CÓMO SON LAS ENTRAÑAS DE UNA GRAN RED MUNDIAL

AUTOR: HELLEN CUBERO

NOVIEMBRE: 2020

San Marcos

INTRODUCCIÓN

Existen diferentes tipos de acceso e infraestructuras básicas que nos permiten conectarnos a la red e inclusive parte de estas zonas, plataformas e infraestructuras que poseen las operadoras nacionales que en definitiva son las que llegan a través de la red fija o móvil.

Si se analiza la red de manera jerárquica desde arriba hacia abajo, lo primero que se encuentra son los grandes "Carriers" del mundo, es decir los que interconecta continentes y países de forma bastante piramidal. (Corletti, 2017)

Contenido

La importancia de los procesos 3
Planos de segmentación de las redes de gestión y servicio 5
Tubos 6
Carriers 7
Protocolo BGP 8
Sistema DNS 8
CONCLUSIONES Y RECOMENDACIONES 10
REFERENCIAS BIBLIOGRÁFICAS 11

La importancia de los procesos

Según Corletti (2017), los procesos juegan un rol fundamental en toda la organización de la seguridad, pues son los que verdaderamente regulan "qué se puede y que no se puede hacer"; sin ellos cualquier persona deja librada a su criterio personal y aislado las diferentes medidas, acciones, decisiones, permisos, rutas, reglas, borrados, cambios entre otros términos que suenan a peligro en alguien que se dedique a estos temas. Por esta razón el autor presenta 8 procesos que cobran importancia básica en la seguridad de redes.

1. **Entrada en producción:** es el conjunto de pasos a seguir desde que un dispositivo, plataforma o servicio es imaginado, pensado o planificado hasta que el mismo entra en producción. Básicamente se deben considerar tres actividades: Análisis técnico, pruebas de laboratorio y pruebas en red (FOA: First Office Application).
2. **Gestión de cambios:** el principal objetivo del proceso es que paulatinamente se esté intentando ajustar al máximo detalles como escalado de privilegios, usuarios genéricos, u otras incidencias de alto impacto, que producen errores, por ausencia de un procedimiento estricto de control de cambios.
3. **Gestión de accesos:** es tener la capacidad de derivar a cada uno exactamente dónde debe acceder. Ni a más, ni tampoco a menos dispositivos/servicios/redes/aplicaciones/funciones que las que le corresponden.
4. **Configuraciones e inventario:** es imposible adoptar medidas o tomar decisiones si no sabemos qué es lo que se debe asegurar. Es imposible abrir una regla de Firewall si no se conoce en detalle la comunicación de extremo a extremo que se está habilitando, no se puede lanzar un plan de continuidad de negocio si no se sabe con qué recursos se cuenta, no se puede crear una VLAN (virtual LAN) si no se sabe cuáles son los elementos que la integran. El inventario de equipos debe ser lo más completo posible (descripción del activo, propietario del activo, encargado del tratamiento del activo, nivel de criticidad, etc).
5. **Gestión del backup:** aunque los dispositivos de red poseen

mucha estabilidad que los de TI (aplicaciones, desarrollos, programas, bases de datos, entre otros), y existen muchísimos menos virus y troyanos para dispositivos de red que para los de sistemas, se suele hacer evidente que el personal no le presta el mismo grado al resguardo y recuperación de sus configuraciones y logs, es frecuente escuchar que el dispositivo nunca se ha caído en sus años de servicio, en muchos casos es cierto, pero también en muchos otros no. Por lo tanto, se considera casi una obligación despertar conciencia sobre la importancia de las copias de respaldo.

6. **Gestión de incidencias:** este procedimiento debe contemplar todas las acciones relacionadas a la notificación, gestión y respuesta a incidentes de seguridad, definiendo claramente las responsabilidades, obligaciones y acciones a realizar en el tratamiento de incidencias. Uno de los aspectos más importantes en este proceso es la recopilación y análisis de evidencias.
7. **Supervisión y monitorización:** para ofrecer un grado de disponibilidad mínimo es necesario contar con una infraestructura de supervisión y monitorización. Desde el punto de vista de Ciberseguridad, no solo interesa por la disponibilidad, sino también por la detección temprana y la generación de alertas ante cualquier actividad anómala en la misma. Ambas funciones se llevan a cabo a través de: NOC (Network Operation Center) y SOC (Security Operation Center).
8. **Gestión de Logs:** el concepto de Logs, muchas veces se relaciona o se denomina "Registro de auditoría", lo cual puede resultar interesante pues en definitiva un Log es un tipo de registro que se genera desde un dispositivo para dejar constancia de un evento.

Para obtener más información visite este enlace, de la página 101 a la 117.

Planos de segmentación de las redes de gestión y servicio

Según Corletti (2017), en toda infraestructura de red se debe un importante esfuerzo por poder "aislar" la red de gestión del resto de las redes, y en particular, de la que presta servicios.
La red de gestión debe ser accesible únicamente por el personal responsable de los dispositivos y a su vez, que cada uno de ellos solo puede acceder a los elementos de su responsabilidad. Se debe tener presente que desde esta red se accede a las plataformas, direcciones y puertos que abren juego hacia el "control total" de los elementos.

A una red de gestión se puede acceder mediante dos metodologías:

- Ubicaciones o centros de gestión: son locales, o edificios que tienen conexión con los dispositivos y, únicamente estando físicamente en esas salas, se alcanzan las direcciones y puertos específicos de gestión de dispositivos.
- Plataformas de acceso a redes de gestión: a través de dispositivos de control de acceso o máquinas de salto, las personas autorizadas, se validan en ellos y desde estos dispositivos tienen acceso a los elementos que se desean gestionar.

Además, en ambos casos, los dispositivos a gestionar deben tener al menos dos interfaces de red, aunque podría hacerse con una sola interfaz física con alias, o más de una dirección IP, no se recomienda hacerlo de esta forma. Para que la red de gestión sea intrínsecamente segura, es necesario también que en todo dispositivo que posea una interfaz conectada a la misma, se configura al menos tres medidas:

- Reglas de firewall locales para que acepte conexiones únicamente desde dispositivos de control de acceso, máquinas de salto o segmento asignado al centro de gestión.
- Limitación de los comandos de gestión, monitorización y troubleshooting.
- Sistema de Logs que registre cualquier acción no permitida y de ser posible los envíen a un servidor externo.

Desde la red de servicio no debería haber ningún tipo de visibilidad hacia

estos rangos de red. La red de servicio en sí debería estar segmentada de forma tal que ofrezca sus funciones únicamente a los usuarios que preste servicio y nadie más.

Tubos

"He confirmado, con mis propios ojos, que Internet es muchas cosas en muchos lugares. Pero una cosa que sí es, en todos los lugares donde existe, es una serie de tubos. Hay tubos debajo del mar que conectan Londres con Nueva York. Tubos que conectan Google con Facebook. Hay edificios llenos de tubos, y cientos de miles de caminos y vías de trenes que tienen tubos corriendo a sus lados. Todo lo que haces en línea viaja dentro de un tubo. Dentro de esos tubos, en general, hay fibras de vidrio. Y dentro de esas fibras, luz. Y, codificado dentro de esa luz, estamos -cada vez más- nosotros."

Según Corletti (2017), estos tubos interconectan a nivel físico todos los extremos del planeta, estos "tubos" para establecer las conexiones podemos clasificarlos en tres categorías:

- Fibras ópticas
- Cables de cobre
- Enlaces de radio

Es lo que se denomina "medio físico" y es el modelo inferior del modelo de capas, los extremos de cada medio físico, se conectan a dispositivos. Estos dispositivos podrían clasificarse en dos categorías:

- Commutadores o Switchs: que operan en el nivel 2 (enlace) del modelo de capas
- Routers: operan en el nivel 3 (red) del modelo de capas.

Los "tubos" llegan a una boca física de un router o switch, se conectan al mismo y a partir de allí ingresan o parten los "paquetes" de datos encapsulados en el protocolo que corresponda.

Para obtener más información visite este enlace, lectura Ciberseguridad de

Alejandro Corletti, páginas 137-140.

Carriers

Según Corletti (2017), los grandes puntos de interconexión son gobernados por Carriers. Se trata de grandes corporaciones que unen esta gran red.
Si se analiza la red de forma jerárquica desde arriba hacia abajo, lo primero que nos encontramos son los grandes "Carriers" del mundo, es decir los que interconectan continentes y paises de forma bastante piramidal.
Existen tres niveles de ellos, Tier 1, Tier 2 y Tier 3.
Observe la siguiente imagen:

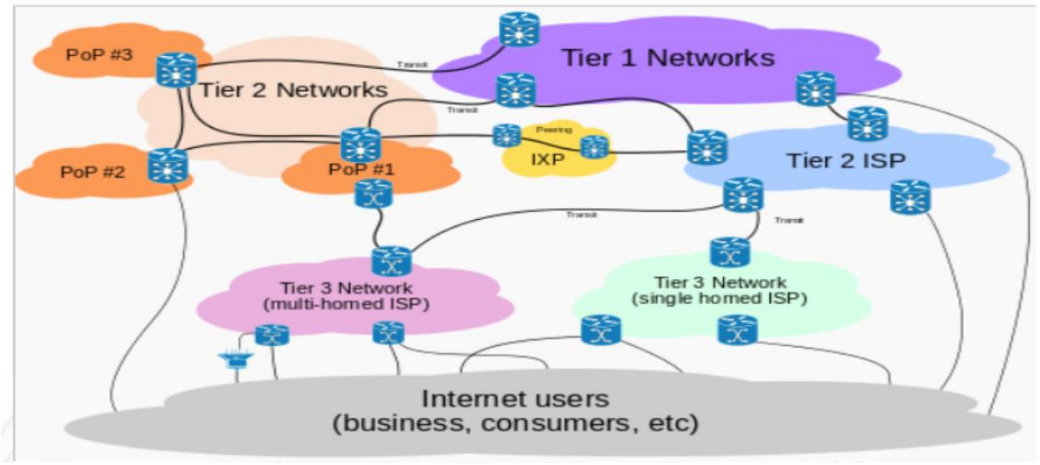

Ilustración 1: Ilustración de Tier
Fuente: Corletti, 2017

El Tier 1 son los grandes operadores globales que tienen tendidos de fibra óptica al menos a nivel continental. Desde la red de un Tier 1 se accede a cualquier punto de Internet, pues todas las redes de Tier 1 deben estar conectadas entre sí. Son backbone, core, núcleo o troncal de Internet.

Para obtener más Información, visite las páginas 140-142 de este enlace.

Protocolo BGP

El protocolo BGP (Border Gateway Protocol), es el responsable de enrutar todos los paquetes de Internet a lo largo del mundo. Este protocolo responde a un esquema de direccionamiento dinámico, es decir que sus rutas se van modificando frecuentemente sobre la base de diferentes métricas, que en definitiva son parámetros lógicos que permiten decidir por cuál interfaz debe sacar un determinado router cada uno de los paquetes que le llegan a él. Estas rutas se van creando sobre la base de información que comparten los dispositivos vecinos (neighbor) que conforman esa comunidad BGP. (Corletti, 2017).
Observe la siguiente imagen:

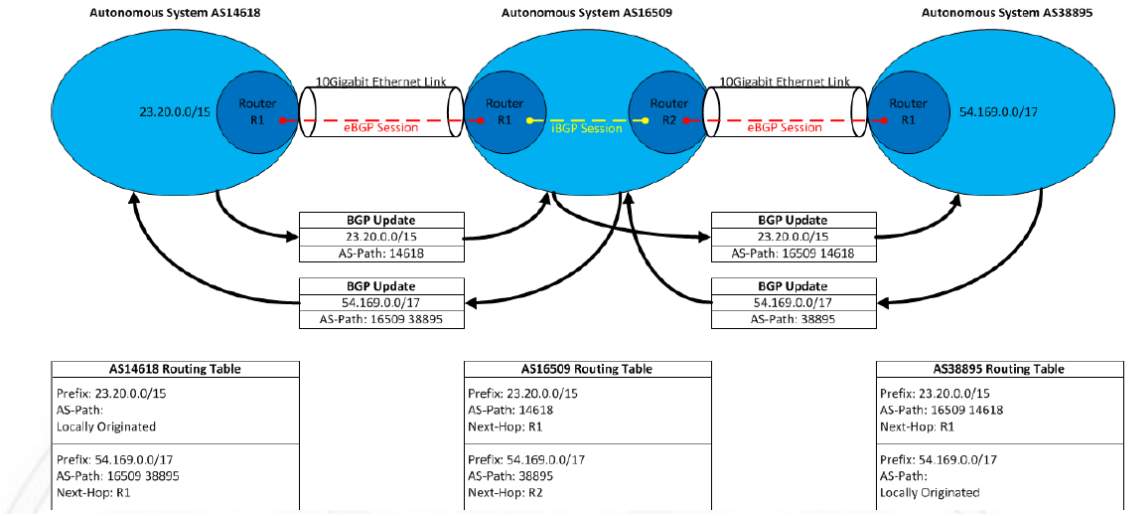

Ilustración 2: Protocolo BGP
Fuente: Corletti, 2017

Sistema DNS

El sistema DNS (Domain Name System), es el responsable de asociar las direcciones IP con los nombres que emplea Internet. Esta actividad se lleva a cabo por un sistema estrictamente jerárquico cuya raíz (root), son exactamente 13 sites (donde cada una de ellas por supuesto está compuesta por más de un servidor con redundancia y balanceo de

carga). Esta jerarquía como concepto de máximo nivel emplea el nombre de la forma FQDN (Fully Qualified Domain Name, o Nombre de dominio completo) que se obtiene a partir del árbol, construyendo el dominio desde abajo hasta arriba, incluido el punto final y como máximo tiene 256 caracteres. (Corletti, 2017)

El sistema DNS resuelve los nombres de las direcciones IP, sin esto es imposible navegar.

Para obtener más información visite las páginas 146 - 151, en este enlace

CONCLUSIONES Y RECOMENDACIONES

Es de suma importancia conocer la composición de la gran red mundial para identificar las debilidades y estar alertas, mediante la ciberdefensa, adoptar medidas contra acciones delictivas, y otorgar solo los accesos correspondientes.

Los países que pueden identificarse como grandes operadores globales que tienen tendidos de fibra óptica a nivel continental son Estados Unidos, Japón, Suecia-Finlandia, India, Alemania, Italia y España

Los puntos neutros o puntos de intercambio poseen como propósito principal, permitir que las redes se interconecten directamente, a través de infraestructura, en lugar de hacerlo a través de una o más redes de terceros. Las principales ventajas de la interconexión son el costo, la latencia y el ancho de banda.

A modo de recomendación, para obtener más información sobre los temas desarrollados, observe los enlace recomendados en cada sección.

REFERENCIAS BIBLIOGRÁFICAS

Corletti, A. (2017). Ciberseguridad. Recuperado de http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/2018/Libro-Ciberseguridad_A.Corletti_nov2017.pd.pdf

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica