La importancia de la trazabilidad para facilitar la investigación forense

Mª Carmen Ortega
Cybersecurity Service Manager de Ingenia

La informática forense, por definición, entra en juego cuando ha ocurrido un incidente y debemos averiguar su causa. Es una ciencia retrospectiva que pretende reconstruir los hechos, identificar actores, flujos, línea temporal y obtener evidencias, manteniendo a lo largo de toda la cadena la integridad de los datos recopilados.

Es un acto posterior al postincidente, *postmortem*, pero que requiere una preparación previa que en muchas organizaciones se ha demostrado insuficiente. ¿Hacemos los deberes antes para que, en caso de necesidad, un análisis forense sea efectivo y concluyente?

Haciendo una analogía con la medicina forense, un médico, por bueno que sea, no logrará determinar la causa de la muerte de una persona con un mechón de pelo. Quizás si indaga mucho y hace varios análisis que le den pistas con técnicas avanzadas pueda averiguar algo, pero haber tenido el cuerpo completo para su análisis habría sido infinitamente mejor y más provechoso para la investigación. Esto también tiene su versión equivalente en el caso de un analista forense informático que debe investigar un sistema postincidente.

Un atacante experimentado tendrá muchas formas de esconder pruebas, pero igualmente contaremos con muchas técnicas y herramientas para descubrirlas, siempre que se den ciertas condiciones iniciales.

Hay un factor muy relevante y que en muchas ocasiones se pasa por alto, de gran ayuda para construir el hilo conductor en toda investigación, para realizar una cronología inicial e identificar información relevante de cara a determinar la causa: hablamos de las trazas, los *logs*, los eventos. Sin trazabilidad, sin pistas, un análisis forense se antoja complicado.

Preparación

Para ello, es crucial preparar nuestros sistemas de información para contar con un nivel de trazabilidad suficiente y así poder reconstruir un incidente. Y no se trata lógicamente de una solución *postmortem* reactiva, sino de una solución claramente proactiva y enfocada en facilitar la recuperación y la recopilación de evidencias en caso de incidente.

Si bien es ideal comenzar la investigación en el escenario de inmediato y lo menos contaminado posible, no siempre es viable; por ejemplo, cuando se trata de una infraestructura crítica que no se puede parar, o porque se tiene constancia del incidente un tiempo después de haberse materializado. En casos en los que técnicas a más bajo nivel pueden haber perdido su efectividad, la revisión de los eventos que se han ido registrando en el sistema puede resultar un punto clave para el análisis.

Cuando una infraestructura es propia, como buena práctica debemos tener identificadas las fuentes de eventos que hay que conservar y vigilar que la salud del *log* sea adecuada. Hablamos, por ejemplo, de directorio activo, DNS, consolas de antivirus, cortafuegos, servicios de correo, servicios publicados, acceso a recursos, etc. A nivel de sistema, se debe asegurar que se registran eventos como los accesos, identificando usuario y origen, accesos como administrador, acciones privilegiadas, acceso a recursos restringidos y objetos, conexión-desconexión de dispositivos externos, llamadas RPC (*Remote Proccess Control*) o bloqueos.

Idealmente, se debe llevar a cabo un bastionado previo y continuo de la red corporativa y los sistemas. Y, en este sentido, la configuración de

■ En la nube se ofrecen múltiples soluciones de seguridad, pero muchas veces los mecanismos deseables para facilitar un análisis forense no vienen configurados por defecto, y en ocasiones hay que contratarlos

auditoría debe ser un punto más y muy importante de dicho bastionado. Mientras más exhaustivo sea este, más fácil será determinar qué operaciones se podrían llegar a hacer desde un dispositivo o un punto de la red con unos permisos determinados.

Pero no solo hay que vigilar que la configuración de los eventos sea adecuada, sino que también se debe contar con una política de rotación de los *logs* que se van generando y de retención que permita volver atrás en el tiempo y recuperar información del pasado.

Nivel de trazado

Igualmente, los desarrollos a medida deben contemplar un correcto nivel de trazado en el aplicativo para que se pueda seguir la pista de las actividades realizadas. En muchos casos, estos aplicativos quedan relegados por error a un segundo plano de control y trazabilidad.

Para evitar que se produzcan borrados en las trazas, es aconsejable enviar en tiempo real los *logs* a otro sistema, como un servidor externo, unidad NAS. Aunque es mejor enviarlos, por ejemplo, a un SIEM (*Security Information and Event Management*) o a un servidor de *syslog*, idealmente ubicado en otro lugar y con permisos y accesos totalmente diferenciados. El SIEM, además, ayudará al análisis forense para correlar eventos, encontrar situaciones sospechosas relacionadas con el suceso y realizar búsquedas avanzadas.

También está bastante extendido el uso de un servidor ELK (ElasticSearch, Logstash, Kibana), varios módulos en conjunción que se utilizan para recoger eventos, procesarlos, realizar búsquedas y elaborar gráficas. Lo importante es contar con algún sitio alternativo para que, si se produce un borrado malintencionado del *log*, podamos seguir conservándolo.

No obstante, si la infraestructura no es *onpremise*, la situación cambia. Cuando se contrata un servicio en *cloud* es fundamental que nos informemos del nivel de trazabilidad que ofrece. Normalmente hay que configurarla, solicitarla o contratarla porque no se incluye de serie. Por dar un par de ejemplos, la contratación de IaaS (*Infraestructure as a Service*) o SaaS (*Software as a Service*).

En la nube se ofrecen múltiples soluciones de seguridad, pero muchas veces los mecanismos deseables para facilitar un análisis forense no vienen configurados por defecto, y en ocasiones hay que contratarlos aparte o contar con un nivel de licenciamiento más avanzado. Puede ser para contar con información de accesos, de intercambio de tráfico o de actividad asociada al servicio. Hay que analizar qué información es necesaria cuando se va a optar por un servicio en la nube y considerar sus costes como parte de este y así asegurar que haya trazabilidad posteriormente.

Análisis previo

En definitiva, y como conclusión general, para poder desarrollar la investigación forense y conseguir resultados concluyentes acerca de un incidente de seguridad es vital hacer un análisis previo de nuestros sistemas y de las posibilidades que ellos mismos o herramientas de terceros nos ofrecen para recopilar información relativa a la trazabilidad de acciones y la generación de evidencias. De esta forma, se garantiza un mejor punto de partida para el analista forense de cara a averiguar la causa raíz del incidente y realizar su reconstrucción.

Teniendo en cuenta que antes o después seremos víctimas de un incidente de seguridad en nuestras organizaciones, de menor o mayor impacto, estar mejor preparados para responder y recuperar en el ámbito forense es, sin duda, una inversión con claro retorno que debemos considerar. ■