Análisis de situación actual:

1. Introducción: Recibimos una llamada del gerente de una organización para decirnos que está recibiendo una gran cantidad de tráfico de red por parte de nuestra empresa TODOTECH. Hemos descubierto que nuestra red ha sido atacada por un ciberdelincuente que nos ha instalado un malware para hacernos pertenecer a una botnet, el cual controla a distancia, para enviar tráfico a otra organización para así colapsarla.
2. Causas de los problemas:
   1. Configuración del servidor de nombres DNS está abierto públicamente en internet.
   2. La red interna y servidores corporativos no disponen de ninguna defensa contra la internet exterior, por ejemplo, un cortafuegos.
3. Efectos:
   1. El DNS es vulnerable y ante una amenaza puede ser atacado, en este caso pasó a ser parte de una botnet. Afectando la reputación de la empresa y a una organización que podrían ser sus socios clave, además afectan a nuestros servicios por la instalación del malware y ocupando los recursos de red.
   2. Provocan un ataque cibernético de manera indirecta a otra empresa.
4. Activos digitales:
   1. Servidores:
      1. Cuentas de usuario (LDAP) (Alta)
      2. Bases de datos (ventas y clientes) (Alta)
      3. Resolución de nombres interno (DNS) (Alta)
      4. Correo electrónico corporativo. (Media)
      5. Página web. (Media)
   2. Red wifi y conexión a internet. (Alta)
   3. Página web tienda online. (Media)

Análisis de la situación futura:

1. Apetito de riesgo: Si bien la empresa sabe que en cualquier momento puede ser objetivo de un ataque cibernético, debería disminuir la cantidad de vulnerabilidades que tienen, para que en el futuro puedan prevenir amenazas y mitigar el riesgo del impacto que producen. Por lo tanto, lo principal es proteger los activos digitales fundamentales de la empresa, es decir, aquellos que comiencen con riesgos altos y muy altos.
2. Estrategia de defensa en profundidad:
   1. Agregar o cambiar políticas y procedimientos:
      1. Priorizar los activos más importantes de la organización.
      2. Asumir los riesgos de cada activo.
      3. Asesorar al personal con buenas prácticas de seguridad cibernética.
      4. Contratar especialistas en ciberseguridad, para evaluación e implementación de controles.
   2. Utilizar VPN.
   3. Cambiar las configuraciones de red:
      1. El servidor DNS tendrá acceso restringido.
      2. Implementar cortafuegos en la red interna y servidores corporativos.
      3. Implementar protocolos de seguridad SSL/SSH
   4. Limitar los privilegios de usuarios y aumentar los controles de autenticación.
   5. Implementar antimalware.
   6. Cifrado de datos e información.
   7. Tener una base de datos de respaldo.
3. Situación: Luego de recuperarse del ciberataque presente en la empresa, la gerencia decide contratar expertos en ciberseguridad para una evaluación de vulnerabilidades y riesgos sobre los sistemas de información de la compañía. Estos a través de un análisis detectan que la empresa TODOTECH no cuenta con casi ningún control de mitigación de ciberataques, y que las configuraciones de red están públicamente abiertas. Por lo tanto, recomiendan un nuevo proyecto estratégico de defensa en profundidad visto anteriormente para la empresa, y TODOTECH acepta el acuerdo.

Después de un tiempo, el registro de ataques de la compañía muestra lo siguiente: pudieron prevenir un 70% de los ataques, del 30% restante pudieron defenderse de un 80%, y de los ataques restantes pudieron recuperarse rápidamente. En el peor de los ataques la empresa realizó una recuperación de respaldo, luego mejoró y aumento el número de controles de seguridad cibernética.

Conclusión: En el escenario que se presentó, dos empresas resultaron afectadas, donde una de ellas realizo un ciberataque a la otra sin saberlo, por la acción de un ciberdelincuente, afectando así la reputación de la empresa y dejando en evidencia sus vulnerabilidades de red. Después del análisis sobre las cusas y los efectos del problema, se realizó un estudio de los activos digitales de la empresa, haciendo énfasis en los más importantes, y realizando un registro de los actuales controles y el potencial riesgo que tienen en caso de recibir otro ciberataque. Finalmente, se propusieron nuevos controles de mitigación como medidas preventivas, para reducir la probabilidad de que ocurran los incidentes y disminuir el impacto que tendrán, así se pudo realizar una estrategia de defensa en profundidad para la empresa.