>> Jorge Dávila

Recuperar el control en los sistemas de información

Conocer lo que está pasando dentro de los sistemas de información es algo que cada día adquiere más importancia y actualidad. La defensa mediante la detección activa de los ataques, y ciertas exigencias normativas inspiradas por el miedo, han reabierto el tema de la monitorización y la auditoría de los sistemas informáticos y de información. Aunque la auditoría de sistemas no es nada nuevo, lo que sí es nuevo es la magnitud con la que se puede hacer la monitorización de sistemas con los nuevos SIMs y eso puede abrir interrogantes y plantear escenarios nuevos.

Alguien dijo una vez que "*si ocurre algo y no se publica, eso es lo más cerca que podemos estar de que no haya ocurrido nunca*". Análogamente, si en un sistema informático, sobre todo si se trata de un servidor, no está activado el sistema de auditoría (*log files*), lo que éste sistema haga, sirva o participe en..., "*se perderá en el tiempo como lágrimas en la lluvia*" [1].

A pesar de los impresionantes avances en las tecnologías que componen lo que hoy conocemos como sistemas informáticos, a fin de cuentas, éstos siguen siendo autómatas deterministas del tipo de los imaginados por Turing, y como máquinas de estados que son, su devenir no es más que un paseo a través de sus respectivos estados. Para saber qué está haciendo una máquina, el observador debe conocer cuáles han sido (todos) los estados por los que ya ha pasado el autómata y, lo más importante, saber interpretarlos de modo que, para él, esa secuencia tenga sentido (información) y no resulte indescifrable como cualquier secuencia elegida al azar.

Para poder saber qué está haciendo o ha hecho una máquina, debemos conocer a través de qué estados ha pasado y debemos poder interpretarlos, comprenderlos. La operación de auditoría significa ser capaz de reconocer qué significado tienen cada uno de los estados visitados, si es que queremos entender lo que está haciendo (o ha hecho) el sistema.

La ausencia de un registro de datos, o la incapacidad para entender qué es lo que significan constituyen la esencia final de la "**intrazabilidad**" y el "**anonimato**" en los sistemas informáticos que conocemos. Los sistemas de auditoría lo que persiguen es desterrar el anonimato en los sistemas, e impedir qué su evolución en el tiempo quede fuera del control de sus operadores. De hecho, la razón original de que existan los *logs* es la de poder depurar el funcionamiento de los sistemas y las aplicaciones. Una vez en producción, ese mismo concepto de registro "*de lo que ocurre*" (y resulta interesante) es una herramienta básica para administrar la máquina (por ejemplo, para facturar [2]). Ahora que hay ordenadores en cualquier parte, y que estamos pasando de los sistemas multiusuario a los usuarios multisistema, la facturación no es tan importante y quizás por ello los *logs* han sido un tanto olvidados durante las últimas décadas en la informática.

El proceso de consolidación de todos los datos de auditoría en un sistema es de suma importancia desde cualquier punto de vista (estratégico, operacional y normativo), ya que es el que permite localizar, cosechar y destilar información vital que antes estaba en forma (nativa) no utilizable.

Si buscamos en Internet encontraremos que hay muchos tipos diferentes de analizadores de los *logs* [3] que producen los sistemas operativos modernos y las aplicaciones de servidor mas utilizadas. Es esta la razón por la que dichos analizadores son, generalmente, sistemas especializados y específicos (analizadores del Unix syslog, del servidor web, del *proxy*, del servidor de correo, del cortafuegos, de los IDSs, etc.). Algunos "convencidos" del análisis de *logs* dicen que "***mientras en seguridad no hay nada seguro, el análisis de* logs *es lo que más se le parece***" y quizás esta afirmación, aún siendo bastante válida, pueda resultar excesivamente optimista, ya que todo depende de cómo se hagan las cosas.

Una de las características más recordada del demonio Unix syslog es que permite la **auditoría remota**. Según este planteamiento, lo mejor es mandar los registros a un servidor especializado (*log host server*) para en él custodiarlos, analizarlos y, a fin de cuentas, gestionarlos. Dentro de este planteamiento, algunos reconocen que ese servidor también puede ser comprometido, pero aducen que eso supone un trabajo doble para los atacantes, que no sólo tienen que atacar la máquina emisora de los registros, sino también a la que se encarga de recibirlos y gestionarlos, y que puede ser una máquina "bastionada" y/o ser "externa" al sistema.

La idea es no sólo proporcionar redundancia en el sistema de auditoría sino, a la vez, poner dificultades suplementarias a los atacantes. Este tipo de estrategias se basan en la creencia, o en la esperanza, de que el *hacker* que ataque el sistema pueda no tener la formación suficiente, o que le falte tiempo suficiente para detectar si existe alguna medida de auditoría remota y poder neutralizarla. No hay que olvidar que cualquier sensación de seguridad obtenida minusvalorando las capacidades del atacante, siempre ha sido una pésima estrategia, pero aun así todavía se pueden encontrar algunos textos donde utilizan este tipo de razonamientos para ensalzar y justificar los diseños de sus sistemas. Como regla general hay que pensar que el atacante lo sabe prácticamente todo sobre el sistema ya que, con toda probabilidad, el ataque seguro que viene "de dentro".

En algunos sistemas el agente de auditoría es de sólo lectura y, en las versiones hardware, llega a ser una desconocida *"caja negra"* enchufada a la línea. En este caso, el sensor actúa como un mero cable de cobre que registra todos los datos que pasan a través de él. En este caso se podría utilizar una interfaz serie para conectar el sensor con el servidor de auditoría de modo que, en este caso, el *logger* no pueda ser accedido para lectura o puesta a cero, excepto a través de una interfaz que no sea accesible por redes externas o internas. Este tipo de planteamientos terminan invocando la existencia de una red paralela a la de explotación para su uso exclusivo en auditoría y eso es caro y más complejo de mantener y utilizar. Además de esto, hay que recordar que los sistemas hardware sólo aportan una seguridad suplementaria frente a la de sus parientes, los sufridos y modificables agentes software, si y solo si podemos autenticar la "caja negra" que tenemos enchufada en nuestro sistema desde hace tiempo [4].

Dada la complejidad de los sistemas actuales, la mera recolección y almacenamiento de *logs*, *per se*, no aporta seguridad alguna, aunque quizás sí pudiese servir como material probatorio que permita el cumplimiento de alguna norma legal; pero, en general, los registros de información de auditoría en estado nativo no resultan útiles por sí mismos. Para que los datos registrados puedan ser de alguna utilidad, es necesario que sean filtrados, que sean consolidados, antes de que puedan ser tenidos en cuenta.

---

[1] "*Yo he visto cosas que vosotros no creeríais, atacar naves en llamas en el cielo de Orión, brillar Rayos C en la oscuridad, cerca de la Puerta de Tannhaüser. Todos esos instantes se perderán en el tiempo, como lágrimas en la lluvia... Es hora de morir*" **Blade Runner**, guión de H. Fancher y D. Peoples. Dirección de Ridley Scott. 1982

[2] Cuando los ordenadores eran caros, exclusivos y difíciles de encontrar, los *logs* del sistema servían, fundamentalmente, para decidir cuánto había que cobrar a cada usuario por el hecho de haberlos utilizado.

[3] http://www.intersectalliance.com/

A cualquiera se le antoja razonable imaginar enterrados en los *logs* mucha información sobre el funcionamiento real y puntual de cualquier empresa o institución, pero lo que quizás no sea tan comprendido es que su extracción no destructiva sea siempre difícil. El proceso de consolidación de todos los datos de auditoría en un sistema es de suma importancia desde cualquier punto de vista (estratégico, operacional y normativo) ya que este proceso es el que permite localizar, cosechar y destilar información vital que antes estaba en forma (nativa) no utilizable.

El análisis de los registros de auditoría de cada una de las máquinas o aplicaciones, por separado, es tedioso, no aporta una visión conjunta de todo el sistema y, en algunos casos, resulta del todo inútil. Muchas veces la información necesaria no está recogida en ninguno de los registros de auditoría considerados por separado, sino que surge del contraste, de la correlación que pueda existir entre ellos; todos o casi todos los eventos interesantes o preocupantes en un sistema se pueden descomponer en un conjunto de operaciones separadas, más sencillas y nada sospechosas por sí mismas. Cualquier error o sesgo en los procesos de consolidación y análisis de los registros, afecta irremediablemente a los resultados finales, por lo que un procesado inadecuado, sin duda, dará al traste con la utilidad y eficiencia del sistema y, lo que es peor, podría inducir a cometer graves errores a los que tomen sus decisiones en función de esos datos mal procesados y/o agregados.

Análisis cooperativo y coordinado

Por todo ello, dada la complejidad que pueden llegar a alcanzar los sistemas informáticos de hoy en día, hay que recurrir necesariamente a aplicaciones que analicen cooperativa y coordinadamente todas las fuentes y todos los datos de auditoría y de monitorización. A estos sistemas se les está dando por llamar **SIM**s (*Security Information Managers*) por algunas empresas proveedoras, aunque han recibido y reciben todavía otros nombres[5]. El objetivo final de este tipo de productos e iniciativas de código abierto, es proporcionar a los operadores especializados del sistema una visión global, precisa y completa de cómo van, en tiempo real –si es posible– los sistemas de información objeto de vigilancia.

Dada la complejidad del problema planteado es natural recurrir a sistemas automáticos que nos faciliten la tarea, pero en ningún momento hay que olvidar que **1)** el proceso de recolección debe ser siempre preciso, exacto y auténtico, **2)** el análisis de datos monitores nunca puede suponer una alteración semántica de los mismos, **3)** los filtros y procesos de consolidación inadecuados pueden destruir datos reales y, a la vez, de forma inadvertida, introducir artefactos instrumentales que falsean gravemente el resultado final, y **4)** no se debe sacrificar, en aras del "tiempo real", el análisis pausado de los datos con una amplia perspectiva temporal ya que los atacantes humanos, jugando con el tiempo, pueden encontrar ritmos y cadencias que pueden disminuir la probabilidad de ser detectados.

Los sistemas de auditoría se están presentando dentro del mercado de la TIs como herramientas para el control consciente de los sistemas y como base para la toma de decisiones (cuadros de mando) en su gestión, por lo que también hay que verlos como un nuevo flanco de ataque sobre el que, personal interesado, puede sembrar puertas traseras, fallos controlados, filtros que alimentan alarmas durmientes, etc.

Quedando claro que la disponibilidad de datos ciertos de auditoría y el consiguiente análisis serio y equilibrado de los mismos es el único mecanismo para intentar saber qué es lo que está aconteciendo en un sistema de información, este mismo objetivo puede suscitar ciertas suspicacias. La pregunta que surge con cierta naturalidad es sobre el por qué de este renacido interés en la auditoría de sistemas, más allá del mero interés "depurador" de los desarrolladores de sistemas. La excusa inicial es siempre la de "La Seguridad", la de poder identificar ataques externos, internos y de toda índole, la de detectar operaciones, en principio, indebidas o prohibidas, la de "*saber para dar un mejor servicio a través del correcto funcionamiento del sistema*" pero, como en muchos otros casos, este interés por la monitorización de sistemas de información puede tener algún subproducto potencialmente pernicioso.

Dado el nivel de informatización que está llegando a tener nuestra sociedad, los sistemas de auditoría informática se convierten, transitivamente, en sistemas de auditoría de nuestras actividades personales y cotidianas. Con unos buenos sistemas de auditoría en todos o en la mayoría de los sistemas de información más utilizados, ya estaría medio desplegado un "*big brother*" que iría mucho más lejos que cualquier sistema *Echelon* que haya existido, y que podría dar cuenta de nosotros de forma bastante puntual y que, por si fuera poco, con datos acumulados en el tiempo, esos mismos sistemas podrían dar información más perenne sobre los gustos, filias y fobias, de todos o algunos de los que interactuasen con el sistema.

Dado que para detectar todos los usos ilegítimos de un sistema es inevitable y absolutamente necesario revisar también todos los usos legítimos, todos los sistemas de auditoría de los sistemas de información son una "tecnología de doble uso" que puede atentar contra la intimidad de las personas. Aunque los gestores de esos sistema digan que nunca espiarán las actividades de sus usuarios, que nunca abrirán esa "caja de Pandora", puede que ellos digan la verdad y que no lo hagan, pero la caja está, y en poco tiempo puede llegar a estar llena de datos que alguien puede "obligar" a entregar o, simplemente, robar. Recordemos que con la excusa de la seguridad se están instalando sistemas automáticos que antes no había[6], que permiten y facilitan la observación detallada y automática de todos sus usuarios, en aras a identificar potenciales actividades terroristas, por lo que los SIMs también deben observarse a la luz de estas tenebrosas luces.

Además de esta dualidad esencial, también hay que recordar que los sistemas de auditoría se están presentando dentro del mercado de la TIs como herramientas para el control consciente de los sistemas y como base para la toma de decisiones (cuadros de mando) en su gestión, por lo que también hay que verlos como un **nuevo flanco de ataque** sobre el que personal interesado puede sembrar puertas traseras, fallos controlados, filtros que alimentan alarmas durmientes, etc.

La instalación de cualquier nuevo instrumento que amplifica el poder que da la abundancia interminable de datos y el saber cómo interpretarlos, es algo que **debe afrontarse con cuidado, prudencia y profesionalidad**, dado que el sistema **puede terminar volviéndose contra nosotros**. Igual que no es razonable guardar armas de fuego en el cuarto de los niños, **quizás no sea siempre razonable aumentar el grado de monitorización y auditoría de nuestros sistemas de información mas allá de lo realmente necesario**. La posesión de datos, incluso en su forma nativa y no procesada, supone la asunción de una responsabilidad que, al ritmo que va la informatización del primer mundo, puede ser importante. La no-trazabilidad y el anonimato son factores que quizás hoy no sean considerados para su defensa por los administradores de sistemas y los propietarios de los sistemas de información, pero puede llegar el día (y puede no tardar mucho) en el que esos conceptos deban ser tenidos muy en cuenta y deban ser defendidos si esos mismos sistemas de información quieren seguir teniendo usuarios. ■

Jorge Dávila Muro
Consultor independiente
Director
Laboratorio de Criptografía
LSIIS – Facultad de Informática – UPM
jdavila@fi.upm.es

[4] Recordemos el impacto que tienen sobre la seguridad de un sistema los *data/key loggers* en hardware que se interponen inadvertidamente entre el teclado y la CPU del sistema.

[5] Ver Luís Rodríguez Berzosa: "Los *logs* como fuente de información de seguridad: Calidad y Coherencia". SIC Nº 71, Septiembre 2006.

[6] Algunos ejemplos son: los intercambios de datos fronterizos y de navegación aérea, las cámaras de videovigilancia en ciudades y en "barrios marginados" y "conflictivos", los sistemas para la identificación y localización automática de equipajes desatendidos, los analizadores automáticos de comportamiento, los analizadores de multitudes, etc., todos ellos proyectos reales o en marcha dentro de las iniciativas estadounidenses en su particular cruzada.