FORO.
Realizar un análisis de riesgos, detección y remediación para el caso de que alguien vía usb o vía ethernet coloque un punto de acceso Wi-Fi en nuestras instalaciones

La presencia de un punto de acceso Wi-Fi no autorizado en nuestras instalaciones, ya sea conectado por USB o Ethernet, representa un riesgo significativo para la seguridad de la red y la información.

Análisis de riesgos:

1. Acceso no autorizado a la red:
Un punto de acceso Wi-Fi no autorizado puede permitir que usuarios externos accedan a la red interna, sin autorización ni control, lo que representa un riesgo de robo de información confidencial, malware, ransomware y otras actividades maliciosas.
2. Intercepción de datos:
El atacante podría interceptar el tráfico de red, incluyendo información sensible como contraseñas, datos financieros o comunicaciones internas, poniendo en riesgo la privacidad y la seguridad de la información.
3. Ataques de denegación de servicio (DoS):
El punto de acceso no autorizado podría ser utilizado para lanzar ataques DoS contra la red principal, saturando el ancho de banda y denegando el acceso a los usuarios legítimos.
4. Suplantación de identidad (spoofing):

El atacante podría suplantar la identidad de otro dispositivo en la red para acceder a recursos específicos o realizar actividades maliciosas bajo la apariencia de un usuario legítimo.

Detección:

1. Monitorización de la red:

Es crucial implementar herramientas de monitorización que detecten la presencia de dispositivos no autorizados en la red, incluyendo puntos de acceso Wi-Fi. Se pueden utilizar herramientas como SNMP, Nmap o Wireshark para identificar dispositivos desconocidos.

2. Análisis de tráfico:

Se debe analizar el tráfico de red en busca de patrones inusuales que puedan indicar la presencia de un punto de acceso no autorizado,por ejemplo, tráfico no identificado o con direcciones MAC desconocidas.

3. Verificación física:

Realizar inspecciones físicas regulares de los puertos USB y Ethernet en los equipos de la empresa para detectar dispositivos sospechosos o no reconocidos.

Remediación:

1. Desconexión inmediata:

Al detectar un punto de acceso no autorizado, se debe proceder a su desconexión inmediata de la red, ya sea física o mediante la configuración del router o switch.

2. Investigación y análisis:

Es importante realizar una investigación para determinar el origen del punto de acceso no autorizado, el tiempo que ha estado activo y el alcance del daño potencial.

3. Implementación de medidas de seguridad:

Se deben implementar medidas de seguridad adicionales para prevenir futuros incidentes, como:

- Habilitar el filtrado MAC: Permitir solo la conexión de dispositivos con direcciones MAC conocidas y autorizadas.
- Utilizar WPA2 con AES: Establecer una configuración de seguridad robusta para la red Wi-Fi con el protocolo WPA2 y cifrado AES. Si fuera posible utilizar WPA3.
- Cambiar las contraseñas por defecto: Modificar las contraseñas de fábrica de los routers, switches y otros dispositivos de red por claves seguras y difíciles de adivinar.
- Implementar un sistema de detección de intrusiones (IDS): Instalar un sistema que detecte y alerte sobre actividades sospechosas en la red (SNORT).

Conclusión:

La presencia de un punto de acceso Wi-Fi no autorizado representa un riesgo significativo para la seguridad de la red y la información. Implementar medidas de detección y remediación proactivas es fundamental para prevenir y mitigar este tipo de amenazas.

Recomendaciones adicionales:

- Capacitar al personal: Es importante que los empleados comprendan los riesgos asociados a los puntos de acceso Wi-Fi no autorizados y cómo reportar cualquier actividad sospechosa.
- Mantener el software actualizado: Asegurar que el firmware de los routers, switches y otros dispositivos de red esté actualizado con las últimas correcciones de seguridad.
- Realizar auditorías de seguridad periódicas: Llevar a cabo auditorías regulares de la red para identificar y corregir vulnerabilidades que puedan ser explotadas por los atacantes.

- También podríamos utilizar un túnel VPN. Así se extiende el cifrado desde el cliente hasta una zona de confianza corporativa siendo protegida la información en tránsito a través de mecanismos robustos de cifrado y autenticación.

5. Modelo de seguridad