INFORME DE SEGURIDAD

Empresa: TechSecure S.A.
Fecha: 29-08-2025
Realizado por: José Miguel Rivera

1.- Resumen ejecutivo

El presente informe procede a detallar la evaluación de activos de información realizada a la empresa TechSecure, con el fin de identificar posibles vulnerabilidades y riesgos de seguridad.

Dentro del análisis realizado, es posible mencionar que:

a) Se ha detectado que las credenciales no tienen establecidas políticas de seguridad en la empresa y pueden ser fácilmente descifrables ya que por defecto se utilizan los 4 últimos dígitos del rut del trabajador.

b) Se ha detectado que se puede ingresar a la red de TechSecure a través de la red interna de la oficina de ventas, por lo que es posible que los roles de usuario no estén definidos y los servidores de información de datos de clientes han quedado expuestos.

c) Se ha detectado que el atacante cambió la contraseña del servidor de clientes, debido a un uso incorrecto de las claves de root por parte de los administradores de sistemas, siendo aprovechado por un atacante con conocimiento de sistemas informáticos.

2.- Descripción detallada

El incidente ocurrido, ha sido expuesto dado que se han descubierto movimientos inusuales en el sistema por parte del usuario del jefe del departamento de ventas, en el cual se han eliminado y modificado registros en favor de al menos 10 rut de extrabajadores de la empresa, estos movimientos han quedado expuestos ya que han sido ejecutados dentro de la empresa en uno de los equipos de la oficina de ventas, determinado por el registro del movimiento ingresado en la base de datos en un día en que el jefe de la sección no se encuentra por estar con licencia médica.

La principal causa se estima que las políticas de contraseñas para las claves de usuario no han sido las más apropiadas, siendo deducidas por el personal con

cierto nivel de conocimiento informático, tomando la vulnerabilidad y aprovechando la situación para conseguir movimientos a su favor.

Para realizar este análisis han sido revisados los siguientes componentes:

- Revisión de pc’s de oficinas
- Revisión de la topología de red y estructura de segmentación, vlans, listas de accesos, comunicaciones
- Revisión de servidores y routers
- Evaluación del equipo de informática y sus roles

Con esto se ha determinado que existen las siguientes vulnerabilidades:

- Las contraseñas del personal pueden ser deducidas con solo saber el rut
- Cualquier usuario puede acceder a la base de trabajadores y revisar su ficha de trabajador
- En ciertos equipos han quedado anclados las unidades de red de servidores, lo que facilita el revisar cuales son las ips que los atacantes pueden usar
- Se pueden instalar programas y ejecutables de tipo portable en todas las máquinas
- Los intentos de acceso a servidores o base de datos no se están reportando al departamento de informática
- Servidores de datos están expuestos por mal uso de la clave de root

3.- Impacto

El impacto es alto, la red ha quedado vulnerable y la empresa no tiene el control absoluto de la red ni de los datos.

Posibles consecuencias: La información está en riesgo y es posible que haya sido copiada para fines lucrativos del atacante.

Se debe considerar que la red ha sido expuesta por lo que la confidencialidad e integridad de la información no está garantizada.

4.- Recomendaciones

Se sugiere realizar una evaluación urgente de los accesos del personal, realizando una correcta redistribución de los roles, accesos de sistema y configuraciones que requiera.

Es fundamental que mejore la política de contraseñas y que obligue al personal a no utilizar por ejemplo solo números, correlativos o iguales, estas deben ser de tipo alfanuméricas e idealmente incorporar símbolos.

Se sugiere integrar al equipo de informática una persona con habilidad de ciberseguridad a fin de que se encuentre monitoreando la red y pueda detectar movimientos inusuales a tiempo.

Idealmente considerar instalar un servidor de backup en el cual se mantenga respaldada la información y las diferencias puedan ser canalizadas a tiempo.

5.- Conclusión

Se sugiere realizar nuevamente una evaluación de la seguridad de la información una vez subsanados los puntos evidenciados.