Informe de evaluación de riesgos de seguridad

Parte 1: Selecciona hasta tres herramientas y métodos de reforzamiento a implementar
Tres de las herramientas de reforzamiento que la organización puede usar para abordar las vulnerabilidades encontradas son: 1. Implementar la autenticación de múltiples factores (MFA) 2. Establecer y aplicar políticas de contraseñas fuertes 3. Realizar el mantenimiento del firewall con regularidad La MFA requiere que los usuarios utilicen más de una forma para identificar y verificar sus credenciales antes de acceder a una aplicación. Algunos métodos de MFA incluyen escaneos de huellas dactilares, tarjetas de identificación, números PIN y contraseñas. Las políticas de contraseñas se pueden refinar para incluir reglas con respecto a la longitud de la contraseña, una lista de caracteres aceptables y un descargo de responsabilidad para desalentar el compartir contraseñas. También pueden incluir reglas relacionadas con los intentos de inicio de sesión fallidos, como que el/la usuario/a pierda el acceso a la red después de cinco intentos. El mantenimiento del firewall implica revisar y actualizar las configuraciones de seguridad regularmente para estar siempre un paso por delante de las amenazas potenciales.

Parte 2: Explica tus recomendaciones
La aplicación de la autenticación de múltiples factores (MFA) reducirá la probabilidad de que un agente de amenaza pueda acceder a una red a través de un ataque de fuerza bruta o similar. La MFA también hará que sea más difícil para las personas dentro de la organización compartir contraseñas. Identificar y verificar las credenciales es especialmente crítico entre los/las empleados/as con privilegios de nivel de administrador en la red. La MFA debe aplicarse regularmente. La creación y aplicación de una política de contraseñas dentro de la empresa hará que sea cada vez más difícil para los agentes de amenaza acceder a la red. Las reglas que se incluyan en la política de contraseñas deberán aplicarse regularmente dentro de la organización para ayudar a aumentar la seguridad de los/las usuarios/as.

El mantenimiento del firewall (cortafuegos) debe realizarse regularmente. Las reglas del firewall deben actualizarse cada vez que se produce un evento de seguridad, especialmente uno que permita el tráfico sospechoso en la red. Esta medida se puede utilizar para protegerse contra varios ataques DoS y DDoS.