INFO & INSIGHTS

RETOS TECNOLÓGICOS:

4 COSAS QUE EL ANTIVIRUS NO HACE

Las organizaciones luchan para protegerse contra las brechas de seguridad. Implementan distintas herramientas y soluciones de seguridad para proteger sus redes, aplicaciones, nube y endpoints.; se esfuerzan para cumplir con cumplimientos normativos; sus equipos de seguridad trabajan para registrar minuciosamente un sinfín de alertas de seguridad y aun así, existe un incremento en brechas de seguridad y pérdida de datos.

¿Por qué?

La respuesta se debe a que las amenazas y los ciberatacantes han evolucionado, mientras que muchas soluciones de seguridad no lo han hecho. Las amenazas se han hecho más sofisticadas, autónomas, de fácil ejecución y sobre todo mutan en segundos, pues se enfocan en crear nuevas familias, todo esto en cantidades mayores a las que las organizaciones están preparadas para poder combatir. Y cómo no, si varias de las herramientas de seguridad, soluciones y plataformas mantienen las mismas prácticas desde hace décadas. El antivirus es el ejemplo perfecto de esto, pues al no tener las firmas actualizadas se abren diferentes brechas de seguridad. Detrás de todo esto se encuentran los cuatro retos tecnológicos principales que el AV no está atendiendo y que para una estrategia de seguridad efectiva se deben contemplar.

1 Las brechas de seguridad se están incrementando y así van a continuar.

El antivirus no hace la detección de nuevas brechas de seguridad.

En el esfuerzo para frenar las brechas y la pérdida de datos, las organizaciones implementan numerosas soluciones de seguridad y de software. Desafortunadamente, muchas de estas soluciones y antivirus tradicionales trabajan de forma reactiva por lo que la mayoría de las veces no tienen éxito al proteger los sistemas. Esto da como resultado un incremento en la frecuencia con la que se presentan brechas de seguridad, tanto en variedad como en sofisticación.

La industria de seguridad se enfoca principalmente en proporcionar detección y tiempos de respuesta de forma eficaz a través de una ventana de tiempo en donde se especifica cuando el ataque sucede y cuando el ataque es detectado.

Ante este escenario el antivirus tradicional es una solución pobre frente a la necesidad de proteger la información más valiosa o crítica de la organización, antes de que sea vulnerada. Con el propósito de reducir la frecuencia e impacto de las brechas de seguridad, debe existir un cambio entre la detección y la respuesta a incidentes para prevenir que las brechas de seguridad sean aprovechadas en una organización.

2 Los antivirus ya no son soluciones suficientemente efectivas para prevenir ciberataques.

El antivirus no hace un análisis de comportamiento sospechoso.

Los ciberdelincuentes han tomado ventaja de herramientas gratuitas y baratas que se encuentran disponibles para generar nuevos tipos de malware, únicos o poli fórmicos y aquellos que además pueden viajar de forma cifrada, lo que los hace ser capaces de evadir la detección del antivirus tradicional basado en firmas. Hoy los ataques aprovechan exploits desconocidos y de día cero para evadir la protección de un AV.

Para protegerse contra las tácticas que aprovechan los cibercriminales a fin de pasar desapercibidos por el antivirus, debes contar con una solución efectiva de protección a nivel

endpoint, capaz de proteger tus computadoras contra malware, amenazas o exploits conocidos y desconocidos.

3 El incremento de la movilidad requiere que las organizaciones aseguren sus equipos endpoint bajo una estrategia integral que va más allá de la protección tradicional al perímetro de la red.

El antivirus no hace nada ante el uso de aplicaciones SaaS.

Las organizaciones están utilizando soluciones SaaS Software-As A-Service de almacenamiento basadas en la nube para conectar recursos internos desde cualquier parte del mundo, dentro y fuera del perímetro de la red de la organización. Estos servicios se sincronizan y distribuyen archivos a través de todos los usuarios en la organización, incrementando la forma en la que los datos se procesan y se comparten también se expone potencialmente a toda la empresa ante exploits y malware. Además, existe el riesgo de la exposición y las amenazas en aplicaciones SaaS, cómo pueden ser la propagación de malware, exposición accidental y la ex filtración mal intencionada.

El objetivo de los ciberataques son los usuarios finales y los equipos endpoints de la red que no tienen completa visibilidad, así los empleados fuera de la red de la organización son más vulnerables al incontable malware avanzado. Para mitigar estas amenazas, la solución de seguridad debe proteger los sistemas más allá del enfoque tradicional de asegurar el perímetro de la red.

4 Para las organizaciones es un reto lidiar con la gestión de parches, proteger software y sistemas sin parches disponibles o en situación EoL (end of life) resulta complejo.

El antivirus no hace la gestión parches o situaciones EoL

Las vulnerabilidades en aplicaciones y sistemas no son inesperadas sino todo lo contrario, pues existen desde mucho antes de que los parches entraran a una etapa de EoL. Ahí el problema, la implementación de parches ya sean críticos o no, no está garantizada.

Ante esta situación, las organizaciones que operan con sistemas y software descontinuados que ya han alcanzado su fin de vida (EoL) quedan vulnerables, lo que deja expuestas a las

organizaciones ante riesgos desconocidos y difíciles de mitigar. Situaciones como éstas dan a los cibercriminales la oportunidad de utilizar estas vulnerabilidades y comprometer aplicaciones o sistemas no parchados.

Con el creciente número de vulnerabilidades de software que se descubre día tras día, y con los kits de exploits disponibles en el mercado negro, aún los atacantes sin mucha experiencia tienen la habilidad de ejecutar ataques sofisticados. Para proteger sistemas y software descontinuados o sin parches disponibles, debes contar con una solución efectiva que sea capaz de protegerte contra la explotación de vulnerabilidades tanto conocidas cómo desconocidas.

Si quieres conocer cómo puedes defenderte de las amenazas protegiendo de forma eficaz tus equipos endpoint, se parte del Entrenamiento de Defensa Integral Hands On con Grupo Smartekh y Palo Alto Networks

IMPLEMENTAR UNA ESTRATEGIA DE PROTECCIÓN A NIVEL ENDPOINT VALE LA PENA

Para todas las organizaciones. No se trata sólo de detectar riesgos para tu negocio, se trata de reducir la superficie de ataque para que las amenazas se ejecuten en tu negocio.