"Preguntas y respuestas sobre ROSI, Retorno sobre la Inversión de Seguridad"
LINK: http://www.ingenieriacomercial.com/article1182.html

P: ¿Qué es ROSI?
R: ROSI es el **Retorno Sobre la Inversión de Seguridad**, derivado del conocido indicador financiero ROI, Retorno Sobre la Inversión.

P: ¿Entonces puede decirse que ROSI es un ROI especializado?
R: Efectivamente. ROSI busca justificar la inversión en seguridad de la información en términos monetarios. Para ello se tiene presente que los efectos de una implementación de seguridad en general no surgen en forma directa como beneficios económicos para una empresa, sino en todo caso como una reducción en las pérdidas que producen incidentes de seguridad como ataques, fallas o errores. ROSI puede tomarse como el componente financiero del caso de negocio de un proyecto de seguridad, con lo cual es más simple "llegar" a niveles de decisión gerenciales no precisamente técnicos.

P: ¿Cómo se maneja ROSI?
R: El esquema de trabajo de ROSI parte de considerar que cada incidente produce pérdidas que se pueden estimar. Para ello se hacen cálculos del escenario original frente a cada incidente, y del que resultaría de aplicar salvaguardas o contramedidas para mitigarlo adecuadamente. La diferencia entre ambos resultados es el valor o beneficio de dichas salvaguardas. Entonces ROSI (análogamente al ROI) es igual a la relación entre el retorno y el costo de las contramedidas (la inversión en el ROI). El retorno -o ganancia incremental- resulta ser el valor (beneficio en el ROI) menos el costo de dichas contramedidas. Un ROSI aceptable debe ser positivo, lo que resulta cuando el valor es mayor que el costo.

P: ¿Cómo se calculan las pérdidas por ataques o fallas?
R: Generalmente se trabaja con la métrica de gestión de riesgos conocida como ALE. Para ello se estiman los valores probables del impacto monetario y de la frecuencia anual de ocurrencia para cada tipo de incidente, de modo tal que el producto de ambas variables resulta ser el ALE correspondiente.
Este modelo se aplica al estado de seguridad original sin tratar y al tratado con salvaguardas adecuadas, para determinar así lo que permiten ahorrar dichas salvaguardas, o sea el valor de las mismas.
Debido a las suposiciones y valores fijos que involucra el ALE, el ROSI total obtenido guarda un margen importante de incertidumbre que dificulta el análisis y la aprobación de un proyecto de esta naturaleza.

P: ¿Qué hacer entonces?
R: Una forma adecuada de producir estimados cuantitativos razonables consiste en aplicar probabilidades y estadística más la simulación Monte Carlo. Esta simulación es un método de producir múltiples muestras de los resultados a partir de números generados aleatoria e independientemente una y otra vez, que se aplican en cada caso a las variables de entrada en base a la distribución estadística que las caracterice.

P: ¿Cómo se aplica en este caso la simulación Monte Carlo?
R: Primero se establecen los tipos de distribución estadística de ambas variables, generalmente una distribución triangular para los impactos y una uniforme para las frecuencias de ocurrencia. Además, en lugar de fijar una serie de valores discretos para las variables, se establecen rangos cada uno con su mínimo y máximo, así como adicionalmente el valor más probable para la distribución triangular.
La simulación Monte Carlo, por su parte, trabajará dentro de los rangos de cada variable de entrada así como con la distribución estadística correspondiente.
Los resultados se presentan como un histograma de las distribuciones de frecuencias de probabilidades para los diferentes rangos de la variable de salida, así como las frecuencias a*****uladas correspondientes. Al finalizar el proceso se podría decir, por ejemplo, que con un alto porcentaje de certidumbre el valor de las salvaguardas estará entre un mínimo y máximo aceptablemente acotados.
Finalmente, como ya se dijo, el retorno será igual a la diferencia de dicho valor y el costo de las salvaguardas, mientras que ROSI se determina dividiendo dicho retorno por el costo de las mismas.

Para conocer más de este tema, se puede visitar la página http://www.angelfire.com/la2/revistalanandwan donde se encontrará información sobre diferentes cursos, así como pedir sin cargo la nota *ROSI, Retorno Sobre la Inversión de Seguridad*,

preparada por el Ing. Carlos Ormella Meyer.
Fuente: *Ing. Carlos Ormella Meyer*"