Evaluación de los riesgos

Marzo
2006

Agustín López

Ing. Informático

Lead Auditor BS7799 certificado por BSI

www.iso27000.es

Los esfuerzos e inversiones en seguridad son únicamente beneficiosos si las medidas de seguridad adicionales son aplicadas allí donde realmente es necesario.

Una evaluación precisa del riesgo, acompañada de una estimación de costes asociada es sinónimo de una inversión bien dirigida y mejor protegida. La alternativa significa no estar preparados para las predicciones de amortización.

Los dos ejemplos prácticos de este artículo tratan de exponer, de forma concisa, cómo se puede realizar la evaluación de los niveles de seguridad según modelos de empresa y situaciones diferentes.

El objetivo es mostrar el desarrollo de sistemas de evaluación adecuados a las disponibilidades internas, a la par que funcionales y fácilmente comprensibles a personal interno o externo que necesite aplicarlo o revisarlo.

La evaluación de los riesgos es una de las tareas fundamentales a desarrollar dentro del ciclo de vida del estándar ISO 27001 y debe evitar, dentro de lo posible, complejidades que pongan en riesgo las capacidades y recursos disponibles dentro de la organización para el propio desarrollo o mantenimiento del modelo.

Los modelos de evaluación sobredimensionados o equivocados ponen en riesgo con frecuencia, el inicio y matenimiento del ciclo de vida completo del propio estándar.

Conexión de un almacén externo

- Requisito previo: Políticas de seguridad internas
- Objetivo: Identificación de riesgos no tolerables
- Nivel de detalle utilizado: Grados de estimación
- Frecuencia del estudio: Una única vez; para el establecimiento de la conexión
- Fase en que se realiza el estudio: Análisis
- Área: Aplicaciones/infraestructura.

En este primer ejemplo, un fabricante de automóviles quiere evaluar el riesgo de una nueva conexión con una empresa externa, que solicita el acceso a sus sistemas para el intercambio de información necesaria.

El análisis debe intentar dentro de lo razonable ser calculado sobre una base de factores evaluables y medibles, en donde no se representen estimaciones de carácter variable o subjetivo.

Se define, para ello, una clasificación para los posibles daños económicos del siguiente modo:

- Categoría 1: Daños menores por un valor inferior a 50.000 EUR/año.
- Categoría 2: Daños medios por un valor inferior a 5 Millones de EUR/año.
- Categoría 3: Daños mayores por un valor superior a 5 Millones EUR/año.

La empresa puede ahora, sobre la base de las categorías, asignar los posibles grados de los daños que se pueden presentar según aspectos y escala considerados a continuación:

- Daños personales: 1= leve, 2= enfermedad, 3= grave.
- Consecuencias para el negocio: 1=retraso en la actividad, 2=interrupción de la actividad, 3=cese de la actividad.
- Pérdidas materiales: 1=insignificante, 2=considerable, 3=fuertes pérdidas.
- Pérdidas inmateriales: 1=afectado, 2=daño, 3=pérdida.

Adicionalmente, se estima la probabilidad de que se ocasionen los daños considerando definiciones lo más claras posibles y relacionadas con el negocio:

- Grado 1= probabilidad baja: El daño no ha ocurrido nunca, se trata de un proceso de negocio sencillo o aislado, en un entorno de seguridad TI bien protegido, con flujos de información y procesos regulados, de pequeñas proporciones, atendido por personal especializado...
- Grado 2= probabilidad media: La posibilidad de que se produzca el daño es concebible o ya se ha producido en el pasado, se trata de un proceso de negocio repetitivo, en un área de seguridad TI sometida a presión, con flujos de información y procesos no regulados suficientemente, con estados críticos y personal inexperto, que puede manipularlo de modo negligente...
- Grado 3= Alta probabilidad: Los daños se producen con regularidad y del mismo modo, se trata de procesos de negocio habituales y/o complejos, en entornos de seguridad TI inestables, con flujos de información y procesos no regulados, de grandes proporciones y personal no cualificado, que deliberadamente viola las reglas de seguridad...

Con este esquema, ya podemos obtener para cada situación su categoría de riesgo asociado, mediante la multiplicación del resultado en la evaluación de cada aspecto considerado por la probabilidad de que efectivamente ocurra.

Como resultado final, las situaciones encontradas con valores resultantes:

Entre 1 y 3: podrán permanecer las medidas preventivas existentes.

Entre 4 y 6: se deberán aplicar las medidas técnicas, organizativas y reguladoras de seguridad adicionales, para reducir el nivel de las debilidades.

Valor 9: son necesarias medidas de extrema urgencia para que, siguiendo el ejemplo planteado, la accesibilidad de la empresa externa no ponga en riesgo el propio negocio.

Centros de producción descentralizados

- Requisito previo: Políticas de seguridad internas
- Objetivo: Diferencias en el nivel de seguridad entre los distintos centros
- Nivel de detalle utilizado: Escala numérica de valores
- Frecuencia del estudio: Regularmente
- Fase en que se realiza el estudio: Mantenimiento
- Área: Aplicaciones/infraestructura

En éste segundo ejemplo, una empresa quiere determinar cuales son los niveles de seguridad TI en sus 50 centros de producción. El nivel de seguridad deberá ser valorado, entre otras cosas, mediante un análisis de la situación actual que permita realizar comparaciones con cada uno de los otros centros.

El procedimiento comprende, por tanto, los siguientes 5 puntos:

- Análisis de la política de seguridad.
- Establecimiento de las necesidades de protección.
- Integración de la gestión de la seguridad TI para el mantenimiento de su nivel.
- Definición de los objetivos de seguridad.
- Establecimiento de un manual de pruebas.

El análisis comprendió diversas áreas TI de la seguridad como el software instalados en los ordenadores de los usuarios, métodos de identificación y autorización, controles lógicos de acceso, pasando por cuestiones concernientes a la continuidad de negocio, así como la integridad de los sistemas y encriptación para la seguridad de la red y entorno de las comunicaciones.

En todas las áreas y con la guía del manual de pruebas fueron llevadas a cabo auditorias generales para todos los centros, logrando una evaluación de las medidas de seguridad desarrolladas en cada uno de los centros.

Para las mediciones del nivel de seguridad fue consultada la documentación existente y fueron tomadas muestras aleatorias para las verificaciones realizadas en las localidades visitadas.

El resultado de esta auditoria global se representa finalmente de forma gráfica en diagramas de barras, donde el estado preciso de cada localidad aparece para cada una de las áreas de seguridad examinadas.

Más Información

http://www.theirm.org/riskforum/presentations.html