**Prácticas adecuadas para recopilar y gestionar registros**

En esta lectura, conocerás algunas de las mejores prácticas relacionadas con la gestión, el almacenamiento y la protección de registros. Entenderlas te ayudará a perfeccionar las búsquedas de registros y te dará más recursos para identificar y resolver incidentes de seguridad.

**Registros**

Las fuentes de datos, como los dispositivos, generan información en forma de eventos. Un **registro** (o log) recopila los eventos que se producen dentro de los sistemas de una organización. Estos registros contienen entradas, y cada una detalla la información correspondiente a un único evento que ocurrió en un dispositivo o sistema. Originalmente, los registros servían solo para solucionar problemas tecnológicos habituales. Por ejemplo, los registros de errores proporcionan información sobre por qué ocurrió un error inesperado y ayudan a identificar el origen del error para que pueda corregirse. Hoy, prácticamente todos los dispositivos informáticos generan algún tipo de registro que brinda información valiosa y que no solo tiene que ver con la resolución de problemas.

En seguridad, los profesionales usan los **análisis de** **registros**, que es el proceso mediante el cual se examinan los registros para identificar eventos de interés. Los registros ayudan a descubrir los detalles que responden a las 5 W de la investigación del incidente: *quién (who)* desencadenó el incidente, *qué (what)* sucedió, *cuándo (when)* ocurrió, *dónde (where)* ocurrió y *por qué (why)* se produjo.

**Tipos de registros**

Según la fuente de datos, se pueden producir diferentes tipos de registro. A continuación, mencionamos una lista de algunos tipos de registros comunes que las organizaciones deberían recopilar:

* **Red**: Los registros de red son generados por dispositivos de red, como firewalls, routers o switches.
* **Sistema**: Los registros de sistema son generados por sistemas operativos, como Chrome OS™, Windows, Linux o macOS®.
* **Aplicación**: Los registros de aplicación son generados por aplicaciones de software y contienen información relacionada con los eventos que ocurren dentro de la aplicación, como una aplicación en un teléfono inteligente.
* **Seguridad**: Los registros de seguridad son generados por varios dispositivos o sistemas, como el software antivirus y los sistemas de detección de intrusiones. Estos contienen información relacionada con la seguridad, como la eliminación de archivos.
* **Autenticación**: Los registros de autenticación se generan cada vez que se produce una autenticación, como un intento de inicio de sesión exitoso en una computadora.

**Detalles de registro**

Los registros suelen contener una fecha, una hora, una ubicación, una acción y el autor de la acción. Este es un ejemplo de un registro de autenticación:

**Login Event [05:45:15] User1 Authenticated successfully**

Los registros contienen información y se pueden ajustar para que incluyan aún más. Elregistro verboso (con abundancia de detalle) recopila información adicional y detallada que excede el registro predeterminado. Este es un ejemplo del mismo registro anterior pero registrado con abundancia de detalle (verbosidad).

**Login Event [2022/11/16 05:45:15.892673] auth\_performer.cc:470 User1 Authenticated successfully from device1 (192.168.1.2)**

**Gestión de registros**

Puesto que todos los dispositivos producen registros, puede resultar complicado para las organizaciones realizar un seguimiento de cada uno de ellos. Para aprovecharlos al máximo, tienes que elegir exactamente qué registrar, saber cómo acceder a ellos fácilmente y mantenerlos seguros, mediante la gestión de registros. La **gestión de registros** es el proceso de recopilar, almacenar, analizar y eliminar los datos de registro.

**Qué registrar**

Lo más importante de la gestión de registros es elegir qué registrar. Cada organización es diferente, y sus requisitos de registro también pueden serlo. Es importante tener en cuenta qué fuentes de registro tienen más probabilidades de contener información útil de acuerdo al evento de interés. Esto podría implicar configurar las fuentes de registro para reducir la cantidad de datos que registran o excluir la verbosidad excesiva. Cierta información, que incluye números de teléfono, direcciones de correo electrónico y nombres, entre otros datos, constituye la información de identificación personal (PII), la cual requiere de una gestión especial. Es posible que en algunas jurisdicciones no puedan registrarse.

**El problema de la saturación de registros**

Desde el punto de vista de la seguridad, registrarlo todo puede resultar tentador. Este es el error más común que cometen las organizaciones. El hecho de que se pueda registrar no significa que *deba* registrarse. Almacenar una cantidad excesiva de registros puede suponer muchas desventajas para algunas herramientas SIEM. Por ejemplo, la saturación de registros puede aumentar los costos de almacenamiento y mantenimiento. Además, puede aumentar la carga en los sistemas, lo que puede generar problemas de rendimiento y afectar la capacidad de uso. Esto, a su vez, dificulta la búsqueda e identificación de eventos importantes.

**Retención de registros**

Algunas organizaciones operan en industrias con regulaciones determinadas. Por ejemplo, ciertas normativas exigen que las empresas retengan los registros durante un período determinado. En estos casos, las organizaciones pueden implementar prácticas de retención de registros en su política de gestión.

Es posible que algunas organizaciones deban modificar su política de gestión de registros para cumplir con las regulaciones. Esto es así para las que operan en industrias como:

* Sector público, como en el caso de la Ley Federal de Modernización de la Seguridad de la Información (FISMA)
* Atención médica, como la Ley de Transferencia y Responsabilidad de los Seguros Médicos, de 1996 (HIPAA)
* Servicios financieros, como el Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI DSS), la Ley Gramm-Leach-Bliley (GLBA) y la Ley Sarbanes-Oxley de 2002 (SOX)

**Protección de registros**

Junto con la gestión y la retención, la protección de los registros es vital para mantener su integridad. Suele ser habitual que los agentes de amenaza modifiquen registros con el fin de engañar a los equipos de seguridad e incluso ocultar su actividad.

Almacenar registros en un servidor de registros centralizado es una forma de mantener su integridad. Cuando estos se generan, se envían a un servidor exclusivo en vez de almacenarse en una máquina local, lo cual dificulta a los atacantes acceder a ellos.

**Conclusiones clave**

Resulta importante entender cómo recopilar, almacenar y proteger adecuadamente los registros, ya que son parte integral de las investigaciones de incidentes. Tener un plan detallado para gestionarlos ayuda a mejorar la utilidad de los registros y la eficiencia de los recursos.