Alumno: Rodrigo Vila

Experto Universitario en Seguridad de la Información

Modulo 6, Unidad 2, Ejercicio 2

Escenario: Un banco

Consigna:

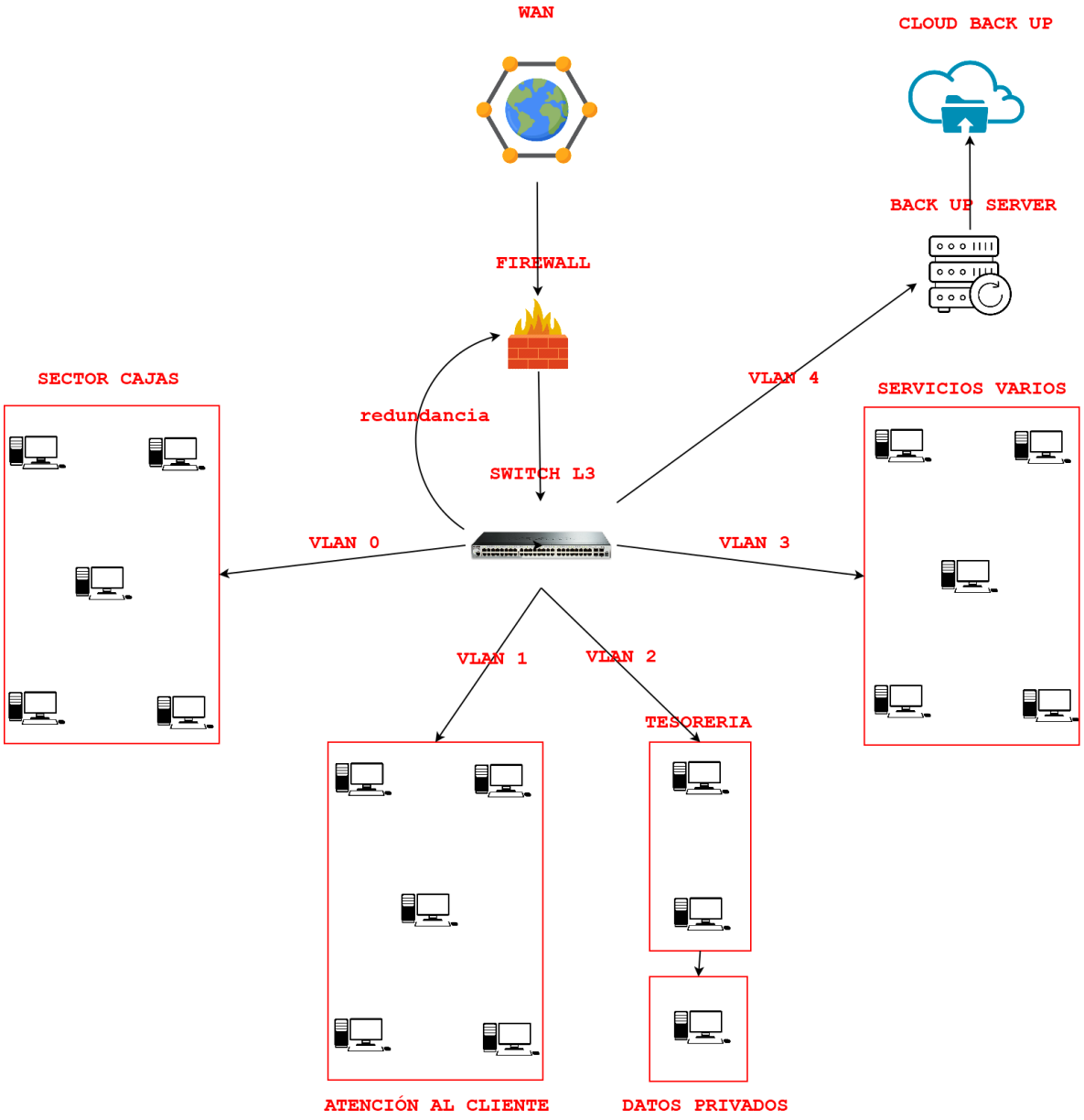
Si fueran administradores de redes y seguridad en un banco, de todo lo expuesto, qué medidas aconsejaría implementar, dentro de un banco, con 16 equipos finales, conectados a un switch con un backup y con un firewall en la WAN.

Imaginen una sucursal que recién abre y que pidieron “para ayer” dejar operativa la misma.

Pensar en los procesos más importantes, por ejemplo, de los 20 equipos finales, 5 son de caja a público, 5 de atención al cliente, 5 de servicios varios (cuentas, tarjetas) y 3 de gerencia (2 de tesorería y 1 de datos privados)

Topología de red:

Vista general:



Medidas de seguridad a implementar en Seguridad Informática:

Firewall: Mantener el firewall WAN configurado para bloquear tráfico no deseado y permitir solo los puertos necesarios.

Segmentación de Red: Utilizar VLANs para separar el tráfico de las diferentes áreas (caja, atención al cliente, servicios, gerencia). Esto limita el impacto en caso de que una parte de la red sea comprometida.

Red Privada Virtual (VPN): Si hay accesos remotos a la red del banco, asegurarse de que utilicen VPN con cifrado fuerte.

Protección de Equipos Finales:

Antivirus y Antimalware: Instalar y mantener actualizado software antivirus y antimalware en todos los equipos finales.

Parcheo y Actualizaciones: Asegurarse de que todos los sistemas operativos y aplicaciones estén actualizados con los últimos parches de seguridad.

Control de Acceso a Información:

Autenticación: Utilizar autenticación multifactor (MFA) para acceder a sistemas críticos y datos sensibles.

Gestión de Contraseñas: Establecer políticas de contraseñas fuertes y asegurarse de que expiren para que se cambien regularmente.

Privilegios de Usuario: Configurar permisos adecuados para cada rol, asegurando que los usuarios solo tengan acceso a la información necesaria para su función.

Respaldo y Recuperación:

Copias de Seguridad: Implementar un sistema de copias de seguridad regulares y asegurarse de que los datos que se almacenan en el back up server esten cifrados. Consideranr una copia de seguridad en la nube para dicho servidor backup.

Plan de Recuperación: Desarrollar un plan de recuperación ante desastres que detalle cómo restaurar sistemas críticos en caso de una interrupción. (Tanto Disaster Recovery como Bussiness Continuity)

Monitorización y Respuesta:

Sistema de Detección de Intrusiones (IDS): Implementaría un IDS para detectar actividades sospechosas en la red.

Registro y Monitoreo: Configurar un sistema de registro y monitoreo para detectar y analizar eventos de seguridad. Pondría un visor de logs centralizado en el sector de Tecnología y Seguridad del banco que sea monitorizado.

Medidas de seguridad a implementar en lo que respecta a la Seguridad Física:

Acceso a la Sucursal: Sistemas de control de acceso como tarjetas magnéticas o biometría para asegurar que solo personal autorizado pueda ingresar a los sectores no públicos de la sucursal.

Áreas Críticas: Utilizar cerraduras electrónicas y controles de acceso adicionales en áreas sensibles como la sala de servidores y la oficina de tesorería.

Monitoreo y Vigilancia:

Instalar cámaras de CCTV en puntos clave como entradas, salidas y áreas sensibles para monitorear cualquier actividad sospechosa.

Asegurarse de que las grabaciones sean almacenadas por un período adecuado y sean accesibles solo para personal autorizado. Aquí implementaría NVR con respaldo a la nube en la sala de sistemas.

Protección contra Desastres:

Implementar medidas para protección contra incendios y desastres naturales, como detectores de humo, sistemas de rociadores y extintores.

Medidas de seguridad a implementar en lo que respecta a la Seguridad Electrónica:

Redundancia de Energía: Utilizar un Sistema de Alimentación Ininterrumpida (UPS) para proteger los equipos de fallos de energía y picos de voltaje. También ubicado en la sala de sistemas.

Control de Acceso Electrónico: Implementar un sistema de control de acceso para el personal utilizando tarjetas de identificación y autenticación biométrica si es necesario.

Alarmas: Implementación de alarmas anti pánico, silenciosas, lockdowns.

CCTV: Control de las áreas con videovigilancia.

Es muy importante capacitar a los empleados regularmente para que sean consientes sobre posibles ataques de phishing, ransomware y otro tipos de peligros informáticos. También realizar simulacros y mantener los SOP actualizados para los distintos eventos de seguridad como puede ser: incendios, amenazas de bomba, asalto, etc.

Rodrigo Vila.-