Sophos email security

Vamos a hablar el día de hoy sobre Sophos email security, un producto de última generación de esta compañía afamada de seguridad.

En HostDime nos interesamos por ser líderes de opinión para nuestros lectores y clientes; es así como al analizar algunos problemas reportados por clientes de servidores de correo, decidimos solicitar un webinar para explorar soluciones avanzadas y protección de nueva generación para los correos y las cuentas de correos; en esta ocasión, nos acompañó Juan Felipe Micolta Lopez , Presales engineer de Licencias Online y Sophos, para esta perspectiva didáctica de dicho producto.

Los ataques vía correo electrónico son de los más persistentes a lo largo del tiempo.

El 53% es phising, el 41% data breach, el 35% malicious code, el 35% software exploit, el 30% Ransomware, el 21% credential deft.

Los sistemas tradicionales de seguridad online para correos electrónicos, están en condiciones de detener 5 de 10 posibles ataques, lo cual deja una abanico muy amplio, un margen de error muy importante que aprovechan los ciberdelincuentes.

La estrategia global usada por la compañía es llamada smart email security que incluye seguridad predictiva con inteligencia artificial, protección de datos sensitivos y protección contra fraude mediante phising.

El sandbox de este sistema inteligente en la nube permite aislar y controlar efectivamente este tipo de amenazas. Otro de los muchos componentes destacados puede ser la

características de reputation checks, sender authentication, header anomalies, anti spam y antivirus, delay queue, la verificación de las urls y la seguridad sincronizada.

Durante la charla se enfatizó en la modularidad y la integración de todas las soluciones de Sophos y como desde Sophos central se puede orquestar su funcionamiento.

De nuevo, al igual que en la charla sobre seguridad endpoint, se hace bastante énfasis en lo crucial del desarrollo de estos productos sobre deep learning, una tecnología superior a la ofrecida por otros proveedores del mercado que se quedaron en machine learning. Esto evita que proliferen los falsos positivos y que se pierda menos tiempo y recursos de la compañía.

Phishing

El phishing es una realidad tecnológica que no podemos eludir; el asunto no es cerrar los ojos para no verlo sino entenderlo para tomar las medidas de rigor frente a este fenómeno de seguridad online. Pero no es la única amenaza reportada por este medio del correo electrónico.

Bloqueo de impostores

Utilizando técnicas de procesamiento de lenguaje natural (una sofisticada extensión de la inteligencia artificial) , Sophos neutraliza a los impostores evitando que los correos comerciales se vean comprometidos. El software en la nube detecta los blancos más expuestos, escanea el correo entrante y analizar las posibles variantes de nombres y expresiones para impedir este tipo de acciones.

Autenticar remitentes

No solo se emplea la ingeniería social sino que se fortalece su accionar preventivo contra la suplantación de marca, el Spf, Dkim, Dmarc más el análisis exhaustivo de los encabezados de los correos electrónicos, entre otras cosas.

Ataques avanzados

Algunos de los ataques sofisticados al o desde un correo electrónico incluyen: suplantación de la marca (correo enviado desde una cuenta genérica), suplantación de personas al interior de la organización, suplantación del nombre de dominio y, cuenta comprometida.

Si alguno de nuestros clientes pudiera necesitar este producto de seguridad de última generación, lo puede adquirir con nosotros. Contáctenos para ampliar la información.

Video webinar

Leer también: De donde proviene, nace el término Spam, de donde salió el nombre, cual es su origen ; Configure su plan de Recuperación de Desastre en 7 pasos ;