sedian

Seguridad Digital
de Andalucía

Métricas relevantes de seguridad

28 de Mayo de 2021

Junta de Andalucía

¿Qué son las métricas de seguridad?

Las métricas de seguridad o métricas de ciberseguridad son un valor medible que demuestra lo bien que una empresa está logrando sus objetivos de reducción de riesgos de ciberseguridad. Las organizaciones usan métricas de seguridad en múltiples niveles para evaluar cómo están cumpliendo con sus estándares de seguridad y requisitos de administración de seguridad de la información.

¿Qué son las métricas de seguridad?

Las métricas de seguridad de alto nivel pueden centrarse en el rendimiento general de la organización y generalmente son propiedad del Director de Seguridad de la Información (CISO) o CTO y se comparten con la alta gerencia, mientras que las métricas de seguridad de bajo nivel pueden centrarse en pruebas de penetración, escaneo de vulnerabilidades, capacitación en seguridad y resultados de evaluación de riesgos. Las métricas de bajo nivel generalmente son propiedad de equipos de seguridad formados por profesionales de seguridad que informan al CISO.

¿Qué son las métricas de seguridad?

Si bien el objetivo principal de las métricas de seguridad es evaluar cómo la organización está reduciendo el riesgo de seguridad, también hay diferentes métricas que pueden proporcionar información sobre el rendimiento del programa en si. Estas métricas a menudo son proporcionadas por herramientas de seguridad diseñadas para proporcionar comentarios procesables en tiempo real.

Independientemente de las métricas que elijas, recuerda que deben ser cuantificables e influir en el comportamiento diario, así como en la estrategia a largo plazo. También deben cumplir con los marcos de seguridad de la información, seguridad de los datos, seguridad móvil y seguridad de la red.

¿Qué son las métricas de seguridad?

Necesitas tener métricas para evaluar la efectividad de los controles de seguridad en los que has invertido.

Las métricas de seguridad son importantes por **varias razones principales:**

El análisis de los indicadores clave de rendimiento (KPI), los indicadores clave de riesgo (KRI) y las posturas de seguridad proporcionan una instantánea de cómo funciona tu equipo de seguridad con el tiempo.

¿Qué son las métricas de seguridad?

Esto te ayuda a comprender mejor que está funcionando, que activos de tecnología de la información están en mayor riesgo y que áreas están empeorando. Esta información ayuda en la toma de decisiones en torno al presupuesto, las personas y la inversión en tecnología.

Las buenas métricas brindan información cuantitativa que puedes usar para mostrarle a la gerencia, a los miembros de la junta, a los clientes e incluso a los accionistas que te tomas en serio la confidencialidad, la integridad y la disponibilidad.

¿Cuales son los KPI o indicadores de seguridad?

Estos siete principios te ayudarán a elegir las métricas de seguridad adecuadas para tu organización:

Propósito: las métricas deben respaldar los objetivos comerciales y los requisitos reglamentarios, conectar las métricas a la empresa puede ayudar con la aceptación de las partes interesadas y garantizar que los recursos se utilicen de manera eficiente.

Controlabilidad: para que las métricas valgan la pena, deben demostrar que se está cumpliendo un objetivo. Por lo tanto, las métricas deben medir procesos y resultados controlables.

Contexto: Responde preguntas como «¿por qué lo estamos recopilando?», «¿Qué historia cuenta?» Y «¿cómo se compara esto con nuestra industria?»

¿Cuales son los KPI o indicadores de seguridad?

Mejores prácticas: sé consciente de lo que estás tratando de lograr y cómo se ve la mejor métrica de su clase.

Cuantitativo: las métricas deben ser cuantitativas para que puedan compararse a lo largo del tiempo y las organizaciones. Dicho esto, el contexto cualitativo en torno a resultados clave objetivos (OKR) es muy importante.

¿Cuales son los KPI o indicadores de seguridad?

Calidad de los datos: las métricas son tan buenas como los datos que se utilizan para crearlas, aseguran que tengan un alto nivel de precisión y fiabilidad.

Facilidad de recopilación y análisis: la mejor métrica es inútil si no puede recopilar y analizar fácilmente los datos necesarios. No debería llevarte mucho tiempo preparar e informar tus métricas. Idealmente, debes tener un tablero siempre actualizado que cualquier persona de tu organización pueda ver.

Ejemplos de KPI

KPI: Número total de incidentes de seguridad

Medir el número total de incidentes de seguridad durante períodos de tiempo definidos (generalmente 1 mes y 1 año) puede brindarte un parámetro de comparación. Este KPI es fácil de calcular ya que es un conteo bruto de la cantidad de incidentes de seguridad en todas las partes de tu sistema. Cuando veas una mayor actividad, tu nivel de amenaza necesita aumentar.

KPI: Interacciones de los empleados

Monitorear las interacciones de los empleados, las conexiones remotas y los software en la nube pueden ayudarte a identificar posibles amenazas. Calcula este número haciendo que el software cuente cada vez que un empleado acceda a la red y el tiempo que permanecen en la red.

Ejemplos de KPI

KPI: Tiempo medio de identificación (MTTI) / Tiempo medio de detección (MTTD)

El tiempo medio de identificación (MTTI), también conocido como tiempo medio de detección (MTTD), mide cuánto tiempo se requiere para detectar una violación de seguridad.

Para calcular esta clase de KPIs de ciberseguridad, cuenta los días entre el comienzo de una interrupción del sistema, mal funcionamiento del servicio u otros problemas de seguridad y la identificación del problema. La violación puede ser detectada por el departamento de TI, equipo de DevOps o por una fuente externa.

Ejemplos de KPI

KPI: Tiempo medio de contención (MTTC) / Tiempo medio de resolución (MTTR)

El tiempo medio de contención monitorea la cantidad de tiempo que se requiere para contener una violación una vez que ha sido identificada. Este es el conteo de días entre que se identifica que existen problemas de seguridad y el momento en que se implementa la solución.

KPI: Costo por incidente

Para calcular este KPI, agrega tres categorías específicas. Los costos directos, como los costos forenses y de investigación, deben ser agregados a los costos indirectos, como el tiempo de recuperación y los costos para comunicar la violación. Finalmente, agrega la oportunidad perdida.

Ejemplos de KPI

KPI: Disponibilidad / Inactividad

La disponibilidad e inactividad simplemente se refieren a la frecuencia con la que tu sitio o software funciona (disponibilidad) o no (inactividad).

Generalmente esto se refleja en un porcentaje y los dos deben sumar un 100%. Por ejemplo, un 97% de disponibilidad/actividad significa que tu sitio web estuvo funcionando durante el 97% del tiempo dado (generalmente un mes) y tu software tuvo un tiempo de inactividad del 3% debido a actualizaciones o a un ataque.

Ejemplos de KPI

KPI: Cumplimiento

En muchas industrias, existen normas de cumplimiento que deben seguirse. Generalmente estas son rankings de terceros que son otorgadas a las compañías después de una revisión. La puntuación de seguridad de cada industria puede ser diferente y representarse en una escala de 0-10 o calificación de A-F.

Métricas que son útiles para medir nuestra seguridad

Resultados de los ataques de phishing simulados. Utiliza ataques de phishing simulados para evaluar que tan bien funciona la capacitación de concienciación y establecer objetivos de mejora.

Tiempo promedio de recuperación. Mide el porcentaje de usuarios afectados por un incidente, la rapidez con la que el equipo de seguridad resolvió el problema y si ese tiempo cumple, excede o no cumple con los tiempos fijados, basándose en el apetito de riesgo establecido por la organización.

Métricas que son útiles para medir nuestra seguridad

Tiempo promedio de detección. Se recomienda utilizar métricas como el tiempo promedio de detección, la medida del tiempo que transcurrió desde el momento en que se produjo un ataque con éxito hasta el momento de la detección, porque eso también indica que tan bien funciona un programa de seguridad y se le puede hacer un seguimiento para mostrar la mejora.

Prueba de penetración. Al igual que los ataques de phishing simulados, las métricas en torno a las pruebas de penetración indican que tan bien puede resistir una organización a tales eventos y rastrear las mejoras a lo largo del tiempo.

Métricas que son útiles para cubrir la normativa

Las métricas que elijas rastrear deben medir de manera efectiva la capacidad de tu organización para mantener los requisitos normativos y generales de protección de datos. Esto no solo es útil para mejorar tu programa de seguridad cibernética, sino que también puede ayudarte a evitar multas, demandas y otras sanciones.

Según la ENS dentro de su guía Esquema Nacional de Seguridad Métricas e Indicadores (CCN-STIC-815) podemos ver tanto métricas e indicadores a utilizar. (ver guía)

https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/525-ccn-stic-815-indicadores-y-metricas-en-el-ens/file.html

Métricas que son útiles para cubrir la normativa

RGPD

El Reglamento General de Protección de Datos (RGPD) de la Unión Europea es una ley extraterritorial diseñada para proteger la información de identificación personal (PII) de los ciudadanos de la UE.

Como ley extraterritorial, se aplica a cualquier organización que maneje datos de ciudadanos de la UE, independientemente de si están en la UE o no. Su objetivo es proporcionar a los usuarios un mayor acceso a sus datos confidenciales.

Métricas que son útiles para cubrir la normativa

Además, cualquier proveedor de terceros que utilices también debe cumplir con el RGPD. Esta es la razón por la que la gestión de riesgos del proveedor se ha vuelto tan importante.

Las multas por incumplimiento son significativas. Hasta 10 millones de euros, o 2% de facturación global anual (lo que sea mayor) o hasta 20 millones de euros, o 4% de facturación global anual (lo que sea mayor).

Los ejemplos de métricas para rastrear el cumplimiento del RGPD incluyen:

·El número de fugas de datos y violaciones de datos detectadas. Ten en cuenta que debes informar las violaciones de datos personales no más de 72 horas después de darte cuenta de ellas.

·La calificación promedio de seguridad de tus proveedores externos.

Métricas que son útiles para cubrir la normativa

Los ejemplos de métricas para rastrear el cumplimiento del RGPD incluyen:

- El número de fugas de datos y violaciones de datos detectadas. Ten en cuenta que debes informar las violaciones de datos personales no más de 72 horas después de darte cuenta de ellas.
- La calificación promedio de seguridad de tus proveedores externos.

sedian Seguridad Digital de Andalucía