Propuesta de un Modelo de Proceso para Resolver Vulnerabilidades de Seguridad en Infraestructura Utilizando Herramientas de Computación Cognitiva

Darío Propato, Jorge Eterovic, Marisa Panizzi, Luis Torres
Facultad de Informática, Ciencias de la Comunicación y Técnicas Especiales,
Universidad de Morón.
Cabildo 134 – CP (1708) – Morón – Prov. de Bs. As. Tel: 5627-2000
dariopropato@gmail.com; jorge_eterovic@yahoo.com.ar; marisapanizzi@outlook.com;
torreslu@ar.ibm.com

Resumen

El objetivo de este trabajo de investigación consiste en el desarrollo de un modelo de proceso que permita resolver vulnerabilidades de Seguridad Informática utilizando herramientas de la computación cognitiva. Este servirá como guía a los profesionales de informática que se desempeñen en áreas de seguridad de la información. Los sistemas cognitivos pueden aprender de sus experiencias, encontrar correlaciones, crear hipótesis y recordar los resultados y aprender de ellos. Esta capacidad de los sistemas cognitivos tendrá una influencia crucial en la toma de decisiones por parte de múltiples interesados y la solución a construir tomara como base las ventajas de este tipo de sistemas. Se realizó una revisión sistemática de un par de modelos de procesos de software como por ejemplo MoProSoft y Métrica versión 3, para considerar de ellos los elementos propuestos y ser contemplados en la propuesta de solución de esta investigación. Para llevar a cabo la [illegible] caso real de una organización.

Palabras clave: Computación cognitiva, Modelo de Proceso, Seguridad en Infraestructura, Vulnerabilidades, Tiempo de Detección.

Contexto

Este trabajo de investigación se encuentra radicado en el Instituto de Ingeniería de Software Experimental perteneciente a la Facultad de Informática, Ciencias de la Comunicaciones y Técnicas Especiales de la Universidad de Morón. El Instituto articula con las cátedras de tesis de la carrera Licenciatura en Sistemas y con la cátedra de Auditoria y Seguridad de los Sistemas de información.

Introducción

Ha sido necesario llevar a cabo una investigación exploratoria documental de antecedentes de la computación cognitiva, y aspectos de vulnerabilidades y modelos de procesos de software.

Según Kelly, los sistemas cognitivos son probabilísticos, significa que son diseñados [illegible] la complejidad e [illegible] información. Interpretan la información, la organizan y ofrecen una explicación de su significado junto con la justificación de sus conclusiones. No ofrecen una respuesta definitiva (John E. Kelly, 2015).

Desde el punto de vista de Briggs, la analítica cognitiva está inspirada en como el cerebro humano procesa información, saca conclusiones y codifica instintos y la experiencia de aprendizaje. En lugar de aprender sobre reglas predefinidas y consultas estructuradas para encontrar respuestas, el análisis cognitivo se basa en tecnología para generar hipótesis de una amplia variedad de información relevante y conexiones (Briggs, 2014).

Entre los desarrollos recientes, basados en computación cognitiva y que actualmente se encuentra funcional es la herramienta Watson de IBM, que es un sistema de inteligencia artificial con la capacidad de responder a preguntas formuladas en lenguaje natural, desarrollado por IBM. Es parte del proyecto del equipo de investigación DeepQA para la generación de hipótesis, la recopilación de pruebas masivas, el análisis y la calificación (DeepQA Project, 2011).

Para la construcción del modelo se tomaron como base modelos de procesos de software y metodologías que actualmente se encuentran validados y permiten una adaptabilidad al proyecto planteado. Algunos de los seleccionados se detallan a continuación:

- Métrica versión 3, es una metodología de planificación, desarrollo y mantenimiento de sistemas de información para la sistematización de actividades del ciclo de vida de los proyectos de software en el ámbito de la administración pública de España. Está basada en el modelo de procesos del ciclo de vida de desarrollo ISO/IEC 12207 así como en la norma ISO/IEC 15504 SPICE (Ministerio de Hacienda y Obras Públicas del Gobierno de España, 2001).
- MoProSoft (Modelo de Procesos para la Industria del Software), es un modelo para la mejora y evaluación de los procesos de desarrollo y mantenimiento de sistemas y productos de software. Está dirigido a las organizaciones dedicadas al desarrollo y mantenimiento de software (NORMA NMX-I-059-NYCE-2005)

Se consideró la revisión de la ISO/IEC 27002, la cual proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran) (ISO/IEC 27002, 2013)

El problema que motiva la elaboración de este trabajo es la existencia de vulnerabilidades en la seguridad de los sistemas de información y los elevados tiempos de detección. El objetivo es solucionar las vulnerabilidades con el uso de computación cognitiva y, a partir del mismo, generar un modelo específico, dado que los modelos propuestos no soportan o no son adecuados para el proceso de seguridad de la información. Es decir, solo son aplicables para el ciclo de vida del software. La computación cognitiva provee un desafío en cuanto a su utilización e implementación por el escaso conocimiento que se tiene de la misma. Todo esto ocasiona que los profesionales de sistemas involucrados en la seguridad de la información no cuenten con

un modelo específico para desarrollar la implementación de una herramienta de computación cognitiva dentro de una organización para solucionar vulnerabilidades de seguridad.

Entre los conceptos de vulnerabilidad informática revisados se puede mencionar el propuesto por Cencini, en el cual la define vulnerabilidad como una falla se convierte en una vulnerabilidad si el comportamiento expuesto es tal que puede ser explotado para permitir el acceso no autorizado, elevación de privilegios o denegación de servicio (Cencini, 2005).

La ISO 27005 define vulnerabilidad como: una debilidad de un activo o grupo de activos que pueden ser explotados por una o más amenazas (ISO 27005, 2008).

La Agencia Europea de Seguridad de las Redes y de la Información (ENISA) conceptualiza vulnerabilidad como la existencia de una debilidad, diseño o error de implementación que puede conducir a un evento inesperado e indeseable que compromete la seguridad del sistema informático, la red, la aplicación o el protocolo involucrado (ENISA, 2016)

Entre las principales vulnerabilidades informáticas analizadas, se seleccionaron aquellas de mayor importancia en los informes anuales de seguridad:

- Malware
- Pishing
- Amenaza interna

Según Moir, el término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto" (Moir, 2003).

El análisis de malwares de Cisco encontró que la mayoría (91,3%) utilizan los DNS (Sistema de Nombre de Dominios) para ganar control y acceso a comandos, filtrar datos y redirigir tráfico." (Cisco Annual Security Report, 2016).

Pishing,"es el intento de obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito (e indirectamente dinero), a menudo por razones maliciosas, disfrazándose como una entidad confiable en una comunicación electrónica" (Ramzan, 2010).

Una Amenaza interna (en Ingles, Insider threat) según el FBI: es una amenaza malintencionada a una organización que proviene de personas dentro de la organización, como empleados, contratistas o asociados al negocio, que tienen información privilegiada sobre las prácticas de seguridad de la organización, los datos y los sistemas informáticos. La amenaza puede incluir el fraude, el robo de información confidencial o comercialmente valiosa, el robo de la propiedad intelectual o el sabotaje de los sistemas informáticos (FBI, 2016).

Una de las amenazas con mayor incidencia son los ataques a las redes informáticas, los mismos tienen variantes y diferentes objetivos, como:

- Los ataques de denegación de servicio, según RFC4732 es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos (RFC4732, 2006).

- Ataques de fuerza bruta, según la Electronic Frontier Foundation: es un ataque criptoanalítico que puede ser utilizado para desencriptar y encriptar datos. Este tipo de ataque es utilizado

cuando no es posible obtener ventajas de otras debilidades en un sistema de encriptación (Electronic Frontier Foundation, 1998)

Las vulnerabilidades mencionadas afectan en la mayoría de los casos a los dispositivos pertenecientes a la infraestructura de sistemas de la compañía. El volumen de información siempre creciente eleva el tiempo de detección (TTD), es decir, "la ventana de tiempo entre la primera observación de un archivo que ha pasado por todas las tecnologías de seguridad para llegar a un punto final y la detección de una amenaza asociada con ese archivo. Se estima en la industria actual un tiempo inaceptable de 100 a 200 días."(Cisco Annual Security Report, 2016).

Resultados y Objetivos

En esta etapa del proyecto se ha llevado a cabo una investigación exploratoria y documental de los tres ejes sobre el cual se basa la solución propuesta: computación cognitiva, vulnerabilidades de infraestructura y modelos de procesos.

Se ha comenzado a bosquejar las fases/actividades/tareas que contemplaran el modelo de proceso de proponer.

También se está analizando cual será el caso testigo para la validación del modelo propuesto.

Formación de Recursos Humanos

Actualmente el equipo de investigación está integrado por un estudiante de la carrera Licenciatura en Sistemas, por dos docentes-investigadores y un docente que inicia su proceso de formación como investigador pertenecientes a la Facultad de Informática, Ciencias de la Comunicación y Técnicas Especiales, Universidad de Morón.

Bibliografía

Kelly, John E., (2015). Computing, cognition and the future of knowing, IBM.

Briggs, Bill. (2014). Tech Trends 2014 Inspiring Disruption. Consulta realizada en https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/technology/deloitte-uk-tech-trends-2014.pdf

IBM Research (2011). DeepQA Project. Consulta realizada en http://www.research.ibm.com/deepqa/deepqa.shtml

Ministerio de Hacienda y Administraciones Públicas del Gobierno de España, (2001). MÉTRICAv3.Consulta realizada en http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Metrica_v3.html

Asociación Mexicana para la Calidad en Ingeniería de Software, (2005). MoProSoft. NMX-059/02-NYCE-2005.

Hurwitz, Judith, (2015). Cognitive Computing and Big Data Analytics: Implementing Big Data Machine Learning Solutions. ISBN: 1118896629.

ISO/IEC 27002:2013, (2007).Information technology Security techniques. Consulta realizada en http://www.iso27001security.com/html/27002.html.

Cencini, Andrew, (2005).Software Vulnerabilities: Full-, Responsible, and Non-Disclosure. Consulta realizada en https://courses.cs.washington.edu/courses/csep590/05au/whitepaper_turnin/software_vulnerabilities_by_cencini_yu_chan.pdf

ISO/IEC FIDIS 27005:2008, (2008). Information technology -- Security techniques-Information security risk management Consulta realizada en http://www.iso27001security.com/html/27005.html

ENISA (2016) ,Vulnerabilities and exploits. Consulta realizada en https://www.enisa.europa.eu/topics/national-csirt-network/glossary/vulnerabilities-and-exploits

Moir, Robert, (2003). Defining Malware. Microsoft Security MVP. Consulta realizada en https://technet.microsoft.com/en-us/library/dd632948.aspx

CISCO, (2016). Annual Security Report. Consulta realizada en http://mkto.cisco.com/rs/564-WHV-323/images/cisco-asr-2016.pdf

Ramzan, Zulfikar, (2010). Phishing attacks and countermeasures. Handbook of Information and Communication Security. ISBN 9783642041174.

FBI, (2016).The Insider Threat: An Introduction to Detecting and Deterring an Insider Spy, , https://www.fbi.gov/file-repository/insider_threat_brochure.pdf.

IETF Trust, (2006). Internet Denial-of-Service Considerations (RFC4732). Consulta realizada en https://tools.ietf.org/html/rfc4732

Electronic Frontier Foundation, (1998) . Cracking DES – Secrets of Encryption Research, Wiretap Politics & Chip Design. ISBN 1- 56592-520-3.

Symantec. (2016). Internet Security Threat Report. Consulta realizada en https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf