1. Introducción

El objetivo de este informe es realizar un análisis de inteligencia de fuentes abiertas (OSINT) sobre la empresa S.B.S. TELECOMUNICACIONES, S.L. para identificar posibles riesgos de seguridad derivados de la información pública disponible.

2. Alcance

La información obtenida a través de fuentes abiertas puede poner en riesgo la seguridad de la organización al proporcionar detalles que pueden ser explotados por actores malintencionados. Este informe evalúa la criticidad de los datos encontrados y su potencial impacto en la seguridad de la empresa.

3. Perfilado de la Organización

Organización de la Empresa:

* Nombre Comercial: S.B.S. TELECOMUNICACIONES, S.L.
* Denominación Social: S.B.S. TELECOMUNICACIONES, S.L.
* NIF: B80067333
* Domicilio Social: C/ Juan Francisco 3 - 5, 28025 Madrid (MADRID)
* Teléfono: 914718938
* E-mail: [sbs@sbstelec.es](mailto:sbs@sbstelec.es) [sbsavisos@sbstelec.es](mailto:sbsavisos@sbstelec.es)
* Nombre de Dominio: [www.sbstelec.es](http://www.sbstelec.es)

Gráfico de Organización:

S.B.S. TELECOMUNICACIONES, S.L.

├── Dirección General

│ ├── Departamento de Ventas

│ ├── Departamento de Marketing

│ ├── Departamento de Finanzas

│ ├── Departamento de Recursos Humanos

│ ├── Departamento de IT

│ └── Departamento de Operaciones

4. Criticidad de los Datos Obtenidos

La información obtenida puede ser crítica por las siguientes razones:

* Datos de Contacto: La disponibilidad de números de teléfono y correos electrónicos puede facilitar ataques de ingeniería social, phishing, y spam.
* Domicilio Social: Conocer la ubicación física de la empresa puede permitir ataques físicos o vigilancia.
* Nombre de Dominio: Información sobre el dominio puede ser utilizada para realizar ataques de suplantación de identidad (phishing) o para buscar vulnerabilidades en el sitio web.
* La web no utiliza el protocolo de seguridad HTTPs, por lo que actores malintencionados podrían capturar los paquetes de datos y acceder a su contenido para leer, modificarlo o eliminarlo, pudiendo realizar ataques “Man in the Middle”.

5. Soluciones o Recomendaciones

En base a los resultados obtenidos, se recomiendan las siguientes acciones para mitigar los riesgos de seguridad:

1. Educación y Concienciación: Capacitar a los empleados sobre los riesgos de ingeniería social y phishing.
2. Seguridad Física: Implementar medidas de seguridad en las instalaciones físicas de la empresa.
3. Seguridad de la Información: Utilizar herramientas de seguridad para proteger el correo electrónico y el sitio web de la empresa.
4. Monitoreo y Respuesta: Establecer un sistema de monitoreo continuo para detectar y responder a posibles amenazas de seguridad.

Gráficos

Para una mejor comprensión, se pueden incluir gráficos que representen la estructura organizativa y los posibles vectores de ataque. A continuación, se muestra un ejemplo de gráfico de la estructura organizativa:

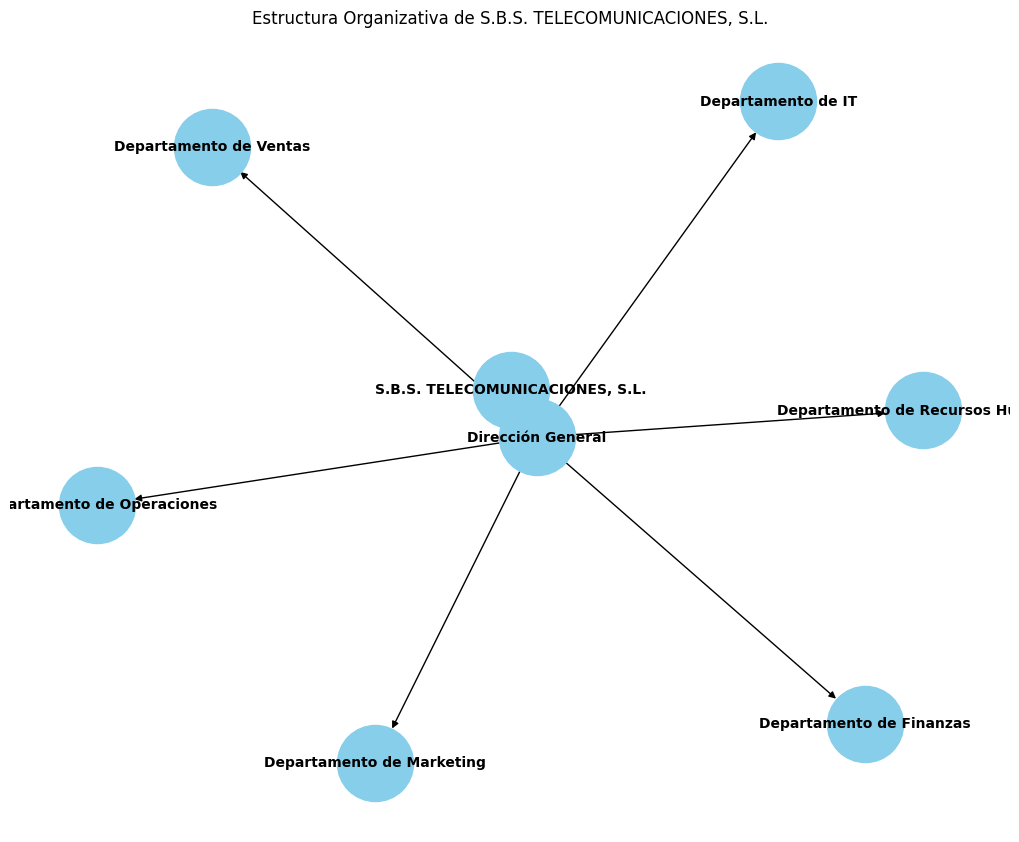


gráfico de posibles vectores de ataque:

