Seguridad informática y amparo legal. Caso Calzalona SA

Autores:
Pablo David Pazmay Pazmay (p.pazmay@pucesa.edu.ec)
Edgar Eduardo Jurado Granja (edjuradogranja@outlook.com)

Afiliación:
Tecnologías de la Información y Comunicaciones / El dominio sobre bienes – nuevas tendencias

Áreas del conocimiento:
Ingeniería en Sistemas
Jurisprudencia

Resumen

En este trabajo se presenta un caso ocurrido en la empresa Calzalona S.A., en el cual se realizó un ataque informático que resultó una intrusión a la red interna y al sistema informático propiedad de la empresa y causando daños directos a la información, tales como la inoperatividad de la red interna, bloqueo de acceso a la información alojada en su servidor local, y la inhabilitación del sistema informático en su totalidad.

Así mismo, el trabajo presenta las causas y consecuencias del hecho suscitado y las soluciones y recomendaciones pertinentes para evitar este tipo de ataques informáticos en cualquier otra red. A la vez que se presenta, la normativa referente al área de tecnologías de la información dentro del marco legal ecuatoriano.

Palabras claves: Ataque informático, red interna, bloqueo de acceso

Abstract

This paper presents a case that occurred in the company Calzalona SA, in which a computer attack was carried out that resulted in an intrusion into the internal network and the computer system owned by the company and causing direct damages to the information, such as inoperability of the internal network, blocking access to the information hosted on your local server, and disabling the entire computer system. Also, the paper presents the causes and consequences of the event and the relevant solutions and recommendations to avoid this type of computer attacks in any other network. At the same time, the regulations regarding the area of information technologies within the Ecuadorian legal framework are presented.

Keywords: Computer attack, internal network, access block

Introducción

El presente trabajo tiene como objetivo analizar y detallar el procedimiento tomado ante la infiltración realizada al sistema informático registrada el 16 de abril de 2017 en las instalaciones de Calzalona S.A., empresa dedicada a la producción de cortes cocidos, ubicada en la ciudad de Ambato en la Panamericana Norte y entrada a la Península. Así mismo, está enfocado en detallar las seguridades informáticas, tanto burladas como ausentes, mediante las cuales se realizó la invasión. Con lo cual, ha sido necesario especificar las medidas de seguridad que se tomaron al respecto, las consecuencias de la intrusión realizada, tanto en acciones como hechos y, sustentar legalmente las mismas, para que se conozcan los derechos a los cuales estuvo suscrita la empresa y las acciones legales pertinentes.

A su vez, se pudo determinar que la empresa no contó con las seguridades adecuadas para evitar cualquier tipo de invasión informática, que consecuentemente, causó un colapso en su red interna, motivo por el cual, se pretende dejar constancia de la importancia de contar con seguridades informáticas y presentar las vías legales a las cuales tiene acceso en el caso de necesitar recurrir a ellas. Por lo tanto, el objetivo general del estudio es: analizar las medidas de seguridad informática y sus aspectos legales a nivel local en la empresa Calzalona S.A.

Desarrollo

Estado del Arte

En ("Tutorial", s. f.) se puede encontrar información pertinente sobre intrusiones informáticas, cómo identificarlas y cómo realizarlas. Así mismo, presta un tutorial paso a paso para lograrlo, ayudando al lector a evadir este tipo de delitos y mantenerlos fuera de su empresa o área de trabajo.

Dentro del área de las intrusiones informáticas, se encuentran las técnicas que se usan para realizar los ataques deseados ("TÉCNICAS DE INTRUSIÓN E INFORMÁTICA FORENSE ** COMPLETO ** - Euskadi+innova", 2007). Este tipo de información es altamente delicada debido a que en las manos equivocadas las redes más básicas y vulnerables pueden ser penetradas y toda su información puede ser sustraída.

En la publicación (Aziz & Salama, s. f.), el autor detalla un proyecto basado en algoritmos genéticos para la creación de un sistema de detección de intrusiones, lo cual evita infiltraciones a sistemas y redes informáticas en un futuro. Al respecto, ("2005_09.CEDI_IDS.pdf", s. f.), presenta una revisión a los métodos usados en el *data mining* para la detección de intrusiones. Tomándose como prioridad la seguridad informática, es por ello, que el trabajo tiene el objetivo de detallar las técnicas de *data mining,* utilizándose a lo largo de los años para la detección de intrusiones en sistemas y redes informáticas.

Las disciplinas que se deben tomar en cuenta para mantener los sistemas y las redes informáticas intactas y sin infiltraciones se encuentran en (Quispe Yujra, /), aun cuando se destaca la auditoría forense. En el documento, se explica detalladamente cómo la informática forense facilita la reconstrucción de evidencia mediante el uso de huellas y rastros digitales.

En la tesis de grado propuesta por (“T-2270.pdf”, s. f.), se establece un modelo para la detección de intrusiones mediante la aplicación de la lógica difusa. Esto pretende superar la vulnerabilidad de no contar con las herramientas necesarias para la protección de sistemas informáticos. Con lo cual, mediante la comparación de las técnicas de seguridad utilizado por diversos sistemas informáticos (“aalonso-PFC-presentacion.pdf”, s. f.), se pretende plantear nuevos y diversos métodos de seguridad, con el fin de evitar intrusiones a sistemas informáticos y presentarlo al público para que cualquier individuo pueda hacer uso del mismo.

Metodología

Se utilizó el método inductivo – deductivo, con el fin de identificar los problemas causados por la intrusión registrada, tales como: bloque de red, impedimento de acceso a información y vulneración de derechos y propiedad; como lo define (“Metodo-Cientifico-Global.pdf”, s. f.). Asimismo, es importante plantear las soluciones del caso basándose en el informe de (Jurado, Coronel, & Figueroa, 2017), presentado por parte de los responsables del área.

A su vez, siguiendo la lógica del método, se detallaron y especificaron los puntos relevantes y necesarios para la investigación. Lo cual, mediante el uso de la técnica de observación de la investigación se pudo constatar la obtención de causas y consecuencias de la negligencia por parte del personal a cargo de proteger los datos, la información y la red de la empresa. Dichos resultados son expuestos en el siguiente apartado.

Resultados

Calzalona S.A., es una empresa ubicada en la ciudad de Ambato en la Av. Panamericana Norte y entrada a La Península dedicada la fabricación de cortes cocidos. Las instalaciones cuenta con un servidor que trabaja con *Windows Server* 2012 R2. Dicho servidor aloja la información de la base de datos, configurada en Oracle, manejada por el sistema informático de planificación de recursos empresariales (ERP) ADempiere.

La información que contempla ADempiere se refiere a órdenes de compra y de venta, facturas de compra y de venta, guías de remisión, producciones, información de terceros (tanto proveedores como clientes y empleados), e información de declaraciones de renta.

La configuración inicial del servidor, realizada en conjunto por la Ing. Mayra Coronel y el Sr. David Figueroa, contempló los siguientes puntos:

- Instalación de *Windows Server* 2012 R2.
- Configuración básica de *Windows Server* (no incluye instalación de roles ni características del paquete del sistema operativo).
- Desactivación del firewall de Windows.
- Asignación de una IP pública estática, mediante coordinación con el proveedor del servicio de internet.
- Instalación del kit y el entorno de desarrollo de Java versión 6.
- Instalación de la base de datos Oracle XE.
- Instalación del ERP ADempiere versión 4.37.0.

Es importante recalcar que dentro del procedimiento de configuración inicial del servidor, no se contempló en ningún momento la instalación de políticas y protocolos de seguridad, sino más bien se omitieron las mismas.

Dentro del amparo legal, contemplado en el artículo 44 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, se establece que:

> "*Cualquier actividad, transacción mercantil, financiera o de servicios, que se realice con mensajes de datos, a través de redes electrónicas, se someterá a los requisitos y solemnidades establecidos en la ley que las rija, en todo lo que fuere aplicable, y tendrá el mismo valor y los mismos efectos jurídicos que los señalados en dicha ley.*"

Y en concordancia con los artículos 230, 232 y 234 del Código Orgánico Integral Penal, se orientan a la interceptación ilegal de datos, a los ataques, a la integridad de sistemas informáticos y al acceso no consentido a un sistema informático, estableciéndose lo siguiente:

El domingo 16 de abril de 2017, aproximadamente a las 23:17, se registra una infiltración al servidor propiedad de la empresa Calzalona S.A., violando el artículo 234 del Código Orgánico Integral Penal que sentencia el acceso no consentida a un sistema informático, entendiéndose por el mismo el servidor violentado. Una vez obtenido el acceso al sistema informático, se realizó un ataque directo a la integridad de los datos, información, archivos y ficheros alojados en el mismo, causando su inutilización y deteniendo todo proceso informático, que para el caso de la empresa se refiere a todos los procesos salvo la producción, y violando así el artículo 232 del

Código Orgánico Integral Penal. Posteriormente, se realiza un bloqueo a la base de datos, inhabilitándola por completo y comprometiendo los datos alojados en la misma (se ha violado también el artículo 230 del Código Orgánico Integral Penal). Todo esto, con el fin de inhabilitar y bloquear el uso de los datos alojados en el sistema informático y solicitar un valor monetario de $200,00 (doscientos dólares americanos) a cambio del desbloqueo de los archivos, ficheros, información, y la eliminación del virus que infectó el sistema.

Una vez entregado el informe de los hechos acontecidos y mediante reunión mantenida entre los directivos de Calzalona S.A., la Ing. Mayra Coronel, el Sr. David Figueroa y el Sr. Edgar Jurado, el día lunes 17 de abril en horas de la mañana se concluyó lo siguiente:

- No se recurrirá al pago por la liberación del sistema informático.
- Se comprobó el último respaldo del sistema con fecha y hora 28 de marzo a las 13:37.
- El personal a cargo de la manipulación del sistema informático, independientemente del área de competencia, debe realizar un informe detallado de las transacciones que ha registrado desde el 28 de marzo hasta la fecha.
- Se restaura el sistema informático en su totalidad con el último respaldo obtenido.
- El personal a cargo de la manipulación del sistema debe volver a ingresar todas las transacciones que ha registrado en el informe presentado por los mismos.
- La Ing. Mayra Coronel y el Sr. David Figueroa debe realizar todas las gestiones pertinentes para la restauración del sistema, tales como:
    - Supervisar los informes entregados por el personal.
    - Constatar las transacciones realizadas con sus respectivas fechas, y el caso de contar con documentos físicos sustentarlas con los mismos.
    - Restaurar el sistema informático en su totalidad.
    - Gestionar, supervisar y apoyar en el ingreso de las transacciones detalladas en el informe.
- El Sr. Edgar Jurado ungirá como asesor en el tema de seguridad informática para el sistema.
- La Ing. Mayra Coronel y el Sr. David Figueroa debe acatar las disposiciones por parte del Sr. Edgar Jurado, en cuanto a seguridad informática se refiere.

Dentro del ámbito de seguridad informática se realizaron las siguientes acciones:

1. Instalación de Windows Server 2012 R2.
2. Configuración de firewall de Windows.
3. Bloqueo de puertos innecesarios e inutilizados.
4. Bloqueo de conexiones entrantes a excepción del acceso a ADempiere.
5. Instalación de Kaspersky Server Enterprise Edition.
6. Restauración del sistema informático con respaldo de 28 de marzo.
7. Configuración del protocolo dinámico de host.
8. Asignación de roles de usuario.
9. Creación y configuración de dominio.
10. Programación de respaldo diario.

Las acciones anteriormente descritas fueron implementadas en Calzalona S.A., con el objetivo de evitar futuras infiltraciones. Lo cual, hasta el momento de esta investigación, no se ha vuelto a presentar.

Conclusiones

- Dentro del amparo legal, una persona natural o una persona jurídica puede recurrir a los artículos 230, 232 y 234 del Código Integral Orgánico Penal, los cuales se los resume en: proteger los datos que viajan en una red evitando así su interceptación sin consentimiento del propietario o sin orden judicial, sanciona a quienes generen ataque a sistemas informáticos comprometiendo la información del mismo, pena la intrusión o el acceso no consentido a sistemas informáticos, respectivamente.
- Tal como establece la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos en el artículo 44: se deben cumplir las formalidades del caso para realizar uso de los servicios electrónicos y se aplicará la ley correspondiente., regulando así las acciones permitidas y no permitidas dentro del ámbito tecnológico.
- Es común que dentro de los sistemas informáticos de las PYMES, se omitan ciertos aspectos, principalmente en el servidor, como utilizar el protocolo de configuración dinámico de host (DHCP), asignación y creación de roles de usuario, configuración de firewall (en el caso de Windows Server) y configuración de accesos y permisos de conexión.
- El ámbito legal dentro de un Estado de Constitucional Derechos y Justicias, según lo tipifica el artículo 1 de la Constitución de la República del Ecuador: el

Ecuador es un país en donde sin importar la religión o etnia asegura y brinda derechos a todo ciudadano soberano, lo cual, a su vez orientado a las seguridades y sistemas informáticos protege a las personas, ya sea de carácter natural o jurídica, para que sus derechos no sean vulnerados y su información esté protegida en todo momento, y en el caso de que estos sean vulnerados facilita a la persona el tomar acciones legales para sentenciar dichas obras a través de sus leyes y códigos. Por lo tanto, dentro del ámbito de la informática, el usuario es capaz de defenderse ante la violación de sus derechos y privacidad.

Referencias Bibliográficas

2005_09.CEDI_IDS.pdf. (s. f.). Recuperado a partir de http://www.mondragon.edu/es/eps/investigacion/grupos-de-investigacion/telematica/publicaciones/2005_09.CEDI_IDS.pdf

aalonso-PFC-presentacion.pdf. (s. f.). Recuperado a partir de http://www.angelalonso.es/doc-presentaciones/aalonso-PFC-presentacion.pdf

Aziz, A., & Salama, M. (s. f.). Artificial Immune System Inspired Intrusion Detection System Using Genetic Algorithm.

Jurado, E., Coronel, M., & Figueroa, D. (2017). *Infiltración a servidor* (p. 7). Ambato, Ecuador: Calzalona S.A.

Metodo-Cientifico-Global.pdf. (s. f.). Recuperado a partir de https://clea.edu.mx/biblioteca/Metodo-Cientifico-Global.pdf

Quispe Yujra, E. (/). Asegurandose contra delitos informaticos. *Revista de Información, Tecnología y Sociedad*, 29.

T-2270.pdf. (s. f.). Recuperado a partir de http://repositorio.umsa.bo/bitstream/handle/123456789/1952/T-2270.pdf?sequence=1

TÉCNICAS DE INTRUSIÓN E INFORMÁTICA FORENSE ** COMPLETO ** - Euskadi+innova. (2007, julio 12). Recuperado 29 de julio de 2017, a partir de http://www.spri.eus/euskadinnova/es/enpresa-digitala/agenda/tecnicas-intrusion-informatica-forense-completo/888.aspx

Tutorial. (s. f.). Recuperado 29 de julio de 2017, a partir de http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap3.html