SEGURIDAD EN REDES DE COMPUTADORAS

Actualmente, cuando hablamos de seguridad en las redes de computadoras, hacemos una gran referencia a Internet, pues es dentro de esa red de alcance mundial que se producen con mayor frecuencia los ataques a nuestras computadoras.

Antes de entrar en el tema, es necesario preguntarnos qué alcance tiene para nosotros el término "seguridad". En general, decimos que una casa es segura cuando se logra reducir las vulnerabilidades de la propiedad. Pero... qué es la vulnerabilidad? Según ISO (International Standardization Organization), en el contexto de la informática se considera "vulnerabilidad" a cualquier flaqueza que pueda ser aprovechada para violar un sistema o la información que éste contiene.

De esta forma, tenemos varias posibles violaciones de seguridad a un sistema, o sea, varias amenazas, entre las cuales destacamos:

- Destrucción de información.
- Modificación de la información.
- Robo, remoción o pérdida de la información o los recursos.
- Interrupción de servicios.

Debemos todavía definir "ataque": es la realización efectiva de una amenaza en forma intencional. Como ejemplos de ataques en computación, tenemos:

- Personificación (enmascarada)
- DDos.
- Replay.
- Modificación.

- Ingeniería social.
- Rechazo o impedimento de un servicio.

Ante los riesgos de la inseguridad en las redes, muchas empresas adoptan políticas de seguridad, que son conjuntos de reglas, leyes y prácticas de gestión que tienen como objetivo la protección. Pueden ser implementadas a través de varios mecanismos, como por ejemplo:

- Criptografía.
- Firma digital.
- Autenticación.
- Control de acceso.
- Rótulos de seguridad.
- Detección, registro e informe de eventos.
- Llenado de tráfico.
- Control de routeo.

De esta forma, al no ser suficientes los mecanismos de seguridad en la red, establecemos medidas de seguridad en las comunicaciones también, como en el correo electrónico. El e-mail utiliza varios mecanismos para que nuestros datos lleguen de la manera más segura posible a destino. Hace uso de protocolos como SMTP (Simple Mail Transfer Protocol) que es considerado débil, S/MIME (Secure Multipurpose Internet Mail Extensions) y PGP (Pretty Good Privacy) que es destinado a la criptografía de e-mail personal.

Actualmente, lo que se utiliza en gran medida son los Firewall's, dispositivos que funcionan como una barrera de protección contra invasores. Existen tanto en forma de software como de hardware, o en la combinación de ambos.

Como ejemplo de buenos firewall's domésticos y gratuitos, podemos citar:
- Comodo Firewall
- Zone Alarm
- Sygate Personal Firewall