CHECKLIST

Cómo proteger la tecnología operacional

La protección contra las amenazas avanzadas requiere automatización e integración en todas las soluciones de seguridad

Las consecuencias de una intrusión en la tecnología operacional (OT) son graves. En las empresas que dependen de sistemas operacionales y de producción industriales, el Chief Information Security Officer (CISO) debe asegurarse de que los equipos de seguridad tengan la arquitectura y las soluciones adecuadas.

7 Consideraciones para el CISO encargado de proteger la tecnología operacional

Fortinet ayuda a los CISO a reducir la complejidad de la seguridad de la red y los costes de añadir continuamente productos aislados para cubrir nuevas amenazas o exposiciones a riesgos.

☑Integración de la seguridad de OT e IT

La protección de las redes tanto de IT como de OT contra las amenazas avanzadas requiere que el CISO adopte un enfoque multidisciplinar. Eso no significa que las soluciones de seguridad deban funcionar de manera independiente. Por el contrario, todas las soluciones que protegen las redes de OT y de IT deben estar estrechamente integradas y ser capaces de compartir información en tiempo real. Esto permite que la detección de una amenaza en un área active una respuesta coordinada en toda la infraestructura de seguridad de la empresa.

Fortinet Security Fabric proporciona justo esa infraestructura. Juntas, las soluciones de Security Fabric ofrecen una protección bien orquestada que llega a todos los perímetros de las redes de OT e IT corporativas. También ofrecen una amplia visibilidad en toda la superficie de ataque, a la vez que facilitan los flujos de trabajo automatizados para aumentar la eficiencia y la velocidad de las operaciones y la respuesta.

☑Control eficaz del acceso a los recursos de OT

Cada vez más empresas optan más la subcontratación de personal u otros cambios en los procesos productivos que requieren conectividad de red para invitados, contratistas y proveedores. En muchos casos, se necesitan capacidades de acceso inalámbrico y remoto, tanto para los empleados como para cualquier visitante que necesite usar la red. Esos entornos exigen una atención cuidadosa del control del acceso, para evitar conexiones no autorizadas a los recursos de la red.

Las organizaciones pueden aprovechar Fortinet Security Fabric para ofrecer sofisticadas soluciones de gestión y reconocimiento de la identidad de los usuarios. Por ejemplo, FortiAuthenticator facilita las políticas de acceso basadas en roles y la autenticación multifactor para todos los usuarios de los sistemas de OT e IT.

FortiAP y FortiSwitch proporcionan acceso inalámbrico seguro y switching de red, respectivamente. Ambos se han diseñado para entornos operacionales y de producción industrial; se presentan en un diseño reforzado que permite su implementación en las condiciones extremas de los sitios de campo y otros entornos de fabricación y almacén.

☑Segmentación de la red para controlar el movimiento lateral entre IT y OT

Situados entre los segmentos de red de OT e IT, los firewalls de última generación (NGFW) pueden controlar los flujos de tráfico y recrear artificialmente la “brecha de aire” que solía mantener los recursos de OT independientes de los sistemas de IT. Los NGFW FortiGate son especialmente competitivos en este entorno. Su lista blanca de aplicaciones de OT puede configurarse para permitir solo protocolos específicos de OT en la red corporativa de OT y para alejar todo el resto del tráfico.

Otra cuestión fundamental a la hora de seleccionar los NGFW FortiGate para la segmentación de red o la seguridad perimetral es el rendimiento. Con algunos firewalls, la activación de características de seguridad avanzadas reduce drásticamente el rendimiento del cortafuegos. Por el contrario, los NGFW FortiGate están específicamente diseñados para minimizar la latencia, incluso con el sistema de prevención de intrusos (IPS) y otras capacidades avanzadas habilitadas.

☑Inteligencia de amenazas integrada

La protección contra nuevas y emergentes versiones de malware requiere la difusión casi en tiempo real de inteligencia de amenazas locales y mundiales en toda la red. Las soluciones en Fortinet Security Fabric integran las fuentes de datos basadas en inteligencia artificial (IA) de los servicios de inteligencia de amenazas de FortiGuard Labs. Con uno de los mayores equipos de expertos en seguridad del sector, FortiGuard Labs estudia continuamente el panorama de las amenazas para identificar las amenazas de día cero, no solo a los sistemas de IT, sino también a los protocolos de OT más comunes y a las vulnerabilidades de las aplicaciones de OT.

☑Busqueda de tecnologías para fraudes y sandboxing para OT

Ningún servicio de inteligencia de amenazas puede identificar todas las amenazas antes de que lleguen a la red corporativa. Las organizaciones también deben implementar soluciones diseñadas para evitar que las amenazas desconocidas lleguen a sus sistemas de OT. En Fortinet Security Fabric, FortiSandbox recibe paquetes sospechosos de otros elementos de Security Fabric y prueba el código en un entorno en cuarentena. En los entornos operacionales, FortiSandbox puede emular las plataformas de OT, abriendo archivos que son exclusivos de determinados sistemas operativos de OT.

Las tecnologías para fraudes también constituyen una parte importante de una infraestructura de seguridad integral. FortiDeceptor implementa aplicaciones o máquinas virtuales (VM) señuelo específicas de OT, con el objetivo de atraer a los atacantes para que se muestren. Debido a que las amenazas avanzadas se encuentran en constante evolución, los CISO deben enfrentar el problema de las amenazas de día cero desde varias direcciones de manera simultánea.

☑Protección frente a amenazas internas

Los ataques intencionales y maliciosos por parte de ciberdelincuentes infiltrados constituyen una amenaza tanto para los entornos de OT como para los de IT. Además, los propios empleados pueden ofrecer involuntariamente a los atacantes la entrada a la red o el acceso a los datos. La solución de análisis de comportamiento de usuarios y entidades (UEBA) FortiInsight supervisa continuamente a usuarios y endpoints. Aprovecha el machine learning (ML) y el análisis para identificar automáticamente las cuentas que se han puesto en peligro cuando los comportamientos son sospechosos, no conformes o anómalos por cualquier otra razón.

☑La supervisión eficaz de la infraestructura de seguridad como prioridad

Los equipos de seguridad deben ser capaces de gestionar las políticas de forma centralizada, en función de los estándares de seguridad de organizaciones como el Instituto Nacional de Estándares y Tecnología (NIST) y el Centro para la Seguridad de Internet (CIS), y de implementarlas de forma eficiente en todas las soluciones de seguridad. También deben tener acceso a informes centralizados y automatizados tanto sobre amenazas detectadas como sobre la respuesta de las soluciones de seguridad. Management Center de Fortinet Security Fabric incluye una sola consola de gestión, informes y análisis con flujos de trabajo automatizados para ofrecer una visibilidad integral del panorama de seguridad, así como la recopilación de datos de seguridad de OT necesarios para las auditorías de la industria y del gobierno.

Conclusiones

Las brechas en la red de OT pueden tener consecuencias catastróficas. Los CISO de los sectores que utilizan OT deben implementar soluciones de seguridad que incorporen los mejores enfoques de detección avanzada de amenazas y que se integren estrechamente para mejorar la visibilidad y la respuesta automatizada a las amenazas.

Fortinet Security Fabric responde a estas necesidades, facilitando una estrecha integración entre las soluciones de Fortinet y las de terceros. Respaldada por las recomendaciones de las principales organizaciones de pruebas como NSS Labs, la integración de Security Fabric convierte a las soluciones Fortinet en las mejores de su clase y en la mejor elección para las organizaciones de OT.

FORTINET®

www.fortinet.com

septiembre 3, 2020 10:51 a. m.

448524-0-1-ES

D:\ARGOS\2020\09_2020\Assignment A-359635-1115252\Work\PAKIET\OT\Checklist_How to Secure Operational Technology\checklist-FA-how-to-secure-operational-technology-522020-A4_es_ES