SGSI (Sistema de Gestión de Seguridad de la Información): La necesidad de los sistemas de gestión en tiempo real.

José M. Rosell Tejada. Socio-Director (jrosell@s2grupo.com)
Antonio Villalón Huerta. Consultor de Seguridad. (avillalon@s2grupo.com)

Grupo S2

Resumen

La puesta en marcha de los SGSI pone de manifiesto, más que en ningún otro caso, la necesidad de dotar a los sistemas de gestión de infraestructuras tecnológicas que les permitan gestionar el proceso en tiempo real. El estado actual de la tecnología permite el diseño de sistemas que gestionan actividades y procesos en tiempo real, monitorizando permanentemente su estado y actuando, incluso, de forma automática ante estímulos del sistema.

Desarrollo

Introducción

Los sistemas de información de las organizaciones desarrollan su misión en un entorno hostil. Las organizaciones son responsables de la protección de la información que gestionan, frente a las amenazas de este entorno y deben, por todos los medios disponibles, garantizar su confidencialidad, integridad y disponibilidad.

Una creciente preocupación por todos los aspectos relacionados con la seguridad se percibe en el ambiente desde hace tiempo. Todas las organizaciones, públicas o privadas, grandes o pequeñas se enfrentan día a día a amenazas contra sus recursos informáticos, con elevado riesgo de provocar incidentes de alto impacto en su actividad.

El imparable avance de las nuevas tecnologías en las organizaciones y, en general, el avance de la "Sociedad de la Información" no hace más que agravar la situación. Los riesgos emergentes relacionados con tecnologías y procesos de negocio, requieren sistemas, soluciones y servicios emergentes. Soluciones para garantizar de forma continuada en el tiempo la actividad de las organizaciones, la seguridad de la información base del negocio y los derechos de los individuos en una sociedad cada vez más informatizada, cumpliendo al mismo tiempo con leyes y directivas.

La seguridad no es un producto: es un proceso. Un proceso continuo que debe ser controlado, gestionado y monitorizado. En esta línea, y siendo conscientes del escenario descrito, se presenta la certificación para los "Sistemas de Gestión de la

Seguridad de la Información", conforme a la recientemente publicada norma UNE 71502:2004, contribuyendo de esta manera a minimizar, en la medida de lo posible, los riesgos de los sistemas de información de las organizaciones a través de una gestión eficaz del proceso de seguridad.

La norma UNE 71502:2004 se presenta como un sistema de gestión de seguridad de la información basado en una norma internacional de reconocido prestigio, la norma UNE ISO/IEC 17799, que se ha configurado como un estándar a la hora de auditar los aspectos relacionados con la seguridad en las organizaciones, y **establece un hito** en la definición de los sistemas de gestión, introduciendo, a través de ella conceptos y controles que **requieren de una gestión en tiempo real**. (gestión de incidencias, detección de intrusos …..)

La empresa en tiempo real

Disponer de acceso inmediato a la información de una empresa se ha convertido, en los últimos años, en una de las claves para hacer las organizaciones más competitivas en la era digital. Gartner habla de la necesidad de avanzar en el concepto de la empresa en tiempo real (Zero Latency Enterprise) y de la monitorización de actividades y procesos de negocio (BAM: Business Activity Monitoring) como clave del éxito de las organizaciones de próxima generación.

Conceptualmente este modelo mediante la monitorización de las actividades clave del negocio informa, en tiempo real, a los agentes que intervienen en la gestión de la empresa, llevando la información dónde hace falta, a quién le hace falta, en el mismo instante en el que se produce y por el medio que tiene a su alcance en ese momento (teléfono móvil, PDA, correo electrónico, etcétera) y dejando traza en todo momento de los estados por los que pasa la información.

Los procesos y actividades de negocio son monitorizados por agentes automáticos distribuidos en posiciones clave de los sistemas de información y de los activos de la organización. Estos sensores, en las condiciones de diseño, disparan eventos o alarmas automáticas que deben ser tratados por sistemas de gestión de eventos y alarmas (EM&A: Event Management and Alerting) y encaminados automáticamente hacia su destino.

El valor de la información decrece con el incremento de la latencia o tiempo transcurrido entre que un evento sucede y que la información relativa al mismo llega al recurso pertinente en la organización.

Hacia los sistemas de gestión en tiempo real

Los sistemas clásicos de gestión necesitan un estímulo para proporcionar una respuesta, es decir, son sistemas de tipo "pull" donde el individuo requiere información al sistema y este, tras un período de procesamiento, se la entrega. Los sistemas de gestión basados en la gestión de eventos son, a diferencia de los anteriores, de tipo "push". Es el mismo sistema el que entrega información de la organización al individuo sin que este la haya solicitado.

Las organizaciones en general son entidades vivas que interactúan con el entorno en base a los estímulos que recibe. Es fácil comprender que la capacidad para la acción de directivos y empleados de una organización es tanto mayor cuanto más próximo está el suceso en el tiempo. Los eventos o sucesos, "estímulos", de las organizaciones tardan en llegar al "cerebro" de las mismas, sus directivos o mandos intermedios, de forma que cuando estos tienen capacidad para la acción el entorno puede haber sufrido variaciones significativas y la acción puede no ser pertinente.

En esta línea, se define la base de los sistemas de gestión de eventos y alarmas (EM&A), sobre los que se diseña un sistema de gestión por procesos (BPM) disparados por eventos para conseguir, en definitiva, la gestión de actividades de negocio en tiempo real (BAM).

En todos los casos nos encontramos ante sistemas dinámicos, cambiantes, no estáticos, aunque la unidad de medida tomada en cada caso no tiene porque ser la misma. La diferencia la marca la latencia y el tiempo de ciclo de mejora. Tal y como estamos viendo nos dirigimos hacia sistemas de gestión monitorizados en tiempo real que tiene evidentemente su repercusión sobre la forma de actuar del ciclo de mejora continua.

Es habitual hablar, en otras disciplinas, de sistemas de control en tiempo real, aunque no tanto de sistemas de gestión en tiempo real. Es impensable no disponer de sistemas de control de una cadena de producción robotizada en tiempo real, así como es impensable no disponer de sistemas de control de navegación de un buque en tiempo real. De igual forma es impensable no disponer de un Sistema de Gestión de la Seguridad de la Información en tiempo real.

SGSI: La necesidad de un sistema de gestión en tiempo real

Como sistema de gestión que es, el Sistema de Gestión de la Seguridad de la Información presenta unos requerimientos similares al resto de sistemas de gestión; definición de la política corporativa, implicación por parte de la dirección, desarrollo de un sistema documental, necesidad de registros y evidencias, formación, integración en la cultura empresarial, etcétera, aunque en este caso se presentan una serie de requisitos que hacen que el SGSI dé un paso adelante.

La definición de los activos que deben ser protegidos, el análisis de riesgos inicial proporcional a la naturaleza y la valoración de los activos y, ante todo, la obligada selección de controles de la norma UNE ISO/IEC 17799 marcan las diferencias fundamentales.

La norma UNE ISO/IEC 17799, pilar en la que se basa el SGSI diseñado por la norma UNE 71502 define seguridad como la suma de tres componentes: confidencialidad, integridad y disponibilidad de la información:

- **Confidencialidad**. Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.

- **Integridad**. Garantía de la exactitud y completitud de la información y de los métodos de su procesamiento.
- **Disponibilidad**. Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

Si bien una parte de los controles definidos por la norma son políticas, prácticas, procedimientos e incluso estructuras organizativas, una buena parte del conjunto global de controles son funciones de software que "vigilan" la seguridad de la organización de forma **continua**, no discreta: Es aquí dónde radica la diferencia primordial con el resto de sistemas de gestión.

El SGSI se diseña para garantizar la seguridad de los sistemas de información en los términos definidos anteriormente y por tanto se diseña el ciclo de mejora continua que garantice la confidencialidad, integridad y disponibilidad de la información, pero ¿cómo se puede conseguir los objetivos marcados si no se dispone de información de los sistemas en tiempo real?, ¿cómo se garantiza la disponibilidad de sistemas, servicios y aplicaciones?, ¿cómo se garantiza que tan solo aquellos recursos autorizados convenientemente acceden a la información confidencial?

En un SGSI los cambios son extraordinariamente rápidos. Una situación estable y segura en un instante determinado puede dejar de serlo en unas horas. Las personas que trabajan con el sistema deben estar informadas permanentemente, incluso en horarios extendidos 24x7 ya que se pueden producir incidencias e incidentes que afecten directamente a la calidad del servicio entregado y a su seguridad, entendida como la suma de disponibilidad, integridad y confidencialidad.

Las estructuras perimetrales de defensa son monitorizadas mediante **agentes** diseñados para tal fin. Los sensores de detección de intrusos, los sistemas cortafuegos, sistemas antivirus y el resto de componentes que configuran las defensas internas y externas de las organizaciones exigidos por los controles de la norma UNE ISO/IEC 17799, disparan eventos en el momento en el que se detecta alguna actividad anómala, requiriendo la participación de los equipos de intervención rápida que atienden las alarmas.

De igual forma que podemos detectar con un sensor de movimiento la entrada en una zona de acceso restringido, podemos detectar, con sensores lógicos o agentes diseñados específicamente, tipos de eventos clave en la gestión de la seguridad como son la baja de un empleado, el acceso con privilegios a sistemas y aplicaciones, intentos de acceso no autorizados, la caída de un sistema, la existencia de contraseñas triviales, etcétera.

Esta estructura basada fundamentalmente en la vigilancia por parte de agentes y en la gestión de los eventos y alarmas de seguridad que generan, permite además a la organización abrir diversos frentes de investigación para el desarrollo del comportamiento de grupos de agentes que permitan una vigilancia física y lógica de sus sistemas de información cada vez más eficiente, y que permitan que la información llegue lo antes posible a su destino y con el mejor contenido posible.

Si es importante que la información llegue en las mejores condiciones a su destino, también es importante que se vigile que el destino recibe la notificación pertinente y sobre todo que actúe en consecuencia. En este sentido se debe monitorizar internamente el cumplimiento del compromiso de calidad de servicio mediante la medición en tiempo real de los tiempos de respuesta y de resolución. En caso de sobrepasar los límites establecidos para cualquiera de estos parámetros el sistema debe generar una alerta de incumplimiento.

Hablando de seguridad resulta primordial centrar los esfuerzos en tareas de mantenimiento predictivo y preventivo, intentando minimizar las actuaciones correctivas que implican, la existencia de un fallo, por lo que el diseño de agentes debe contemplar no sólo la detección del fallo, sino también la prevención y la predicción del mismo mediante, por ejemplo, esquemas de auditorías de vulnerabilidades automáticas y periódicas sobre los recursos críticos de la organización. La única forma de hacer efectivas estas medidas en los sistemas de información vuelve a ser el diseño de agentes y comunidades de agentes y los sistemas de actuación y gestión en tiempo real.

En este contexto, donde la medición y el control cobran especial importancia, es importante prestar una atención especial a los procesos de calibración de los agentes y los sensores, requiriendo el sistema de gestión un procedimiento de calibración de los “aparatos de medida” que son en este caso los agentes distribuidos por los sistemas de información de la organización y su integración con la gestión de eventos y alarmas.

En definitiva, si, como se ha comentado, en condiciones normales las organizaciones avanzan hacia la gestión de sus procesos en tiempo real, el proceso de gestión de seguridad de la información, que en muchas compañías se presenta ya hoy en día como un proceso clave del negocio, exige para ser eficaz y eficiente, la puesta en marcha de sistemas de gestión de eventos y alarmas que aseguren que los sucesos son notificados en tiempo real a recursos de la organización con capacidad para la acción, y por tanto exige el diseño de **“Sistemas de Gestión en tiempo real”**.

Igual que en otros sistemas de gestión nos podemos preguntar cuál es el coste de la “no calidad”, no deberíamos preguntarnos: ¿Cuál es el coste de la latencia ante un incidente de seguridad? o ¿cuál es el coste de la latencia ante un evento que nos previene de un incidente de seguridad inminente o futuro?...