NOTA DE PRENSA

SARENET COMPLETA SU OFERTA DE SEGURIDAD CON Intercept X DE SOPHOS

-Añade otra capa a sus soluciones de seguridad gestionada adaptable y configurable a las necesidades de cada cliente.

-End-Point Intercept X de Sophos utiliza la tecnología Deep Learning para hacer frente a amenazas, detener el ramsonware y repeler a los atacantes.

Zamudio, 22 de enero de 2019.- Sarenet (https://www.sarenet.es), el operador de voz y datos y servicios de alojamiento, especializado en empresas y con más experiencia de cuantos hoy desarrollan su actividad en España, ha firmado un acuerdo de colaboración con **Sophos (https://www.sophos.com)** para ofrecer a sus clientes una capa adicional a sus soluciones de seguridad gestionada.

Consciente de que los antivirus tradicionales no son suficientes para proteger los servidores y puestos de trabajo, **Sarenet** ha decidido dar un paso más con la incorporación de **End-Point Intercept X de Sophos,** una **tecnología predictiva** basada en **Deep Learning** para hacer frente a la más amplia variedad de **amenazas**, detener el **ransomware** y **repeler a los atacantes.** Esta solución viene a sumarse a la oferta de seguridad gestionada de **Sarenet,** donde destacan los cortafuegos tradicionales, los cortafuegos de aplicaciones y la defensa perimetral frente a ataques de denegación de servicio (DDoS).

El operador de telecomunicaciones empresariales apunta a **tres momentos** diferentes para protegerse de los virus informáticos, lo que desencadena la puesta en marcha de distintas estrategias de defensa. El primer estadio sucede **antes de la ejecución del virus**. En este nivel se utilizan las técnicas habituales en base a firmas descargadas del fabricante que identifica el fichero con un virus y puede evitar su descarga. Aunque esta defensa sigue siendo válida, **actualmente no es suficiente**, ya que los ficheros mutan muy rápidamente. Algunos fabricantes, como es el caso de **Sophos,** dan un paso más allá e implementan técnicas que permiten identificar que el fichero aún sin disponer de la firma o sin ser conocido es un virus.

El segundo estado está relacionado con la post ejecución del virus. Las técnicas para inocular un virus son cada vez más sofisticadas y, utilizando ingeniería social o un simple mensaje falso, **se puede llegar a ejecutar el virus en los equipos**. Aquí es donde **Intercept X de Sophos** es realmente atractivo. Las técnicas que se emplean tienen que

ver con las que utilizan los virus para hacerse con el control. En la actualidad **Intercept X es capaz de detectar el mayor número de vectores del mercado**.

Existe un último estadio que tiene que ver con la **post explotación de un PC infectado.** Por ejemplo, las redes de ordenadores que atienden instrucciones externas para envíos de mensajes o ataques de denegación de servicios. Incluso en este punto, **Intercept X** es capaz de detectar tráficos extraños y ofrecer protección.

Deep Learning aplicado a la Ciberseguridad

Intercept X se basa en una tecnología predictiva diseñada para proteger no solo contra las amenazas conocidas, sino también contra las amenazas nunca antes vistas. Con la potencia de sus funciones avanzadas y de la tecnología **Deep Learning**, permite hacer frente a la más amplia variedad de **amenazas** y detener el **ransomware**, con una tecnología especialmente diseñada para bloquear el cifrado malicioso de archivos y del registro de arranque maestro. También **repele a los atacantes,** privándoles de las herramientas y técnicas de las que dependen para llevar a cabo sus acciones.

Sophos aplica el **Deep Learning a la ciberseguridad** utilizándolo para determinar si un archivo es benigno (benignware) o malicioso (malware). No utiliza firmas, sino que extrae millones de atributos de un archivo, lo ejecuta a través de su modelo de **Deep Learning** y determina si es benigno o malicioso en función de sus atributos.

Intercept X también incluye el análisis de causa raíz para ofrecer una visión inmediata de las amenazas, así como la eliminación instantánea de malware para garantizar que no quede ningún remanente del ataque, lo que le convierte en la protección para **endpoints** más completa del mercado. **Intercept X** funciona además de forma paralela a los productos antivirus tradicionales de **Sophos** y de otros fabricantes. De esta forma, si un antivirus ya instalado no detecta un fichero infectado **IntercepX** puede frenar su ejecución.

Con esta incorporación **Sarenet** completa su oferta de seguridad gestionada y cumple con las **nuevas normativas legales o requerimientos del Esquema Nacional de Seguridad,** que obligan a retener la información necesaria para monitorizar, analizar e investigar las actividades indebidas o no autorizadas. En estos casos, el complemento **EDR** (End Point Detection and Response) permite realizar un análisis forense sencillo y detallado. De forma gráfica, permite ver quién, qué, cuándo, dónde y cómo sucedió el incidente de seguridad.

Para más información:
Alex Etxebarria
alex.etxebarria@sarenet.es
609 32 48 19