CASO PRÁCTICO

Una Universidad Del Norte Del Estado De Nueva York Consigue Una Mayor Visibilidad De Todos Los Dispositivos Conectados Para Ayudar A Gestionar El Riesgo Interno

Armis le proporciona al Russell Sage College información procesable para ayudar a reforzar la seguridad, cumplir con la normativa y marcar las casillas del seguro de ciberseguridad.

Sector

Educación superior

Entorno de TI

Alrededor de 2500 estudiantes y 450 empleados, y un entorno compuesto por dispositivos gestionados, no gestionados y de IoT

Introducción

Fundado hace más de un siglo como institución femenina de educación superior, el Russell Sage College ha evolucionado hasta convertirse en una institución mixta que se enorgullece de sus programas académicos flexibles y de su entorno de aprendizaje solidario. Con el deseo de mejorar la visibilidad de los dispositivos y reducir los riesgos de seguridad desde el interior de la red, el departamento de TI implementó Armis. La plataforma multiplicó por 15 el inventario de dispositivos de TI, lo que permitió que el equipo encontrara activos que antes habían pasado desapercibidos, aplicara las actualizaciones necesarias, retirara los equipos antiguos y ajustara las políticas. Armis también ayudó a que la universidad satisficiera los estrictos requisitos de cumplimiento y seguro de ciberseguridad.

Fundado en 1916 por la feminista Margaret Olivia Slocum Sage y bautizado con el nombre de su difunto marido, el Russell Sage College de Troy (Nueva York) se orientaba de forma exclusiva a mujeres y les ofrecía una sólida educación en artes liberales y preparación profesional en diversos campos. Hoy es una institución mixta con programas de pregrado, grado y posgrado en artes y ciencias, educación, ciencias de la salud y gestión empresarial. La universidad tiene más de 2500 estudiantes y 450 empleados, incluidos más de 100 profesores a tiempo completo en sus dos campus del norte del estado de Nueva York (Troy y Albany). El Russell Sage College se enorgullece de su entorno de aprendizaje solidario y de alto compromiso, con una proporción de 10 alumnos por profesor y un promedio de 15 alumnos por clase.

Cuando lo propio no es suficiente, Armis hace el trabajo

El subdirector de Informática e ingeniero en sistemas John Harris — que forma parte de un equipo de seis personas— ya lleva 15 años trabajando en la universidad y supervisando todos los aspectos técnicos, desde la seguridad y el cumplimiento hasta el centro de atención al usuario del servicio de TI y los recursos audiovisuales. El parque de TI gestionado consta de alrededor de 150 conmutadores, 300 servidores, 2000 terminales y dispositivos periféricos, como impresoras, escáneres, cámaras y proyectores. La cantidad de dispositivos no gestionados, que son aquellos que utilizan principalmente los estudiantes y algunos empleados, es de unos 15 000 (cinco dispositivos por estudiante). La universidad cuenta con políticas de uso aceptable bien definidas que rigen la forma en que los estudiantes, los profesores, el personal y los invitados deben utilizar los equipos que pertenecen a la universidad y sus propios dispositivos personales conectados a la red.

Durante años, Harris había utilizado una herramienta propia para gestionar la situación de seguridad de estos activos, pero cada vez se frustraba más por los falsos positivos, y no obtenía una imagen completa de lo que se conectaba a la red. «No tenía ni idea de lo que hacía la gente en Internet hasta que alguien activó una alerta de firewall», expresó. «Necesitábamos una mejor solución y, por eso, evaluamos a Armis».

Harris contactó con un socio de Armis y decidió realizar una prueba de valor (PdV). En solo dos o tres días, Armis demostró sus capacidades, al identificar hasta 30 000 dispositivos en la red de la universidad.

Armis descubre lo inusual

Armis descubrió una cantidad de dispositivos sorprendentes, que incluían varios dispositivos de Internet de las cosas (IoT) que el departamento de mantenimiento había instalado sin informar a Harris e, incluso, un automóvil conectado. También se enteró de que mucha gente utilizaba sistemas operativos obsoletos, como Microsoft Windows 98, que son un claro riesgo para la seguridad. Además, había varios televisores inteligentes de bajo costo utilizados con fines educativos y de entretenimiento que inundaban la red y lavadoras inteligentes situadas en las residencias de estudiantes. Todo ello ralentizaba de forma considerable el rendimiento de la red.

Obstáculos

- Visibilidad de los riesgos internos.
- Detección de dispositivos no gestionados y de IoT.
- Acatamiento de los requisitos del cumplimiento de la normativa y el seguro de ciberseguridad.

«Armis también nos ha ayudado mucho con nuestras impresoras. No nos dimos cuenta de que estábamos utilizando tantos protocolos diferentes para estos periféricos, y que agentes malintencionados podían explotarlos. En consecuencia, establecimos una política que solo permite el protocolo de comunicación TCP/IP para estos dispositivos. Cuando eliminamos todos los demás protocolos, el tráfico de red disminuyó de forma considerable», explicó Harris.

Armis también descubrió las cámaras Hikvision, producidas por Hangzhou Hikvision Digital Technology Co., Ltd., fabricante y proveedor de equipos de vigilancia por vídeo para fines civiles y militares que pertenece al gobierno chino. Armis ayudó a Harris a supervisar las comunicaciones salientes y le permitió aislar estos dispositivos para evitar que actividades potencialmente maliciosas se propagaran por la red de la universidad.

Ajustes dañados o vulnerabilidades 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 potencian a Armis

Harris y su equipo integraron Armis con soluciones clave de la pila tecnológica de la universidad, lo que incluye a Microsoft Defender para la protección antimalware, VMware para habilitar instancias de virtualización, Tenable para el análisis de vulnerabilidades, Microsoft InTune para la gestión de dispositivos corporativos y BYOD, Microsoft SCCM para la gestión de la configuración y firewalls de Palo Alto Networks. Según lo describe Harris, todas estas integraciones permiten que Armis realice mejor su trabajo.

«Si algo activa la integración del firewall de Armis-Palo Alto Networks, el firewall lo bloquea e impide que salga, y eso es muy ingenioso», remarcó. En este caso práctico, Harris configuró la capacidad de cuarentena autorizada automatizada en el firewall de Palo Alto Network. Incluso si la alerta es un falso positivo, para su equipo es fácil despejarla. La integración del firewall de Armis- Palo Alto Networks elimina el tiempo y el esfuerzo que se necesitan para entrar en el firewall, realizar cambios y volver a cargar.

Resultados de Armis

- Visibilidad de todos los dispositivos — gestionados, no gestionados e IoT— en ambos campus
- Corrección más rápida basada en información procesable sobre la postura y el comportamiento de seguridad de los dispositivos
- Detección y respuesta automatizadas gracias a las integraciones

Armis simplifica la visibilidad interna, la gestión de activos y la seguridad

Como señala Harris, su equipo efectuó un trabajo admirable para mantener a la universidad a salvo de amenazas externas. Pero mantener segura a la universidad frente a amenazas internas potencialmente maliciosas —que no suelen ser intencionales— ha sido todo un reto, ya que los estudiantes y los profesores utilizan dispositivos personales que no siempre están actualizados con los sistemas operativos y las protecciones de seguridad más recientes.

Armis ha simplificado de forma notable esa tarea para Harris y su equipo, ya que no solo supervisa de modo pasivo los dispositivos de la red para detectar comportamientos maliciosos, sino que también cataloga una gran cantidad de información sobre ellos, desde la dirección IP y el sistema operativo hasta el tipo de conexión y los dominios de Internet a los que se accedió. Y esto también se aplica a la IoT. Armis ayudó al equipo a identificar y retirar dispositivos IoT obsoletos.

Para la gestión de activos, Harris utiliza Snipe-IT, de código abierto. Armis funciona sin problemas con este software y permite a Harris mantener actualizado su inventario. Harris señaló que es fácil realizar escaneos con Armis y clasificar los dispositivos por categorías.

«Todos los ordenadores de nuestra universidad son de determinados modelos, y Armis realiza un gran trabajo al crearles las huellas digitales. Podemos introducir los datos de los activos de modo directo en nuestro software de gestión y asegurarnos de que los dispositivos estén debidamente actualizados con el sistema operativo y los parches de seguridad más recientes», observó. «Si alguien me pregunta por un dispositivo determinado, puedo averiguar en minutos dónde está con exactitud, qué estuvo haciendo y con qué se comunica. Armis nos ha hecho la vida mucho más fácil y nuestro campus mucho más seguro».

Resultados de Armis

- Adherencia al cumplimiento de la normativa
- Mejora de la postura de seguridad para cumplir con los requisitos del seguro de ciberseguridad
- Menor carga para el equipo de TI.

Superación de los obstáculos del cumplimiento de la normativa y el seguro de ciberseguridad

Armis también ayudó a que la universidad satisficiera los estrictos requisitos de seguro de ciberseguridad. En el pasado reciente, Harris y su equipo contrataron un servicio de evaluación de la seguridad para que les ayudara a comprender su postura de seguridad y su puntuación de riesgo. La universidad obtuvo una buena puntuación en casi todos los parámetros, excepto en el hecho de que se utilizaban muchos dispositivos y navegadores antiguos, sobre todo por parte de los estudiantes. Pero el servicio no proporcionó más información sobre los dispositivos. En cambio, Armis amplía la visibilidad del equipo, le permite desglosar los detalles de los dispositivos y adoptar medidas correctivas. Por ejemplo, si Harris ve un dispositivo con un navegador antiguo, puede enviar al usuario una advertencia y pedirle que actualice el navegador.

Como cualquier institución educativa, a Russell Sage se le solicita que cumpla con la Ley de Derechos Educativos y Privacidad de la Familia (FERPA), que protege la privacidad de los expedientes educativos de los alumnos. Por cada dato de los estudiantes que se vea comprometido, las universidades pueden recibir multas de hasta USD 100 000. El centro de bienestar de la universidad también debe cumplir con la Ley de Portabilidad y Responsabilidad de Seguros de Salud (HIPAA, Health Insurance Portability and Accountability Act), que protege la información confidencial de los pacientes. Dado que Armis se ajusta a los controles de seguridad crítica estándares del sector del Centro para la Seguridad de Internet (CIS, Center for Internet Security), ayuda a la universidad a cumplir estos requisitos. Por ejemplo, si hay un Número de Seguro Social que va por el cable, Armis proporciona visibilidad inmediata de esos datos y bloquea el tráfico.

«Si alguien me pregunta por un dispositivo determinado, puedo averiguar en minutos dónde está con exactitud, qué estuvo haciendo y con qué se comunica. Armis nos ha hecho la vida mucho más fácil y nuestro campus mucho más seguro».

John Harris
Subdirector de Informática e Ingeniero en Sistemas
Russell Sage College

Planes para el futuro: aprovechar todo el potencial de Armis

En la agenda para el futuro figura aprender a aprovechar más las capacidades de Armis y encontrar nuevos casos para él.

«Apenas hemos visto lo que Armis puede hacer, y deseamos explorar su funcionalidad con mayor profundidad y pasar más tiempo con él. Prácticamente hemos recolectado todos los frutos maduros, y ahora nuestro objetivo es seguir mejorando el uso de Armis», remarcó Harris.

También sabe que, a medida que él y su equipo profundizan en el conocimiento y el uso de la plataforma, la ayuda está siempre a mano. «Estoy muy impresionado por el equipo de asistencia de Armis. Si alguna vez tengo un problema, se ocupan de él y no cierran el asunto hasta que estemos contentos con la resolución», dijo Harris.