Universidad de Palermo
Facultad de Ingenieria

SEGURIDAD EN REDES

TRABAJO PRACTICO GRUPAL

Prof.: Dionofrio, Gerardo Oscar

Alumnos: Alvarez Bianco, Exequiel
Canepa Carballo, Joel Santiago
Orue Marighetti, Guillermo
Zarate, Cesar Ezequiel
Carrizo, Alvaro Joaquin

cursada 2024

1. Descripción de la organización

Sur Distribuciones S.A. es una empresa dedicada a la distribución mayorista de productos alimenticios orgánicos para supermercados, restaurantes y tiendas minoristas. Su misión es garantizar el abastecimiento de productos frescos y de alta calidad en todo el sur del país.

Fundada en 1995, la empresa cuenta con más de 29 años de experiencia en el mercado de distribución alimentaria. Con una sede principal (desde ahora en adelante “Casa Central”) en la ciudad de Rosario, provincia de Santa Fe, Argentina, y dos sucursales estratégicamente ubicadas en Bahía Blanca y Mar del Plata para asegurar una cobertura eficiente en las provincias del sur del país, SurDistribuciones se ha consolidado como un socio confiable para sus clientes. Cuenta con aproximadamente 250 empleados, distribuidos en sus tres sedes. El personal incluye conductores, personal de depósito, administrativos, vendedores y equipo de logística.

- **Casa Central:** En la sede principal se gestionan las operaciones logísticas y administrativas. Aquí se encuentran las oficinas de dirección, ventas y recursos humanos, además de los depósitos de almacenamiento y la flota de camiones para distribución.

- **Sucursal Bahía Blanca:** Dedicada principalmente al almacenamiento y distribución de productos secos y congelados para clientes de la zona sur de la provincia de Buenos Aires.

- **Sucursal Mar del Plata:** Especializada en la distribución de productos frescos como lácteos, frutas y verduras a comercios y restaurantes de la costa atlántica.

2. Problemática Actual

Actualmente, la empresa cuenta con el hardware necesario para llevar a cabo sus operaciones; sin embargo, todos sus dispositivos (de ahora en más "**activos**") se encuentran en **constante amenaza** debido a la **vulnerabilidad de su red**.

Todo **dato** perteneciente y/o allegado a nuestro cliente estaba **comprometido** debido a que **no está encriptado** el tráfico de información.

SurDistribuciones no cuenta con procedimientos claros ante la ocurrencia de un **ataque sobre** la **integridad**, **confidencialidad** y **disponibilidad** de la **infraestructura de la red** y sus **activos** relacionados. Es una **entidad** completamente **indefensa**.

En cuanto a sus **redes LAN**, en **ninguna** tiene **implementada** la segmentación mediante **VLANs**; tampoco se monitoriza y/o filtra el tráfico entrante, saliente ni interno de la red.

Además, la organización busca implementar el **trabajo remoto** de manera **segura**, permitiendo a sus empleados adoptar un modelo de trabajo híbrido que favorezca su flexibilidad y productividad.

3. Diagrama de la Red Actual

Casa central

La red cuenta con un **WiFi público** para los clientes, además, se alojan dos servidores principales: uno para la **web pública** y otro para los sistemas de **ERP/CRM**, los cuales están conectados a la **red de la sucursal**, la cual no se encuentra segmentada de ninguna manera y todos sus nodos/activos están conectados directamente a los puertos LAN de un router (el cual está vinculado con el ISP directamente, esto es, salida a Internet sin ningún filtro ni aseguración).

Sucursales Bahía Blanca y Mar del Plata

Se comunican con los recursos de la casa central a través de Internet utilizando la IP pública de la casa central. Estas sucursales tienen su propia **red interna**, donde se conectan las **computadoras locales** que acceden a los recursos de la **Casa Central**, como el **ERP/CRM** sin ningún tipo de seguridad. Además, cuenta con un **WiFi local** para el acceso de los visitantes.

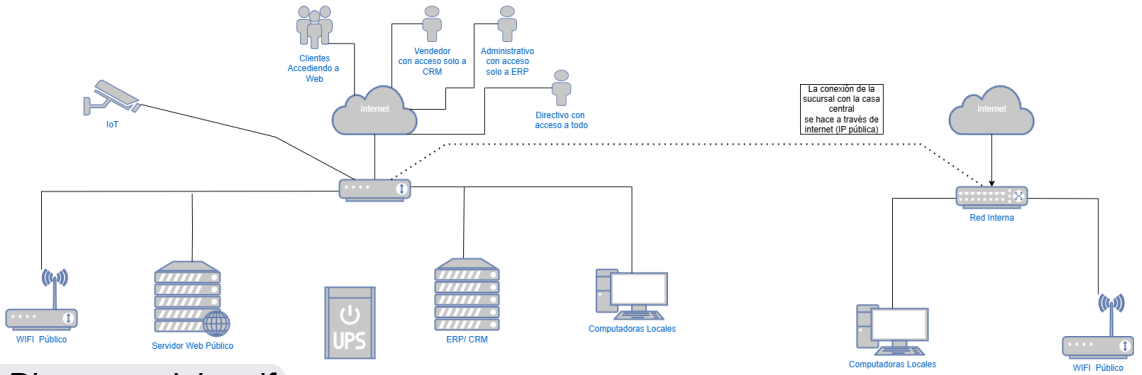

Diagrama viejo.pdf

4. Definición de Activos de Riesgo

- Servidor Web Público
- ERP/CRM
- Workstations (Computadoras locales)
- Servicio de conexión inalámbrica a la red (Wi-Fi público)
- Fuentes de energía ininterrumpida (UPS s)
- Servicios IoT
- Personal
- Inventario

5. Análisis de vulnerabilidades y riesgos

N° Amenaza	Activo	Amenaza	Vulnerabilidad	Impacto	Probabilidad
1	ERP/CRM	Interceptación de tráfico. Robo y modificación de datos	Tráfico sin encriptación	Alto	Alta
2	Servidor Web	Explotación de vulnerabilidades y ataques (por ej. DDOS, XSS, SQLi)	Exposición a Internet	Alto	Alta
3	Red WiFi públicas	Intrusión en la red, reconocimiento y explotación de vulnerabilidades	Falta de autenticación y segmentación en la red	Alto	Alta
4	Estaciones de trabajo y Personal	Ataque de Ingeniería Social, malware y ransomware	Falta de concientización	Alto	Alta
5	Estaciones de trabajo y Personal	Ataque de malware y ransomware	Falta de software Antivirus	Alto	Alta
6	Personal	Inclusión en la red de dispositivos ajenos a la empresa	Falta de estandarización	Alto	Alta

7	Servidor Web	Fuga de datos sensibles de clientes	Mala configuración y falta de cifrado	Alto	Alta
8	Fuentes de energía ininterrumpida (UPS)	Fallos en las baterías, sobrecargas en la fuente de alimentación	Mala planificación de mantenimientos preventivos	Medio	Bajo
9	Dispositivos IoT	Accesos no autorizados	Firmwares desactualizados, contraseñas default	Alto	Medio
10	Dispositivos IoT	Daños a la infraestructura por ciberataques o sabotajes físicos	Huecos de seguridad debido a falta de estándares y configuración	Alto	Alto
11	Personal	Filtracion de informacion interna o sabotaje de procesos	Insuficiente monitoreo o supervisión de actividades	Alto	Alto
12	Inventario	Infección / pérdida de vida útil de los alimentos inventariados.	Inoperancia de los servicios IoT	Alto	Alto

6. Acciones de mitigación

	Acción
1	Instalación de servidores VPN para proteger el acceso a recursos internos de la empresa de forma remota, cifrando la comunicación del usuario a casa central.
2	Instalación de un servidor Radius para validar el acceso de los trabajadores en modalidad remota a los recursos de la entidad mediante los servidores VPN.
3	Instalación en la red de un WAF para proteger las conexiones con las aplicaciones del servidor web de distintos tipos de ataques.
4	Instalación de dispositivos IoT y de seguridad para infraestructura (tales como cámaras IP) para asegurar la integridad de los activos y mantener un registro de la actividad en todas las sucursales.
5	Estandarización de dispositivos “workplace” tales como computadoras fijas/móviles (que todas pertenezcan a la empresa y no se muevan de las sucursales)
6	Correcta configuración de los dispositivos estándar de la red LAN y registro de usuarios y logins para monitorear incidencias.
7	Instalación en las estaciones de trabajo de un software antivirus para protegerlos contra ataques de malware y tratar de evitar la propagación dentro de la red.
8	Configuración de WPA2 PSK en la red Wi-Fi y segmentación de la red para aislarla de los recursos internos, evitando accesos no autorizados.
9	Planificación y ejecución de programas de concientización y capacitación para el personal.
10	Planificación de mantenimientos preventivos para toda la infraestructura IT.

11	Re-diseño de la red e instalación de un firewall de perímetro para monitorear y controlar el tráfico entrante y saliente de la red.
12	Configuración de túneles IPSEC entre sucursales para tener una comunicación segura y privada entre ellas.
13	Instalación de un IDS/IPS para monitorear y detectar intrusiones en la red de la organización.

Nuevas implementaciones - Soluciones específicas

VPN

Situación Actual

SurDistribuciones no cuenta con un sistema seguro para permitir acceso remoto de sus empleados a los recursos de la red de la empresa. Las conexiones remotas cuando se realizan son basadas en la IP pública de la casa central, **exponiendo los sistemas internos** a **riesgos de seguridad** significativos (debido a falta de cifrado y autenticación). No hay forma de garantizar que los empleados remotos estén autorizados y autenticados a usar los recursos de la empresa.

Solución Propuesta

Proponemos la implementación de un **servidor VPN**, instalado en la Casa Central, este permitirá a los empleados conectarse de forma segura, y nos permitirá mitigar posibles riesgos. Podríamos usar **OpenVPN** o **túneles IPSec**.

También el **tráfico** se **encriptará** de **extremo a extremo**, usando **AES-256** para proteger la confidencialidad de los datos mientras se transmiten entre la red de la empresa y los dispositivos de los empleados.

Se implementa a su vez, un sistema de registro y monitoreo de conexiones VPN, lo que facilitará la auditoría de accesos y permitirá identificar rápidamente posibles intentos de acceso no autorizados.

A.A.A

Situación Actual

La organización **no cuenta** con **métodos** para **autenticar y validar** la **identidad de los usuarios** cuando **ingresan** al **sistema CRM o ERP**, lo que evidencia la ausencia de controles de acceso **comprometiendo la seguridad** de **información crítica**. Además, la red no dispone de un sistema seguro para conectar a los usuarios remotos, lo que aumenta el riesgo de accesos no autorizados y de exposición a amenazas externas.

Solución Propuesta

Para mitigar los riesgos asociados con la falta de autenticación y control de acceso, se propone la implementación de un **servidor RADIUS** como solución centralizada de autenticación. Este servidor se configurará para integrarse tanto con el servidor de VPNs como con los sistemas CRM y ERP, garantizando que solo los usuarios autenticados y autorizados puedan acceder a los recursos críticos de la organización.

Especificaciones técnicas

Para la implementación de RADIUS debemos contar con un servidor en el que podamos instalar el software correspondiente contando con los requisitos de hardware que tiene. Podemos utilizar **FreeRADIUS**.

En cuanto a protocolos, utilizaremos **EAP**, que nos permite usar diversos métodos de autenticación, como contraseñas, certificados o tokens, lo que lo hace más seguro y adaptable, específicamente **EAP-TLS** que introduce cifrado de extremo a extremo.

Firma Digital

Situación Actual

La organización no tiene una solución de firma digital, lo que **dificulta** la **firma** de **documentos y contratos** de manera electrónica con otras entidades (por ejemplo clientes o proveedores). Esto puede generar un riesgo en términos de validez legal de la documentación y no se podría garantizar la autenticidad de los acuerdos y documentos firmados de forma remota, **dando lugar a posibles fraudes, suplantación de identidad, etc**.

Solución Propuesta

Las soluciones de firma digital requieren de una **infraestructura de clave pública (PKI)** para su funcionamiento. Estas suelen ser muy costosas de implementar y deben estar bajo reglamentación. Nuestra propuesta es la contratación de un servicio SaaS de firma digital. De esta forma, se podrá integrar en el procedimiento de trabajo actual de la organización (en conjunto con el ERP y CRM) y tenemos garantizada la validez legal de las firmas emitidas.

Especificaciones técnicas

Contratación del servicio de PKI, firma digital de una empresa reconocida como **Adobe Sign, Digicert, Entrust**.

Seguridad Perimetral

Situación Actual

Actualmente la red de la empresa está **expuesta** a internet **sin** ninguna **protección** de perímetro, no cuenta con un firewall que filtre y monitoree el tráfico entrante o saliente.

Las sucursales Bahía Blanca y Mar del Plata acceden a los recursos de Casa Central mediante una IP pública, sin túneles de seguridad, lo que **aumenta** la **vulnerabilidad ante ataques externos**.

Los sistemas de red no tienen segmentación adecuada, el tráfico de la red pública y el de la red interna están mezclados, **aumentando el riesgo de accesos no autorizados**.

Solución Propuesta

Proponemos la instalación de un **firewall perimetral** en Casa Central y en cada una de las sucursales. Este dispositivo será configurado con **políticas de control de acceso** para monitorear el tráfico entrante y saliente, bloqueando conexiones sospechosas o no autorizadas.

A su vez, la instalación de un **WAF** será beneficioso para la entidad, debido a que protegerá las aplicaciones del servidor web frente a ataques como inyecciones SQL, XSS y otros vectores de ataque comunes contra aplicaciones web.

Implementar **IDS/IPS** para monitorear el tráfico de la red en tiempo real y detectar intentos de intrusión. Servirá como una capa adicional de seguridad. Además, segmentar la red LAN en VLANs nos permitirá tener un control granular sobre la infraestructura de la red.

7. Conclusiones

a. Diagrama de la Red Actual

Casa central

Se alojan dos servidores principales: uno para la **web pública** (separado de la red interna) y otro para los sistemas de **ERP/CRM**, que está dentro de la **red interna** protegida.

La red cuenta con un **WiFi público** para los clientes, aislado y segmentado de los recursos críticos. Además, se ha implementado un **servidor VPN** que permite el acceso remoto y seguro a la red interna, facilitando que los empleados puedan conectarse desde fuera de la oficina para acceder a los **servidores ERP/CRM**.

Se implementó adicionalmente un servidor **RADIUS** para asegurar y proteger la autenticación de los usuarios con la VPN y el ERP/CRM.

Todo el tráfico es controlado por el **Firewall de perímetro**, que garantiza la protección de la red. Además, se agregó un **IDS/IPS** que monitorea todo el tráfico entre las **VLANs** internas, para detectar y prevenir posibles intrusiones o comportamientos sospechosos.

Para reforzar la seguridad de la web pública, se ha implementado un **WAF** encargado de proteger las aplicaciones del servidor web. La red interna está segmentada mediante VLANs para garantizar una mayor seguridad y un control eficiente del tráfico.

Sucursales Bahía Blanca y Mar del Plata

Están conectadas a la **Casa Central** mediante un **túnel IPsec** site-to-site para garantizar una conexión cifrada y privada entre las redes.

Estas sucursales tienen su propia **red interna**, donde se conectan las **computadoras locales** que acceden a los recursos de la **Casa Central**, por ejemplo el **ERP/CRM**, a través del túnel seguro.

La red de la sucursal está protegida por su propio **Firewall**, que gestiona el tráfico entrante y saliente, y garantiza que sólo el tráfico autorizado puede acceder a los recursos de la Casa Central. Además, cuenta con un **WiFi local** para el acceso de los visitantes, separado de la red interna.

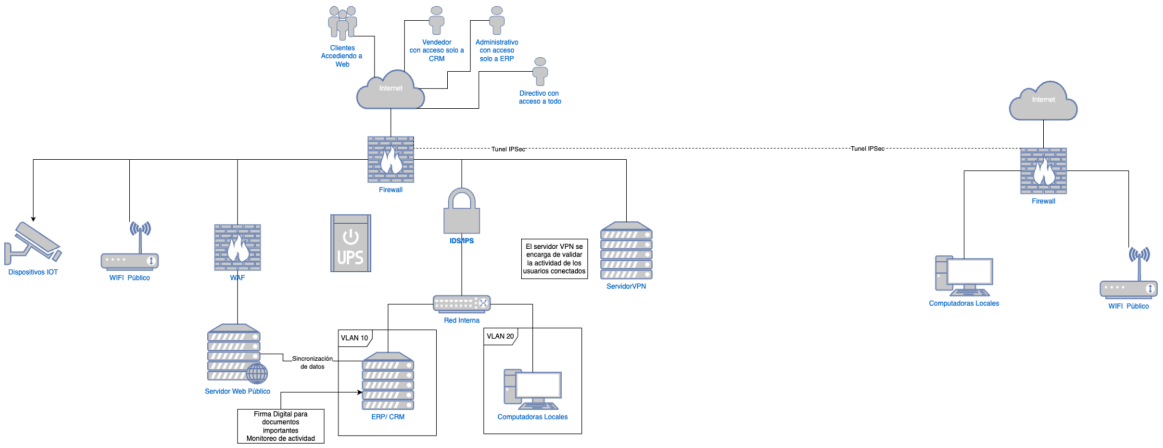

Diagrama nuevo.pdf

Las nuevas implementaciones mejorarán el nivel de seguridad para SurDistribuciones S.A., siendo propulsoras de estas la definición de activos, comprensión de riesgos y el impacto que estos pueden producir si las amenazas evolucionan a hecho.

Bianco, Canepa, Orue, Zarate, Carrizo