CONCLUSIONES

"Un largo camino comienza con su primer paso"

Proverbio Chino

AISLAMIENTO VS GLOBALIZACIÓN

Abierta, Universal, Económica y Segura. Esas son las propiedades que adjudican algunos a la información. Lograr estándares en el mundo altamente tecnificado de hoy es quizás la principal barrera con las que chocan los profesionales para "asegurar la Seguridad".

Por otro lado, la situación internacional actual exige una concientización, por parte de todos, que la información es conocimiento y como tal debemos atribuirle la importancia que merece. Esta importancia incluye estudiar y lograr la forma de protegerla.

Esto plantea una paradoja:

- si sumamos seguridad, bajan las posibilidades de acceder a la información, lo que es igual al Aislamiento y la Marginación.
- si sumamos información, lo hacemos de forma insegura, lo que nos hace Globalmente Vulnerables.

La convergencia de los sistemas multiplica exponencialmente los problemas de seguridad planteados. El equilibro es difícil, el espectro a cubrir es amplio y, como dificultad

extra, el campo de trabajo es intangible. Esto hace necesario desarrollar técnicas y/o adaptar las existentes de forma tal de circunscribir nuestro trabajo de conseguir información–conocimiento dentro de un marco de seguridad.

DISEÑO SEGURO REQUERIDO

Cuando se diseña un sistema se lo hace pensando en su Operatividad–Funcionalidad dejando de lado la Seguridad

Será necesario establecer una correspondencia y pertenencia entre las técnicas adoptadas conformando un sistema de seguridad; y no procedimientos aislados que contribuyan al caos general existente. Esto sólo puede lograrse al integrar la seguridad desde el comienzo, desde el diseño, desde el desarrollo.

LEGISLACIÓN VIGENTE

Las tecnologías involucradas en estos procesos condicionan las técnicas empleadas, los tiempos condicionan esas tecnologías y, paradójicamente, las legislaciones deben adaptarse a los rápidos cambios producidos. Esto hace obligatorio no legislar sobre tecnologías actuales, sino sobre conceptos y abstracciones que podrán ser implementados con distintas tecnologías en el presente y el futuro.

Es urgente legislar un marco legal adecuado, no solo que castigue a los culpables sino que desaliente acciones hostiles futuras.

TECNOLOGÍA EXISTENTE

Existen infinidad de métodos (muchas veces plasmados en herramientas) que permiten violar un sistema.

El profesional cuenta con la misma tecnología para la evaluación de la seguridad del bien a proteger y otras pensadas para la protección como fin. Esto hace que muchas veces, la seguridad, sea asunto de la idoneidad del profesional.

En algunos campos, la Tecnología deberá ampararnos ante la desaparición de elementos naturales. Por mencionar un ejemplo: la firma digital (Tecnología Criptográfica) debe cubrir la brecha que deja la inexistencia de la firma caligráfica en archivos de información.

DAÑOS MINIMIZABLES

Algunos pocos métodos realmente novedosos de infiltración ponen en jaque los sistemas de seguridad. Aquí, se prueba la incapacidad de lograr 100% de seguridad, pero también es hora de probar que los riesgos, la amenaza, y por ende los daños pueden ser llevados a su mínima expresión.

Muchas veces vasta con restringir accesos a información no utilizada o que no corresponde a los fines planteados. Otras veces la capacitación será la mejor herramienta para disminuir drásticamente los daños.

RIESGOS MANEJABLES

He probado (me he probado) que: La Seguridad Perfecta requiere un nivel de perfección que realmente no existe, y de hecho dudo que algún día exista, pero los riesgos deben y pueden ser manejables.

COSTOS

El costo en el que se incurre suele ser una fruslería comparados con aquellos luego de producido un daño. El desconocimiento y la falta de información son el principal inconveniente cuando se evalúa la inclusión de seguridad como parte de un sistema.

PERSONAS INVOLUCRADAS

El desarrollo de software es una "ciencia" imperfecta; y como tal es vulnerable. Es una realidad, y espero haberlo demostrado en el extenso capítulo de "Amenazas Humanas", que la Seguridad involucra manipulación de naturaleza humana.

Es importante comprender que:

1. La Seguridad consiste en Tecnología y Política. Es decir que la combinación de la Tecnología y su forma de utilización determina cuan seguros son los sistemas.
2. El problema de la Seguridad no puede ser resuelto por única vez. Es decir que constituye un viaje permanente y no un destino.
3. En última instancia la Seguridad es una serie de movimientos entre "buenos" y "malos".

A manera de despedida deseo dejar un resumen realizado por el equipo de Microsoft Security Response Center sobre la forma y el cuándo nuestra computadora deja de ser nuestra.

Las 10 Leyes Inmutables de la (in)seguridad

I. Si una mala persona puede persuadirlo para ejecutar su programa en SU computadora, esta deja de ser suya.
II. Si una mala persona puede alterar el sistema operativo en SU computadora, esta deja de ser suya.
III. Si una mala persona tiene acceso físico sin restricción a SU computadora, esta deja de ser suya.
IV. Si usted permite a una mala persona, subir un programa a SU sitio web, este deja de ser suyo.
V. Las contraseñas débiles constituyen un atentado a la seguridad.
VI. Una sola máquina es segura en la medida que el Administrador es fidedigno.
VII. Los datos encriptados son seguros en la misma medida que la clave de desencriptación lo sea.
VIII. Un antivirus desactualizado sólo es parcialmente mejor que ninguno.
IX. La anonimicidad absoluta no es práctica, ni en la vida real ni en la web.
X. La tecnología no es una panacea.