TIC

TALENTO TECH

REGIÓN 3

CAUCA – NARIÑO

LECCIÓN 3 UNIDAD 1

Universidad Tecnológica de Pereira

faceIT

Lección 3: Sistemas de protección a nivel de redes:

Como se vio en el apartado anterior, los ataques a nivel de red son muchos y variados. El mantener seguras las redes requiere de monitoreo de estas, así como revisión constante de los niveles de carga en las CPU de los servidores. También es necesario tener en cuenta técnicas de cifrado para evitar que los datos sean falsificados en la red. No existen soluciones únicas para todos los problemas, pero combinando software y hardware es posible mitigar buena parte de los ataques. Algunas de las técnicas son:

- **Firewalls** El firewall es la primera línea de defensa en una red. Regularmente es un dispositivo que se encuentra entre internet y la red local y se encarga de filtrar todo el tráfico que sale y entra a la red. El firewall puede ser un dispositivo físico (hardware) o un programa (software). Su funcionamiento se basa en reglas que bloquean el tráfico en puertos y desde conexiones que se consideran inseguras, mientras que permite el paso del tráfico por las conexiones y puertos admitidos.

- **Uso de software antivirus:** Los virus son programas maliciosos. Existen todo tipo de virus tanto para dispositivos móviles como para servidores. Con el uso de software antivirus, los servidores y los ordenadores clientes pueden validar qué cambios están haciendo los programas en su interior (en segundo plano) y bloquear aquellos que tengan comportamientos sospechosos, como el envío de grandes cantidades de datos a otros servidores, copia o manipulación no autorizada de datos, entre otros.

- **Medidas de control de acceso a la red:** Si bien se puede bloquear tráfico desde el firewall, se puede mejorar la seguridad bloqueando directamente a los dispositivos que no están autorizados a estar en la red. Estas soluciones también suelen controlar qué se puede hacer en las redes, por ejemplo, forzar a que el ingreso a la red sea con doble factor de autenticación, impedir la conexión con sitios en una lista de sitios inseguros, entre otras medidas que mejoran la seguridad.

- **División de la red en partes:** Una forma efectiva de controlar el tráfico y los ataques a una red consiste en la división de una red física en redes virtuales con numeración independiente. Este tipo de soluciones permiten restringir el acceso a cada segmento de red y evitar que dispositivos no permitidos se conecten a una subred privada o con niveles de confidencialidad más altos. Si un atacante ingresa de forma maliciosa a una subred, no podrá desplazarse horizontalmente a las otras redes para buscar incrementar el daño.

- **Uso de redes privadas virtuales:** Las redes virtuales privadas o VPN son una solución que cifra todos los datos a través de internet incrementando sustancialmente la seguridad en el tráfico por internet. Las redes VPN cifran cada paquete de datos y los ocultan, haciendo imposible que en internet se sepa cual es la identidad del dispositivo remitente de los datos. Estas soluciones hacen que a los atacantes les sea altamente complicado falsificar paquetes, colocar ataques del tipo man in the middle y robar información. Por este motivo se recomienda que al usar redes WiFi públicas se haga uso de VPNs.