficiencia de la protección tradicional de la infraestructura perimetral ha disminuido. A las organizaciones les resulta difícil hacer frente a las continuas disrupciones a la vez que protegen usuarios, dispositivos, activos y aplicaciones. Esto aumenta las ineficiencias operativas y el riesgo de brechas de seguridad.

Aplique ya mismo el modelo Zero-Trust en OT. Consejos iniciales

- El modelo Zero-Trust debe ir más allá de la definición tradicional de usuarios e identidad para incluir todos los dispositivos y activos.
- Garantice la visibilidad completa en la red para poder identificar y supervisar todos los dispositivos, incluido el origen y destino de las comunicaciones de datos, así como sus emisores físicos y personales.
- Automatice la aplicación de políticas, así como la detección y el bloqueo de amenazas.
- Segmente la red para aplicar los principios de Zero-Trust en todos los entornos mediante la creación de zonas: la empresa, IoT y OT se pueden tratar como entornos independientes.
- Contenga todos los dispositivos sin parches, vulnerables o no seguros conocidos aislados en zonas más lejanas para reducir la superficie de ataque.

¿Qué supone todo esto para OT?

En seguridad de TI, la confidencialidad se encuentra en el vértice superior del triángulo CIA (confidencialidad, integridad y disponibilidad). Sin embargo, en entornos OT, el aspecto más importante es la disponibilidad, lo que requiere un cambio en las estrategias de gestión de riesgos.

La aplicación del modelo Zero-Trust en las implementaciones OT puede ayudar a reforzar la seguridad y reducir los riesgos asociados a este contexto. No obstante, para adoptar este enfoque se requiere una comprensión profunda del funcionamiento de todos los activos de la red, no solo de los terminales tradicionales de TI. Esto permitirá a las organizaciones tomar las decisiones de segmentación correctas para reducir la superficie de ataque y el riesgo general sin que la disponibilidad se vea afectada.

Los activos conectados pueden convertirse fácilmente en el talón de Aquiles o el punto de entrada a cualquier organización. La aplicación del modelo Zero-Trust en las implementaciones OT puede ayudar a reforzar la seguridad y reducir los riesgos asociados a este contexto. No obstante, para adoptar este enfoque se requiere una comprensión profunda del funcionamiento de todos los activos de la red, no solo de los terminales tradicionales de TI. Esto permitirá a las organizaciones tomar las decisiones de segmentación correctas para reducir la superficie de ataque y el riesgo general sin que la disponibilidad se vea afectada.

La opinión de IDC

La convergencia de TI y OT ha sido una tendencia imparable en los últimos años. Para muchas empresas, constituye un avance hacia operaciones de toma de decisiones más resilientes, que se adaptan a los futuros requisitos operativos. Antes eran dos mundos completamente diferentes, pero ahora TI y OT se comunican entre sí y se integran cada vez más, lo que mejora el rendimiento operativo de las organizaciones. Además, esta unión cubre la brecha histórica entre procesos operativos y procesos empresariales, aunque expone al mismo tiempo a OT a un amplio y avanzado panorama de ciberamenazas.

La adopción de un enfoque Zero-Trust, no solo para la infraestructura de TI tradicional, sino también para los entornos OT con permisos de acceso a datos granulares a nivel de aplicación, aumentará la interoperabilidad entre TI y OT. Además, se reforzará la conectividad segura y se reducirán los riesgos y las amenazas asociados a las operaciones en este contexto.

Mensaje del patrocinador:

El enfoque OT Zero-Trust de TXOne protege a las organizaciones contra los ciberataques altamente eficaces, que se han convertido en una amenaza común para el comercio. Aplique de manera sencilla las políticas basadas en el modelo OT Zero-Trust con **las soluciones nativas de ICS**.