Inseguridad informática: Un concepto dual en seguridad informática[!]

Jeimy J. Cano, Ph.D (*)
Profesor de Cátedra
Departamento de Sistemas y Computación

Resumen

Este documento desarrolla una breve reflexión donde sugiere al lector repensar la seguridad informática como un continuo entre técnicas de *hacking* y análisis de riesgos, que permita a las organizaciones aprender de sus fallas de seguridad y fortalecer sus esquemas de seguridad, no para contar con mayores niveles de seguridad, sino para evidenciar el nivel de dificultad que deben asumir los intrusos para ingresar a los sistemas.

Abstract

This article develops a brief reflection related with hacking techniques and risk analysis strategies as a continue line, in order to rethink computer and information security concept, that enable organizations to learn about its security vulnerabilities and enhance its security architectures, not to increase computer security levels but determine difficulty level required for intruders to compromise information systems.

Introducción

Al terminar un año e iniciar el siguiente, generalmente se presentan los resultados de la gestión del que concluye y se establecen los pronósticos sobre el venidero. El tema de seguridad informática no es ajeno a esta dinámica del mundo, es quizá uno de los tópicos donde los especialistas en el área buscan afanosamente establecer líneas de acción sobre características especiales de los acontecimientos que pasaron y podrán ser influyentes en el futuro.

Revisando algunos de los pronósticos para el 2004 en el tema de seguridad [GREGORY, P. 2003, SAVAGE, M. 2003] encontramos que temas como: el SPAM, los firewalls personales, los dispositivos de almacenamiento USB, organizaciones criminales en internet, las crecientes regulaciones en el ámbito tecnológico, entre otros, serán elementos importantes donde muchos cambios y actividades tomarán lugar y generarán eventos que impactarán las organizaciones y la operación de las mismas.

Observando las reflexiones sobre las predicciones y concentrándonos en la estructura de pensamiento plasmada en las mismas, es frecuente observar que estos pronósticos muchas veces responden a eventos que en el pasado han ocurrido y se manifiestan como posibles tendencias, reflejando un pensamiento lineal que sugiere continuidad y avance, pero algunas veces negación de los temas en sí mismos. Es decir, las predicciones responden a causas y efectos que pueden ser establecidos y revisados. Sin causas no habría efectos, lo que se conoce en el pensamiento filosófico como dualismo.

[!] Este artículo fue publicado en: Revista de Ingeniería. No.19. Universidad de los Andes. Facultad de Ingeniería. Mayo 2004. ISSN:0121-4993.

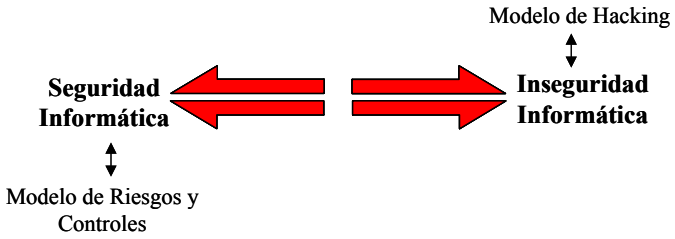

Figura 1. Dualismo de la Seguridad Informática

El dualismo, ha sido factor clave para el desarrollo de muchos conceptos que hoy en día son fundamentales para el avance de la tecnología y la seguridad informática, pero no es la única estrategia para abordar los fenómenos de nuestra realidad. En la perspectiva del dualismo un sistema es seguro o inseguro, lo que implica reconocer y profundizar en un lado de la línea de pensamiento. Es decir, o aplicamos técnicas de seguridad informática para reducir los riesgos e implementar controles, ó vemos como podemos saber que tantas vulnerabilidades tenemos que nos hacen inseguros, para tomar medidas correctivas.

En este sentido, presentamos la estrategia de la dualidad, como una manera complementaria de explorar los hechos mismos en el mundo, para reconocer las causas y los efectos en su contexto, sin negar la posibilidad de considerar que uno surge a partir del otro, es decir, reconocer que la seguridad informática surge a partir de considerar la inseguridad informática y viceversa; un continuo de aprendizaje que muchas veces no corresponde a una causa específica sino a la relaciones existentes entre los componentes objeto del análisis. (ver figura 2)

Con estas ideas planteadas se desarrolla este breve documento donde revisamos el concepto de inseguridad informática desde una perspectiva dual como una manera complementaria de comprender los elementos, relaciones y efectos de la seguridad informática en el contexto de una realidad cambiante y dinámica. Los planteamientos sugeridos en este artículo responden a reflexiones recogidas de la experiencia de la industria al tratar de enfrentar la variabilidad de los escenarios y sus vulnerabilidades y, las ideas de la academia para profundizar en eventos predecibles e inesperados de la dinámica entre la tecnología, la organización y los individuos.

La dualidad de la Inseguridad Informática

En múltiples investigaciones realizadas se considera el tema de la seguridad informática como una disciplina del conocimiento donde se busca cerrar la brecha de los eventos inesperados que puedan comprometer los activos de una organización y así contar con estrategias para avanzar ante cualquier eventualidad.

Consideremos ahora el estudio de la inseguridad informática, como una disciplina dual donde los académicos y practicantes de la industria buscan las maneras detalladas para que ocurran eventos inesperados, establecer las condiciones extremas de funcionamiento de los dispositivos o estrategias, todo con el fin de hacer caminar en condiciones límite la operación de la organización y sus negocios. La estrategia dual sugiere contextualizar en un escenario real la incertidumbre inherente de la seguridad informática para revisar entre otros aspectos: [SCHNEIER 2003, pag. 51]

- ¿Cómo funciona el sistema?
- ¿Cómo no funciona el sistema?
- ¿Cómo reacciona ante una falla?
- ¿Cómo hacerlo fallar?

Por tanto, la inseguridad informática como disciplina dual en el estudio de la seguridad informática, establece un paradigma complementario (es decir dual a la seguridad informática) que comprende las propiedades emergentes de los sistemas (analizados) bajo condiciones y realidades extremas, las cuales no son viables en una estrategia de protección causal (dualismo) sugerida por la seguridad informática actual. En este sentido, se quiere plantear la necesidad de revisar nuestra manera de abordar el tema de la protección de los activos de una organización, no solamente establecer las causas y los efectos, sino comprender las relaciones entre los objetos revisados y considerar las reacciones mismas entre estas que pueden sugerir efectos no predecibles en los modelos causales. Es decir conociendo que tan inseguros somos, podemos comprender que tan seguros podríamos llegar a ser.

Cuando se plantean las condiciones de análisis de la seguridad y las pruebas de los elementos de los sistemas se consideran, entre otros, algunos elementos comunes como son: [WHITTAKER 2003, pag. 3]

- Se requiere que el equipo de pruebas trabaje sobre la descripción del comportamiento del producto o sistema,
- Se requiere que el producto o sistema sea ejecutado en un ambiente real o simulado,
- Se requiere que la funcionalidad del producto o sistema sea explorada de una manera metódica y que los resultados de las pruebas bien sean positivos o negativos, puedan ser analizados en contexto y así ofrecer un concepto formal del mismo;

en este contexto, las relaciones causales deben ser determinadas y concretadas de tal manera que sea posible detallar y sustentar los posibles estados exhibidos por el sistema al ser sometido a las pruebas de comportamiento sugeridas dentro del dominio de la definición del producto mismo. Esta estrategia si bien aporta elementos detallados sobre el sistema y su funcionamiento futuro, nos ofrece pocas luces sobre comportamientos inesperados y condiciones extremas de operación, dado que no se abre la posibilidad a una lógica de la inseguridad informática como reflexión dual del ejercicio.

Al revisar la inseguridad informática como estrategia de pensamiento estratégico reconocemos que un sistema es tan seguro como su falla de seguridad más reciente, que cuando ocurre o se manifiesta un problema de seguridad las personas se vuelven mas experimentadas y saben que hacer, que los sistemas mal diseñados (pensamiento natural en seguridad informática) no están preparados para fallar (pensamiento dual en inseguridad informática). En pocas palabras, comprender la inseguridad informática del sistema en evaluación para hacer el sistema dinámico y flexible ante nuevos ataques, atacantes o fallas de seguridad. [SCHNEIER 2003, Cap.9]

La inseguridad informática como pensamiento dual en seguridad informática descubre que las relaciones entre los elementos del sistema son capaces de producir efectos positivos y negativos, los cuales son capaces de comprometer su supervivencia. En este sentido, comprender la inseguridad informática como el dual de la seguridad informática, en el contexto organizacional, representada esta última en sus participantes, sus procesos y tecnología [CANO 2004], nos permite revisar las propiedades emergentes de la seguridad informática en un escenario con múltiples variables, repensar la seguridad misma mas allá de una directriz de la corporación, como una mente pensante que aprende y evoluciona en su hacer.

Explorando la dualidad de la Seguridad: La mente segura

El concepto de la organización como una mente pensante y actuante, con un pensamiento complementario (dual) nos sugiere que la seguridad informática, como una distinción mas de la organización, representa una dinámica de acción que podríamos recrear considerando los elementos de la mente segura sugeridos por Day. Para Day [DAY 2003, pág.5] una mente segura consiste en la revisión y práctica de *virtudes* y *reglas de seguridad*[1] con el fin de tomar decisiones claras, consistentes y efectivas. Complementario a esta propuesta, la existencia de la mente insegura, como realidad presente de la organización, es un punto de análisis adicional que se considera, no solo para dar sentido a la práctica de las virtudes y reglas de seguridad, sino para mantener la perspectiva de la incertidumbre inherente al proceso de la seguridad informática.

La mente insegura como dual de la mente segura, puede sugerir elementos de análisis de situaciones extremas en las organizaciones que lleven no solamente a considerar las vulnerabilidades y riesgos de las información de los procesos de la empresa, sino repensar los procesos mismos para hacerlos mas confiables, en la medida que se consideren las diferentes perspectivas de la seguridad implícitas en cada uno de los participantes de los mismos. La mente insegura es una posibilidad de caminar y repensar el análisis de riesgos como un modelo de *hacking* [HORTON, M y MUGGE, C. 2003,

[1] Las virtudes de la seguridad son: La seguridad deber ser una consideración diaria, la seguridad debe ser un esfuerzo comunitario, las prácticas de seguridad deben mantener un foco generalizado, las prácticas de seguridad deben incluir medidas de entrenamiento para todo el personal de la organización.
Las reglas de seguridad son: Regla del menor privilegio, Regla de los cambios, Regla de la confianza, Regla del eslabón más débil, Regla de separación, Regla de los tres procesos, Regla de la acción preventiva y Regla de la respuesta apropiada e inmediata

pág.38] consistente de reconocimiento del sistema objetivo, manipulación y compromiso del objetivo, apalancamiento del ataque y conquista de nuevos objetivos.

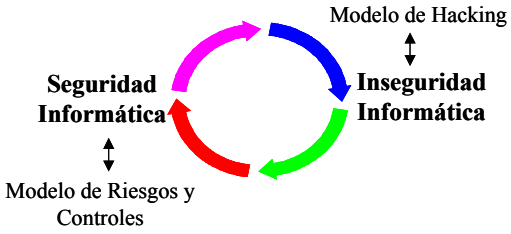

Figura 2. Concepto Dual de la Inseguridad Informática

En razón a lo anterior, la mente insegura, al igual que la inseguridad informática son parte de un mismo continuo que busca entender que la seguridad informática como necesidad organizacional, no es mas que el resultado de una propiedad emergente de un sistema que conoce sus condiciones extremas, su operación límite, así como sus recursos y posibilidades para darle sentido a la razón de su misión. Es decir, reconocer que los ataques y fallas de seguridad informática son una constante y por tanto, se requiere conocer y validar los niveles de siniestralidad o falla que la organización puede manejar en la operación de su negocio.

Reflexiones Finales

Mientras la seguridad informática es un concepto subjetivo [SCHNEIER, B. 2003, pág.23], es decir propio al sujeto, la inseguridad informática es objetiva, es decir propia al objeto. No es posible evitar la inseguridad informática pues es una propiedad inherente a los objetos. Por tal motivo, se hace necesario explorar en profundidad dicha propiedad, pues mientras mas se comprenda la realidad de la inseguridad, con mejores ojos podremos comprender la seguridad informática de las organizaciones.

Considerar la inseguridad informática como parte del ejercicio de seguridad informática de las organizaciones, sugiere la capacidad de las organizaciones para cuestionarse sobre la situación real del balance entre seguridad, facilidad de uso y funcionalidad [COLE, E. 2002,pág. 23] no para lograr mayores niveles de confiabilidad y aseguramiento de sus arquitecturas, sino para evaluar el nivel de dificultad requerido por los atacantes para ingresar y vulnerar los medios de protección. Con un pensamiento de este nivel, las organizaciones no buscarán solamente incrementar la confianza de sus clientes, sino comprender que la seguridad no es un problema de tecnología, sino un problema de riesgos y las diferentes maneras de comprenderlos y manejarlos: una mente segura.

Mientras más se conoce la inseguridad informática más se comprenden las acciones y resultados de la seguridad en las organizaciones. En este sentido, la detección de posibles problemas de seguridad no generaría valor sin una adecuada respuesta. Una respuesta que reconozca la inseguridad informática como insumo y el ataque de seguridad como una variante a considerar en la protección de los activos. En consecuencia cuando somos capaces de reconocer y actuar en situaciones inesperadas, nuestra capacidad de análisis y

control aumenta, pues nuevas perspectivas se abren a las relaciones que exhibe la inseguridad informática.

Finalmente las palabras "impenetrable", "invulnerable" o "seguro", nos recuerdan que existen procesos, muchas veces ocultos a nuestro pensamiento, que pondrán a prueba la realidad de los sistemas y sus propiedades. La inseguridad informática es pues una estrategia de reflexión y acción para repensar la seguridad informática como una disciplina que es al mismo tiempo concepto y realidad.

Referencias

CANO, J. (2004) Hacia un concepto extendido de la mente segura. Pensamiento sistémico en seguridad informática. Artículo de investigación (En revisión). Universidad de los Andes

COLE, E. (2002) Hackers beware. Defending your network from the wiley hacker. New Riders.

DAY, K. (2003) Inside the security mind. Making the tough decisions. Prentice Hall.

GREGORY, P. (2003) Security predictions for 2004. ComputerWorld. http://www.computerworld.com/printthis/2003/0,4814,88113,00.html. Diciembre.

HORTON, M y MUGGE, C. (2003) Hacknotes. Network Security Portable Reference. McGraw Hill.

SAVAGE, M. (2003) Time to act. New Challenges in 2004. Secure Computing Magazine. http://www.scmagazine.com/scmagazine/2003_12/cover/index.html. Diciembre.

SCHNEIER, B. (2003) Beyond Fear. Thinking Sensibly about security in an uncertain world. Copernicus Books.

WHITTAKER, J. (2003) How to break software. A practical guide to testing. Addison Wesley.

Datos del Autor:

Jeimy J. Cano, Ph.D

Profesor de Cátedra de la Facultad de Derecho y del Departamento de Sistemas y Computación de la Universidad de los Andes, donde se concentra en los temas de Seguridad Informática, Computación Forense y Evidencia Digital.

Coordinador Académico de la IV Jornada Nacional de Seguridad Informática – ACIS 2004. Mayor información: http://www.acis.org.co. Contacto: *jcano@uniandes.edu.co*