SAM para la Ciberseguridad

LAST CALL

Esta generación de entornos de TI está siendo fuertemente influenciada por cuatro factores clave: soluciones en la nube, dispositivos móviles, redes sociales y grandes bases de datos, que están impulsando una transformación dentro de la mayoría de las organizaciones. Al mismo tiempo, los riesgos de seguridad y las amenazas cambiantes están creciendo rápidamente. Un estudio de IDC estimó que, en 2014, las empresas gastarían $491 mil millones debido al malware asociado con el software pirateado.

Ciberseguridad SAM Engagement

Éste se centra en brindar una vista del software desplegado en su entorno para identificar áreas de riesgo potencial y proporcionar orientación de alto nivel sobre sus programas y políticas de seguridad cibernéticas para ayudar a habilitar la gestión adecuada de activos de software de TI.

Con un crecimiento e innovación sin precedentes en tecnología de la información y un mundo cada vez más conectado, las apuestas en torno a la ciberseguridad están aumentando.

El SAM Engagement de ciberseguridad brinda análisis sobre la madurez del programa de ciberseguridad de su organización en relación con los diferentes modelos disponibles, como los Controles Críticos de Seguridad (CSC) publicados inicialmente por el Consejo de Seguridad Cibernética o el Modelo de madurez de Ciberseguridad de Microsoft. Sin embargo, para que un programa general de ciberseguridad sea efectivo, es necesario tener primero una comprensión de su infraestructura de TI y cómo se conecta con otras organizaciones, como su socio financiero, proveedores, proveedores y clientes. Estos son algunos desafíos que puede estar enfrentando y algunos de los beneficios que puede obtener al trabajar con un socio de Microsoft SAM en un compromiso de SAM de seguridad cibernética.

Retos

Los entornos modernos de TI pueden ser complejos, aumentando el riesgo de ciberseguridad debido a:

- Software antiguos que ya no son compatibles
- Descarga de malware sin saberlo a través de descargas digitales no genuinas o compras en línea de proveedores desconocidos
- Los medios extraíbles como las unidades flash utilizadas para instalar software inadecuado
- Dispositivos personales no autorizados que se conectan a la red corporativa
- Terminó vendedores o empleados que siguen teniendo acceso a los sistemas de TI

Oportunidades

La implementación de mejores prácticas y procedimientos de seguridad cibernética te ayudarán en:

- Administrar de forma segura los activos de software y promover prácticas adecuadas de seguridad cibernética
- Construir una infraestructura de TI flexible y adaptable que pueda responder rápidamente a las amenazas
- Podrás asegurarte de tener una infraestructura de TI segura que proporcione una defensa eficaz contra los ataques
- Minimizar la pérdida de datos, el fraude por robo y el tiempo de inactividad de los empleados, lo que redunda en una disminución de los costos y una mayor eficiencia

Que esperar de un SAM Engagement

Cada compromiso será ligeramente variado dependiendo de su infraestructura, necesidades y metas. A un nivel alto, un compromiso puede desglosarse en cuatro fases: planificación, recolección de datos, análisis de datos y presentación final.

Planificación La fase de planificación consiste en recopilar información de su infraestructura y en identificar los planes y objetivos, establecer citas y organizar el acceso para comenzar la recopilación y el análisis de datos.

Recopilación de datos Consiste en el ensamblado de toda la información relacionada con el descubrimiento e inventario de activos de software, usando una herramienta de inventarios seguido por el mapeo de datos de inventario, uso y los derechos de licencias. Además, incluye la recopilación de datos relacionados con las recomendaciones de evaluación de la seguridad cibernética. Pueden emplearse cuestionarios y entrevistas con las principales partes interesadas para asegurar que se recopilan todos los datos e información pertinentes para proporcionar un análisis completo y preciso.

Análisis de datos La fase de análisis de datos incluye la revisión y validación de todo el uso recopilado, derechos de licencia, despliegue y otros datos. También se realizará un análisis de su actual estado de ciberseguridad en comparación con su estrategia a largo plazo y sus metas. Durante esta fase, los resultados incluirán una evaluación de las vulnerabilidades potenciales de su empresa y la madurez general de la seguridad cibernética y ofrecerán recomendaciones sobre cómo minimizar su riesgo de ciberseguridad.

Recomendaciones finales Al concluir el compromiso SAM, su socio SAM presentará sus resultados, recomendaciones y próximos pasos en una presentación general junto con un conjunto de informes detallados.

Microsoft

LAST CALL