CASO PRÁCTICO

Un Grupo De Expertos Sobre Energía Presenta Armis A Empresas De Servicios Públicos Como Componente Clave De Una Red Más Segura

Una mayor concienciación sobre los ciberataques ayuda a que los proveedores de electricidad coordinen sus defensas en las redes de TI y TO.

© Copyright Armis 2023

Sector

Energía

Entorno de TI

Alrededor de 1000 empleados repartidos en varias oficinas en más de una docena de países.

Introducción

Después de los recientes ataques a sistemas energéticos, este grupo de expertos que se encuentra en EE. UU está canalizando su investigación innovadora y su liderazgo de opinión para proporcionar soluciones viables a las empresas de servicios públicos que les permitan reforzar su infraestructura de ciberseguridad. El laboratorio de ciberseguridad del grupo de expertos está llevando a cabo simulaciones y otros proyectos con el fin de demostrar el poder de Armis para aumentar la visibilidad de la superficie de ataque de TO y TI. El grupo de expertos prevé un futuro en el que las empresas de servicios públicos adopten un enfoque con respecto a la seguridad que abarque la confianza cero, una pila tecnológica integrada y visibilidad desde un único panel.

Este grupo de expertos sin ánimo de lucro y neutral respecto del vendedor se enfoca en todos los aspectos del ecosistema energético para reducir los costos, mejorar la eficiencia e impulsar soluciones sostenibles desde un punto de vista ambiental. Ha funcionado durante más de 60 años y está presente en una docena de países. Más de 1000 miembros financian al grupo de expertos, quienes representan principalmente a las empresas de energía que generan y suministran el 90 % de la electricidad en EE. UU., junto con agencias gubernamentales, corporaciones y otras organizaciones de más de 40 países. El grupo de expertos proporciona liderazgo de opinión e investigación sobre todo tipo de temas, desde la mejora del uso y el suministro de energía eléctrica y nuclear hasta problemas relacionados con la sostenibilidad ambiental.

En la actualidad, el grupo de expertos cuenta con tres laboratorios de última generación en los que se realizan pruebas, experimentos e investigaciones sobre aplicaciones tecnológicas. Uno de los laboratorios aloja una instalación de ciberseguridad en la que se ayuda a las empresas de servicios públicos a probar, simular y analizar escenarios de ciberataques a la red eléctrica —como DDoS y ataque de intermediario (MiTM, man-in-the-middle)— y a desarrollar soluciones de mitigación.

© Copyright Armis 2023

Las empresas de servicios públicos se toman en serio el escalamiento de las medidas de seguridad

Como señala el responsable de investigaciones sobre ciberseguridad, el grupo de expertos ha observado un renovado interés en EE. UU. en cómo prevenir ataques que podrían desmontar subestaciones y crear un efecto cascada en toda la red. Esto se debió a diversos factores:

- El ataque de malware con motivaciones políticas a Industroyer, que saboteó los controladores industriales de una empresa eléctrica ucraniana en 2016
- El ataque de ransomware de 2021 a Colonial Pipeline, que provocó el cierre de las operaciones del oleoducto con sede en Texas después de impactar en sus sistemas de facturación y contabilidad. Aunque el ransomware afectó a la infraestructura de TI, la infraestructura de TO conectada sufrió como consecuencia de ello, ya que algunos de los equipos de TO de la empresa se administran mediante ordenadores y otros equipos de TI
- Aumento de los costos de los seguros cibernéticos de las empresas de servicios públicos debido a las crecientes amenazas a la tecnología operativa (TO, operational technology). Las aseguradoras han redoblado sus exigencias y solicitan a las empresas de servicios públicos que presenten registros completos de la actividad de las amenazas y demuestren medidas preventivas para evitar futuros ataques.

Armis ofrece visibilidad inmediata de las amenazas internas y el comportamiento de riesgo de los dispositivos

El responsable de investigaciones sobre ciberseguridad del grupo de expertos se enteró de la existencia de Armis cuando un colega asistió a un ejercicio del estilo capturar la bandera, en el que los participantes “trabajaban con nuevas tecnologías para identificar vulnerabilidades y problemas. El equipo quedó tan impresionado con Armis que adquirió la plataforma sin una prueba de valor (PoV, proof of value). Armis se implementó en el primer semestre de 2019.

Obstáculos

- Identificar la actividad de los dispositivos asociada a comportamientos internos no autorizados
- Obtener una visión de las posibles interacciones de riesgo entre las redes de TI y TO
- Ayudar a las empresas de servicios públicos a reforzar sus defensas contra los ciberataques

© Copyright Armis 2023

Aunque el equipo ya conocía los 188 dispositivos de TI conectados que tenía en el laboratorio, Armis brindó una mayor visibilidad de los nuevos dispositivos, los nuevos protocolos y el tráfico de Internet.

«Cuando adquirimos Armis por primera vez, nuestra prioridad era conseguir que la mayor cantidad posible de dispositivos se comunicaran con Armis, lo que incluía dispositivos de TI, TO e IoT, como nuestras cámaras Honeywell. Al lado, tenemos una estación de capacitación para operadores de red, que cuenta con varios dispositivos de TO, así que también los incluimos en Armis», explica el responsable de investigaciones sobre ciberseguridad.

Armis ha simplificado notablemente el inventario de activos. Ahora solo lleva una hora exportar la información del dispositivo desde Armis hasta una hoja de cálculo de inventario de Microsoft Excel, mientras que antes llevaba días examinar los datos de registro y juntar esa información.

«Una de las cosas que más nos gustan de Armis es que establece una línea de base 'verificada' con la que podemos comparar la actividad o el tráfico anómalos», señala el responsable de investigaciones sobre ciberseguridad. «Cuando me conecto de forma remota a Armis desde casa y no veo ningún tipo de tráfico ni una línea plana, sé que hay problemas de conectividad. Entonces puedo investigar y tomar medidas para solucionar la situación».

Para el laboratorio, la rentabilidad de Armis fue inmediata. De hecho, Armis se encuentra entre las cinco principales soluciones de ciberseguridad que se muestran cuando las empresas de servicios públicos vienen a hacer visitas.

«Empezamos a mostrarlo poco después de ponerlo en marcha. Cuando hacemos recorridos por el laboratorio, le mostramos a la gente las últimas novedades, en especial soluciones de vanguardia como Armis», remarcó el responsable de investigaciones sobre ciberseguridad.

Uno de los casos prácticos más importantes para Armis es la detección de amenazas internas. Después de la implementación de Armis, el laboratorio supervisó los dispositivos con el fin de buscar comportamientos inusuales, en especial, cuando la gente trabaja de forma remota.

«Armis nos permitió determinar qué dispositivos utilizaban protocolos de escritorio remoto (RDP, remote desktop protocols) para conectarse a otros sistemas a través de la red. También nos ayudó a supervisar el tráfico del sitio web y a prevenir posibles problemas relacionados con los datos, al permitirnos ver lo que sale del laboratorio o lo que ingresa en él», explicó el responsable de investigaciones sobre ciberseguridad.

Resultados de Armis

- Mejor visibilidad de las conexiones que cruzan los límites de TO y TI
- Comparación de la actividad inusual con una línea de base «verificada»
- Inventario simplificado de activos

© Copyright Armis 2023

Por ejemplo, la descarga de un archivo ISO de 5 GB, que es una imagen de disco en forma de archivo almacenado (un CD, DVD o Blu-ray) no es inusual. Sin embargo, el supervisor de investigaciones sobre ciberseguridad se preocupa cuando Armis envía una alerta después de detectar que un dispositivo descarga o sube un archivo de 20 GB. Armis incluso descubrió un dispositivo TO, un controlador de automatización Schweitzer 3355 con Microsoft Windows que reside en la sala de capacitación y que se conecta al sitio web de Walmart.

Además, el laboratorio utiliza Armis para obtener información sobre actualizaciones sospechosas de firmware que se sabe que contienen malware. Armis también proporciona información sobre problemas de la pila TCP/IP, como configuraciones erróneas, ajustes dañados o vulnerabilidades que pueden causar interrupciones en la conectividad a Internet y dar lugar a ataques DDoS, MiTM o de suplantación de puertos. Sobre la base de este tipo de comentarios de Armis, el equipo pudo establecer políticas de seguridad automatizadas para diversos escenarios.

Las integraciones preparan el camino para compartir la inteligencia

El equipo del laboratorio de ciberseguridad integró Armis en el controlador de la red LAN inalámbrica, los conmutadores del laboratorio cibernético y Splunk. Splunk es un sistema avanzado de gestión de eventos e información de seguridad (SIEM, security information and event management) que analiza y vincula grandes conjuntos de datos que proceden de sensores, sitios web, aplicaciones y dispositivos.

La integración Armis-Splunk ayuda a cerrar las brechas de visibilidad y seguridad de los entornos de TI y TO, y puede sentar las bases para que las empresas de servicios públicos compartan de forma comunitaria los datos de amenazas. Los proveedores de electricidad buscan cada vez más una forma de ver cómo las empresas similares reciben ataques y qué dispositivos se encuentran comprometidos.

«Desean que este tipo de inteligencia valiosa se comparta de forma comunitaria para que puedan detener ataques similares antes de que lleguen a su sistema. Este nivel de intercambio de información provocará que el ecosistema general de la red sea mucho más fuerte», observó el responsable de investigaciones sobre ciberseguridad.

Resultados de Armis

- Información sobre el comportamiento sospechoso de personas con información privilegiada
- Alertas que activan la investigación y la resolución de problemas
- Integración que enriquece la información
- Consola de único panel para facilitar la gestión y la elaboración de informes

© Copyright Armis 2023

Armis desempeña un papel destacado en la estrategia de confianza cero para los servicios públicos

Según el responsable de las investigaciones sobre ciberseguridad, la confianza cero está empezando a ganar terreno en el mundo de los servicios públicos. En una arquitectura de confianza cero, todos los dispositivos y usuarios se consideran sospechosos de manera predeterminada y se examinan antes de otorgarles conectividad y acceso a los recursos. El incidente de Colonial Pipeline puso de relieve que los límites entre las redes de TI y TO se están desdibujando, ya que los dispositivos de TI se suelen utilizar como consolas de gestión para controlar los equipos de TO.

«Nadie puede decir que está realmente desconectado de Internet. Las conexiones entre los dispositivos de TI y TO aún pueden verse comprometidas. Por eso, las soluciones como Armis deben estratificarse en una arquitectura de confianza cero», afirma el responsable de investigaciones sobre ciberseguridad.

El responsable de ciberseguridad también ha notado que, cada vez más, las empresas energéticas se alejan de un enfoque segmentado de la seguridad y se inclinan por un enfoque de centro de operaciones de seguridad integrado con visibilidad de un único panel que abarca tanto TI como TO. «La plataforma Armis, con su exhaustivo panel de control fácil de usar y su integración con las herramientas que ya tienen la mayoría de las empresas de servicios públicos, es un gran paso en esa dirección», remarcó.

Fortalecimiento de las empresas de servicios públicos frente a futuros ataques y vulnerabilidades

El próximo año, el grupo de expertos planea aprovechar Armis en los estudios de DNP3. DNP3 es un protocolo de comunicaciones utilizado en sistemas de supervisión, control y adquisición de datos (SCADA, communications protocol used in supervisory control and data acquisition), que se utilizan en sistemas remotos de control y suministro de energía en

«Armis nos permitió determinar qué dispositivos utilizaban protocolos de escritorio remoto (RDP, remote desktop protocols) para conectarse a otros sistemas a través de la red. También nos ayudó a supervisar el tráfico del sitio web y a prevenir posibles problemas relacionados con los datos, al permitirnos ver lo que sale del laboratorio o lo que ingresa en él».

Responsable de investigaciones sobre ciberseguridad
Energy Research Institute

© Copyright Armis 2023

empresas eléctricas y de agua. El protocolo DNP3 transmite varios tipos de datos hacia sistemas de TO y desde ellos, y se utiliza de forma habitual en las subestaciones de servicios públicos.

«Estamos investigando cómo podemos utilizar Armis para detectar posibles ataques o anomalías de mensajes de DNP3 que, hasta ahora, eran indetectables. En nuestro laboratorio, intentamos alterar los datos de un mensaje de DNP3 para que parezca un ataque MiTM y después utilizar Armis para detectar que los datos estén fuera de los valores. Cuando Armis detecta que se han manipulado los datos, el protocolo DNP3 debe enviar un mensaje que indica que los datos no son válidos. Si nuestro experimento funciona, prevemos que las empresas de servicios públicos integrarán Armis en su pila de seguridad de confianza cero», expresa el responsable de investigaciones sobre ciberseguridad.

Además del proyecto de DNP3, el grupo de expertos planea construir un cuarto laboratorio de ciberseguridad en la costa oeste e implementará Armis para ayudar a las empresas regionales de servicios públicos a realizar simulaciones de ciberseguridad de TO.

El responsable de investigaciones sobre ciberseguridad también tiene previsto implementar la gestión de vulnerabilidades de activos de Armis (AVM, Asset Vulnerability Management), que proporciona información sobre vulnerabilidades para todos los activos y cubre las lagunas de los activos identificados por escáner. Esto no solo es valioso para las operaciones internas del laboratorio, sino que también es vital para las empresas de suministro eléctrico, ya que las ayudará a priorizar los riesgos y solucionar los problemas con mayor rapidez para evitar interrupciones o fallos en la red.

Por último, el responsable de investigaciones sobre ciberseguridad tiene el compromiso de fomentar una relación continua con Armis para ayudar al grupo de expertos y a sus miembros a mantenerse al día con respecto a los últimos avances tecnológicos. Todo ello forma parte de la misión de la organización de beneficiar a la sociedad al ayudar a las empresas energéticas a mantener una red resiliente y de confianza de la que todos puedan depender en su vida cotidiana.

ARMIS.

Armis, la empresa de ciberseguridad de inteligencia de activos, protege toda la superficie de ataque y gestiona la exposición a los riesgos de ciberseguridad de la organización en tiempo real.

En un mundo en constante evolución y sin perímetros definidos, Armis garantiza que las organizaciones puedan ver, proteger y gestionar de manera continua todos los activos críticos.

Armis protege a empresas Fortune 100, 200 y 500, así como a gobiernos nacionales y entidades estatales y locales, para ayudar a mantener seguras y protegidas las infraestructuras críticas, las economías y la sociedad las 24 horas del día, los 7 días de la semana.

Armis es una empresa privada con sede en California.

1.888.452.4011

Website
Platform
Industries
Solutions
Resources
Blog

Try Armis
Demo
Free Trial