SEGURIDAD EN LAS TELECOMUNICACIONES.

INTRODUCCIÓN Y ANTECEDENTES:

En cuestión de seguridad informática, no está dicha la última palabra; cada vez los piratas informáticos, conocidos como “ hackers ” desarrollan técnicas avanzadas para tratar de evadir los sistemas de protección de redes. Sin embargo, siempre hay que estar un paso más allá y eso depende de la iniciativa de las personas encargadas de la administración de la red. Los proveedores de telecomunicaciones son el blanco principal de ataques cibernéticos pues operan y administran las redes mundiales, las transmisiones de voz y datos, y almacenan también grandes cantidades de información confidencial.

Uno de los riesgos más importantes y que podría significar pérdidas económicas o de reputación es el robo o secuestro de información, sin embargo también existen ataques de negación de servicio, los cuales afectan la disponibilidad de los servicios informáticos como son los portales web. También el robo de identidad afecta a las telecomunicaciones y éste en particular se ha incrementado debido a la proliferación del uso de dispositivos móviles dentro de las redes corporativas, los accesos remotos de usuarios móviles y la falta de controles administrativos en políticas de seguridad enfocada a los accesos de estos dispositivos. Desde la década de los años noventa era evidente la necesidad de un instrumento más complejo para resolver “la falta de un intercambio efectivo de información”

OBJETIVOS.

- Comprender el impacto y relevancia de los incidentes de seguridad en las tecnologías de la información y las comunicaciones.
- Conocer las vulnerabilidades, componentes y mecanismos de seguridad en los sistemas de comunicación y las redes.
- Conocer la metodología y tipos de ataques a la seguridad de los sistemas y servicios.
- Capacidad de diseño y administración de la seguridad de un entorno de comunicaciones, establecida ésta en niveles de profundidad.
- Comprender y usar herramientas hardware y software específicos para el control y administración de la seguridad de los sistemas.
- Conocer y usar las principales tecnologías de seguridad relacionadas con la confidencialidad, autenticación, no repudio, disponibilidad y control de accesos.
- Conocer los fundamentos de los protocolos involucrados en las comunicaciones seguras.
- Protegerse de actuaciones de usuarios malintencionados.
- Permitir el acceso y uso del sistema a usuarios conocidos o de confianza.
- Dotar de privacidad.
- Definir las políticas o reglas de uso.
- Anticipar cualquier posible fallo en el sistema.
- Garantizar que los servicios no se interrumpen.
- Conocer y comprender los aspectos involucrados en la seguridad de entornos de red.

CHECKLIST.

1. Gestión de la seguridad en las redes.

La gestión se puede definir como el conjunto de actividades que controlan o vigilan el uso de los recursos en la red. Se debe proporcionar la posibilidad de supervisar el estado, medir el rendimiento, reconocer actividades anormales y recuperar el servicio.

Las funciones de red se suelen agrupar en dos categorías:

- Supervisión de red. Se considera una función de ``lectura'' y se encarga de observar y analizar el estado y el comportamiento de la configuración y componentes de la red.
- Control de red. Se le considera como una función de ``escritura'' y se encarga de alterar los parámetros de los distintos componentes de la configuración de la red y hacer que lleven a cabo las acciones que se determinen.

a. Control de red.

- Los equipos suelen formar parte de una red de equipos. Una red permite que los equipos conectados intercambien información. Los equipos conectados a la red pueden acceder a datos y demás recursos de otros equipos de la red. Las redes de equipos crean un entorno informático potente y sofisticado. Sin embargo, las redes complican la seguridad de los equipos.
- Por ejemplo, dentro de una red de equipos, los sistemas individuales permiten el uso compartido de información. El acceso no autorizado es un riesgo de seguridad. Debido a que muchas personas tienen acceso a una red, el acceso no autorizado es más probable, especialmente como consecuencia de errores del usuario. Un mal uso de contraseñas también puede originar el acceso no autorizado.

b. Mecanismos de seguridad asociados a servicios en red.

- La Seguridad en redes, es la protección a toda la infraestructura de computadoras y también de toda la información contenida. Existen algunos estándares, protocolos, métodos, reglas y herramientas para hacer que el riesgo sea mínimo en la infraestructura e información.

Los mecanismos de seguridad se dividen en tres grupos:

- **Prevención**: Evitan desviaciones respecto a la política de seguridad.
- **Detección:** Detectan las desviaciones si se producen, violaciones o intentos de violación de la seguridad del sistema.
- **Recuperación:** Se aplican cuando se ha detectado una violación de la seguridad del sistema para recuperar su normal funcionamiento.

Dentro del grupo de mecanismos de prevención tenemos:

- Mecanismos de identificación e autenticación.
- Mecanismos de control de acceso.
- Mecanismos de separación.
- Mecanismos de seguridad en las comunicaciones.

c. Segregación de redes.

La segregación de redes acota el acceso a la información y, consiguientemente, la propagación de los incidentes de seguridad, que quedan restringidos al entorno donde ocurren.

La red se segmentará en segmentos de forma que haya:

A. Control de entrada de los usuarios que llegan a cada segmento.
B. Control de salida de la información disponible en cada segmento.
C. Las redes se pueden segmentar por dispositivos físicos o lógicos.

2. Intercambio de información con partes externas.

Es aquella que se dirige al público exterior, es decir, la que emite un mensaje fuera de la empresa. Este tipo de comunicación está enfocada a la opinión pública. El principal objetivo de la comunicación externa es informar sobre la empresa, a la vez que actuar e influir sobre la imagen que se da de ésta.

Herramientas de la Comunicación Externa

- Uno de los principales mecanismos de la comunicación externa es el gabinete de prensa, un organismo encargado de gestionar toda la información de la empresa para los medios de comunicación, como las notas de prensa o las entrevistas.
- Relaciones públicas.
- La web corporativa de la empresa.

a. Políticas y procedimientos de intercambio de información.

El intercambio de información de la empresa, entre organizaciones o terceras partes debe estar controlado y se deben cumplir todas las legislaciones y normas que correspondan. Para mantener una adecuada protección de la información Geoconsult CS, establece procedimientos y controles de intercambio por medio de la utilización de todo tipo de servicios de comunicación.

- Se deben usar transportes o mensajeros fiables.
- Los medios informáticos o de transporte físico de información del EPIS deben estar lo suficientemente protegidos contra daño físico que pueda ocurrir durante su transporte.
- No se deben dejar mensajes en contestadores automáticos.
- Activar el cifrado de los datos en el dispositivo móvil y a continuación almacenar la información a ser transportada.
- Borrar la información del dispositivo móvil en el momento que ya no se requiera su almacenamiento en éste.

b. Acuerdos de intercambio.

Así, tratándose de operaciones relativas a la fiscalidad internacional, a través del intercambio de información, la autoridad tributaria tiene certeza de la operación, y evita prácticas fiscales que podrían considerarse como agresivas, además promueve la transparencia al tener acceso directo a la información relacionada con el otro país que mantiene el Acuerdo Amplio. Finalmente, cabe hacer mención que los instrumentos precisados relativos al intercambio de información crean el precedente para la implementación del Plan BEPS a nivel global. Éste se enfoca en poder determinar la veracidad de toda la información de grupos transnacionales para poder fiscalizar efectiva y eficazmente mediante las revisiones cruzadas y los intercambios de información.

c. Mensajería electrónica.

El correo electrónico se ha convertido en una herramienta de trabajo cotidiano que ha venido a incrementar la productividad de las organizaciones, al proporcionar una

manera flexible de comunicación especialmente en el mundo del Marketing. Esta herramienta ha venido eliminando llamadas telefónicas para el manejo del trabajo cotidiano, las citas y todas aquellas actividades de oficina que requieren de comunicación entre individuos, a través de mensajes y archivos electrónicos.

Históricamente, la mensajería se ha encontrado relacionada con la evolución de las computadoras:

- La Mensajería en sistemas basados en un host.
- La Mensajería en sistemas con base en host distribuidos y minicomputadoras.
- La Mensajería basada en sistemas operativos de red.

d. Acuerdos de confidencialidad y secreto.

- Libre y exento de todo peligro, daño o riesgo.
- Mecanismos que garantizan buen funcionamiento, previniendo fallos, etc., de manera que los recursos e información sean accesibles y utilizados de la forma y por aquellos que se preveía.
- Sinónimo: protección, invulnerabilidad, defensa, robustez
- Funcionamiento de sistemas
    - Corrección
        - Ante una entrada de usuario, se genera la salida esperada
        - Más funcionalidades ⇒ mejor sistema
    - Seguridad
        - Ante un entrada inesperada de un atacante, el sistema no falla
        - Más funcionalidades ⇒ más posibilidades de fallos

PUNTOS DE APLICACIÓN.

“El sector empresarial es quien más se ha preocupado y ocupado por prevenir y mitigar amenazas disruptivas debido a que la información que contiene en sus centros de datos es más crítica y en un momento dado con mayor afectación a su negocio”, declaró. Debido al acelerado cambio en los sistemas de comunicación y cómputo, dijo que es importante una revisión y análisis continuo de políticas, mecanismos y tecnologías que se utilizan en las empresas para la protección de datos, por lo que mencionó las siguientes prácticas para controles básicos de seguridad:

- Segmentar redes, usuarios, servidores, invitados, etc.
- Generar una red de administración con protección a los accesos.
- Limitar accesos a información crítica y confidencial.
- Implementar aseguramientos básicos como firewall, antimalware y un Sistema de Prevención de Intrusos (IPS, por sus siglas en inglés) de host.
- Evitar el uso de carpetas compartidas en la red.
- Realizar análisis periódicos de vulnerabilidades.
- Analizar destinos de navegación y correos electrónicos.
- Limitar y controlar sitios en Internet.
- Restringir cargas y descargas desde y hacia Internet.
- Definir y reportar el acceso a bases de datos.

Las empresas de telecomunicaciones son los proveedores de servicios, sin embargo los controles o mecanismos de seguridad que se pueden aplicar son limitados y van de acuerdo a la oferta hacia cada uno de sus clientes.

INFORMACIÓN Y ELEMENTOS ADICIONAL.

- Tania G. Rojo, Jorge H. Acosta y Humberto Guerrero Staff Seguridad en América miércoles 16 de mayo del 2018
- J. Long, 2005, Web Hacking: Attacksand Defense, 2002, Addison Wesley.
- J. Mirkovic, S. Dietrich, D. Dittrich, P. Reiher, 2004, Internet Denial of Service: Attack and Defense Mechanisms, Prentice Hall. Téllez Valdez, Julio, 1996, Derecho informatico, México, Mc Graw Hill.
- TÉLLEZ VALDEZ, Julio. Derecho Informático. 2ª. Edición. Mc Graw Hill. México. 1996 Pág. 103.