Marco Lógico de Ayuda a Principiantes que Planifican en Seguridad Telemática

M. Torrealba y M. Morales

Departamento de Computación y Tecnología de la Información, Universidad Simón Bolívar, Venezuela

1. Asegurar un Sistema Telemático Equivale a Usar la Tecnología como un Medio para Proteger los Procesos del Mismo

El diseño o plan de cualquier régimen de seguridad requiere de ciertas habilidades y conocimientos en la materia que no son fáciles de adquirir. Son muchas las dificultades que se tienen que enfrentar para preparar personal calificado y bien entrenado en el área de sistemas y redes de seguridad [PAR08], también es conocida que la formación académica sigue siendo marginada en esta materia [AGU01]. Además, para algunos trabajadores del conocimiento, implementar la seguridad en los sistemas telemáticos, es equivalente a aplicar una receta. Esto significa que para cada peligro en particular, una solución específica es conocida. Así que los problemas se clasifican en áreas tales como control de acceso, integridad, confidencialidad, disponibilidad y se limitan a la búsqueda de la solución que se considera apropiada. Este mecanismo puede servir en algunos casos, pero difícilmente para todos, porque en la práctica, los sistemas están relacionados entre sí y forman sistemas más complejos que requieren un análisis exhaustivo de la inseguridad. Es importante considerar un conjunto de aspectos relevantes cuando se trata de proteger un sistema telemático, ellos son:

* La seguridad telematica no se consigue a través del empleo de soluciones tecnológicas. La seguridad es un proceso, una percepcion y una condicion.
* La seguridad es variable y puede ser medida con indicadores.
* Como no hay sistema seguro, proveer seguridad significa reducir la inseguridad a niveles tolerables. Esos niveles dependen de los requerimientos, costes y recursos presentes para cada contexto y durante un tiempo.
* Para asegurar un sistema hay que estudiar sus partes y los elementos externos que le afectan. Las fronteras de lo que se va a proteger deben ser colocadas mas allá del mismo.
* Los sistemas telemáticos se vinculan con dependencias funcionales, por lo que un exhaustivo estudio de dichas interacciones debe ser realizado.
* Si se desea proteger un sistema automatizado, el factor humano siempre resulta relevante de considerar. Los sistemas son construidos, configurados, operados y usados por gente. Las personas se equivocan, se confunden, son engañadas, amedrentadas, chantajeadas, sobornadas, a veces actúan malintencionadamente o caen en conflictos de intereses.
* Asegurar un sistema telemático demanda analizar su estructura, dependencias, elementos criticos, premisas de diseño, relaciones de confianza, como puede ser operado y usado.
* A veces la vulnerabilidad que permite subvertir un sistema se apoya en el modo como este es usado, en la forma como ha sido configurado, en la composicion que le dio su fabricante o en la traición de quien se supone lo mantiene o protege. Cada uno de estas amenazas demanda una contramedida diferente y a menudo propia.
* Un sistema telemático opera según principios de funcionamiento. Cada principio se soporta sobre consideraciones de seguridad. Para protegerlo, hay que reconocer y construir sobre los principios de la seguridad presentes, que demarcan la confiabilidad del mismo sistema.
* Los principios de seguridad se reflejan en el modo como los procesos operan. La seguridad puede ser mejorada, reforzando protecciones ante cada riesgo considerable que pueda perjudicar la ejecución de un proceso con el sistema.

2. Principios de la Seguridad Telemática

Para elaborar un plan eficaz en materia de seguridad telemática, el diseñador debe comprender y evaluar la aplicación de ciertos principios de la seguridad. Un principio es algo que sirve como la base, el origen o fundamento de algún fenómeno y se utiliza para explicar su naturaleza. Estos principios de seguridad son los enunciados que se pueden llevar a cabo o no, pero cuya presencia se establecerá cómo la inseguridad o la seguridad en el sistema. A continuación se muestra una lista de ellos: El daño fácil, la protección temporal, el enlace débil, el menor privilegio, la separación de privilegios, estado seguro contra fallas, la correcta economía, aceptación del uso, mediación completa, autoridad concedida, achicar y estirar el tiempo, auditoría externa, base de la confianza, toma de decisiones distribuidas, consolidación a tiempo de la información, protección primero al protector.

3. Planificación de la Seguridad Telemática

La Planificación de la seguridad puede ser modelada en cuatro actividades principales: percepción de la inseguridad, aplicar el marco de seguridad lógico, decidir sobre las protecciones y, por último, la evaluación contra la realidad. La Figura 1 muestra este proceso cíclico. El primer módulo es el nivel de percepción que es muy importante porque si hay algún peligro o riesgo y no se trata, el resto del trabajo puede estar equivocado.

El segundo módulo es donde el marco lógico puede ayudar, porque nos permite ver y organizar toda la compleja realidad de la inseguridad del sistema. El tercer módulo es donde la toma de decisiones se llevará a cabo y cada decisión dará lugar a otros, que tendrán menos influencia sobre la estructura completa del sistema. La salida de este módu-

lo es principalmente planes, pero las políticas de seguridad también se pueden obtener de la organización. Estos son los planes para mitigar los riesgos y para la educación de la comunidad acerca de la inseguridad. La política corporativa va a generar métodos, mecanismos y procedimientos. Algunos de ellos pueden ser muy técnicos e incluso podrían ser automatizados, como pueden ser las tareas diarias de los administradores de sistemas. El último módulo es donde la validación del proceso se lleva a cabo. Para hacer este trabajo bien, aquí es obligatorio el uso de parámetros reales, por ejemplo, los incidentes de seguridad. Otros parámetros, como el retorno sobre la inversión (ROI) que son productos de tareas especializadas deben ser incorporados en el control [ROS07].

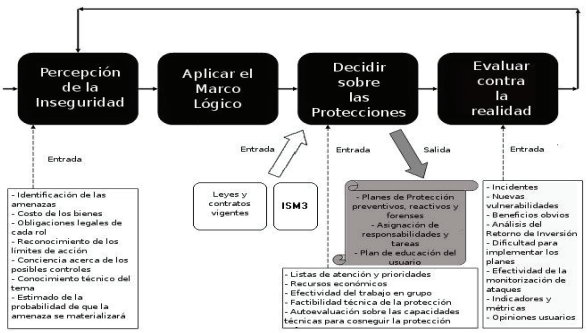

Figura 1: *Etapas de la Planificación*

4. Marco de Seguridad Lógico

A continuación, se presenta la estructura del marco de seguridad lógico. Consta de cuatro componentes fundamentales. En general, el primero está dedicado al diseño del sistema o de planificación, el segundo tiene los principios de la teoría que son el núcleo de la operación. El tercero es sobre los métodos y procedimientos del uso del sistema o de gestión, y el cuarto se refiere exclusivamente a la administración técnica, tal y como se muestra en la Figura 2.

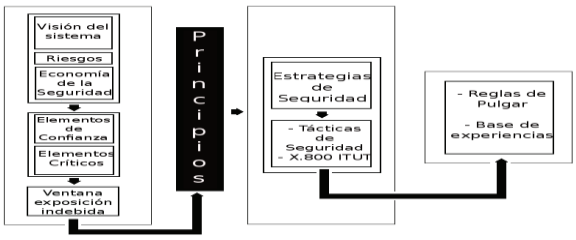

Figura 2: *Núcleo del Marco Lógico*

5. Estratégias de Seguridad Telemática

Para lograr los objetivos de reducir los riesgos en los sistemas telemáticos, la estrategia de seguridad de la organización debe estar alineada con el plan de organización estratégica [CAR04]. En este nivel el impacto de la selección de las actividades realizadas por la directiva, o la alta dirección, será muy importante para todas las acciones y decisiones en los niveles de ejecución de otros. La estrategia afectará a la política de seguridad de las TIC en todos los niveles inferiores. Entre el conjunto de estrategias se deben considerar las siguientes: Seguridad a través de la oscuridad, revelación absoluta, seguridad a través de la diversidad, seguridad a través de la minoría, el costo como el elemento crítico, la facilidad de uso como el elemento crítico, la confidencialidad como el elemento crítico, el tiempo de respuesta como elemento crítico, máximo de transacciones como elemento crítico, la simplicidad y facilidad como ejes del sistema, el desempeño con base al peor caso, la responsabilidad en manos de los expertos, la responsabilidad en manos de todos.

6. Algunas Tácticas de Seguridad Telemática

En este nivel táctico, las directrices deben indicar la forma de aplicar los procesos y tareas. Este nivel es para el administrador técnico, administrador de sistemas o de los operadores. Algunas tácticas son las siguientes: Negación por omisión, aceptación por omisión, enumerar cada peligro, enumerar cada bien a proteger, secuencia de barricadas o alcabalas, usar señuelos, simular debilidad o fortaleza según convenga, dar una área para ganar otra, pretender ir tras algo mientras se persigue otra, usar camuflaje, copiar o generar clones, crear puntos de choque, usar sumideros, amenazar con la vigilancia perenne, incluir ventajas ocultas, esconder la capacidad de respuesta real, usar el ruido para confundir, aplicar la cantidad exacta de hábitos y rutinas, evitar rigidez en localización de los controles y la vigilancia, no olvidar los canales encubiertos, crear distracciones.

Referencias

[AGU01] AGUIRRE J.: Introducción de las Enseñanzas de Seguridad Informática en los Planes de Estudio de las Ingenierías del Siglo XXI. *Jornadas de Enseñanza Universitaria de la Informática. Documento en línea [Microsoft Word®]. Disponible en http://www.criptored.upm.es/guiateoria/gt_m001c.htm* (Recuperado Marzo 27, 2008), (JENUI' 2001).

[CAR04] CARALLI R.: The critical success factor method: establishing a foundation for enterprise security management. Technical report CMU/SEI-2004-TR-010 ESC-TR-010. *Documento en Línea [PDF].Disponible en http://www.sei.cmu.edu/reports/04tr010.pdf.* (Recuperado Abril 3, 2010).

[PAR08] PARQUER D. Skills for the Future. *Documento en Línea [HTML]. Disponible en http://www.securityfocus.com/columnists/464.* (Recuperado Marzo 22, 2008).

[ROS07] ROSENQUIST M. Measuring the Return on IT Security Investments. Intel Corporation Whitepaper. *Documento en línea [PDF]. Disponible en http://communities.intel.com/servlet/JiveServlet/downloadBody/1279-102-1-13 05/Measuring%20the%20Return%20on%20IT%20Security%20Investments.pdf.* (Recuperado Mayo 5 2010).