Procedimientos de CiberSeguridad en un Laboratorio de Educación, Desarrollo e Investigación (EDI) para la identificación de vulnerabilidades en su red informática.

Fabián Gibellini; Roberto Muñoz; Analía Lorena Ruhl; Juliana Notreni; Cecilia Sánchez; Ignacio Sánchez; Marcelo Auquer; Milagros Zea.

Universidad Tecnológica Nacional – Facultad Regional Córdoba – Maestro Marcelo Lopez esq. Cruz Roja Argentina, Ciudad Universitaria (X5016ZAA)- Córdoba, Argentina.
{fabiangibellini, robertmunioz, analialorenaruhl, julinotreni, csanchezjuriol, ignaciojsb, marcelo.auquer, milyzc}@gmail.com

Resumen

Cuando se habla de seguridad de una red informática se debe tener en cuenta tanto la seguridad física como la seguridad lógica de la misma. Se tiene que considerar todas las actividades, técnicas y herramientas relacionadas con el fin de proteger los datos que manejan los sistemas de la organización, tanto sistemas de uso interno como los sistemas expuestos a los usuarios finales, con la premisa que estos datos no sean accedidos o interferidos por personas no autorizadas, ni destruidos accidental o intencionalmente. Este estudio está inserto y forma parte de un proyecto de investigación denominado "Determinación de Indicadores, técnicas y herramientas que evidencian buenas prácticas en la ciberseguridad de la infraestructura tecnológica en un laboratorio de Educación, Investigación y Desarrollo de la UTN - FRC.", homologado por la Secretaría de Ciencia y Tecnología bajo el código SIUTNCO0005366
La gran contribución de este paper es un modelo de ciberdefensa en profundidad que relaciona las vulnerabilidades latentes de la red informática y sus medidas de seguridad a través de la cual la vulnerabilidad es mitigada.

Palabras clave: ciberseguridad; redes informáticas; seguridad

1 Introducción

La seguridad informática engloba tanto la seguridad física, seguridad en los sistemas desarrollados y administración de la seguridad en una red informática. Según la norma ISO/IEC 27002 la seguridad física o ambiental tiene como objetivo "evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información" [1].

Por otro lado, administrar la seguridad lógica en una red informática, es de vital importancia porque está generalmente tiene más de un servidor y maneja datos de

muchos sistemas. Han existido ataques a través de internet que han causado graves daños a diferentes sectores (por ejemplo: personal, económico, empresarial, organizaciones y gobierno), entre los que podemos recordar el ataque a Sony Pictures en el 2014 que le costó a la empresa quince millones de dólares [2].

Se han creado diferentes procedimientos, procesos o técnicas que ayudan a implementar seguridad en una red como procedimientos de autenticación y autorización a la red [3], sistemas de detección de intrusos (IDS), IDS basados en data mining y machine learning de forma complementaria [4].

Rojanakul y Liang [5] afirman que la estabilidad y seguridad de la red es muy importante enfocándose en una estrategia de asegurar y configurar políticas de seguridad para resguardar la infraestructura. Para lo cual divide la red en dos zonas, la de uso externo y la de uso interno.

Dees y Rahman [6] identifican ciertas contramedidas para estas amenazas, como implementar una infraestructura fuerte y luego asegurarla a través de la implementación de capas y políticas en cada capa, encriptar transmisiones (cableadas y no cableadas), educar y entrenar a los empleados en las cosas que pueden y no pueden hacer mientras están conectados a la red, educar en la necesidad de crearse usuario y contraseña que sean seguras.

Otro de los procedimientos que suman y se han vuelto clave al momento de implementar seguridad son los backups [7] de toda información (documentos, programas, servidores, máster de equipos) que se crea necesarios para el correcto funcionamiento.

Un laboratorio de Educación, Investigación y Desarrollo (EDI), cuenta con un gabinete informático que debe estar preparado para estudiantes, docentes, profesionales e investigadores, donde las necesidades y exigencias día a día son mayores en lo que concierne a software, aplicativos y hardware. Es indispensable contar con la infraestructura acorde para afrontar los diversos pedidos que se realizan por parte de todos los actores involucrados.

Teniendo presente la heterogeneidad de software que se debe implementar para satisfacer las necesidades de cada cátedra/materia/curso que solicita un servicio y de los investigadores que integran los Proyectos de Investigación, Desarrollo e Innovación que se llevan a cabo utilizando los mismos recursos, es indispensable llevar a cabo acciones que den continuidad a los servicios protegiendo la confidencialidad, integridad y disponibilidad de estos.

En el caso del Laboratorio de Ingeniería en Sistemas de Información (LabSis) de la UTN-FRC se atienden a todos los servicios nombrados anteriormente y se tiene especial cuidado en la disponibilidad e integridad de los datos que intervienen en los servicios prestados, ya que el dictado de clases, toma de parciales y exámenes finales e investigación dependen de estas características.

En LabSis, se aplican distintas técnicas y herramientas de seguridad en las diferentes capas de la red para evitar que, accidental o intencionalmente, algún servicio quede fuera de funcionamiento. Si bien el LabSis está en continuo funcionamiento, es real la necesidad de hacer un análisis de reingeniería de los métodos y procesos hasta ahora implementadas con el objetivo de alcanzar un conjunto de procedimientos que sinérgicamente colaboren a la ciberseguridad de la infraestructura tecnológica de un laboratorio de Educación, Desarrollo e Investigación (EDI) y desarrollar una base de

conocimientos basadas en indicadores de vulnerabilidades, técnicas y herramientas que fortalezcan la seguridad.

La principal necesidad identificada fue mitigar los riesgos relacionados a las vulnerabilidades de la red, en la cual coexisten tres modelos de uso de la infraestructura Educación, Desarrollo e Investigación (EDI), de forma tal de evitar un mal uso que genere pérdidas o daños, ya sea por desconocimiento o equivocación de los usuarios de la red informática.

En cambio, en un ambiente de educación, desarrollo e investigación, más precisamente un laboratorio EDI, un modelo de organización tradicional no es del todo representativo, dado que las actividades que se realizan en el mismo no son cotidianas, o mejor dicho el periodo para que puedan ser consideradas lo más cercano a rutinarias es más amplio que un día, por ejemplo, si se considera la parte de educación, en los servicios que se brindan en gabinete informático a docentes y estudiantes, la rotación de estudiantes cambian todos los años para cada cátedra, al igual que en los talleres eventuales, como lo son las competencias de programación [8], los seminarios y olimpiadas informáticas [9], y en lo que compete a investigación y desarrollo se tiene una variabilidad media debido a que los proyectos tienen una duración entre dos y tres años y, una vez implementados ó finalizados, su variabilidad pasa a ser constante.

Por todo lo expuesto se puede plantear que el objetivo principal presentado en este proyecto es "Determinar los factores que colaboren en el control de seguridad de la red informática en el ámbito de un laboratorio de Educación, Investigación y desarrollo (EDI), proponiendo técnicas, herramientas e indicadores que evidencian buenas prácticas en la ciberseguridad de la infraestructura tecnológica del Laboratorio de Ingeniería en Sistemas de Información de la UTN - FRC (LabSis)".

2 Metodología

Para el desarrollo de este proyecto se utilizará el método empírico [10][11], siendo que en algunas actividades utilizarán el método científico durante su ejecución, las cuales culminarán en la aceptación o refutación de hipótesis sobre evidencias de buenas prácticas en LabSis.

Toda investigación o estudio llevado a cabo, fluctúan sobre la seguridad informática en redes de información que operan sobre infraestructuras tecnológicas de un ámbito público, como ser el Laboratorio de Ingeniería en Sistemas de Información (LabSis) de la Universidad Tecnológica Nacional de la Facultad Regional Córdoba.

Teniendo en cuenta que los servicios que debe prestar esta entidad a docentes y la protección de datos sensibles (uno de ellos son los parciales y exámenes finales) y cuya incumbencia concierne únicamente a la Universidad en que se realiza, es que este proyecto se inserta dentro de la línea de investigación de ciberseguridad en una infraestructura tecnológica.

Se realizará una investigación exploratoria a los fines de profundizar y poder cumplir con la detección de las técnicas y herramientas de ciberseguridad utilizadas en actividades relacionadas a la seguridad informática de la red, realizando un estudio y análisis de las técnicas y herramientas de ciberseguridad.

Posteriormente se analizarán las actividades que se realizan en el LabSis identificando las técnicas y herramientas de ciberseguridad utilizadas actualmente con el fin de determinar un conjunto de indicadores cuantificables relacionados a la ciberseguridad que sean aplicables en un laboratorio EDI, de esta manera daríamos cumplimiento al objetivo planteado.

Para determinar el conjunto de buenas prácticas del LabSis con las técnicas y herramientas que contribuyan a la ciberseguridad en laboratorios de Educación, desarrollo e investigación se dará categoría a los actores involucrados en el Labsis y a los servicios exigidos por los mismos, realizando una evaluación del análisis de riesgo con el que cuenta actualmente el LabSis. De la evaluación que se realice se procederá a analizar y seleccionar indicadores que muestren evidencias de buenas prácticas. Se formulará una descripción de la infraestructura y para poder crear una base de conocimiento relacionada a ciberseguridad que a partir de los registros de eventos de la infraestructura tecnológica del LabSis y de recolectar información pertinente a los indicadores identificados.

Se realizará el análisis de las técnicas de redes neuronales y machine learning que colaboren con la seguridad del LabSis, identificando a dichas técnicas como método de prevención y de colaboración con la ciberseguridad de infraestructura del LabSis. Con las recolecciones tomadas y las mediciones que se llevan a cabo, se definirá una guía de buenas prácticas para laboratorios EDI que fortalezcan la seguridad.

3 Desarrollo

En primera medida es necesario elaborar Mapas de Procesos que permitan conocer mejor el funcionamiento del laboratorio EDI, detectando procesos y en cada uno ellos los procedimientos que están relacionados con cada proceso. Con el mapa de procesos y el detalle de cada uno de los procesos identificados se debe realizar un análisis de riesgos basados en los procedimientos que detallan las actividades de cada proceso.

El análisis de riesgo obtenido debe ser evaluado y aprobado por el personal y dirección que integran el laboratorio EDI. Para el mismo se debe tener en cuenta la realización del inventario de activos más críticos, luego se deben identificar las amenazas que pueden afectar a los activos y valorando cada una de ellas basada en el impacto que puede tener si las misma ocurrieran, también se debe identificar las vulnerabilidades de los activos y ponderarlas. Una vez identificados los activos, amenazas y vulnerabilidades se debe realizar un análisis de las medidas de seguridad, técnicas y herramientas que ya están implementadas en el laboratorio EDI. Esto es la base para diseñar una metodología de ciberseguridad basado en un modelo de defensa.

3. Resultados, Avances/Discusión

Se plantea el siguiente esquema para identificar medidas existentes y necesarias para cubrir las amenazas identificadas, especificando las técnicas y herramientas a considerar en cada capa:

<table>
<tr>
<td>1- Capa de Políticas y Procedimientos
- Política de Seguridad de la Información
- Organización de la Seguridad
- Roles y Responsabilidades de Seguridad
- Procedimientos y estándares
- Capacitación de seguridad</td>
<td>2- Capa de Seguridad Física:
- Control de Acceso Físico
- Alarmas.
- Seguridad Perimetral
- Controles Ambientales</td>
</tr>
<tr>
<td>3- Capa de Perímetro
- Test de Penetración
- Firewall.
- VPNs
- Sistema de detección de intrusos (IDS)
- Sistema de Protección de intrusos (IPS)</td>
<td>4- Capa de Red Interna
- Listas de Control de Acceso (ACLs)
- Red de área local virtual (VLANs)
- Secure Shell (SSH)
- Secure Sockets Layer (SSL)
- Transport Layer Security (TLS)
- Auditorías de Seguridad</td>
</tr>
<tr>
<td>5- Capa de Host
- Hardening del Sistema Operativo
- Registros de Seguridad (Logs)
- Control de contraseñas.
- Antimalwares/Antivirus.
- Escaneo de vulnerabilidades
- Gestión de Parches de Seguridad</td>
<td>6- Capa de Aplicación
- Código Seguro
- Controles de acceso
- Políticas de contraseñas
- Gestión interna de los ambientes de desarrollos.
- Seguridad en el ciclo de vida del desarrollo del software</td>
</tr>
<tr>
<td colspan="2">7- Capa de Datos
- Criptografía/ofuscación
- Data Leak Prevention (DLP)
- Sanitización de los datos
- Clasificación
– Resguardo de los datos</td>
</tr>
</table>

Cada técnica o herramienta descripta es considerada un punto de control que colabora a la ciberseguridad en el modelo de defensa planteado. Teniendo en cuenta las amenazas identificadas en el análisis de riesgo debe ser siempre posible lograr una trazabilidad para cada una de estas amenazas a una medida de seguridad implementada en el laboratorio EDI (Tabla 1).

Vulnerabilidades identificadas	Ponderación de la vulnerabilidad	Medida de Seguridad implementada en el Laboratorio

Tabla 1. Cuadro de relación de trazabilidad entre amenaza identificada (Vulnerabilidad) y medida de seguridad implementada.

La ponderación es un atributo de la vulnerabilidad y está relacionado al impacto de la amenaza que representa dicha vulnerabilidad en el análisis de riesgo.

El trabajo expuesto tiene como finalidad obtener una visibilidad global de las amenazas o vulnerabilidades latentes en una red informática de un laboratorio EDI. De forma tal que cada amenaza identificada pueda ser rastreada a una medida de seguridad implementada en cada capa del modelo de defensa planteado. A partir de esto se puede detectar indicadores que puedan ser medidos y posteriormente conformar una guía de buenas prácticas con una base de ciberseguridad a Laboratorios de Educación, Desarrollo e Investigación de organizaciones, principalmente educativas como universidades, institutos educativos de educación media y superior, academias y otras organizaciones que tengan infraestructuras tecnológicas para brindar servicios.

El modelo de defensa presentado fue planteado teniendo en cuenta la heterogeneidad de los usuarios de un laboratorio EDI y la masividad de usuarios que pasan diariamente por estos laboratorios, identificando los perfiles de estos y asegurando que puedan realizar las actividades planificadas. Por lo que laboratorios con las mismas características pueden aplicarlo, lo que no quita el hecho que entornos más homogéneos también lo puedan hacer.

Referencias

[1] Norma Chilena. Tecnologías de la información - Código de prácticas para los controles de seguridad de la información. Número de referencia NCh-ISO 27002:2013. Pág. 43. (2013).

[2] The Interview revenge hack cost Sony just $15m. Recuperado de https://www.theguardian.com/film/2015/feb/04/guardians-peace-revenge-hacksony-finances-unscathed. (2014).

[3] Todd, M., Rahman, S. (Noviembre 2013). COMPLETE NETWORK SECURITY PROTECTION FOR SME'SWITHIN LIMITED RESOURCES. International Journal of Network Security & Its Applications (IJNSA). Vol. 5, Nro. 6.

[4] Zurutuza, R., Uribeetxeberria, R. (). Revisión del estado actual de la investigación en el uso de data mining para la detección de intrusiones.

[5] Rojanakul, K., Liang, H. (2009). Network Security Infrastructure Management. IEEE.

[6] Dees, K., Rahman, S. (2011). ENHANCING INFRASTRUCTURE SECURITY IN REAL ESTATE. International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6.

[7] Dharma, R., Sake, S., Manuel, M. (2013). Backup and Recovery in a SAN. Versión 1.2. EMC2 Techbooks.

[8] Castillo, J., Cárdenas, M., Serrano, D. (2011). Experiencias en el Desarrollo de Competencias de Programación en UTN-FRC. Dpto. Ingeniería en Sistemas de Información - Universidad Tecnológica Nacional – Facultad Regional Córdoba. TE&ET 2011. Recuperado el 12, Junio, 2018 de http://sedici.unlp.edu.ar/handle/10915/18414.

[9] Marciszack, M., Muñoz, R., Castillo, J., Delgado A., Serrano, D., Gatto, S. (2013) Colaboración entre el Gobierno de la Provincia de Córdoba y la UTN - FRC para el desarrollo de Olimpíadas Informáticas". Recuperado el 12, Junio, 2018 de http://conaiisi.frc.utn.edu.ar/PDFsParaPublicar/1/schedConfs/4/234-650-1-DR.pdf.

[10] Bunge, M. (1998). La ciencia su Método y su Filosofía. Editorial Siglo Veinte. Buenos Aires

[11] Barchini (2005). G. Métodos “I+D” de la Informática. Universidad Nacional de Santiago del Estero, Argentina.