tenable.ot™
Powered by Indegy

CONVERGENCIA ACCIDENTAL

UNA GUÍA PARA OPERACIONES DE TI/TO SEGURAS

DOCUMENTO TÉCNICO

Índice

La iniciativa de convergencia

Las organizaciones industriales y de infraestructura crítica actuales dependen, en gran medida, del entorno de tecnologías operativas (TO) para producir sus bienes y servicios. Más allá de las operaciones tradicionales de TI que utilizan servidores, enrutadores, PC y conmutadores, estas organizaciones también dependen de la TO, como los controladores lógicos programables (PLC), los sistemas de control distribuido (DCS) y las interfaces hombre-máquina (HMI) para hacer funcionar sus plantas y fábricas físicas. Si bien los dispositivos de TO están en uso comercial desde fines de la década de 1960, se ha producido una transformación completa, que cambió la manera en que operamos en el entorno de TO, cómo interactuamos con dicho entorno y cómo lo aseguramos.

Muchas organizaciones optaron por hacer converger sus entornos de TI y TO, lo que puede aportar muchos beneficios; al mismo tiempo, estas decisiones no están exentas de riesgos. La convergencia puede producir nuevos vectores y superficies de ataque; esto puede generar filtraciones que se inicien en un lado de la infraestructura convergente y tengan un avance sigiloso lateral hacia el otro, de la TI a la TO, y viceversa.

Las amenazas que afectan a las operaciones de TO no son las mismas que las que afectan a los entornos de TI. Por lo tanto, las herramientas de seguridad y las políticas operativas que se necesitan son diferentes. La implementación de las herramientas y políticas correctas puede permitir aprovechar todos los beneficios de una operación convergente sin incrementar el perfil de exposición de seguridad de la organización. Es importante que las organizaciones establezcan una estrategia planificada cuidadosamente antes de llevar a la práctica cualquier iniciativa de convergencia, en lugar de incorporar la seguridad solo por si acaso.

El argumento del aislamiento de las redes inseguras

¿Qué sucede cuando el área de negocios toma la decisión estratégica de NO converger sus operaciones de TI y TO? Muchas organizaciones siguen este camino por diversas razones, entre ellas, factores estratégicos, técnicos y de negocios. Al mantener separados los sistemas de TI y TO, estas organizaciones implementan una estrategia de seguridad de "aislamiento de las redes inseguras".

El aislamiento de las operaciones de TO de otras redes se considera el estándar de oro para la seguridad de entornos industriales y de infraestructuras críticas. La infraestructura de TO opera como un "circuito cerrado" sin ninguna interfaz con el mundo exterior, por lo que está físicamente aislada de cualquier entorno externo. Sin datos que salgan del entorno, y sin que ingrese nada del exterior, esta medida de protección se considera la metodología definitiva para proteger a una organización de las amenazas a la seguridad.

Aunque la noción de aislamiento de las redes inseguras parece bastante simple, es sumamente difícil de mantener. El simple hecho de cortar las conexiones es solo una parte del mantenimiento de un entorno estéril, y hay muchos otros caminos hacia lo que es, supuestamente, una infraestructura aislada. Por ejemplo, el verdadero aislamiento requiere la eliminación de la radiación electromagnética de los dispositivos en una infraestructura de TO. Esto requiere la implementación de una jaula de Faraday enorme, para eliminar los posibles vectores de filtración.

A lo largo de los años, se han descubierto otros vectores de ataque, incluyendo las señales de frecuencia FM de una computadora a un teléfono móvil, los canales de comunicación térmica entre computadoras aisladas, la explotación de frecuencias celulares y los canales de transmisión de datos en proximidad (NFC). Incluso los pulsos de luz LED entre los equipos de TO, expusieron los sistemas críticos a actividades maliciosas.

Hay innumerables ejemplos de instalaciones aisladas de redes inseguras, altamente resguardadas, que sufrieron una filtración debido a algo tan simple y aparentemente inocuo como una computadora portátil externa, que se utilizaba como HMI o una unidad USB utilizada para activos de TO. En un entorno de TO promedio, más del 20 % de la infraestructura se compone de equipos de TI. Para las organizaciones que implementaron una iniciativa de Industria 4.0, como la IoT industrial, la cantidad de equipos relacionados con la TI puede llegar al 40 % de la infraestructura de TO.

Las organizaciones que no tienen iniciativas específicas para la convergencia de TI y TO se encuentran entre las que corren mayor riesgo, dado que no se implementa ningún tipo de seguridad adicional más allá del aislamiento de las redes inseguras. Proteger las operaciones, requiere más que construir una fosa digital alrededor de la infraestructura de TO. Incluso en las circunstancias más favorables, este aislamiento es casi imposible de mantener. La introducción de una variable aparentemente inofensiva en un entorno estéril, puede destruir de forma permanente el aislamiento más estricto. Esto se conoce como "convergencia accidental".

Exploits en entornos aislados de redes inseguras

Se cree que los entornos aislados están entre los más seguros. Sin embargo, los ataques recientes, que aprovechan vectores de ataque previamente desconocidos, demostraron que también pueden explotarse. Algunos de los métodos que se utilizan para esto son los siguientes:


acústico


por luz


sísmico


magnético


térmico


radiofre-
cuencia


medios
físicos

Convergencia accidental

Aunque el aislamiento de los activos de TO del "resto del mundo" se considera, a menudo, el estándar de oro para la seguridad de los entornos de TO, no es infalible. De hecho, muchas organizaciones se dejan llevar fácilmente por una falsa sensación de seguridad, a pesar de que su infraestructura de TO aislada es de todo menos aislada; y como resultado, es de todo menos segura.

En los últimos diez años, cada vez más incidentes de ataques se han dirigido a la fabricación y la infraestructura crítica. Entre ellos, hay ejemplos de ataques sofisticados que aprovecharon la "convergencia accidental" para infiltrarse e incursionar dentro de las organizaciones. Estos son algunos ejemplos:

- En 2010, se usó un USB para infectar una instalación nuclear. Al conectar el USB a la red, este lanzó un ataque y ajustó las RPM de las centrifugadoras lo suficiente como para destruirlas. Una parte secundaria del ataque infectó las HMI para mostrar que las centrifugadoras funcionaban con normalidad. Desde entonces, los USB se utilizan a menudo para vulnerar redes aisladas, incluyendo ataques documentados como Turla MiniDuke, RedOctober, Fanny, Remsec y otros más.

- En 2018, los EE. UU. acusaron a Rusia de "romper el aislamiento" e infectar innumerables operaciones de la red de suministro, y de obtener, esencialmente, el acceso a funcionalidades críticas para desactivar las operaciones de la red en el momento en que quisieran. Este fue un punto de inflexión en lo que respecta a convertir proactivamente un ataque de TO en un "arma", para su uso en una fecha posterior. Estos ataques se conocieron como Dragonfly y Energetic Bear.

- En 2019, una instalación nuclear implementó unas PC último modelo con sistema operativo Windows en su red de TO, para fines de comando y control. Estas nuevas PC llegaron con una importante vulnerabilidad de seguridad. Apenas unas semanas después, la vulnerabilidad fue explotada, lo que ocasionó un incidente en los activos de TO que provocó el cierre de emergencia de dos de los reactores.

La convergencia accidental de los entornos de TI y TO puede ocurrir en cualquier momento. Lo que resulta aún más preocupante, es que se produce en muchas organizaciones sin su conocimiento y sin consecuencias, debido a la creencia errónea de que el aislamiento de las redes inseguras es suficiente para evitarla. Después de establecerse dentro de los activos de la organización, estos ataques pueden continuar durante semanas e, incluso, meses, hasta que se produzca una falla catastrófica. La seguridad que se creía que existía era una ilusión alejada la realidad.

Agentes maliciosos

Para comprender cómo proteger el entorno de TO, debemos comprender quiénes son los agentes maliciosos clave.

Ataques externos

Las amenazas del exterior suelen ser el vector que contemplamos primero como el origen principal de un ataque, y por una buena razón. Durante más de tres décadas, la comunidad de seguridad de TI, muy a su pesar, jugó al gato y al ratón con los cibercriminales, persiguiendo constantemente las últimas amenazas cibernéticas. Los hackers suelen buscar el eslabón más débil para explotar, y ahora su atención pasó a los activos de TO, que en general, están mucho menos protegidos. Los hackers externos tienen diversas motivaciones, que van desde el simple vandalismo cibernético hasta obtener ganancias del robo de datos y credenciales. Si bien estas motivaciones resultan válidas para los activos de TI, con los activos de TO, hay otras facciones involucradas, incluyendo terroristas cibernéticos y estados-nación corruptos.

Agentes maliciosos con acceso a información privilegiada

Los agentes con acceso a información privilegiada de las organizaciones, suelen tener credenciales con un alto nivel de acceso, que les permiten entrar a espacios a los que el público en general no puede ingresar. Este segmento de la población es el grupo de potenciales agentes maliciosos de más rápido crecimiento, debido a que las organizaciones otorgan credenciales de acceso a un público cada vez más numeroso y heterogéneo. Este grupo puede incluir a empleados, socios, subcontratistas y otros individuos. Si bien la gran mayoría de este segmento de público actúa en beneficio de la organización, cualquier agente deshonesto que tenga acceso a información privilegiada puede infligir un daño incalculable, dado el acceso que se le proporciona para desempeñar sus labores de rutina.

Errores humanos

Tanto si se trata de un error de configuración, una negligencia o una acción pasada por alto, los errores humanos son, por lejos, el vector de amenaza más común. Pueden deberse a la falta de capacitación, a una falta momentánea de sensatez o a un simple descuido. Si bien todas las organizaciones tienen la intención de mantener una buena postura de seguridad, los errores humanos son la razón principal por la que se producen las filtraciones, y son la actividad más común que genera la convergencia accidental.

Planificación anticipada de la seguridad

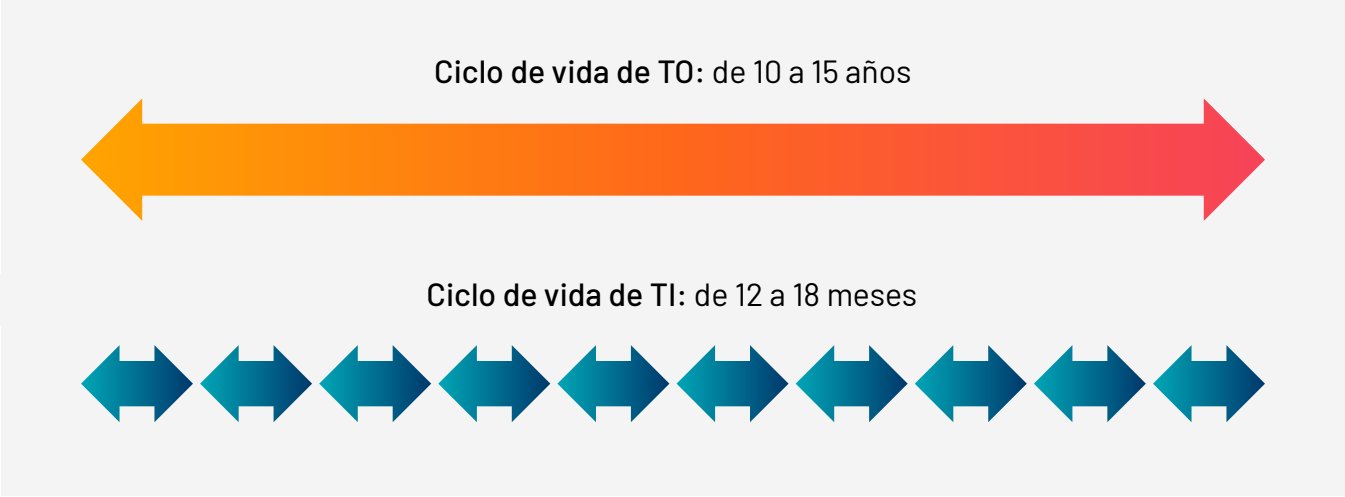
Para la mayoría de las organizaciones industriales, la necesidad de una seguridad atenta no es nada nuevo. Los vectores de amenaza y los pronósticos de seguridad están en constante evolución, dadas las amenazas emergentes. La convergencia de las operaciones de TI y TO, ya sea planificada o no, es en casi todos los casos, una realidad. El establecimiento de las medidas de protección adecuadas ayudará a garantizar la seguridad de las operaciones de su organización. ¿Qué debería considerar?

Visibilidad que se extiende más allá de las fronteras tradicionales

Hasta este momento, la seguridad de los activos de TI y de las infraestructuras de TO habitaban mundos completamente diferentes, por lo que la capacidad de ver hacia cualquiera de los dos entornos se bifurcaba en estas dos líneas. Como se ilustra en este documento, los ataques modernos son amorfos y "viajan" a través de las fronteras de seguridad tradicionales de los activos de TI y TO sin ningún reparo. Nuestra capacidad para dar seguimiento a estos tipos de rutas de propagación requiere descompartimentar los parámetros de visibilidad tradicionales. Es esencial poder obtener una visión única de los equipos de TI y TO, junto con las interacciones que se producen entre los dos mundos. La visión de "tablero de control único", puede ayudar a clarificar los posibles vectores de ataque y los puntos ciegos de los activos que puedan haber omitido las estrategias de seguridad tradicionales.

Análisis situacional a profundidad

Independientemente de si hay una iniciativa de convergencia planificada en proceso, es importante reconocer la diferencia significativa entre los ciclos de vida de TI y de TO. Mientras que las infraestructuras de TI se actualizan periódicamente, las infraestructuras de TO suelen continuar sin cambios durante años, incluso décadas.



No es raro que una infraestructura de TO sea tan antigua como la propia planta. El resultado es que el inventario completo de los activos, junto con los registros de mantenimiento y gestión de cambios, pueden no estar actualizados. Por lo tanto, pueden faltar datos fundamentales, incluyendo detalles importantes como el número de modelo, la ubicación, la versión del firmware, el nivel de parche, los detalles del plano posterior y otros. Dado que es imposible proteger los activos que tal vez ni siquiera sabe que existen, contar con un inventario detallado de su infraestructura de TO que pueda actualizarse automáticamente cuando cambien las condiciones, es esencial para proteger sus operaciones industriales.

Reducción del riesgo cibernético

En los entornos modernos de TO, las amenazas cibernéticas pueden originarse en cualquier lugar y viajar a todas partes. Por consiguiente, es importante utilizar la mayor cantidad posible de capacidades y metodologías para encontrar y mitigar el riesgo de exposición. Esto incluye lo siguiente:

- Detección basada en redes con:
  - Aprovechamiento de las políticas para utilizar las capacidades de crear y mantener listas blancas y negras.
  - Detección basada en anomalías que pueda encontrar ataques de día cero y dirigidos, y que se base en comportamientos de referencia únicos de su organización.
  - Bases de datos de ataques de código abierto, como Suricata, que centralizan la inteligencia de amenazas de la comunidad de seguridad más amplia. La idea es que cuanto más se vigile una posible amenaza, la respuesta de seguridad será mucho mejor.

- Dado que la mayoría de los ataques se dirigen a los dispositivos y no a las redes, es fundamental utilizar una solución que realice consultas activas a los dispositivos y proporcione seguridad a nivel de estos. Debido a que los protocolos de los dispositivos de TO pueden variar mucho, las verificaciones de seguridad y de estado deben ser únicas para la marca y el modelo del dispositivo, incluyendo su lenguaje. Estas verificaciones profundas no deben escanear los activos, sino que deben ser precisas en la naturaleza y la frecuencia de las consultas.

- En 2019, se dieron a conocer más de 20 000 vulnerabilidades nuevas, que afectaban a los dispositivos de TO, así como también a los activos de TI tradicionales. Sin embargo, menos de la mitad de estas vulnerabilidades tenían un exploit disponible. Tener un conocimiento completo de las vulnerabilidades que son relevantes para su entorno, junto con una lista jerarquizada de las vulnerabilidades explotables y los activos críticos, le permitirá priorizar las amenazas con la mayor puntuación de riesgo, y de este modo, se reducirá drásticamente su perfil de Cyber Exposure.

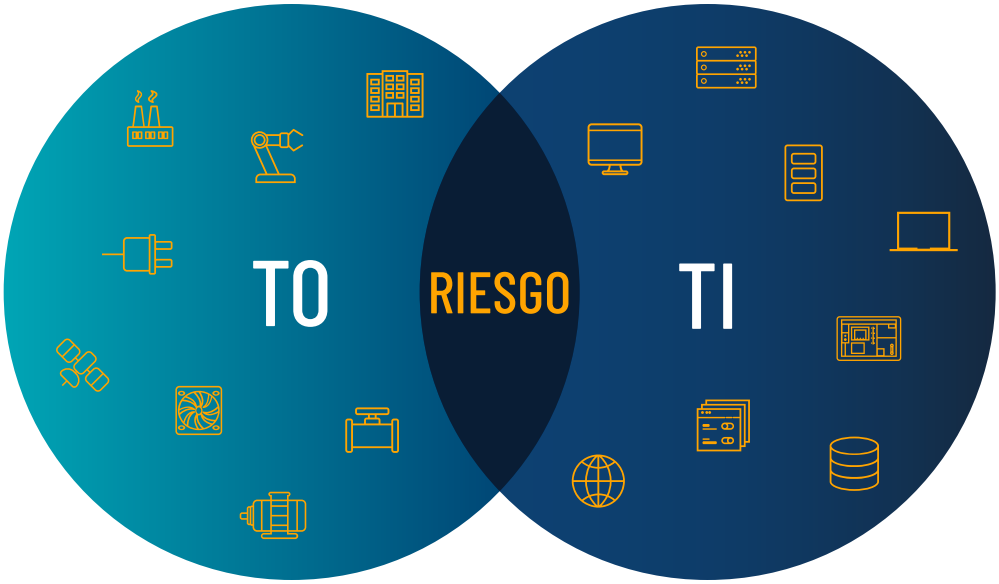
Seguridad que contribuye al ecosistema de confianza

Si bien es importante identificar y aprovechar los mejores productos de seguridad para los activos de TI y de TO de su entorno, es aún más importante que los productos funcionen juntos. La antigua noción de un abordaje de seguridad por capas y cooperativo, en el que los productos específicos pueden trabajar juntos, crea una capa impermeable: la totalidad de la solución se vuelve mayor que la suma de sus partes.

Un ejemplo de ello es una solución de seguridad para los activos de TO, que suministra detalles valiosos a un sistema de gestión de información y eventos de seguridad (SIEM) o a un firewall de próxima generación (NGFW), lo que proporciona al ecosistema de seguridad una visión totalmente nueva e importante de las operaciones industriales. Esto no solo mejora el monitoreo y la respuesta de seguridad, sino que también otorga un mayor valor y utilidad práctica a las inversiones en seguridad existentes.

Soluciones que se pueden escalar

Como se señaló anteriormente, el linaje y el abordaje de los equipos tradicionales de TI y TO no podrían ser más opuestos. Y esta polaridad va mucho más allá de los plazos del ciclo de vida de los productos.



Los equipos de TI suelen regirse por KPI que implican disponibilidad, integridad y confidencialidad, lo que genera una mentalidad que busca que los activos estén "siempre protegidos". Los equipos de TO monitorean las métricas relacionadas con el entorno, la seguridad y la regulación, lo que da como resultado un abordaje "siempre activo: configúrelo y olvídese".

La necesidad actual de abordar la seguridad eficazmente a lo largo de toda la organización —no solo en los activos de TI o en los de TO—, requiere que estas personas con formaciones tan diferentes se unan y encuentren puntos en común para trabajar como una sola. De lo contrario, la organización quedará con una enorme Cyber Exposure, que, si no se aborda, podría tener consecuencias inimaginables.

Convergencia accidental, seguridad intencional

Los equipos de TI y TO deben encontrar puntos en común, para eliminar los sustanciales factores de riesgo que implica la convergencia TI/TO, tanto planificada como accidental. Pero la misión no termina ahí. Las soluciones de seguridad para los activos de TO que trabajan en conjunto con las soluciones de seguridad para los activos de TI, pueden ser el catalizador que no solo proporcione la visibilidad, la seguridad y el control necesarios para frustrar nuevas amenazas cibernéticas, sino que también reúna a estos equipos, que antes estaban separados, para brindar la seguridad común que toda organización industrial, de manufactura o de infraestructura crítica necesita para cumplir con su misión principal de manera eficiente y segura.

Acerca de Tenable

Tenable®, Inc. es la compañía de Cyber Exposure. Más de 30 000 organizaciones de todo el mundo confían en Tenable para comprender y reducir el riesgo cibernético. Como creador de Nessus®, Tenable extendió su conocimiento sobre vulnerabilidades a fin de ofrecer la primera plataforma del mundo para ver y proteger los activos digitales en cualquier plataforma de cómputo. Entre los clientes de Tenable, se encuentran más del 50 % de las compañías de la lista Fortune 500, más del 30 % de las compañías de la lista Global 2000 y grandes instituciones gubernamentales. Para obtener más información, visite es-la.tenable.com.

tenable.ot™
Powered by Indegy