JORNADAS DE SEGURIDAD INFORMÁTICA
3ª EDICIÓN | 2019

CHACO
Gobierno del Pueblo

Seguridad Perimetral de Redes de Datos

ECOM

POLICÍA DEL CHACO
División Cibercrimen

POLICÍA DEL CHACO

Ministerio de Seguridad Pública
Gobierno del Pueblo del Chaco

Subsecretaría de Niñez, Adolescencia y Familia
Gobierno del Pueblo del Chaco

Ministerio de Desarrollo Social
Gobierno del Pueblo del Chaco

Dirección General de Tecnologías de Información y Comunicación
Gobierno del Pueblo del Chaco

Subsecretaría de Modernización del Estado
Gobierno del Pueblo del Chaco

Secretaría General de Gobierno y Coordinación
Gobierno del Pueblo del Chaco

IPAP CHACO

CHACO
Gobierno del Pueblo

Introducción.

¿Porqué el cuidado de la seguridad de nuestras redes de datos es necesario para todos, desde empresas de menor porte hasta ciudadanos en sus residencias?

La premisa *«soy pequeño, nadie me conoce y es poco probable que vayan a atacar a mi empresa»* no es aplicable para *ataques oportunistas y masivos*. Ej: ransomware, phishing, botnets.

Aunque su empresa no trabaje con información sensible a proteger, es probable que necesite asegurar *la disponibilidad* permanente de algún recurso (acceso a Internet por ej.) con lo cuál el mismo se vuelve un activo a cuidar para evitar un perjuicio al negocio.

¿Qué es la seguridad perimetral de redes de datos?

Podría definirse como la integración de elementos y sistemas emplazados en una arquitectura de red con el fin de proporcionar protección a las redes privadas frente a amenazas, ataques y denegaciones de servicio provenientes de otras redes externas.

El principal objetivo de la seguridad perimetral es constituirse como la primer línea de defensa ante intentos de acceso externos no autorizados a los recursos e información de la organización.

Características de una buena seguridad perimetral de redes:

- Resiliencia: debe ser capaz de resistir a los ataques externos.
- Identificación: debe de ser capaz de identificar los ataques y alertar sobre ellos de manera inmediata.
- Aislamiento: debe ser capaz de aislar y segmentar los distintos servicios y sistemas en función de su exposición a los ataques.
- Filtrado: debe filtrar el tráfico permitiendo únicamente aquel que sea autorizado o absolutamente necesario, restringiendo y bloqueando el resto.

¿Qué es un perímetro?

Un perímetro no es más que una línea imaginaria que separa un área estableciendo un límite o frontera respecto de terceros y/o respecto del ambiente, usualmente con el objetivo de mantener controlada y protegida dicha área.

¿Qué es un perímetro de red?

Un perímetro de red, no es más que una línea imaginaria que separa la red de una empresa y sus recursos (computadoras, servidores, etc.) de redes de terceros o bien públicas (por ejemplo Internet).

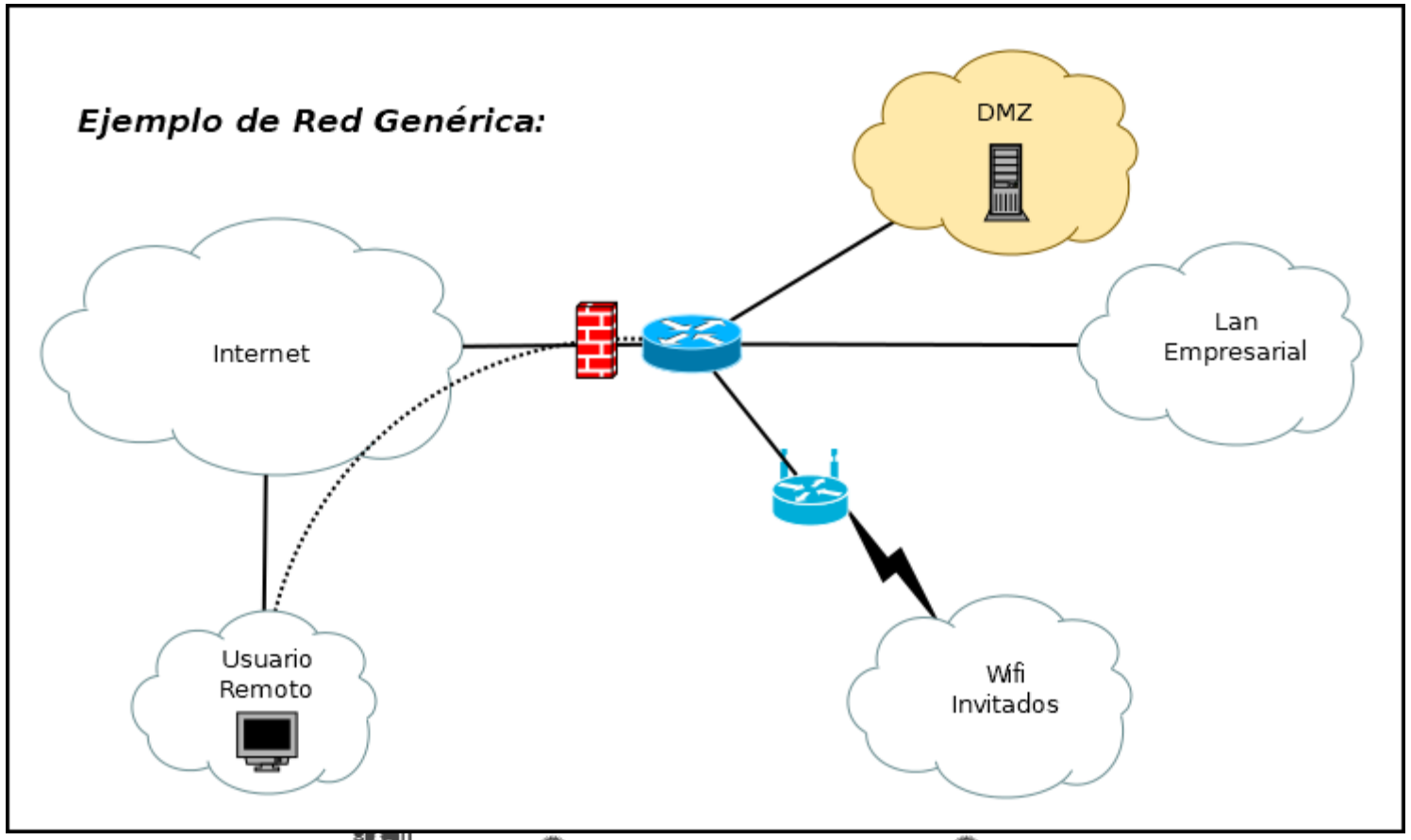
Un perímetro de red es el límite "seguro" entre el lado privado y administrado localmente de una red (la intranet de la empresa), y el lado público y/o fuera de nuestro control.

¿Por qué es importante un perímetro de red?

El concepto de perímetro de red, su establecimiento y su constante evolución permite a las organizaciones pensar de manera efectiva sobre cómo proteger sus recursos e información de posibles vectores de ataque, actores no confiables o maliciosos y riesgos en general con el fin de lograr una buena seguridad perimetral informática.

Un perímetro de red podría incluir y estar conformado por diversos dispositivos trabajando en conjunto como ser:

- Routers de borde
- Cortafuegos
- Zonas Desmilitarizadas / Protegidas (DMZ)
- IDS/IPS
- Honeypots


Ejemplo de Red Genérica:
DMZ
Internet
Lan
Empresarial
Usuario
Remoto
Wifi
Invitados

Complejidades del perímetro de red:

En las empresas modernas, no existe un límite único defendible entre los activos internos de una empresa y el mundo exterior.

Los usuarios se conectan desde redes externas y utilizan dispositivos móviles para acceder a recursos internos.

Los datos y las aplicaciones ya no se alojan en servidores que las empresas poseen, mantienen y protegen físicamente.

Complejidades del perímetro de red: (continuación)

Las tecnologías de Cloud Computing, SaaS, IaaS, IoT, presentan nuevos desafíos de seguridad en los entornos empresariales.

Si bien el concepto de "perímetro de red" tiene significado para ciertas configuraciones de red sencillas, en los entornos complejos debe tratarse de manera abstracta, como una frontera subjetiva y dinámica.

¿Qué podemos hacer al respecto?

- Implementar Buenas Prácticas de seguridad informática.
- Implementar Políticas de control de acceso, que ayudan a determinar quién y bajo qué circunstancias puede acceder a la información.
- Recopilar y auditar la información de seguridad obtenida directamente desde las aplicaciones, hosts y dispositivos en general.
- Hardening de dispositivos móviles e IoT que se conectan a la red. Utilizar STIGs y en lo posible implementar SCAP para ello.

STIGs:

Una guía de implementación técnica de seguridad es una metodología para estandarizar protocolos de seguridad dentro de redes, servidores, computadoras y diseños lógicos con el fin de mejorar la seguridad general.

Estas guías, cuando se implementan, mejoran la seguridad del software, hardware, arquitecturas físicas y lógicas para reducir aún más las vulnerabilidades. Es decir se utilizan para realizar Hardening.

SCAP:

El protocolo de automatización de contenido de seguridad es un método para utilizar estándares específicos para permitir la gestión automatizada de vulnerabilidades, la medición y la evaluación de cumplimiento de políticas de los sistemas implementados en una organización, incluyendo, por ejemplo, el cumplimiento de STIGs. Un ejemplo de una implementación de SCAP es OpenSCAP. Es decir permite automatizar el proceso de implementar STIGs.

¿Y a futuro que podemos esperar?

- Confianza Zero
- Protección Perimetral Multicapa
- Perímetro Definido por Software

Confianza Cero:

Este modelo aplica el principio “Nunca confies, siempre verifica” para definir su arquitectura y framework de trabajo.

No permite ningún tipo de confianza por defecto para ninguna entidad (dispositivos, aplicaciones, usuarios, etc) sin importar su tipo o si pertenece o se encuentra en la red de la empresa.

Es aplicable tanto a dispositivos como a usuarios.

Protección Perimetral Multicapa:

Se define como una estrategia de seguridad perimetral reforzada y multicapa.

Mediante el uso de cifrado y autenticación de nivel de datos dinámico, asegura los datos del usuario en varios niveles. Este enfoque multinivel es factible para los más avanzados sistemas informáticos como IoT, cloud computing, etc., ya que funciona en arquitecturas multicapa.

Perímetro definido por software:

Perímetro definido por software (SDP) se basa en un modelo de necesidad-de-conocer o nube negra, en el que se verifica la postura y la identidad del dispositivo antes de otorgar el acceso a la infraestructura de la aplicación que en principio es invisible e inaccesible.

El SDP parte desde el supuesto de Cero Disponibilidad y Cero Visibilidad en tanto el dispositivo/usuario no se haya identificado y autenticado correctamente. El perímetro se ajusta dinámicamente según los requerimientos del dispositivo/usuario.

¿Dudas y Consultas?

Gracias por su tiempo y participación!!!