Dom. Cien., ISSN: 2477-8818
Vol. 6, núm. 2, abril-junio 2020, pp. 835-846

DOI: http://dx.doi.org/10.23857/dc.v6i2.1197

Ciencias de la computación

Artículo de investigación

Importancia de la seguridad de los sistemas de información frente el abuso, error y hurto de información

Importance of the security of information systems against the abuse, error and theft of information

Importância da segurança dos sistemas de informação contra abuso, erro e roubo de informações

Felipe Emiliano Arévalo-Cordovilla [I]
farevaloc@unemi.edu.ec
https://orcid.org/0000-0003-0666-8004

Ingrid Beatriz Ordoñez-Sigcho [II]
iordonezs@unemi.edu.ec
https://orcid.org/0000-0003-0666-8004

Milton Fabián Peñaherrera-Larenas [III]
mpenaherreral@unemi.edu.ec
https://orcid.org/0000-0001-8603-7522

Verónica Janeth Suárez-Matamoros [IV]
vsuarezm@utb.edu.ec
https://orcid.org/0000-0001-6269-1394

Correspondencia: farevaloc@unemi.edu.ec

***Recibido:** 25 de enero de 2020 ***Aceptado:** 25 de febrero de 2020 *** Publicado:** 16 de abril de 2020

I. Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones, Ingeniero en Sistemas Computacionales, Analista de Sistemas, Universidad Estatal de Milagro, Milagro, Ecuador.

II. Máster Universitario en Diseño y Gestión de Proyectos Tecnológicos, Ingeniera en Sistemas Computacionales, Universidad Estatal de Milagro, Milagro, Ecuador.

III. Diploma Superior en Currículo por Competencias, Ingeniero en Sistemas Computacionales, Analista de Sistemas, Universidad Estatal de Milagro, Milagro, Universidad Técnica de Babahoyo, Babahoyo, Ecuador.

IV. Ingeniera en Sistemas Computacionales, Universidad Técnica de Babahoyo, Babahoyo, Ecuador.

Resumen

El presente artículo tiene como finalidad analizar los puntos vulnerables que existen en los sistemas de información, estos que podrían afectar a la empresa o a las personas en general, buscando, por lo consiguiente, sistemas o medidas de seguridad que se podrían tomar para evitar estos problemas debido a las fallas en los sistemas.

Palabras clave: Sistemas de información; vulnerabilidad; seguridad informática; delitos informáticos.

Abstract

The purpose of this article is to analyze the vulnerable points that exist in the information systems, these that could affect the company or people in general, seeking, therefore, systems or security measures that could be taken to avoid these problems due to system failures.

Keywords: Information systems; vulnerability; Informatic security; Cybercrime.

Resumo

O objetivo deste artigo é analisar os pontos vulneráveis existentes nos sistemas de informação, que podem afetar a empresa ou as pessoas em geral, buscando, portanto, sistemas ou medidas de segurança que possam ser tomadas para evitar esses problemas. devido a falhas no sistema.

Palavras-chave: Sistemas de informação; vulnerabilidade; segurança informática; crimes de computador.

Introducción

A partir del nacimiento de la computación, también nacieron sistemas y software que permitieron a aquellas maquinas operar. Si bien estos aparatos electrónicos manejan la información de manera precisa, lo cierto es que los programas que las controlaban eran de desarrollo y diseño humano, y por lo tanto su código son propensos de contener toda clase de errores a lo que se define como vulnerabilidad.

En seguridad informática, la palabra vulnerabilidad hace referencia a una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

Las vulnerabilidades son el resultado de bugs o de fallos en el diseño del sistema. Aunque, en un sentido más amplio, también pueden ser el resultado de las propias limitaciones tecnológicas, porque, en principio no existe sistema 100% seguro.

La delincuencia informática es difícil de comprender o conceptualizar plenamente. A menudo, se la considera una conducta proscrita por la legislación y/o la jurisprudencia, que implica la utilización de tecnologías digitales en la comisión del delito; se dirige a las propias tecnologías de la computación y las comunicaciones; o incluye la utilización incidental de computadoras en la comisión de otros delitos.

Varios delitos informáticos atacan a las propias tecnologías de la información y las comunicaciones, como los servidores y los sitios web, con virus informáticos de alcance mundial que causan considerables perjuicios a las redes comerciales y de consumidores.

Un delito informático es toda aquella acción, típica, antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de internet.

La importancia de conocer lo vulnerable que somos frente a la red más grande a nivel mundial nos hace crear un ambiente de preocupación, ya que debido a la globalización y evolución de la tecnología nos hace innovar cada vez más en nuestros negocios personales y a su vez las industrias y grandes organizaciones, lo cual, a causa de la falta de seguridad podríamos perder información fundamental e incluso obtener perdidas de efectivo que podría hasta incluso llevar al cierre definitivo de las actividades laborales.

Lo que se busca frente a esta situación, es crear un plan de contingencia y/o implantar medidas de seguridad la cual, nos ayude hacer frente a los posibles" fantasmas informáticos" y evitar el robo masivo de información preciada para los directivos.

Desarrollo

Para O'Brien & Marakas, (2006), "un sistema de información (SI) puede ser cualquier combinación de personas, hardware, software, redes de comunicación y recursos de información que almacene, recupere, transforme y disemine información en una organización." (pág. 6).

Un sistema de información también lo podemos definir en un conjunto de herramientas que interactúan entre sí con un fin común; que permite que la información esté disponible para

satisfacer las necesidades en una organización, un sistema de información no siempre requiere contar con recuso computacional, aunque la disposición del mismo facilita el manejo e interpretación de la información por los usuarios.

Las herramientas que se enlazan para la obtención de dicho fin para Fernández Otero & Navarro Huerga, (2014) son: "una estructura de decisión, una actividad transformadora u operante, concretada en un conjunto de reglas de gestión y un conjunto de informaciones." (pág. 16)

En un sistema informático lo que queremos proteger son sus activos, es decir, los recursos que forman parte del sistema y que podemos agrupar en:

Hardware: elementos físicos del sistema informático, tales como procesadores, electrónica y cableado de red, medios de almacenamiento (cabinas, discos, cintas, DVD).

Software: elementos lógicos o programas que se ejecutan sobre el hardware, tanto si es el propio sistema operativo como las aplicaciones.

Datos: comprenden la información lógica que procesa el software haciendo uso del hardware. En general serán informaciones estructuradas en bases de datos o paquetes de información que viajan por la red.

Otros: fungibles, personas, infraestructuras, aquellos que se 'usan y gastan' como puede ser la tinta y papel en las impresoras, los soportes tipo DVD o incluso cintas si las copias se hacen en ese medio, etc.

Los sistemas de información dan soporte a las operaciones empresariales; los gerentes o directivos al mando de la organización utilizan estos sistemas como instrumento estratégico para innovar, competir y alcanzar los objetivos en un entorno globalizado.

Estos sistemas de información generalmente son manipulados por personas, por lo tanto, son propensos a caer en errores de calibración e implementación de poca seguridad. A esta limitación por parte de las personas se las conoce como vulnerabilidad y de acorde al tema tratado se define como vulnerabilidad informática.

Según Feito, (2007) la vulnerabilidad, en tanto que posibilidad del daño, es considerada la misma raíz de los comportamientos morales, al menos de aquellos en que el énfasis se sitúa en la protección y en el cuidado, más que en la reclamación de derechos.

Aplicado en los Sistemas de Información (SI), vulnerabilidad es conocida como aquella debilidad de cualquier tipo que compromete la seguridad del sistema informático.

Castro (2011) nos data que "los robos de información o de sistemas, actualmente es el delito con mayor crecimiento a nivel mundial, causando no solamente el desconcertó y enojo por lo sucedido, sino, que causa grandes pérdidas económicas a nivel empresarial."

Las vulnerabilidades de los sistemas informáticos las podemos agrupar en función de:

- Diseño. - Debilidad en el diseño de protocolos utilizados en las redes. Políticas de seguridad deficientes e inexistentes.
- Implementación. - Errores de programación. Existencia de "puertas traseras" en los sistemas informáticos. Descuido de los fabricantes.
- Uso. - Mala configuración de los sistemas informáticos. Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática. Disponibilidad de herramientas que facilitan los ataques. Limitación gubernamental de tecnologías de seguridad.

Por qué son vulnerables los sistemas

Cuando en una empresa se almacenan de forma electrónica grandes cantidades de datos o información, son vulnerables a muchos tipos de amenazas que a cuando estaban en forma manual. La falta de seguridad en los accesos o también la falta de seguridad en la forma de comunicarse y traspasar información en vías de internet puede resultar peligroso a tal punto de que los hackers puedan tomar dicha información y seas victimas de ellos.

Vulnerabilidad de internet

Las grandes redes públicas, como internet, son súper vulnerables, ya que están abiertas prácticamente a todas las personas. Internet es tan grande que cuando ocurren abusos pueden tener un gran impacto en cualquiera que sea la situación que nos encontremos como en la organización o en el departamento de cobro e información de una "x" empresa de créditos.

Los grandes robos de internet son producidos por los famosos hackers que según Laudon & Laudon, (2016) "un hacker es un individuo que intenta obtener acceso sin autorización a un sistema computacional. Estos hackers obtienen este acceso al encontrar debilidades en las protecciones de seguridad empleadas por los sitios Web y los sistemas computacionales; a menudo aprovechan las diversas características de Internet que los convierten en sistemas abiertos fáciles de usar." (pág. 311)

Las actividades de los hackers han crecido exponencialmente más allá de las barreras existentes en internet, para realizar robos de bienes e información, así como daños en los sistemas y el cibervandalismo, que se entiende como la interrupción, desfiguración o destrucción internacional de un sitio Web o sistema de información corporativo.

Los hackers comúnmente intentan ocultar sus verdaderas identidades utilizando direcciones de correos falsos o se hacen pasar por alguien más. El spoofing también puede implicar el hecho de redirigir un vínculo Web a una dirección distinta de la propuesta, donde el sitio se camufla como el destino esperado.

Para poder identificar estos crímenes informáticos se utiliza comúnmente el sniffer (husmeador) que no es más que un programa que monitorea la información que viaja a través de una red. Cuando se utilizan de manera legal, los husmeadores ayudan a identificar puntos de problemas potenciales que puede dañar el sistema, pero cuando se utilizan para fines criminales pueden ser dañinos y muy difíciles de identificar. Estos husmeadores permiten a los hackers robar información propietaria de cualquier parte de una red, como mensajes de correo, archivos secretos de la compañía, etc.

Crimen por computadora.

La mayoría de las actividades realizadas por los hackers son delitos criminales; todos los casos y situaciones que se detalló en párrafos anteriores también los convierten en objetivos para otro tipo de crímenes por computadora. El delito por computadora se lo define como “cualquier violación a la ley criminal que involucra el conocimiento de una tecnología de computadora para su perpetración, investigación o acusación.

De acuerdo con el Estudio Anual del Costo de Delitos Cibernéticos de Ponemon Institute, (2013), patrocinado por HP Enterprise Security, “hasta el 2013 fue de 11.56 millones de dólares, lo que representa un aumento del 78% desde el estudio inicial realizado hace 4 años”.

Sistemas de Seguridad para evitar delitos informáticos.

Para poder dar frente a estos problemas informáticos que pueden provocar dolores de cabeza tanto a los gerentes con a las personas que encabezan un negocio, es importante implantar medidas de seguridad, mediante una administración adecuada de un sistema y el uso de herramientas de seguridad de la información, se pueden reducir significativamente el riesgo existente en este tipo de entorno.

La seguridad informática según Baca Urbina, (2016) "es la disciplina que, con base en políticas y normas internas y externas de la empresa, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos, a los que está expuesta". (pág. 12)

Distintas maneras para proteger tu información de delitos informáticos son:

Firewalls, sistemas de detección de intrusos y software antivirus.

Para aquellas empresas que se encuentran sin protección contra el malware y los intrusos, es un verdadero riesgo conectarse a internet. Los Firewalls, sistemas de detección de intrusos y software antivirus se han vuelto herramientas esenciales de negocios.

Firewall

Para Laudon & Laudon, (2016) "los firewalls evitan que los usuarios sin autorización accedan a redes privadas. Un firewall es una combinación de hardware y software que controla el flujo de tráfico de red entrante y saliente. Por lo general se colocan entre las redes internas privadas de la organización y las redes externas que no son de confianza como Internet, aunque también se pueden utilizar firewalls para proteger una parte de la red de una compañía del resto de la red".

Sistema de detección de intrusos.

Para Hernández, (2015) "el sistema de detección de intrusos no es más que una herramienta de seguridad que monitoriza eventos dentro de una computadora o red de computadoras, que posteriormente se analizan en busca de intrusiones o intento de ellas."

Software antivirus

Kramer & Bradfield, (2009) define que "los programas que detectan códigos maliciosos o mal intencionados que pueden dañar el funcionamiento de las computadoras son los softwares de antivirus. Se consideran software malicioso los virus, troyanos y gusanos, entre otros, que alteran el funcionamiento de la computadora".

Algunas clases de antivirus que pueden ayudar al fortalecimiento de la seguridad de información empresarial o personal son:

Antivirus de Escritorio

Para Costas Santos, (2014) "los antivirus de escritorio se suelen utilizar en modo residente para proteger al ordenador en todo momento de cualquier posible infección, ya sea al navegar por Internet, recibir algún correo infectado o introducir en el equipo algún dispositivo extraíble que esté infectado. No necesitan que el ordenador esté conectado a Internet para poder funcionar, pero sí que es necesario actualizarlos frecuentemente para que sean capaces de detectar las últimas amenazas de virus". (págs. 149-150).

Antivirus en línea

También podemos encontrar que los antivirus en línea son útiles para analizar el ordenador con un segundo antivirus cuando sospechamos que el equipo puede ser infectado. Para ejecutarlo es necesario tener conexión a internet.

Estos antivirus solamente nos sirven para detectar que nuestros ordenadores no estén infectados, mas no nos ayudan a prevenir la infección, para es solo sirven los antivirus de escritorios.

Antiespías de escritorio

Los antiespías de escritorio para Costas Santos, (2014) "son aquellos que requieren de instalación en el PC. Se suelen utilizar en modo residente, analizan cualquier fichero al que accede el PC en tiempo real, como complemento a los antivirus para proteger al ordenador en todo momento de cualquier posible infección de código espía. No requieren de conexión a Internet para poder funcionar, pero sí necesitan estar actualizados para que sean capaces de detectar las amenazas más recientes". (pág. 155)

Antiespías en línea

Los antiespías en línea son accesibles a través de un navegador web y no necesitan de una instalación de una aplicación completa en nuestro equipo para su funcionamiento. Necesitan por tanto de una conexión a Internet para acceder a ellas, y, al estar disponibles directamente en línea se accede a la versión más actualizada de la herramienta.

Otras herramientas antimalware

Herramientas de bloqueo:

Antifraude

Estas herramientas nos informan sobre la peligrosidad de los sitios que frecuentamos, algunas veces, nos informan de forma detallada, que enlaces de páginas se consideran peligrosos y cuál es el motivo.

Útiles antispam

El spam podemos definirlo como el envío masivo de correo electrónico no solicitado. Los útiles antispam son programas que filtran los correos electrónicos y tratan de eliminar los que se consideren spam.

Anti-Dialer

Este tipo de herramienta nos permite controlar a qué números de teléfono se conecta nuestro módem, para que no utilice ningún número que no esté en la lista de números permitidos, ya que hay algunos programas que cambiaban estos números por otros de tarificación especial, y las llamadas salían mucho más caras. Este tipo de fraude ha quedado reducido a conexiones de 56 kbps, con módem de marcación sobre línea telefónica, conexiones ya en desuso.

Análisis de URL

Herramientas para el análisis de direcciones de páginas web, que sirven para determinar si el acceso a dicha URL puede afectar o no a la seguridad de nuestro sistema.

Estas y otras herramientas son muchas de las protecciones que podemos aplicar a nuestros servidores de nuestro sitio de trabajo, ya que de esta manera podemos evitar los crímenes de internet que pueden causar como lo antes mencionado perdidas de información e incluso pérdidas económicas.

Conclusión

Para concluir, podemos decir, que en la actualidad la falta de atención a los sistemas con los cuales trabajamos a diario permiten que nuestros sistemas se vuelvan vulnerables y demos paso a los delitos informáticos que son, en la mayoría de los casos, provocado por los hackers dejando como resultado perdida de información valiosa o incluso perdidas económicas dentro del sector organizacional.

La implementación de un sistema de seguridad eficaz y eficiente, es de suma importancia, pues con ello contribuye para que la información dentro de la organización se encuentre segura bajo el sistema, frente a la malicia, abuso o malas intenciones que tengan terceras personas con la organización.

En la actualidad, la globalización permite que todas las empresas innoven desde las maquinarias más grandes hasta los sistemas con los cuales estas se desarrollan, es, por tanto, que un sistema de información ayuda mantener estable frente a la competitividad a vuestra organización y por eso es de mucho valor mantener la información confidencial y de interés a salvo y seguro.

Referencias

1. Baca Urbina, G. (2016). Introduccion a la Seguridad Informatica. Mexico: Grupo Editorial Patria.
2. Castro, R. L. (08 de 04 de 2011). welivesecurity. Obtenido de https://www.welivesecurity.com/la-es/2011/04/08/robo-identidad-cifras-america-latina/
3. Costas Santos, J. (2014). Seguridad Informatica. Madrid: RA-MA, S.A.
4. Feito, L. (2007). Vulnerabilidad. sciELO.
5. Fernández Otero, M., & Navarro Huerga, M. (2014). SISTEMA DE INFORMACION EN LA EMPRESA. España: Servicio de Publicaciones, Universidad de Alcala.
6. Hernandez, R. S. (2015). Sistemas De Deteccion De Intrusos. Granada: Universidad De Granada.
7. Kramer, S., & Bradfield, J. C. (2009). Journal of Computer Virology and Hacking Techniques. ERIC FILIOL.
8. Laudon, K., & Laudon, J. (2016). Sistemas de informacion gerencial. Mexico: Pearson.
9. O'Brien, J., & Marakas, G. (2006). Sistemas de informacion gerencial. Mexico.
10. Ponemon Institute. (2013). Obtenido de https://www.ipusergrouplatino.com/articles/article/8845868/175750.html

References

1. Baca Urbina, G. (2016). Introduction to Computer Security. Mexico: Grupo Editorial Patria.

2. Castro, R. L. (08 of 04 of 2011). welivesecurity. Obtained from https://www.welivesecurity.com/la-es/2011/04/08/robo-identidad-cifras-america-latina/
3. Costas Santos, J. (2014). Informatic security. Madrid: RA-MA, S.A.
4. Feito, L. (2007). Vulnerability. sciELO.
5. Fernández Otero, M., & Navarro Huerga, M. (2014). INFORMATION SYSTEM IN THE COMPANY. Spain: Publications Service, University of Alcala.
6. Hernandez, R. S. (2015). Intrusion Detection Systems. Granada: University Of Granada.
7. Kramer, S., & Bradfield, J. C. (2009). Journal of Computer Virology and Hacking Techniques. ERIC FILIOL.
8. Laudon, K., & Laudon, J. (2016). Management information systems. Mexico: Pearson.
9. O'Brien, J., & Marakas, G. (2006). Management information systems. Mexico.
10. Ponemon Institute. (2013). Obtained from https://www.ipusergrouplatino.com/articles/article/8845868/175750.html

Referências

1. Baca Urbina, G. (2016). Introdução à segurança de computadores. México: Grupo Editorial Patria.
2. Castro, R. L. (08 de 04 de 2011). Welivesecurity. Obtido em https://www.welivesecurity.com/la-es/2011/04/08/robo-identidad-cifras-america-latina/
3. Costas Santos, J. (2014). Segurança informática. Madri: RA-MA, S.A.
4. Feito, L. (2007). Vulnerabilidade. sciELO.
5. Fernández Otero, M. & Navarro Huerga, M. (2014). SISTEMA DE INFORMAÇÃO NA EMPRESA. Espanha: Serviço de Publicações, Universidade de Alcala.
6. Hernandez, R. S. (2015). Sistemas de detecção de intrusão. Granada: Universidade de Granada.
7. Kramer, S., & Bradfield, J. C. (2009). Journal of Computer Virology and Hacking Techniques. ERIC FILIOL.
8. Laudon, K. & Laudon, J. (2016). Sistemas de informação gerencial. México: Pearson.
9. O'Brien, J. & Marakas, G. (2006). Sistemas de informação gerencial. México.

10. Instituto Ponemon. (2013). Obtido em https://www.ipusergrouplatino.com/articles/article/8845868/175750.html