ISSN 0121-1129
eISSN 2357-5328

Estudio y gestión de vulnerabilidades informáticas para una empresa privada en el departamento de Boyacá (Colombia)

Information Vulnerabilities' Study and Management, for a Private Enterprise in the Boyacá Colombian Department

Estudo e gestão de vulnerabilidades informáticas para uma empresa privada no Estado de Boyacá (Colômbia)

Fecha de Recepción: 20 de Mayo de 2014
Fecha de Aceptación: 10 de Junio de 2014

Julián Alberto Monsalve-Pulido*
Fredy Andrés Aponte-Novoa**
David Fernando Chaves-Tamayo***

Resumen

Se expone el resultado del diagnóstico de seguridad informática realizado a una organización privada en el departamento de Boyacá (Colombia), y de la creación y aplicación de un plan de gestión de vulnerabilidades diseñado a la medida de las necesidades de dicha organización. Se inició la investigación con el levantamiento del inventario tecnológico de la empresa, para identificar los problemas que pueden causar alguna vulnerabilidad que afecte la seguridad de la información. Tras una etapa de 6 meses de monitoreo del plan de gestión dentro de la empresa, se evidenció la efectividad de éste, pues se logró una reducción del 70% en las vulnerabilidades, con la aplicación de algunos remedios previamente diseñados. Por otro lado, en el artículo se muestran algunos cuadros comparativos de herramientas informáticas que fueron seleccionadas y utilizadas en la aplicación de las etapas del plan de gestión, ya que pueden ayudar a investigaciones futuras a la selección de herramientas para el monitoreo y gestión de vulnerabilidades.

Palabras clave: Análisis de riesgos, Seguridad de la Información, ISO 27000, Vulnerabilidades.

* M.Sc. Universidad Santo Tomás (Tunja-Boyacá, Colombia). julian.monsalve@usantoto.edu.co
** M.Sc. Universidad Santo Tomás (Tunja-Boyacá, Colombia). fredy.aponte@usantoto.edu.co
*** Universidad Santo Tomás (Tunja-Boyacá, Colombia). manfredsoft@gmail.com

Abstract

The paper shows an informatics security diagnosis' results, applied to a private organization in the department of Boyacá, Colombia. It developed and implemented a vulnerability plan management, tailored according to that organization's needs. It began by raising the company's technological inventory, in order to identify the real problems that can cause any information security vulnerabilities. This research showed the plan's effectiveness, within the company, achieved after a 6-month monitoring period. It reached 70% vulnerabilities' reduction, by applying some remedies previously designed. Furthermore, the paper shows several comparative informatics tools' tables, which were selected and used in the management plan's application stage that could be a help for a future research, in the tools selection for monitoring and vulnerability's management.

Keywords: Information Security, ISO 27001, Risk analysis, Vulnerabilities.

Resumo

Expõe-se o resultado do diagnóstico de segurança de informática realizado a uma organização privada no Estado de Boyacá (Colômbia), e da criação e aplicação de um plano de gestão de vulnerabilidades desenhado à medida das necessidades de dita organização. Iniciou-se a pesquisa com o levantamento do inventário tecnológico da empresa, para identificar os problemas que podem causar alguma vulnerabilidade que afete a segurança da informação. Trás uma etapa de 6 meses de monitoramento do plano de gestão dentro da empresa, se evidenciou a efetividade deste, pois se logrou uma redução do 70% nas vulnerabilidades, com a aplicação de alguns remédios previamente desenhados. Por outro lado, no artigo se mostram alguns quadros comparativos de ferramentas informáticas que foram selecionadas e utilizadas na aplicação das etapas do plano de gestão, já que podem ajudar a pesquisas futuras à seleção de ferramentas para o monitoramento e gestão de vulnerabilidades.

Palavras chave: Análise de riscos, Segurança da Informação, ISO 27000, Vulnerabilidades.

I. Introducción

En la actualidad, las empresas tanto del sector público como del privado priorizan la seguridad de la información, que es catalogada como uno de los bienes más preciados para la continuidad del negocio y el punto de diferencia con la competencia. La seguridad de la información dentro de una empresa tiene varios aspectos: seguridad de acceso, seguridad de dispositivos, manejo de contraseñas y control de vulnerabilidades, entro otros, y cada uno de estos requiere un estudio, un presupuesto y una aplicación, ya sea preventiva o correctiva, sobre los temas de seguridad que se puedan encontrar; además, es imposible encontrar sistemas completamente seguros, ya que cada día se descubren nuevos riesgos en distintos niveles. La investigación se centró en la creación y aplicación de un *Plan para la gestión de vulnerabilidades*, el cual, según [1], tiene como objetivo reducir los riesgos originados por la explotación de vulnerabilidades técnicas publicadas. Debido a lo anterior, se creó un método efectivo, sistemático y cíclico para gestionar las vulnerabilidades, además de poder tomar medidas y verificar avances; dentro de esta gestión deben involucrarse los sistemas operativos de los equipos y el software que se esté usando en ellos. El artículo inicia con la presentación de un estado del arte de la seguridad de la información en varios entornos empresariales; después se explica la aplicación de la estrategia de creación y ejecución del plan de gestión de vulnerabilidades en la empresa, y, por último, se entregan los resultados y las conclusiones de la investigación.

II. Estado del arte

La seguridad de la información digital para una organización depende de diferentes frentes: el físico, referente al alojamiento de la información; el social, relacionado con el grado de discrecionalidad del personal que la manipula, y el lógico, que se refiere a la configuración de sus niveles de accesibilidad y disposición. Es así como técnicamente se ha caracterizado que un esquema seguro debe corresponder al ajuste de los niveles de confidencialidad, integridad y disponibilidad de la información, según la norma ISO 27001. Cuando se describen las anteriores características, se encuentran implícitas en la información, por lo que las organizaciones deben complementar el ciclo de seguridad con la constitución de marcos efectivos para que su información fluya dentro de procesos bien estructurados, constituyendo los denominados Sistemas de Gestión de Seguridad de la Información (SGSI).

En la actualidad, la determinación del nivel de inseguridad (visto desde la óptica de vulnerabilidad y riesgo) de la información trasciende los niveles de su uso u operatividad, de forma que es necesario interpretar sus unidades de portabilidad y los medios por los que se transmite, donde se abren nuevas configuraciones al fraude, a la alteración y al uso indebido; esto ha guiado al asentamiento de áreas forenses, cibercrimen e inteligencia sobre la información.

Para esta investigación se identificó que hay varios problemas de protección de la información en algunas empresas de Boyacá, por la ausencia de un SGSI, o por una mala aplicación, pero no es solo en un contexto local, sino global. A continuación se relacionan algunos estudios que se tomaron como base para la investigación.

El primer estudio [2] identificó que el 28% de los casos de robo de información se ejecuta dentro de las organizaciones, porcentaje significativo, pues su impacto en las organizaciones puede ser fatal, dado que los atacantes internos se pueden considerar delincuentes informáticos y para su identificación se puede utilizar el modelo SKRAM (sigla en inglés de: Habilidad, Conocimiento, Recursos, Acceso y Motivo) [3].

El modelo de negocio de las empresas de hoy se está encaminando al uso de las tecnologías de la información y las comunicaciones (TIC), aumentando el uso de medios informáticos por parte de los usuarios y las probabilidades de ser vulnerables por medio de delincuentes informáticos. Se realizó un estudio que identifica procesos del modelo de negocio e identifica los costos ocultos que tiene la reingeniería de procesos para la implementación de políticas de seguridad en el caso de la empresa General Electric Energy's, en el que se utilizó un enfoque de análisis de riesgos matricial estructurado con la unión de activos de la empresa y controles de seguridad [4]; como conclusión de esta investigación, los autores describen que en la organización los sistemas distribuidos deben estar integrados a unas necesidades específicas de

cada uno de los departamentos, para que los gerentes tomen decisiones centralizadas y encaminadas a la implementación de un Sistema de Gestión de la Seguridad.

Por otro lado, [5] propone un estudio de las inversiones que realizan las empresas en seguridad de la información, proponiendo dos modelos de estudio de competencias: Bertrand y Cournot, para la identificación de inversión económica en seguridad de la información en empresas pequeñas; el estudio concluyó que la competencia Cournot implica una inversión más eficaz para la organización en un proceso de inversión de seguridad para una Mipyme; sin embargo para lograr un buena sinergia organizativa en la implementación de un sistema de gestión de la seguridad de información es necesario trabajar colaborativamente en red para el cumplimiento de objetivos, reducir el riesgo y proteger la inversión. Según [6], se debe contar con una red de expertos de seguridad de la información, y que las personas que intervienen en el proceso cuenten con una confianza marcada y una actitud de compartir el conocimiento; así se puede cumplir con cada uno de los objetivos propuestos.

Según [7], con el pasar del tiempo las organizaciones a nivel mundial han venido reconociendo la importancia de la información, de los activos y de la tecnología como un elemento diferenciador para lograr ventaja sobre sus competidores. Más de 6600 organizaciones de todo el mundo están implementando un Sistema de Gestión de Seguridad (SGSI o ISMS, sigla del inglés Information Security Management System); esta implementación se realiza según la norma ISO/IEC 27001. Implementar un sistema de gestión de seguridad de la información (SGSI) basado en la norma 27001 es un proceso complejo; comprende tareas como la identificación de activos y de amenazas, el análisis de riesgos y el razonamiento de seguridad; además, la norma exige considerar leyes y reglamentos, así como la preocupación de privacidad. Todos estos requerimientos se convierten en desafíos multidisciplinarios para los ingenieros de seguridad.

Las exigencias de la ISO 27001 para estos retos multidisciplinarios y los sistemas de computación en la nube fueron analizados por [8], quienes, con base en este análisis, proporcionan un método que se basa en métodos de ingeniería de requisitos existentes y patrones para varias tareas de seguridad, como son: descripción de contexto, análisis de amenazas y definición de políticas. Este método puede producir la documentación necesaria para la ISO 27001 y ayudar a disminuir el esfuerzo necesario para establecer un SGSI.

Por su parte, [9] exponen un caso presentado en la Facultad de Tecnología de la Información de la Universidad Zayed, en los Emiratos Árabes Unidos; en este estudio identificaron que a pesar de que esta facultad se rige por las directrices de la Association for Computing Machinery (ACM) para los programas de seguridad de la información, los egresados no cumplen cabalmente las expectativas y necesidades de los empleadores. En este trabajo se presenta un enfoque nuevo para la enseñanza y participación de los estudiantes en el campo de la seguridad de la información según la norma ISO 27001: los resultados de la investigación recalcan la importancia de integrar normas internacionales en los programas académicos de las instituciones educativas.

El Instituto Nacional de Tecnologías de la Comunicación (Inteco), de España, realizó en el 2012 un estudio sobre seguridad de la información y continuidad de negocio en las empresas españolas, el cual se enfocó en la realización de un diagnóstico de la percepción del nivel de preparación ante los peligros de seguridad y la adopción de estrategias de continuidad de negocio por las Pymes españolas que usan internet como parte de su negocio. Para el desarrollo de la investigación, Inteco realizó encuestas a Pymes de menos de 250 empleados, localizadas en toda España, además de entrevistas a los encargados de la seguridad informática de estas empresas. En las conclusiones de la investigación se presenta un contraste de la situación percibida por las Pymes en relación con los aspectos fuertes y débiles de seguridad de la información y continuidad de negocio, al igual que con los factores externos asociados [10].

III. Metodología

La investigación se desarrolló bajo un entorno investigativo exploratorio; se inició con un estado del arte global y se fueron construyendo bases para fundamentar el problema y poder sacar las conclusiones. Este desarrollo se realizó en 4 fases: se

inició con la búsqueda y organización de un estado del arte, que ayudará a identificar variables para la investigación; en una segunda fase se realizó una capacitación al grupo de trabajo sobre herramientas y metodologías que fueron aplicadas en el estudio; en la tercera fase se realizó un diagnóstico tecnológico a la empresa, donde se desarrollaron tareas como inventario tecnológico inicial de la organización, identificación y priorización de vulnerabilidades y aplicación de remedios manuales y automáticos, y en la última fase se realizó un informe final con recomendaciones.

IV. Resultados

A. Inventario tecnológico de la empresa

Antes de iniciar con el inventario de los recursos tecnológicos de la empresa, fue necesario realizar un cuadro comparativo de algunas soluciones de software para realizar esta tarea; en la Tabla 1 se muestra el resumen de esta comparación.

Tabla 1
Comparativo soluciones de software para Inventario Tecnológico

Característica	Ocs Inventory	Kaseya	Veo Ultimate
Licencia	GNU General Public License, Version 2.0	Propietaria, Pago según servicios.	Versión de prueba
Inventario de equipos en red	OCS hace un inventario de los equipos en red, identificando las interfaces donde están funcionando.	Kaseya hace un inventario de equipos en la red identificando las interfaces donde funcionan.	Veo también hace un inventario General de los equipos que se encuentran en red.
Inventario de hardware	Permite identificar equipos, switches, impresoras y demás, al igual que la velocidad del procesador, la capacidad de RAM y números de serial, entre otros.	Permite identificar equipos, switches, impresoras y equipos móviles; del mismo modo, la velocidad del procesador, la capacidad de RAM y los números de serial, entre otros.	Permite identificar equipos, switches, impresoras y demás; del mismo modo, la velocidad del procesador, la capacidad de RAM y los números de serial, entre otros.
Inventario de software	Sistemas operativos, parches de actualización, drivers y demás programas instalados.	Sistemas operativos y drivers de hardware existentes, parches.	Sistemas operativos y drivers de hardware existentes.
Inventario de usuarios	OCS reconoce los usuarios a los cuales pertenece el equipo.	Permite saber qué usuario pertenece a ese equipo.	Permite saber qué usuario pertenece a ese equipo.
Soporte de plugins	Al ser software libre, permite el libre desarrollo de plugins que se acomoden a las necesidades de cada una de las compañías donde se necesite.	No permite.	No permite.

Característica	Ocs Inventory	Kaseya	Veo Ultimate
Sincronización con otros productos	OCS permite sincronizarse con diferentes productos de administración IT y Tareas, además, software para asignación de equipos y demás.	No permite	No permite
Backups de información	Permite hacer un backup que va a ser almacenado en la base de datos.	Permite hacer backups de información.	Permite hacer backups de información.
Exportar datos	OCS permite exportar los datos de cualquier consulta que se realice.	Exporta datos generales.	Exporta datos generales.

Dentro de este análisis y selección se tuvieron en cuenta aspectos como la licencia, inventario de equipos en red, inventario de hardware, inventarios de software, inventarios de usuarios, soporte de plugins y exportación de datos, obteniendo como resultado la selección del software Open Computer and Software Inventory Next Generation (OCS), con licencia GNU General Public License, Version 2.0.

B. Monitoreo de vulnerabilidades e inventario y priorización de las vulnerabilidades

La etapa de monitoreo es esencial en las organizaciónes, es el paso principal para lograr un plan que sea repetible con el fin de que pueda ser evidenciado el progreso que tenga el proyecto a lo largo del tiempo. Como resultado de esta etapa se seleccionó la herramienta de monitoreo de los equipos, además de una serie de datos para el inventario de vulnerabilidades del software. Para esta tarea se utilizó la herramienta Retina Community Security Scanner, la cual permite trabajar de la mano con sistemas existentes, redes de comunicación, bases de datos de seguridad e interfaces de usuario, donde se prueba regularmente la integridad de la red para descubrir y corregir vulnerabilidades de seguridad.

Con los resultados obtenidos en el monitoreo de vulnerabilidades con la herramienta Retina Community Security Scanner se realizó un inventario y priorización de vulnerabilidades, con el objetivo de solucionar las que presentan mayor riesgo. Para esta tarea se utilizaron tablas dinámicas, también llamadas pivot tables, que son una herramienta para análisis de bases de datos (BD), pues se encargan de resumir y ordenar la información contenida en la BD. Esta clase de tablas permiten analizar solo una porción de la BD, es decir, en una base de datos con muchos campos o columnas, ayudan a visualizar únicamente la información relevante, con lo que el análisis se torna más sencillo.

C. Creación de base de datos y pruebas de remedios

Con la información del inventario y priorización de las vulnerabilidades se generó una base de datos de remedios que luego fueron aplicados en la etapa de pruebas. Aunque la creación de esta base de datos parece una tarea sencilla en trabajo informático, es de gran importancia en el desarrollo del proyecto. En esta tarea se utilizó la herramienta WSUS, dado que la empresa en estudio cuenta con el software, y que este cumple con la función de automatización de vulnerabilidades; además, si bien es cierto que no es capaz de hacer una remediación completa de todo el software instalado en las diferentes estaciones de trabajo, sí cumple con la instalación de muchos remedios que harían extenuante el trabajo; WSUS ayuda con alrededor de un 60 a 70 por ciento de las instalaciones de remedios de productos Microsoft. También se utilizó la herramienta PsExec, pues facilita la creación de inventarios y la ejecución de software en forma remota.

D. Despliegue de remedios y automatización de remedios

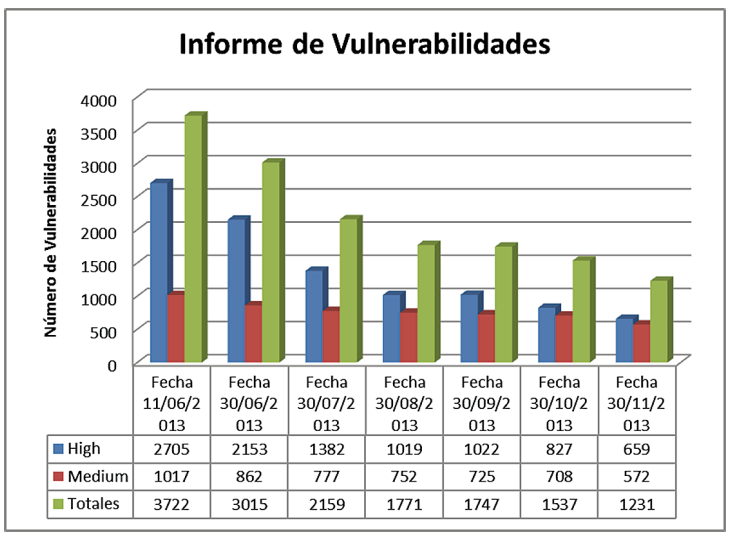
Esta etapa fue una de las más importantes y más desgastantes de todo el proyecto, ya que el despliegue de algunas actualizaciones Microsoft y de todas las de terceros fue necesario hacerlo en un proceso Manual y, en ocasiones, semiautomático. Esta etapa fue iterativa, y en cada uno de sus ciclos se realizó el proceso de remediación de las vulnerabilidades de los equipos.

En la penúltima etapa del proyecto se buscó automatizar las actualizaciones mediante el uso del software de Microsoft WSUS; esta etapa complementa el proceso en general de mejora continua de la organización y en especial del departamento de sistemas.

E. Seguimiento de las vulnerabilidades

Las vulnerabilidades se clasifican de acuerdo con el nivel del exploit que las herramientas de análisis identifican durante el escáner, por ejemplo, si son de tipo alto es porque el exploit es conocido, y otorgan privilegios de usuario tipo SYSTEM y, en consecuencia, ejecutan un daño bastante efectivo hacia una desestabilización completa a la máquina. La clasificación de tipo media es cuando las vulnerabilidades tienen un impacto no directo al sistema operativo; en la gran mayoría afecta a algunas aplicaciones de usuario sin privilegios de administrador, pero igual con posibilidades de escalar a un nivel alto. Las anteriores clasificaciones son tomadas por Retina Community Security Scanner de los proyectos de seguridad de Core Security Technologies, Metasploit Project, Exploit Data Base y las normas CVSS (Common Vulnerability Scoring System).

Como el objetivo principal de la investigación fue ayudar a la organización en el mejoramiento de la seguridad de la información, se realizó un análisis de la efectividad del plan de gestión de vulnerabilidades durante 6 meses, lapso durante el cual se identificaron y caracterizaron las vulnerabilidades en altas y medias, como lo muestra la Figura 1. También se evidenció una reducción paulatina de las vulnerabilidades en cada una de las muestras tomadas, la cual alcanzó más del 72% desde el inicio de la investigación y durante los 6 meses del análisis. La información se manejó de manera confidencial, y en la actualidad la empresa está aplicando las recomendaciones, como el cambio de algunas herramientas de software y equipos como servidores, firewalls y workstations, para ir reduciendo vulnerabilidad y que el plan sea más efectivo.



	Fecha 11/06/2013	Fecha 30/06/2013	Fecha 30/07/2013	Fecha 30/08/2013	Fecha 30/09/2013	Fecha 30/10/2013	Fecha 30/11/2013
High	2705	2153	1382	1019	1022	827	659
Medium	1017	862	777	752	725	708	572
Totales	3722	3015	2159	1771	1747	1537	1231

Fig. 1. Informe de vulnerabilidades

V. Conclusiones

La investigación se centró inicialmente en el estudio de métodos y normas, que permitió la elección de documentos para generar un plan de mejoramiento adaptado a las necesidades de la empresa.

Se formularon recomendaciones específicas a la empresa para la aplicación de un plan de remedios a la medida; se inició con una aplicación manual en algunas de las estaciones de trabajo y se terminó con un proceso automatizado aplicado a toda la red.

Con los resultados de la investigación y con la aplicación del plan de gestión de vulnerabilidades se utilizaron herramientas técnicamente viables y aprobadas por la empresa, cuyo objetivo fue el cierre de vulnerabilidades.

Se obtuvieron mejoras en el proceso de gestión de vulnerabilidades con el cierre de más de un 70% en un tiempo de 6 meses.

Se documentaron todas las etapas de la investigación, y se evidenció el cumplimento de los objetivos ante la organización, dotándola de herramientas metodológicas, herramientas informáticas y procesos aplicados hacia la protección de la información en la empresa.

Referencias

[1] ISO27002 (2014) [Online]. Disponible en: www.iso27002.es

[2] R. A. Siponen and M. B. Willison, "Overcoming the insider: Reducing employee computer crime through Situational Crime Prevention", *Communications of the ACM*, pp. 133-137, 2009.

[3] D. Parker, *Fighting Computer Crime: a New Framework for Protecting Information*, 1998.

[4] S. Chen and V. Goel, "Can business process reengineering lead to security vulnerabilities: Analyzing the reengineered process", *International Journal of Production Economics*, pp. 104-112, 2008.

[5] W. Zhong, S. Mei and X. Gao, "Differential game approach to information security investment under hackers' knowledge dissemination", *Operations Reorch Letters*, pp. 421-425, 2013.

[6] M. S. Bin Babaa, H. Tamjidb and R. G. Alireza Tamjidyamcholo, "Information security – Professional perceptions of knowledge-sharing intention under self-efficacy, trust, reciprocity, and shared-language", *Computers & Education*, pp. 223–232, 2013.

[7] M. Stoll, M. Felderer and R. Breu, "Information management for holistic, collaborative information security management", in *6th International Joint Conference on Computer, Information, and Systems Sciences, and Engineering, CISSE 2010*, Bridgeport, CT; United States, 2010, pp. 211-224.

[8] K. Beckers, I. Côté, S. Faßbender, M. Heisel and S. Hofbauer, "A pattern-based method for establishing a cloud-specific information security management system - Establishing information security management systems for clouds considering security, privacy, and legal compliance", *Requirements Engineering*, pp. 1-53, 2013.

[9] M. Abu Talib, A. Khelifi and T. Ugurlu, "Using ISO 27001 in teaching information security", in *38th Annual Conference on IEEE Industrial Electronics Society, IECON 2012*, Montreal, QC; Canada, 2012, pp. 3149-3153.

[10] INTECO (2012) [Online]. Disponible en: http://www.inteco.es/Estudios/Estudio_pymes_seguridad_2012%E2%80%8E