Auditorías de seguridad

Por Alfonso Franco Gómez

Responsable de Preventa y Tecnología.
División Seguridad Lógica.
Germinus XXI S.A.

El objetivo de este artículo es introducir al lector en los conceptos asociados a una auditoría de seguridad. La auditoría de seguridad es algo cada vez más frecuente dentro de las empresas, debido a la obligatoriedad de la realización (en algunos casos) de una auditoría bianual impuesta por la Ley Orgánica de Protección de Datos (en su Reglamento de Medidas de Seguridad). Sin embargo, en muchos casos, se desconocen todos los aspectos relacionados con una auditoría de seguridad o incluso los distintos tipos que existen. Este artículo pretende mostrar las distintas aproximaciones y técnicas para realizar una auditoría de seguridad.

Clasificación

Las auditorías de seguridad se pueden clasificar primeramente en técnicas, que se centran en los riesgos existentes en los sistemas de información de la organización y en la calidad técnica de las medidas de protección introducidas (correcta configuración de los equipos, etc.), y no técnicas o procedimentales, que habitualmente estudian el cumplimiento efectivo de la Política de Seguridad de la organización y de sus procedimientos.

Auditorías técnicas

Centrándonos ahora en las auditorías técnicas, dependiendo de la profundidad de los trabajos, hablaremos de auditorías de vulnerabilidades, que tratan de localizar configuraciones erróneas o relajadas en exceso y agujeros de seguridad en el software directamente explotables, habitualmente con el apoyo de herramientas que automatizan parte del trabajo, y proyectos de hacking controlado, pruebas de intrusión o auditorías a nivel de aplicación, en la que los trabajos se expanden para dejar sitio al lado más "creativo y artesano" de los auditores de seguridad, que tratan de explotar errores de programación, la arquitectura de red y las relaciones de confianza, las debilidades de los protocolos de comunicación y los controles de acceso para simular los ataques a una infraestructura de red bajo los perfiles que se consideren de interés (atacante externo con distinto nivel de calificación, usuario interno, auditor, administrador, competencia...) bajo las mismas circunstancias y capacidades (información inicial, puntos de acceso, recursos disponibles...).

Por otro lado, dependiendo de la aproximación que tomemos para realizar las auditorías técnicas, hablaremos de pruebas de caja negra, que buscan las debilidades desde el exterior de los sistemas (habitualmente realizadas de forma remota, desde Internet), y pruebas de caja blanca, que realizan una revisión de seguridad analizando la configuración del propio sistema, con acceso al mismo.

Una auditoría de seguridad de caja negra normalmente comienza con trabajos desde el exterior, para encontrar puntos débiles y ganar algún tipo de acceso a los sistemas, y una vez conseguido este acceso, examinar el sistema para escalar privilegios y tomar control sobre él. Estas pruebas desde hace tiempo se vienen realizando basándose en el estándar OSSTMM (Open Source Testing Methodology Manual) o el documento SP 800-46 del NIST (instituto de estándares americano) que contemplan las pruebas a realizar para realizar una revisión de seguridad técnica completa.

En el caso de una auditoría de caja blanca el objetivo no es lograr el acceso (la empresa lo proporciona para realizarla) sino revisar las medidas de seguridad implementadas en el sistema y su conformidad, o no, con estándares reconocidos y guías de "buenas prácticas", como por ejemplo, los trabajos del instituto de estándares norteamericanos, NIST, el CSI, Center of Internet Security, o del SANS Institute.

Pruebas de caja negra

Las pruebas de caja negra, para que sean realmente efectivas, deben realizarse sin ningún conocimiento de la infraestructura, garantizando de esta forma que el análisis no tratará de utilizar ningún tipo de información que facilite la tarea de análisis. El propósito de estas pruebas es que el auditor se comporte como si realmente fuese un "atacante" de la infraestructura. Durante un análisis de caja negra normalmente se llevarán a cabo pruebas de visibilidad (para conocer los servicios y versiones de éstos activos y visibles desde el exterior en cada uno de los sistemas), pruebas de identificación de servicios (para determinar qué programas ofrecen los servicios ofrecidos, a través de las cabeceras obtenidas o respuestas programáticas y no fiándose de la lista de puertos TCP/IP conocidos), obtención de información (recuperación de información o datos de configuración del sistema final o sistemas adyacentes que desvelen detalles de la infraestructura auditada) y pruebas de vulnerabilidades en software estándar.

Estas últimas pruebas son las más complejas y se realizarán una vez determinados los servicios que se están corriendo, junto con la información disponible de versiones y sistemas operativos. Se basan en una parte que puede ser realizada por herramientas de diagnóstico automáticas y otra parte que debe ser realizada de forma manual por el auditor. Esta fase tiene que realizarse con ciertas precauciones puesto que son frecuentes los casos en que las pruebas de vulnerabilidades que puedan tener éxito produzcan cortes de servicio o caídas en los sistemas auditados.

Una vez se ha conseguido penetrar con éxito en un sistema, la auditoría de caja negra puede continuar hacia otros sistemas adyacentes (generalmente más expuestos una vez traspasado el perímetro) y también derivar hacia análisis de caja blanca.

Pruebas de caja blanca

Por el contrario, las pruebas de caja blanca, como se ha mencionado anteriormente, examinan el sistema desde su interior. Por lo tanto es necesario tener un acceso a los sistemas. Este acceso generalmente se obtiene porque directamente se le proporciona al auditor un acceso al equipo para que pueda realizar un análisis en profundidad de la configuración del sistema, aunque en algunos casos una prueba de caja negra se convierte en caja blanca por haber logrado un acceso al sistema a través de alguna vulnerabilidad del mismo u obtener información que pueda analizarse de esta forma (por ejemplo, el código fuente de las aplicaciones utilizadas).

Es importante destacar que estas pruebas son complementarias de las anteriores, ya que el hecho de no haber encontrado vulnerabilidades en las pruebas de "caja negra", no significa que no las haya, si no que generalmente significará que no se han dedicado recursos suficientes a descubrirlas. Dicho de otra forma, el hecho de que un sistema sea o no vulnerable no radica en que se encuentre una vulnerabilidad, si no en que exista dicha vulnerabilidad.

Siguiendo con esta filosofía, es necesario ampliar la información que se posee sobre los sistemas al máximo, incluyendo topología, protocolos utilizados, reglas en los cortafuegos, software empleado, etc.

Así, durante esta fase normalmente se realizan las siguientes tareas:

- Análisis de la configuración de todos los sistemas operativos implantados: usuarios, ficheros, etc.
- Análisis de la robustez de las contraseñas utilizadas.
- Análisis de la configuración del software de base (Web, Mail, cortafuegos, etc.).
- Análisis del código fuente de las aplicaciones instaladas o desarrolladas a medida.
- Determinación de las vulnerabilidades presentes en los sistemas debido a la desactualización en la aplicación de parches de seguridad (obsolescencia de los sistemas).

En algunos casos estas tareas de análisis pueden ser automatizadas con algunas herramientas

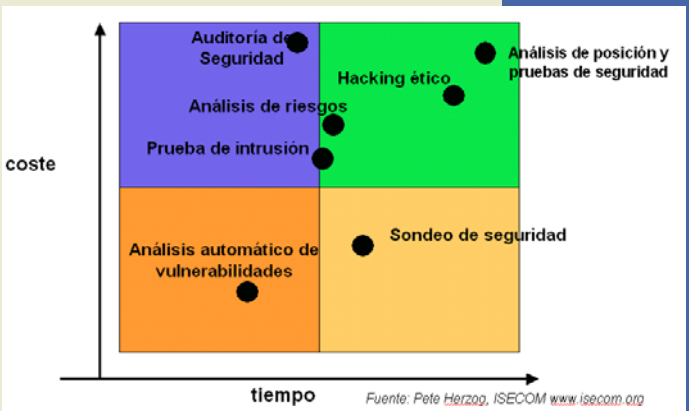

Ilustración 1: Tipos de auditoría

pero en la mayoría de los casos se realizarán de forma manual y requerirán de un conocimiento profundo de los sistemas auditados, recomendaciones del fabricante, etc. Generalmente estas inspecciones, aunque más laboriosas hacen que la tarea analítica-correctora produzca un resultado cualitativamente superior.

Auditoría de procesos y gestión

La realización de una actividad de auditoría debe realizarse siguiendo fielmente los códigos de buenas prácticas de seguridad de sistemas de información reconocidos internacionalmente, en este caso la norma ISO-17799 y la guía del NIST SP 800-26. En Germinus entendemos que este tipo de auditoría debe realizarse con un conocimiento previo de los distintos riesgos y controles que son aplicables a una organización, debido a la amplitud del código de buenas prácticas ISO-17799 no tiene sentido auditar todos los controles recomendados si éstos no son aplicables a la organización, bien por-

que no existe un riesgo en ese sentido, bien porque el coste de implantación de dichos controles se ha considerado superior al coste resultante de la materialización de una amenaza (impacto) o del propio activo.

Es por ello que la actividad de auditoría de procesos y gestión estará precedida por un trabajo de análisis del entorno de la organización incluyendo:

- Análisis de la política de seguridad.
- Análisis de los procesos implantados, incluyendo, entre otros, los de gestión y administración.
- Entrevistas con los responsables de la seguridad de información de la organización para determinar los controles establecidos.
- Revisión de los análisis de riesgos realizados previamente y en función de los cuales se han implantado los controles.
- Revisión de las auditorías previas realizadas.

Toda vez que se haya realizado el análisis del entorno se procederá a realizar una revisión exhaustiva de los controles implantados, la correcta implantación de los procedimientos y la concordancia con el código de buenas prácticas. Para ello se realizarán entrevistas con distinto personal de la organización, el personal concreto a entrevistar será definido basándose en el estudio del entorno y de la organización previamente realizado. Entre el personal entrevistado se incluirán a:

- Los responsables de gestión.
- El personal técnico encargado de la gestión de la seguridad de cada uno de los sistemas.
- Usuarios de los sistemas de información (muestra aleatoria)

Conclusión

Como ha podido verse a lo largo de este artículo, existen diversas aproximaciones a la hora de realizar una auditoría de seguridad. Pese a que la solución ideal suele ser la realización de un proyecto de auditoría completo, que incluya todas y cada una de las aproximaciones comentadas en este artículo, en algunos casos, dependiendo del tipo de organización y de sus necesidades, únicamente se realizan algunas de ellas. Pese a la existencia de metodologías concretas para el desarrollo de auditorías informáticas, el factor clave que sin duda hará que los resultados de las mismas respondan a las exigencias de las empresas se encuentra sobre todo en la experiencia y conocimiento de los auditores. ❑