UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD INGENIERIA EN CIENCIAS APLICADAS

CARRERA INGENIERIA EN ELECTRÓNICA Y REDES DE COMUNICACIONES

HACKING ÉTICO PARA DETECTAR FALLAS EN LA SEGURIDAD INFORMÁTICA DE LA INTRANET DEL GOBIERNO PROVINCIAL DE IMBABURA E IMPLEMENTAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI), BASADO EN LA NORMA ISO/IEC 27001:2005.

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

AUTOR: BRAULIO FERNANDO ORTIZ BELTRÁN

DIRECTOR: MSC. EDGAR MAYA

IBARRA – ECUADOR

ENERO 2015

Hacking ético para detectar fallas en la seguridad informática de la intranet del Gobierno Provincial de Imbabura e implementar un sistema de gestión de seguridad de la información (SGSI), basado en la norma ISO/IEC 27001:2005

Ortiz, Fernando
Universidad Técnica del Norte
Ibarra-Ecuador
fher_ortiz_b@hotmail.com

Resumen— El proyecto consiste en identificar los activos de información más importantes del Gobierno Provincial de Imbabura, es decir dispositivos que forman parte de la intranet de la institución relacionada directamente con el transporte, almacenamiento o modificación de la información cuya evaluación consiste en realizar un análisis de riesgos y posteriormente detectar fallas en los servidores del Gobierno Provincial de Imbabura mediante la utilización de técnicas de Hacking Ético desde una perspectiva de caja negra, como es el desconocimiento total de las características de los servidores.
Con los resultados de los tres análisis se procede a utilizar la norma ISO/IEC 27001:2005 para diseñar el Sistema de Gestión de Seguridad de la Información (SGSI) mediante el análisis de la selección de los controles más adecuados como medida para el tratamiento de los riesgos; finalmente elaborar los documentos que forman parte del SGSI como son la política de seguridad de la información, los procedimientos, las normativas y los estándares de seguridad.

Palabras Clave— Sistema de Gestión de Seguridad de la Información, Hacking Ético, ISO/IEC 27001:2005.

I. INTRODUCCIÓN

En la actualidad las instituciones sin importar su dimensión prestan gran parte de su atención a las actividades económicas en las cuales se desempeñan, sin embargo olvidan el tema de la seguridad de la información, es decir actualmente la información es considerada como un activo de gran valor para cualquier institución en especial cuando se procesan datos críticos de gran importancia la misma que si es obtenida por usuarios maliciosos pueden causar un gran daño económico, social, político entre otros, por lo cual asegurar los dispositivos y la información debe ser una tarea primordial.

La implementación del Sistema de Gestión de Seguridad de la Información (SGSI) requiere del cumplimiento de tres requisitos iniciales solicitados por la norma ISO/IEC 27001:2005 los cuales son:

- Los activos de información.
- Identificación de vulnerabilidades.
- El análisis de riesgos.

La norma ISO en mención no determinada la forma de realizar dichas tareas por lo que estos aspectos deja a criterio del evaluador, sin embargo para el presente proyecto se utiliza la Metodología Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) para realizar los dos primeros requisitos.

Los activos de información de la red del Gobierno Provincial de Imbabura (GPI) inmersos el proyecto son los siguientes:

1. Servidor de gestión documental - Quipux
2. Servidor de correo electrónico - Zimbra
3. Servidores web
4. Servidor proxy
5. Servidor de telefonía IP - Elastix
6. Servidor de ordenamiento territorial - Gis
7. Servidor contable financiero – Olympo
8. Atención al público
9. Servidor blade
10. Switch de core
11. Switch de acceso
12. Firewall
13. Packet Shaper
14. Router CNT
15. Computadoras
16. Cableado estructurado
17. Backbon
18. Sistema de aire acondicionado

19. UPS[1]
20. Sistema de energía eléctrica
21. Control de Acceso
22. Cámaras de seguridad
23. Sistema de monitoreo ambiental
24. Sistema contra incendio
25. Teléfono IP
26. Internet

El proceso correspondiente a la identificación de las vulnerabilidades o Hacking Ético es desarrollado desde una perspectiva de caja negra o black-box, es decir el atacante o evaluador desconocen las características técnicas de los servidores, por lo que es necesario utilizar software especializado sobre el tema. Para el presente proyecto se utilizó un sistema operativo basado en Debian el cual es Kali Linux debido a que posee herramientas preinstaladas especializadas para dichas tareas entre las cuales se utilizaron las siguientes:

- Nmap (Escaner de puertos y servicios)
- Metasploit (Framework de explotación)
- Sqlmap (Herramienta de inyección SQL[2] a la base de datos).
- Nessus (Escaner de vulnerabilidades)
- Armitage (Framework de metasploit)
- Ping (Envío de paquetes ICMP)
- Software cliente para aplicaciones

II. DISEÑO DEL SGSI

El diseño parte del análisis de riesgos el cual especifica las amenazas que se encuentra sujeto cada activo de información, para ello Magerit evalúa las amenazas agrupados en cinco categorías:

- Desastres naturales.
- Desastres industriales.
- Errores y fallos no intencionados.
- Ataques intencionados.

Cada amenaza por activo de información se le asigna una valoración en función de varios criterios propuestos por la metodología Magerit entre las que constan la tipificación de los activos, la dependencia entre activos y la valoración propia y acumulada de las propiedades de la información como son la confidencialidad, la disponibilidad y la integridad.

El tratamiento de riesgos especifica los controles seleccionados del Anexo A de la norma ISO/IEC 27001:2005 que serán implementados en el SGSI de la institución. Los controles son seleccionados analizando los resultados el informe de análisis de riesgos y los informes de vulnerabilidades de los servidores es decir por cada amenaza y/o vulnerabilidad seleccionar uno o varios controles que permita aceptar el riesgo, evadirlo, transferirlo o mitigarlo.

III. IMPLEMENTACIÓN

La implementación del SGSI corresponde al desarrollo de los documentos exigidos por la norma ISO/IEC 27001:2005 los cuales obedecen a un nivel jerárquico de la siguiente manera.

- Política de la seguridad de la información
- Normativas y procedimientos de seguridad de la información.
- Estándares.
- Registros de seguridad

A. Política de la seguridad de la información.

La política de la seguridad de la información es el documento más importante de la institución, establece los lineamientos generales, necesidades y requisitos de seguridad de la información como medidas adoptar para mantener a salvo la información y los activos que lo procesan, transportan o almacenan para garantizar las actividades de negocio de la institución.

B. Las Normativas.

Las normativas de seguridad implementan uno o varios controles relacionados centrándose en un área de la seguridad definiendo las condiciones y los activos a proteger bajo escenarios o situaciones específicas previamente definidos en la política de la seguridad de la información. Las normativas desarrolladas en la implementación del SGSI del GPI se listan en la Tabla 1.

[1] UPS: Fuente de suministro eléctrico ininterrumpido.
[2] SQL: Lenguaje de consulta estructurado de acceso a la base de datos.

C. Los Procedimientos

Son las acciones o actividades a realizar describiendo el procedimiento a ejecutar relacionado con la seguridad de la información y los funcionarios responsables de su vigilancia, actualización y cumplimiento. Los procedimientos desarrollados en el SGSI se listan en la Tabla 1.

D. Los Estándares

Determina las acciones necesarias para completar el proceso de un procedimiento específico para ser considerado como estándar o común para todos los usuarios de un servicio, el presente proyecto SGSI ha desarrollado dos estándares expuestos en la Tabla 1.

E. Asignación de responsabilidades.

La Tabla 1 resume las normativas, procedimientos y estándares elaborados como parte de la implementación del Sistema de Gestión de Seguridad de la información y la asignación respectiva para cada dependencia del departamento de Informática del GPI.

TABLA I
ASIGNACIÓN DE LOS DOCUMENTOS DEL SGSI A LAS SUBDIRECCIONES DEL DEPARTAMENTO DE INFORMÁTICA

.

DOCUMENTOS DEL SGSI	**DEPENDENCIAS DEL DEPARTAMENTO DE INFORMÁTICA DEL GPI**		
NORMATIVAS	**Gestión de Servicios**	**Gestión de Infraestructura**	**Gestión de Proyectos**
Normativa de acuerdos con terceras partes		✓	
Normativa de administración de incidentes de seguridad de la información	✓	✓	
Normativa de administración de seguridad de la red		✓	
Normativa de buenas prácticas de seguridad de la información	✓		
Normativa de control de acceso	✓	✓	
Normativa de control de cambios		✓	✓
Normativa de gestión de continuidad del negocio		✓	✓
Normativa de mantenimiento de equipos e instalaciones		✓	
Normativa de protección contra software malicioso		✓	
Normativa de requisitos de seguridad de la información para nuevas instalaciones y adquisición de software	✓	✓	✓
Normativa de roles y responsabilidades de seguridad de la información	✓	✓	✓
Normativa de segregación de funciones	✓	✓	
Normativa de seguridad de la información para la gestión del recurso humano	✓	✓	
Normativa de seguridad de la información	✓	✓	✓
Normativa de software licenciado	✓		✓
Normativa de suministro electric		✓	
Normativa de uso de internet	✓	✓	
PROCEDIMIENTOS			
Procedimiento de contacto con grupos de interés en materia de seguridad de la información	✓		✓
Procedimiento de disposición de medios de almacenamiento y equipos de cómputo	✓	✓	

Procedimiento de generación y almacenamiento de backups		✓	
Procedimiento de protección y revisión de registros de auditoria		✓	
Procedimiento de seguridad física y ambiental del data center		✓	
Procedimiento para la creación, modificación y eliminación de acceso de usuarios en sistemas		✓	
Procedimiento para la identificación y clasificación de activos de información	✓	✓	
ESTÁNDARES			
Estándar de contraseñas para usuarios y administradores	✓	✓	✓
Estándar de etiquetado de activos de información	✓	✓	

IV. RESULTADOS

Uno de los procedimientos de mayor importancia del proyecto consiste en la identificación de las vulnerabilidades de los servidores del GPI mediante un enfoque de Hacking Ético mediante técnicas de explotación, acceso tanto a servicios e información confidencial.

La siguiente tabla resume los tipos de vulnerabilidades detectadas en los servidores del Gobierno Provincial de Imbabura, marcados los servidores afectados con la respectiva vulnerabilidad.

TABLA II
VULNERABILIDADES MÁS COMUNES DE LOS SERVIDORES DEL GPI.

	SERVIDOR						
VULNERABILIDAD	1	2	3	4	5	6	7
XSS-Secuencias de comandos en sitios cruzados		x	x	x	X		x
Acceso a la base de datos		x	x	x			
Inyección SQL			x		X		
Revelación de información	x	x	x	x	X	x	
Error en PHP	x						
Control de acceso		x	x	x			x
Transmisión de credenciales sin cifrar		x	x	x	X		x

La norma ISO/IEC 27001: 2005 exige al finalizar el proyecto la redacción del documento final "Declaración de aplicabilidad" el cual establece los controles implementados con los respectivos documentos del SGSI desarrollados, y los controles no implementados justificar su exclusión.

V. CONCLUSIONES

El proceso de Hacking Ético reveló grandes fallas en los servidores del Gobierno Provincial de Imbabura, no sólo errores por parte de los administradores o desarrolladores, también por parte de los usuarios porque más del 60 % utilizan el nombre de usuario del correo electrónico como la contraseña. Las vulnerabilidades se deben en gran parte a la desactualización de las aplicaciones informáticas.

El reconocimiento de las características de los servidores tanto de los puertos como de las versiones de los servicios no tuvo mayores impedimentos por parte de los mecanismos de protección perimetrales como el firewall, el router o el switch o los propios servidores, sin embrago existe más controles de bloque desde el interior de la red, es decir se ha dejado descubierto los ataques desde cualquier punto del internet, y este punto se evidenció en la facilidad de explotación de las vulnerabilidades reportadas por cada servidor.

La política de seguridad de la información es el documento más importante en el que se basan la toma de decisiones y acciones a emprender en temas de seguridad, ninguna normativa interna o procedimiento está sobre la política y cualquier violación a la misma deberá ser sancionada conforme al reglamento interno.

Los funcionarios debe respetar sus roles, responsabilidades y privilegios de acceso hacia los sistemas de información y no intentar sobrepasar los límites de acceso asignados o poner en peligro la

integridad de la información o los equipos con acciones ilegales o negligentes.

VI. RECOMENDACIONES

La adecuada selección de los controles de seguridad depende directamente del correcto análisis de riesgos de los activos de información y de la identificación de todas las vulnerabilidades leves o graves de los activos, porque dichos resultados dirigen el desarrollo del resto del proyecto hasta la implementación del SGSI.

La norma ISO/IEC 27001:2005 claramente establece realizar un monitoreo periódico del funcionamiento de las medidas adoptadas en favor de la seguridad de la información, y actualizar o realizar cambios en base de la experiencia o falencias encontradas hasta el momento de la revisión.

Es recomendable capacitar y practicar las acciones a emprender en caso de suscitarse cualquier contingencia por parte del personal de apoyo, así al momento de actuar cada uno conocerá las responsabilidades asignadas y los procesos en los que tendrá que intervenir para gestionar los incidentes de seguridad de la información.

La protección de la información debe ser compromiso de todos los funcionarios del Gobierno Provincial de Imbabura, cada colaborador debe tomar conciencia acerca del daño potencial si se pone en peligro la seguridad de la información al cometen actos con malicia, beneficio propio o negligencia. Motivar al personal a tomar la iniciativa y capacitase en temas de seguridad de la información o indagar cualquier duda o conocimiento que necesite aclararse.

Hasta el momento el Gobierno Provincial de Imbabura no ha sufrido ningún incidente de seguridad grave con los activos de información, pero las vulnerabilidades existen y es razón de tiempo hasta que algún atacante malicioso arremetida contra la infraestructura tecnológica de la institución, sin embargo también es imperioso la implementación de un centro de operaciones de seguridad (SOC) que prevea, monitoree y controle la seguridad en las redes y en Internet.

VII. REFERENCIAS

[1] Ali, S., & Heriyanto, T. (2011). BackTrack 4: Assuring Security by Penetration Testing. Birmingham: Packt Publishing Ltd.

[2] Calles García, J. A., & González Pérez, P. (2011). La Biblia del Footprinting. Obtenido de Flu Project: Flu Project.com

[3] Graves, K. (2010). CEH: Certified Ethical Hacker Study Guide. Indianapolis: Wiley.

[4] ISO, & 27001, I. (2005). Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos.

[5] López Neira, A., & Ruiz Spoh, J. (2012). El portal de ISO 27001 en Español. Obtenido de http://www.iso27000.es/sgsi.html#section2a

[6] Nieves, R. (2010). Teoría del Delito y Práctica Penal – Reflexiones dogmáticas y mirada crítica. Santo Domingo, D.N.: Editora Centenario, S. A.

[7] The hacker news. (2012). CVE-2012-2122 : Serious Mysql Authentication Bypass Vulnerability. Obtenido de http://thehackernews.com/2012/06/cve-2012-2122-serious-mysql.html?m=1

Ortiz B., Autor

Nacido el 25 de Febrero de 1988, en el cantón Ibarra - Ecuador. Obtuvo su título de bachiller en Ciencias especialización Físico Matemático en el Colegio Nacional "Teodoro Gómez de la Torre". Realizó los estudios Universitarios en la Universidad Técnica del Norte, en la carrera de Ingeniería en Electrónica y Redes de Comunicaciones. Ha trabajado como Técnico Integral en la Corporación Nacional de Telecomunicaciones (CNT) desde Julio de 2011 hasta Septiembre de 2013.

Maya E., Director

Edgar Alberto Maya Olalla nació el 22 de Abril de 1980, Obtuvo el título de Ingeniero en Sistemas Computacionales de la Universidad técnica del Norte (2006), posee un Diplomado Superior en Investigación (2009) y el título de Magister en Redes de Comunicaciones (2014).

Obtuvo las certificaciones como instructor de la Academia CISCO-UTN en los cuatro niveles de CCNA e IT Essentials en la Academia CISCO ESPOL de la ciudad de Guayaquil.

Ha participado en varios seminarios, talleres, y cursos de especialización con 1146 horas de formación académica profesional y en proyectos de investigación.

Actualmente se desempeña como docente de la Carrera de Ingeniería en Electrónica y Redes de Comunicación de la FICA en la Universidad Técnica del Norte y como instructor de la Academia CISCO-UTN.