SEGURIDAD EN INTERNET

Lic. José Piedra Isusqui

La seguridad en Internet, es uno de los temas que más atención está demandando principal mente por las transacciones financieras. El problema de seguridad en Internet surge, porque fue creada para libre acceso a la información y regida principalmente por las políticas de buen uso de la red.

A partir de 1990, comienza la preocupación principal por la seguridad, debido a que la sociedad comercial encontró en Internet un canal de flujo hecho a la medida: rápido, barato y cada vez más extendido y eficiente. Desde entonces, hemos visto cómo periódicos y grandes compañías incrementan su difusión por Internet; las empresas basan sus comunicaciones externas en ella y cada día son más las operaciones financieras que se hacen a través de Internet, que poco a poco está reemplazando a los tradicionales medios de comunicación.

Lógicamente, conforme más información hay disponible en Internet, más importancia cobra la protección de esa información y el control del acceso a la misma. Dentro de este panorama, nos enfrentamos a una creciente realidad, la necesidad de seguridad en los datos, los servicios, las transacciones, y las partes involucradas.

Las redes contienen agujeros de seguridad, con los que, no queda más remedio que convivir, y que ya consideramos como normales. Los sistemas operativos incluyen rutinariamente configuraciones por inseguras y con dispositivos de seguridad incompatibles, debido a defectos de producción, que dan su correspondiente dosis de agujeros. Además, tampoco se considera excepcional que las aplicaciones fallen, ni encontrar organizaciones donde dichos asuntos ni siquiera sean preocupación u ocupación de alguien en particular.

Los sistemas cada vez están más accesibles, ya sea por la incorporación de elementos externos a nuestra organización (proveedores o clientes), o ya sea por el extenso acceso de usuarios propios. Los datos, aplicaciones, servicios y plataformas, cada vez están más expuestos, la seguridad cada vez es más compleja, por lo que debe considerarse los mecanismos apropiados de seguridad, previa evaluación.

La calidad del sistema y su funcionamiento operacional correcto y sin interrupciones, definitivamente impactan positivamente sobre los beneficios de las organizaciones, en el mismo sentido que la capacidad, y por su propia naturaleza, los sistemas de información se vuelven de «misión crítica».

OBJETIVO DE LA SEGURIDAD

El objetivo de la seguridad, es garantizar la privacidad de la información y la continuidad del servicio, tratando de minimizar la vulnerabilidad de los sistemas o de la información contenida en ellos, así como tratando de proteger las redes privadas y sus recursos, mientras que se mantienen los beneficios de la conexión a una red pública. Asimismo, se deben implementar los mecanismos de seguridad física y lógica apropiados en el sistema informático de la empresa.

CAUSAS DE LA INSEGURIDAD EN LAS REDES

El crecimiento acelerado de las redes empresariales y particularmente Internet, aunado a que el diseño de las redes se asumía en ambientes seguros controlados a través de usuarios autorizados y sin vislumbrar la futura conexión a redes externas, además de que

protocolos de comunicación, como el TCP/IP no fueron concebidos teniendo en cuenta aspectos de seguridad, son las principales causas de la inseguridad en las redes.

Existen algunas ideas erróneas acerca de la seguridad, como el pensar que estamos totalmente protegidos con la asignación de contraseñas a todos los recursos, usuarios funcionales y aplicaciones, o comprar un Firewall o equivalente, o suponer que los usuarios funcionales o posibles atacantes tienen bajo conocimiento.
También es un error sentirse seguros con un celador en la puerta del centro de cómputo, o poner simplemente protección contra posibles atacantes y no contra usuarios funcionales autorizados, así como también es un error pensar en que a mayor complejidad del sistema de seguridad, obtenemos mayor seguridad.

RIESGOS DE LA INSEGURIDAD EN LAS REDES

A la hora de utilizar el comercio electrónico por Internet cualquier usuario se cuestionará si las transacciones que realiza son realmente seguras. De hecho, la posible evolución del comercio por la red, está supeditada a los sistemas de seguridad que permitan al usuario comprar tranquilamente y sin riesgos.

Sin precauciones de seguridad en estas transacciones, cualquier persona podría darse un paseo por los datos que estamos transmitiendo, entrar en una conversación o llegar a obtener nuestro número de tarjeta de crédito, incluyendo nuestro número de identificación personal.

Para garantizar la seguridad de los datos, es importante, considerar la Confidencialidad, Integridad y Autenticación. Hoy existen muchas formas de garantizar estas propiedades a nuestras transmisiones en Internet: El empleo de clave privada y clave pública, el uso del cifrado de datos o encriptación, la firma digital, las tarjetas de crédito para uso sólo en Internet.

Otro riesgo para nuestros datos, es el provocado por los virus informáticos, por ello se debe considerar una política para el empleo de antivirus en nuestras instalaciones de cómputo. Se debe evaluar la implementación de un Firewall, y un servidor Proxy, que garantice los accesos de adentro hacia fuera de la empresa y viceversa, desde afuera hacia adentro. Esto último aliviara nuestro posible problema con la sociedad de los hackers en Internet.