INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN

AUTOR: HELLEN CUBERO

NOVIEMBRE: 2020

San Marcos

INTRODUCCIÓN

La seguridad de la información es un tema amplio que podría considerar muchos aspectos para fortalecer la protección a los datos e información relevante a las empresas.

Con el avance de la tecnología los sistemas de información se convirtieron en las herramientas esenciales de las organizaciones para el análisis, los datos históricos y la toma de decisiones, con el objetivo de buscar siempre el camino correcto hacia dónde dirigir sus negocios, sin embargo, esto significó un aumento considerable en los fraudes y delitos informáticos que se presentan a diario, por lo tanto en la presente lectura se exponen técnicas y buenas prácticas para la protección de la información, así como términos de conocimiento e identificación de vulnerabilidades o riesgos exponenciales de los sistemas y equipos que almacenan información valiosa.

Contenido

Practique la informática segura

¿Qué es seguridad de la información?
Es la protección de la información y de los sistemas de información del acceso, uso, divulga-ción y destrucción no autorizada a través de estándares, procesos, procedimientos, estrate-gias, recursos informáticos, recursos educativos y recursos humanos.La seguridad de la información protege a esta de una amplia gama de amenazas, a fin de garantizar la continuidad de una organización. (Avenía Delgado, s.f).

Poner en práctica principios de seguridad de informática permite a los usuarios navegar en internet de manera más segura. Según la Universidad Internacional de Valencia (2016), la seguridad informática previene el robo de datos, información de tarjetas de crédito, contraseñas, documentos relacionados con el trabajo, entre otros. Además, indica que la seguridad informática es algo esencial durante las comunicaciones de hoy día.

Por otra parte, señala algunas medidas para el mantenimiento y prevención de intrusiones, como las siguientes:

- Asegurar la instalación de software legalmente adquirido
- Instalación de antivirus
- Hardware y software cortafuegos, para ayudar con el bloqueo de usuarios no autorizados que intentan ingresar a los equipos.
- Uso de contraseñas complejas y grandes, utilizando caracteres especiales.
- Tener especial cuidado con la ingeniería social que se presenta a través de redes sociales, los ciberdelincuentes pueden intentar obtener datos e información.
- Criptografía, especialmente la encriptación para mantener la información sensible, segura y secreta.

A ingresar a internet es recomendable revisar los enlaces antes de presionarlos, los ciberdelincuentes homologan las páginas web, especialmente las de entidades financieras, con el fin de obtener datos importantes.

Como lectura complementarias observe

Cómo funciona internet

¿Qué es internet?
Es el término en forma abreviada para decir Inter Network, que significa entre redes, por lo que podría entenderse que el término Internet se refiere a interconexión de redes, específicamente redes de computadores a escala mundial. (Ariza Agámez, 2017).
La transferencias de información en internet se efectúa mediante la tecnología o modelo cliente servidor. El modelo cliente-servidor surge de la idea de distribución de tareas que se creó desde los años 70 para la organización del trabajo entre un Banco Central y sus sucursales.
Se trata de un proceso distribuido o sea de la distribución de aplicaciones y datos en una red de computadores. La tecnología cliente/servidor puede definirse como un conjunto, tanto de elementos de software como de hardware, entre los cuales se destacan tres tecnologías: el cliente, el servidor y la red. El servidor central quien acepta y procesa los requerimientos de otro elemento llamado cliente, quien es el encargado de recibir el resultado del proceso; estos dos elementos son unidos por medio de una red de comunicaciones.
La existencia del software cliente, le permite al usuario o solicitante de la información, enviar una solicitud de información al servidor o proveedor de información (software servidor) y leer los resultados de la respuesta emitida por el servidor en la propia computadora del cliente sin importar el lugar donde se encuentre. (Fresno Chávez, 2018).

Para obtener más información, observe este enlace

Una defensa exhaustiva

Los ataques cibernéticos son cada vez más frecuentes, y para defenderse de manera correcta es necesario analizar los puntos débiles por donde puede ser atacado un equipo o sistema, como lo menciona Díaz (2004), para entender bien cómo defenderse de un ladrón, hay que

pensar como un ladrón y, aunque no se pretende hacer ninguna apología de la inseguridad de las redes, si se va a realizar un análisis, suficiente exhaustivo, de sus debilidades y problemas de seguridad. Por ejemplo: configurar de manera correcta los firewalls, routers y switches.
Establecer defensa perimetral, incluyendo no solo las DMZ (zona desmilitarizada, hace referencia a una red local que se ubica entre la red interna de la organización y una red externa), sino también a los ordenadores portátiles que envían contenido a internet e implementando restricciones a través de herramientas de antivirus. Además de establecer políticas de seguridad a nivel interno y capacitar al usuario final en seguridad informática y técnicas para proteger la información.

El enemigo

Según el Instituto Nacional de Ciberseguridad (2019), los términos ransomware, ciberlincuentes, bonet, cracker son los enemigos de la seguridad de la información y generan diversos ataques con objetivos específicos: realizar ataques dirigidos, infecciones con códigos maliciosos, denegación de servicios, accesos no autorizados, daños físicos, entre otros que atentan con la seguridad de la información de las organizaciones.

Tipos de atacantes

Los tipos de atacantes definidos por Roa Buendía (2013), son los siguientes:

- Hacker: ataca la defensa informática de un sistema solo por el reto que supone hacerlo.
- Cracker: también ataca la defensa, pero a diferencia de hacker si quiere hacer daño: robar datos, desactivar servicios, alterar información, entre otros.
- Script kiddie: son aprendices de hacker y cracker que encuentran en internet cualquier ataque y lo lanzan sin conocer bien lo que están haciendo.
- Programadores de malware: expertos en programación de sistemas operativos y aplicaciones capaces de aprovechar

vulnerabilidades de alguna versión de software, para generar un programa que les permita atacar.

- Sinffers: expertos en protocolos de comunicaciones capaces de procesar una captura de tráfico de red para localizar la información interesante.
- Ciberterrorista: cracker con intereses políticos y económicos a gran escala.

Ataques comunes y qué hacer con ellos

Según Díaz (2004), los ataques que los ciberdelincuentes realizan siempre tienen al menos uno de los siguientes objetivos:

- Obtener información sobre los equipos y redes que se pretende atacar.
- Acceso no autorizado a información, con intención de verla, eliminarla, cambiarla o una combinación de tales actividades.
- Denegación de servicio, sea de la red, del acceso a internet, de un servidor, entre otros.

Además, menciona que los ataques pueden ser:

- Externos: cuando el atacante realiza su ataque desde el exterior de la organización, mediante un sitio desconocido de internet o desde una dirección en la que se confía, pero que ha sido suplantada.
- Internos: cuando se realiza desde la organización. Puede haber ataques profesionales internos, pero también, por mala aplicación de la política de seguridad, ataque no maliciosos de usuarios internos que solo prueban herramientas con toda su buena intención.

Por otra parte, menciona que los ataques también pueden ser estructurados (son ataques que se enfocan como un proyecto, donde se emplean muchos métodos y herramientas) y no estructurados (son ataques habitualmente inocentes, basados en herramientas normales y fácilmente reconocibles), o realizados a través de robo de contraseñas y nombres de

cuentas y basados en relaciones de confianza.

Para evitar ser sorprendido con alguno de estos ataques es necesario establecer políticas de seguridad para resguardar la información y prevenir intrusiones, por ejemplo:

- Identificar la ingeniería social, el phishing, la suplantación de identidad y diferentes técnicas utilizadas por los ciberdelincuentes: generalmente se realiza a través de correos electrónicos y redes sociales y enlaces, por lo que los usuarios deben revisar argumentos como la dirección de correo, la redacción incongruente del correo electrónico, eliminar correos spam.
- Contar con herramientas antivirus.
- Deshabilitar el ping en los servidores (el ping permite obtener información de qué direcciones IP tienen las máquinas en la red).
- Deshabilitar protocolos que no están siendo utilizados, por ejemplo el protocolo de escritorio remoto en Windows (RDP).
- Cambiar los puertos por defecto, por ejemplo el puerto 22, para ingresar a través del protocolo ssh.
- No instalar aplicaciones de terceros en los diferentes dispositivos.
- Habilitar accesos físicos y de sistemas únicamente a las personas autorizadas.
- Mantener las aplicaciones de software actualizadas, entre otros.

Seguridad en la vida real

Actualmente los delitos informáticos continúan incrementándose, las técnicas de ingeniería social, phishing, suplantación de identidad, los fraudes vía telefónica, enlaces maliciosos, entre otros métodos de ataque se presentan en muchos sitios, especialmente los relacionados con dinero.

El INCIBE (2020), advirtió de una campaña de envío de correos electrónicos fraudulentos que tratan de suplantar a la agencia tributaria para difundir malware.

Harán (2020), en una investigación realizada por Eset Security, mencionó que durante la pandemia creció el ecommerce y aumentaron

las estafas y los incidentes de seguridad.

En Costa Rica, estas campañas fraudulentas no son la excepción, las personas denuncian fraudes cibernéticos, utilizando técnicas como ingeniería social y suplantación de identidad, sin embargo, las empresas y entes encargados de la ciberseguridad como el Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT), también realiza campañas sobre seguridad informática y buenas prácticas para proteger la información (como por ejemplo, respaldos de información, roles en los sistemas de información, acceso físico restringido), además comunica las vulnerabilidades presentadas en sistemas operativos y aplicaciones así como las posibles soluciones para evitar los fraudes y/o intrusiones que pongan en riesgo la seguridad de la información.

PARA OBTENER MÁS INFORMACIÓN OBSERVE LAS PÁGINAS 16-46 DEL LIBRO LA SEGURIDAD INFORMÁTICA ES COMO EL SEXO SEGURO

CONCLUSIONES Y RECOMENDACIONES

La información es el activo más importante que poseen las empresas e instituciones y con el avance de la tecnología, los fraudes y la ciberdelincuencia se han incrementado. La seguridad completa es imposible de alcanzar pero puede fortalecerse con técnicas de seguridad informática y buenas prácticas.
Por otra parte, existen diferentes tipos de atacantes y de ataques, pero todos buscan vulnerar los sistemas o las reglas establecidas (accesos restringidos), aunque algunas veces se realiza de manera inconsciente.

Los principales objetivos de la seguridad de la información buscan garantizar:

- La confidencialidad, de manera que sea utilizada solo por los usuarios y máquinas que lo necesitan.
- La integridad, intenta que los datos almacenados por un usuario no sufran ninguna alteración sin su consentimiento.
- La disponibilidad, se refiere a todas las técnicas dirigidas a mantener activo un servicio.

A modo de recomendación, para obtener más información sobre los temas desarrollados, observe los enlaces recomendados en cada sección.

REFERENCIAS BIBLIOGRÁFICAS

Avenía Delgado, C.A. (s.f). Fundamentos de seguridad informática. Recuperado de https://digitk.areandina.edu.co/bitstream/handle/areandina/1367/Fundamentos%20de%20seguridad%20inform%c3%a1tica.pdf?sequence=1&isAllowed=y

Universidad Internacional de Valencia. (2016).¿Qué es la seguridad informática y cómo puede ayudarme?. Recuperado de https://www.universidadviu.com/co/actualidad/nuestros-expertos/que-es-la-seguridad-informatica-y-como-puede-ayudarme

Fresno Chávez, C. (2018). ¿Cómo funciona Internet?. Editorial Ciudad Educativa. https://elibro.net/es/ereader/usanmarcos/36728?page=16

Ariza Agámez, D. (2017-12.). *Gestión de la información.* Bogotá: AREANDINA. Fundación Universitaria del Área Andina.

Díaz, G. (2004). Seguridad en las comunicaciones y en la información. UNED - Universidad Nacional de Educación a Distancia. https://elibro.net/es/ereader/usanmarcos/48351?page=89

Instituto Nacional de Ciberseguridad (Incibe). (2019). Incidentes de seguridad, conoce a tus enemigos. Recuperado de https://www.incibe.es/protege-tu-empresa/blog/incidentes-seguridad-conoce-tus-enemigos

Harán, J.M. (2020). Crece el ecommerce y aumentan las estafas y los incidentes de seguridad. Recuperado de https://www.welivesecurity.com/la-es/2020/11/25/crece-ecommerce-aumentan-estafas-incidentes-seguridad/

Roa Buendía, J. F. (2013). Seguridad informática. McGraw-Hill España. https://elibro.net/es/ereader/usanmarcos/50243?page=22

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica