tenable.ot™
Powered by Indegy

PREDICCIÓN DE UN ATAQUE DE TO

DOCUMENTO TÉCNICO

Redefinición del paradigma en el área de seguridad de los activos de TO

Durante los últimos 30 años, hemos sido testigos de cambios lentos pero constantes en el funcionamiento de la tecnología operativa (TO). Con los avances de la cuántica y los puntos de intersección de la tecnología en los entornos de fabricación y de infraestructura crítica, podemos ser más eficaces y eficientes, y al mismo tiempo alcanzar los estándares rigurosos exigidos.

Al mismo tiempo, y en particular durante la última década, los entornos de TO se enfrentan de forma creciente al nuevo reto de mantener entornos seguros. Tal y como hemos visto en TI, la TO está cada vez más en el punto de mira de los incidentes de seguridad que pueden afectar o desactivar las operaciones por completo.

Sin embargo, se puede argumentar que el impacto de un incidente de seguridad en la TO puede tener consecuencias más duraderas y graves cuando implica el cierre de procesos como el tratamiento del agua, la electricidad, el transporte aéreo o la fabricación de automóviles, dispositivos médicos o alimentos.

Tradicionalmente, la seguridad creció en una época de "gato y ratón" donde el hacker "villano" y el "héroe" de la seguridad están en un constante juego de una sola persona. La única meta de ambos es superar al otro, y así crear un juego de salto entre el ataque y la seguridad existente, diseñada para proteger el objetivo. Siempre hay organizaciones e individuos que quedan atrapados en el cerco de seguridad y se convierten en las próximas víctimas.

Este documento técnico analiza las prácticas de seguridad estándar actuales y cómo estamos empezando a cambiar nuestra respuesta y a adoptar un nuevo método para proteger nuestros entornos de TO, una medida que se basa en la detección temprana y la prevención antes de que se produzcan daños.

Filtración de datos de dispositivos

Los agentes maliciosos predicen la mayoría de los ataques dirigidos a un dispositivo particular como un servidor, un interruptor, un PLC, etc. Encontrar un dispositivo débil en una red es la meta principal del reconocimiento, por ejemplo, un dispositivo no protegido, un dispositivo que utiliza una contraseña predeterminada o un exploit con base en una vulnerabilidad sin parches.

Los hackers necesitan tiempo para encontrar un punto débil en infraestructuras de gran tamaño y a menudo distribuidas. Una vez que los atacantes logran eso, ingresan, mapean su red y llevan a cabo el ataque, todo sin que se los detecte. No es raro que el reconocimiento pueda demorar semanas o meses, y puede necesitar más tiempo que el ataque en sí.

Por el contrario, el personal de seguridad de su organización es responsable de asegurarse de que se refuerzan los dispositivos a través de un sistema robusto para identificar los dispositivos objetivo. Por ejemplo, la gestión de acceso a auditorías, la actualización de contraseñas y/o la corrección de vulnerabilidades. En caso de producirse un ataque, las alarmas deben activarse antes de que se produzcan daños y debe ponerse en marcha un conjunto exhaustivo de medidas en el área de seguridad para repelerlo.

Proliferación del ataque

Cuando un hacker se afianza mediante un dispositivo vulnerado, un ataque puede proliferar a otras áreas de la infraestructura. Los atacantes logran esto mediante el aprovechamiento de aquello que conecta diferentes dispositivos, es decir, su red. Los hackers no dependen únicamente de una red para realizar reconocimientos, sino también para extender un ataque y encontrar otros dispositivos que puedan desactivar o utilizar para llegar a otras partes de su entorno que antes estaban protegidas. Tal fue el caso de muchos ataques recientes, entre ellos el de LockerGoga, que comenzó en la infraestructura de TI y proliferó lateralmente hasta la TO, o puede haber avanzado en la dirección opuesta.

El personal en el área de seguridad, ya sea responsable de TI o de TO, utiliza "balizas de alerta temprana" para garantizar la detección de la proliferación de ataques. La seguridad clásica incluye métodos de detección con base en lo siguiente:

Política

- Permitir y rechazar conjuntos de reglas. Imagine que son leyes con actualizaciones constantes a medida que los investigadores identifican nuevas amenazas cuando se hacen realidad.

Anomalía

- Señalar comportamientos anormales en el entorno. Las medidas en el área de seguridad del tipo IDS, una vez puestas a punto, pueden detectar eventuales ataques para los que aún no se ha publicado ninguna política, como es el caso de un ataque de día cero o un ataque dirigido.

Firma

- Una base de datos de código abierto (por ejemplo: SNORT y Suricata) en la que la comunidad en el área de seguridad colabora a medida que detectan nuevas firmas de ataque. La idea aquí es: cuanto más ojos se fijen en una amenaza, más probable es que la comunidad identifique antes los ataques. Esto a su vez, permite a la comunidad en el área de seguridad en su conjunto protegerse con cada persona que contribuye a una base de datos de ataques.

TO en el punto de mira

Si bien los entornos de TO han existido durante más de 50 años, los ataques dirigidos han aumentado de manera notable en la última década. Se han registrado casos de ataques que afectan a casi todas las industrias concebibles de fabricación y de infraestructura crítica. Está demostrado que otras facciones rebeldes han obtenido la funcionalidad del "botón rojo"; es decir, son dueños del entorno y esperan lanzar un ataque cuando quieran.

El motivo del aumento de los objetivos en el entorno de TO se debe simplemente a que existen y son vulnerables. Mientras que en el pasado, los entornos de TO se encontraban confinados en gran medida y eran inalcanzables debido al aislamiento de redes inseguras. En la actualidad, esta medida en el área de seguridad resulta muy poco eficaz.

Las organizaciones que pretenden ser más eficientes y con consciencia de los costos se inclinan por la convergencia de TI y TO, mientras que otras implementan la tecnología de Industria 4.0 o IoT. Estas dos iniciativas generan enormes beneficios, pero también crean nuevos vectores y superficies de ataque que antes no existían, lo que pone en grave peligro a las organizaciones que no están preparadas.

Redefinición del paradigma en el área de seguridad

Como se ha señalado, el juego del gato y el ratón entre los hackers y el personal en el área de seguridad se remonta a los primeros incidentes de seguridad. La seguridad construye una ratonera que se mantiene hasta que un hacker encuentra un camino para evitarla. La seguridad construye una nueva ratonera y el círculo vicioso continúa.
El resultado desfavorable de este paradigma es que alguien tiene que sufrir primero las consecuencias de las vulneraciones antes de que se produzca el desarrollo y la adopción de productos de seguridad mejorados.

La realidad demuestra que siempre hay una organización que sufre una vulneración y se convierte en un caso de prueba en la vida real. En este sentido, la comunidad en el área de seguridad está cambiando el paradigma operativo alejándose de la detección de intrusos hacia la prevención, o simplemente frustrando un ataque antes de que comience.

Vectorización de ataques

Décadas de experiencia en seguridad de TI nos aportan importantes lecciones que podemos aplicar a la TO. Por ejemplo, se sabe que la simple intervención de la red y la "escucha" de las consecuencias no capta todos los ataques. La profundización del nivel de los dispositivos, el objetivo de la mayoría de los ataques, es un método fundamental de detección temprana antes de que un ataque comience a propagarse y encuentre nuevos objetivos a conquistar. Esto es de particular interés en los entornos de TO donde hasta el 30 % de los activos de TO están inactivos; es decir, nunca se comunican a través de su red. En estas situaciones, la red o la detección únicamente pasiva nunca captaría un dispositivo infectado inactivo.

Una nueva forma de seguridad toma en cuenta tanto su red como los dispositivos que la componen. Esto se conoce como vectorización de ataques.

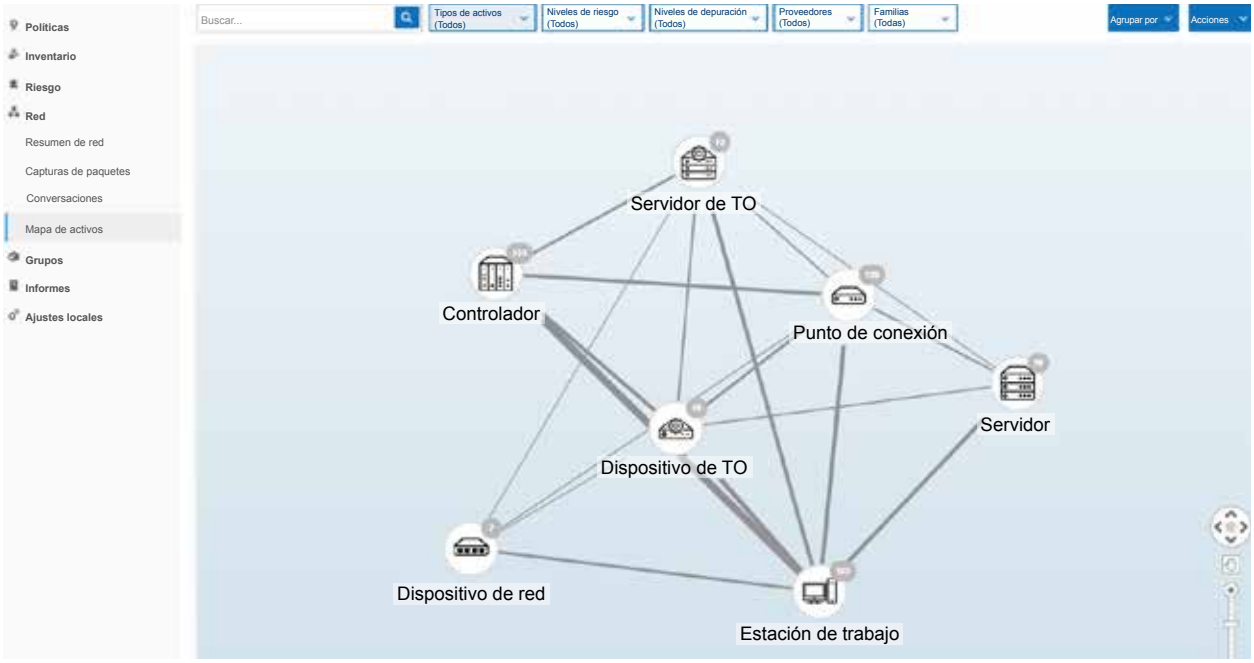

Fig 1: Tenable.ot agrupa los activos por tipo junto con los enlaces de comunicación entre grupos de activos.

La vectorización de ataques replantea la forma en que se los puede afrontar mediante la identificación de las trayectorias de alto riesgo que puede tomar un ataque si se produce en su entorno de TO. La realización de simulaciones puede determinar de mejor manera los puntos débiles y las áreas en las que se necesitan intervenciones en el área de seguridad antes de que se inicie un ataque.

Como vemos en la Figura 1, Tenable.ot identifica y mapea cada activo por tipo de dispositivo. Al hacer clic en cada dispositivo se obtiene un conocimiento situacional profundo del dispositivo, incluyendo la marca, el modelo, la versión del firmware, las vulnerabilidades, la integridad/software, los detalles de la placa base y mucho más.

También podemos ver las vías de comunicación entre dispositivos de la red, que pueden incluir dispositivos de TI, TO e IoT. Tenable.ot analiza cada vía y dispositivo así como también los vectores probables que tomaría un ataque si se produjera en su entorno. También podemos identificar aquellos activos a los que se puede acceder por quién y desde dónde, y luego cerrar posiblemente las vías o limitar el acceso innecesario, con lo que se reduce aún más la exposición.

Los vectores de ataque agrupan dispositivos que comparten una placa base como los PLC. Los diferentes dispositivos que comparten una placa base (PLC, adaptadores de comunicación, tarjetas de E/S) calculan y determinan el riesgo de impacto. El mapeo de vías ilustra los casos en que la reducción o eliminación de riesgos más cerca del punto de demarcación puede disminuir el riesgo más profundamente en su red.

La capacidad de clasificación puede llegar a ser nula en determinados dispositivos, sectores o lugares de su entorno de TO que necesitan una atención o intervenciones especiales.

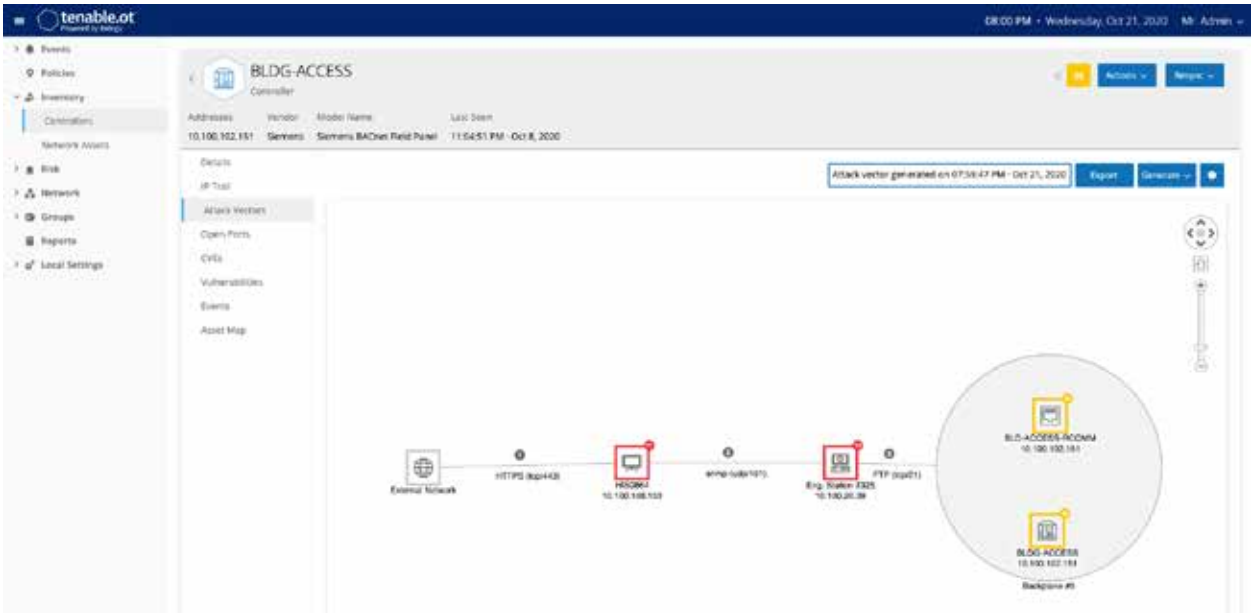

Figura 2: La vectorización de ataques puede ubicar áreas específicas de su entorno que exigen una atención específica.

Usted puede -y debe- realizar una vectorización de ataque con regularidad sobre los activos críticos con el fin de identificar los puntos débiles y los cambios en el perfil de riesgo en constante evolución que son exclusivos de cada entorno individual.

La predicción de una debilidad genera la fortaleza de la TO

Los entornos de TO afectan a todos los sectores de la sociedad moderna y no podemos vivir sin ellos. Los nuevos avances en materia de tecnología y prácticas de negocio ofrecen formas innovadoras de sacar provecho de la TO de manera más eficiente y eficaz con un ahorro considerable, pero no están exentos de riesgos. Los incidentes en el área de seguridad que tienen como objetivo los entornos de TO apenas son el comienzo. Si no se cuenta con una seguridad de los activos de TO adecuada e incorporada, estos sistemas, de los que depende la sociedad, están en riesgo evidente y manifiesto.

La seguridad de los activos de TO está atravesando un cambio de paradigma evidente. El aislamiento de redes inseguras ya no es un medio de seguridad confiable. En muchos casos, la convergencia de TI y TO, y la adopción de la tecnología de IOT eliminó completamente este aislamiento de redes. Sabemos a partir de las lecciones aprendidas en el campo de la TI que el hecho de esperar a que un ataque triunfe antes de implementar nuevos métodos de seguridad puede afectar de forma directa a la seguridad y viabilidad a largo plazo de su organización.

La seguridad en general está adoptando con rapidez un abordaje más proactivo para proteger los entornos de TO, incluyendo este tipo de abordaje para la identificación y la detención de los ataques antes de que se produzcan.

El hecho de obtener conocimiento situacional exhaustivo de todos y cada uno de los dispositivos de su entorno, la identificación de las vías de comunicación, la información de acceso y más, puede ayudar a poner de relieve los puntos débiles y los posibles puntos de desembarco de nuevos ataques. Permite además que la comunidad en el área de seguridad reduzca el riesgo y la cyber exposure. Esto fortalecerá y reforzará a las organizaciones que utilizan sistemas de TO y mejorará su perfil de seguridad cibernética, en lugar de ocuparse de un incidente después de ocurrido.

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