SAM para la Ciberseguridad

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

Migesa GRUPO MIGESA

Recolección de datos y análisis

El objetivo al interpretar sus datos de inventario es detectar qué activos necesitan ser protegidos y localizar áreas que plantean riesgos, incluyendo conexiones a sistemas externos como su socio bancario, proveedores de la cadena de suministro y clientes. Su Microsoft Certified SAM Partner identifica áreas de mejora y desarrolla un conjunto de recomendaciones y procesos para ayudar a su empresa a optimizar sus inversiones de software y mantenerse en conformidad. La recopilación y el análisis de datos incluirán las categorías definidas a continuación.

Inventario de activos
Como punto de partida, su socio SAM trabajará con usted para elegir las herramientas adecuadas, definir el alcance de las máquinas que se van a inventariar, identificar los pasos adicionales necesarios para recopilar datos de dispositivos y redes que no sean fácilmente accesibles y preparar entornos Para escanear y recopilar datos. Las herramientas de inventario utilizadas deben recopilar una amplia gama de puntos de datos para incluir cualquier máquina que esté ejecutando software obsoleto o no compatible. Una vez que el inventario esté completo, su socio SAM trabajará con usted para llevar a cabo la evaluación de la seguridad cibernética.

Interpretación de datos y requisitos técnicos
El análisis de los resultados de la recopilación de datos de inventario implica la identificación y documentación de todas las implementaciones de productos, el uso y los derechos de licencia. Su socio consolidará los datos recolectados de diferentes herramientas de inventario y mapeará los datos a la información crítica que le apoya para tomar decisiones informadas. Por ejemplo, asignar datos de implementación a los ciclos de vida de soporte del producto le proporcionará información sobre cuándo es necesario actualizar el software. Su socio también analizará cómo se controla actualmente el software y el acceso a la red.

Consideraciones sobre la implementación
Su Partner identificará cualquier cambio potencial que deba implementarse para disminuir su riesgo de seguridad cibernética. Esto puede incluir instalar regularmente actualizaciones de seguridad, mantener el software antivirus activo y actualizado con las versiones más recientes del software y empezar a supervisar y administrar el uso de dispositivos personales en el trabajo.

Consideraciones sobre la concesión de licencias
Para identificar las necesidades de licenciamiento, tu Partner te ayudará a evaluar si tienes la licencia adecuada para el uso de dispositivos móviles, así como determinar las mejore opciones de licenciamiento para alinearse con sus planes futuros del negocio basados en la información recopilada durante el análisis.

Mejoras de Políticas
Otro aspecto importante de cualquier programa de seguridad cibernética es el de ser proactivo para evitar los riesgos asociados con las amenazas cibernéticas estableciendo políticas en torno a la piratería de software, malware, robo de información, fraude y otras formas de ciberdelincuencia. Su SAM Partner le ayudará a definir e implementar políticas y procesos para administrar un programa de seguridad cibernética en curso.

Entregables

Antes de iniciar el proceso, usted recibirá una carta compromiso y una declaración completa de que esperar durante su proceso de SAM. Al termino del ejercicio usted recibirá los reportes detallados a continuación.

Informe General Ejecutivo	Contiene un resumen ejecutivo de alto nivel del alcance del ejercicio, los resultados, recomendaciones y los próximos pasos.
Despliegue Establecido	Proporciona detalles relacionados con todo el software desplegado actualmente dentro de tu infraestructura de IT.
Posición Efectiva de Licencia (ELP)	El informe ELP proporciona detalles relacionados con los derechos de licencia que se asignan a los despliegues e identifica los gaps o subutilización en la organización.
Informe de Evaluación SAM de Ciberseguridad	Este informe incluye una evaluación de su madurez global de seguridad cibernética y recomendaciones para minimizar los riesgos que su empresa enfrenta al combatir las amenazas cibernéticas.
Informe de Optimización de Licencias	Este informe proporciona recomendaciones sobre cómo optimizar su programa de licencias de Microsoft y estructura para su empresa. El informe detalla los riesgos, responsabilidades y oportunidades de las prácticas actuales de licencias de su empresa y recomendaciones sobre cómo administrar mejor sus licencias para minimizar el riesgo futuro y alinearse con su estrategia de seguridad cibernética.
Usos Adicionales del Reporte de Datos	El Informe de Usos Adicionales de Datos incluye recomendaciones sobre cómo usar los datos que ya ha recopilado para otros propósitos, como el desarrollo de un mapa de virtualización, un plan de migración de nube o una evaluación de cargas de trabajo de SQL.

Qué es Software Asset Management

http://www.microsoft.com/en-us/sam/overview.aspx

Microsoft