



Implemente la ciberseguridad de la red con WiFi administrado

Controles de ciberseguridad WiFi administrados

- ❑ Control de acceso a la red, elige autorizar el dispositivo o autorizar al usuario.
- ❑ Autorización de dispositivos a través de una base de datos de direcciones MAC de dispositivos, monitoreo de duplicación de MAC (MAC spoofing).
- ❑ Autorización de usuarios a través de una base de datos de contraseñas que permiten al usuario acceder desde cualquier dispositivo.
- ❑ La autenticación de usuario también se puede realizar mediante autenticación de 2 factores (código a través de texto)
- ❑ Bloquear el acceso a Internet a categorías de sitios web evaluados como dañinos (Cisco Umbrella).
- ❑ Bloquee el acceso a servicios que podrían usarse para instalar un virus troyano, por ejemplo, cuentas de correo electrónico personales.
- ❑ Supervise la red WiFi en busca de intentos de acceso no autorizado.



La tendencia posterior a la pandemia hacia el trabajo híbrido desde el hogar y la oficina ha significado que el personal haya cambiado de computadoras de escritorio con cable a computadoras inalámbricas y dispositivos móviles.

Las empresas han ampliado las redes WiFi al tiempo que reducen los requisitos de seguridad. WiFi es ahora un vector de ataque fácil tanto local como remotamente para un hacker que intenta robar datos o plantar ransomware.

Las empresas deben evaluar WiFi como parte de una evaluación de seguridad.

Managed WiFi es una tecnología que se desarrolló para controlar y monitorear el uso de redes WiFi con el fin de proteger la red WiFi del acceso de dispositivos no autorizados que pueden ser utilizados por piratas informáticos para robar información o bloquear la base de datos de la empresa mediante Ransomware.

1. EVALUACIÓN DE LA SEGURIDAD

Asegúrese de que la red Wi-Fi empresarial esté incluida en la evaluación de seguridad, considere actualizar el cifrado de WPA2 a WPA2-enterprise o WPA3 para dificultar la piratería.

2. DESPLIEGUE DE PROTECCIONES DE SEGURIDAD

Además del firewall de Internet y el filtrado de correo electrónico comercial para eliminar enlaces dañinos, considere agregar los controles de ciberseguridad de Wi-Fi administrado que se enumeran en el cuadro de la izquierda.

3. MONITOREO CONTINUO

El control de acceso WiFi administrado proporciona una visualización en tiempo real de los intentos de acceso a la red WiFi. Supervise la situación y bloquee el acceso a direcciones MAC no autorizadas que soliciten una dirección IP.

4. BENEFICIOS ADICIONALES DEL WiFi ADMINISTRADO

WiFi administrado monitoreará el rendimiento de la red WiFi y puede proporcionar una alarma de falla cuando falla cualquier dispositivo WiFi. Esto es muy importante ya que no se nota una falla en el punto de acceso inalámbrico porque el dispositivo inalámbrico se conectará a otro punto de acceso inalámbrico más alejado con una velocidad de datos más lenta. Eventualmente, los usuarios se quejarán de que la "red es lenta". La detección de fallas del dispositivo WiFi administrado identificará el dispositivo que debe ser reemplazado

Llame al 1-800-213-0106 o escriba a: support@guest-internet.com