**BGP (Border gateway protocol, protocolo de la pasarela externa)**

BGP es un protocolo muy complejo que se usa en la interconexión de redes conectadas por un backbone de internet. Este protocolo usa parámetros como ancho de banda, precio de la conexión, saturación de la red, denegación de paso de paquetes, etc. para enviar un paquete por una ruta o por otra. Un router BGP da a conocer sus direcciones IP a los routers BGP y esta información se difunde por los routers BGP cercanos y no tan cercanos. BGP tiene su propios mensajes entre routers, no utiliza RIP.

BGP es usado por grandes proveedores de conectividad a internet. Por ejemplo una empresa (A) tiene alquilada una línea a telefónica-data. La empresa A no hace BGP y posiblemente los routers más cercanos no utilizarán BGP pero si los que interconecten Telefónica-Data con Hispanix (punto neutro de interconexión en España).

El Border Gateway Protocol (BGP) es el sistema que utilizan los grandes nodos de Internet para comunicarse entre ellos y transferir una gran cantidad de información entre dos puntos de la Red. Su misión es encontrar el camino más eficiente entre los nodos para propiciar una correcta circulación de la información en Internet.

¿Dónde reside el fallo del BGP?

Internet se diseñó para facilitar la comunicación, no tanto para ser segura. Este punto de partida, que ha facilitado un grandioso crecimiento de la Red, es también su parte más endeble, pues permite que ciertas personas exploten sus vulnerabilidades para sus propios intereses.

¿En qué consiste exactamente el fallo ahora descubierto?

Los grandes nodos que permiten que la información fluya por Internet suelen utilizar routers que funcionan bajo el protocolo BGP. Cuando una persona envía un correo electrónico desde Madrid a, por ejemplo, Montevideo, los sistemas de su proveedor de Internet buscarán el camino más rápido para que dicho e-mail llegue a su destinatario.

Alguien con el equipo necesario podría engañar al router del proveedor haciéndole creer que ese camino más corto pasa por su sistema. La información seguiría llegando a su destinatario, pero el nuevo intermediario podría monitorizar los datos.

¿Cuál es la solución?

Los organismos ya están trabajando en un desarrollo del protocolo que impida malas actuaciones. Sin embargo, es necesario que los usuarios de Internet tengan cuidado cuando navegan, de la misma manera que si alguien visita por primera vez una ciudad no entra en según qué barrios sin saber dónde se mete o sin tomar ciertas precauciones.

Cifrar los datos enviados, utilizar un firewall (cortafuegos), un antivirus y saber algo sobre el sistema operativo del ordenador es fundamental. También es muy importante exigir a la ISP (proveedores de acceso a Internet) un mayor nivel de seguridad.

