Anuncios

S21Sec automatiza la respuesta a incidentes de seguridad con IBM Resilient

Madrid - 01 oct 2019: Cuando se trata de la respuesta a incidentes de ciberseguridad, la velocidad lo es todo: los incidentes de ciberseguridad que tardan más de 30 días en contenerse cuestan un millón de dólares más que los que se detienen dentro del periodo de 30 días (1).

Por esta razón, cada vez es más importante que las empresas cuenten con un equipo especializado y tecnológicamente preparado para responder a incidentes, ya que es uno de los factores que más reduce el coste derivado de un ciberataque (2).

S21Sec, empresa dedicada a los servicios de ciberseguridad con más de 500 expertos, ha confiado en la tecnología IBM Resilient para automatizar y orquestar la respuesta ante incidentes de seguridad, permitiendo que los profesionales expertos de seguridad de S21Sec puedan centrarse en tareas más estratégicas y resolver los incidentes graves más rápido.

S21Sec cuenta con un Centro de Operaciones de Seguridad (SOC) en funcionamiento durante las 24 horas del día, un equipo de emergencias de respuesta ante incidentes de seguridad, y una colaboración precisa con instituciones tales como Europol o el FBI. El objetivo fundamental de S21Sec consiste en ayudar a las organizaciones a alinear la ciberseguridad con su visión de negocio, objetivos y proyectos de innovación. En esta línea, ofrece diferentes servicios de seguridad, que van desde la protección de infraestructuras críticas y datos de las personas hasta soluciones para la securización de la información y los procesos. Sus clientes son principalmente gobiernos, infraestructuras críticas de energía, instituciones financieras o empresas de telecomunicaciones.

“S21sec es una de las mayores empresas de servicios de ciberseguridad de Europa, la primera en tener un SOC (Security Operation Center) para servicio a clientes en 2006, y la primera en contar con la certificación CERT en 2009. Actualmente el SOC de S21sec gestiona y monitoriza una media de 12.000 ciberamenazas diarias que ocurren dentro y fuera de España”, subraya Jorge Hurtado, vicepresidente de Servicios Gestionados y CSO de S21sec.

Mediante la implementación de IBM Resilient en su SOC, S21Sec va a poder coordinar la respuesta ante cualquier incidente de forma automatizada y dinámica ganando en rapidez y eficacia. Ante un ataque, el tiempo es vital para bloquear una brecha de seguridad y fuga de datos. Con IBM Resilient, S21Sec va a pasar de minutos a segundos para orquestar la necesaria implicación de los diferentes equipos de profesionales y recursos afectados: desde la evaluación del incidente, implicaciones técnicas y legales, atención al cliente o comunicación externa.

Estos son los pasos que con IBM Resilient S21Sec es capaz de automatizar ante un incidente de seguridad:

- Identificación de la amenaza: S21Sec va a integrar el proceso de respuesta a un incidente de seguridad con QRadar, la plataforma tecnológica de IBM capaz de identificar avanzados ataques cibernéticos gracias a sus capacidades de analítica de datos. Sin la tecnología adecuada una amenaza puede tardar en detectarse meses. Una vez identificada la amenaza, IBM Resilient en coordinación con QRadar procederán a realizar en pocos minutos, de manera automatizada, una investigación inicial para definir conceptos generales del incidente, impacto, severidad, activos afectados, personas involucradas, y servicios de negocio afectados.
- Una vez obtenida una visión general de la incidencia, S21Sec se centra en la contención y la respuesta, donde el objetivo es minimizar y parar el incidente lo antes posible a partir de una excelente coordinación entre las actuaciones de las personas y de la tecnología. La solución IBM Resilient es capaz de automatizar tareas repetitivas -desde mandar un email, hasta bloquear un dispositivo perdido, cambiar una contraseña de una cuenta de correo potencialmente contaminada, etc-. Si en el proceso de evaluación inicial se identifica que se trata de un problema menor, la

automatización de la respuesta permite que los profesionales expertos de seguridad de S21Sec puedan centrarse en tareas más estratégicas y resolver los incidentes graves más rápido. En términos generales, gracias a la automatización de todo el proceso con estas tecnologías, se reduce considerablemente el tiempo desde que salta la primera alerta de una brecha de seguridad hasta que se cierra.

- Por último, una vez detenido el incidente y resuelto, IBM Resilient es capaz de realizar un análisis del evento, de la respuesta ante este y de las lecciones aprendidas. Adicionalmente, IBM Resilient ayudará a los clientes de S21Sec a cumplir con la normativa GDPR: la solución incluye en el proceso de respuesta ante incidentes y de manera sencilla, qué pasos son necesarios realizar para la notificación a reguladores. Esto es crítico y exigido en varias regulaciones que obligan que las empresas afectadas por un incidente con datos personales notifiquen dentro de las primeras 72 horas del incidente.

Ante un creciente número de ataques de ciberseguridad y cada vez más sofisticados, este acuerdo de S21Sec con IBM, supone un avance extraordinario para resolver y minimizar el impacto de las ciberamenazas en los clientes, gobiernos, infraestructuras críticas, financieras y por tanto, en el conjunto de la sociedad.

(1). IBM/Ponemon Institute Report. https://newsroom.ibm.com/2019-04-11-IBM-Study-More-Than-Half-of-Organizations-with-Cybersecurity-Incident-Response-Plans-Fail-to-Test-Them

(2). IBM/Ponemon Institute Report. https://newsroom.ibm.com/2019-04-11-IBM-Study-More-Than-Half-of-Organizations-with-Cybersecurity-Incident-Response-Plans-Fail-to-Test-Them

Contacto(s)

Patricia Núñez Canal

IBM Comunicación Externa +34 91 3977782 patricia.nunez@es.ibm.com