Evaluación de Riesgos de Seguridad 2024-05-16 #1

GL Gráfica - San Lorenzo 3176 Eldorado

Descripción General del Reporte

Se analizará la situación utilizando el Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST CSF). El CSF es un marco voluntario que consta de estándares, directrices y mejores prácticas para gestionar el riesgo de ciberseguridad.

Se creará un reporte de evaluación de riesgos de seguridad para demostrar un enfoque proactivo de la seguridad, mejorar la comunicación y la transparencia con las partes interesadas y mejorar las prácticas de seguridad dentro de la organización.

Se identificará qué medidas de seguridad se deben aplicar en respuesta a las necesidades comerciales y se determinará cuáles son las mejores opciones disponibles en lo que respecta a la seguridad de la red.

Contexto

Se realizó un reporte de evaluación de riesgos de seguridad, como analista de ciberseguridad externo para la empresa GL Gráfica que ofrece servicios de diseño web, diseño gráfico y soluciones de marketing en redes sociales a pequeñas empresas.

La organización ha sufrido anteriormente una violación de datos, que ha puesto en peligro la seguridad de la información personal de sus clientes, como nombres y direcciones.

La organización quiere implantar prácticas sólidas de endurecimiento de la red que puedan llevarse a cabo de forma coherente para evitar ataques y violaciones en el futuro.

Como analista, al inspeccionar la red de la organización, descubrí cuatro vulnerabilidades importantes.

Las cuatro vulnerabilidades son las siguientes:

1. Los empleados de la organización comparten contraseñas.
2. La contraseña de administrador de la base de datos está configurada por defecto.
3. Los cortafuegos no tienen reglas establecidas para filtrar el tráfico que entra y sale de la red.
4. No se utiliza la autenticación multifactor (MFA).

Si no se toman medidas para solucionar estas vulnerabilidades, la organización corre el riesgo de sufrir otra violación de datos u otros ataques en el futuro.

| **Herramientas y métodos de endurecimiento para implementar** | |
| --- | --- |
| Tres herramientas de refuerzo que la organización puede utilizar para abordar las vulnerabilidades encontradas incluyen:   1. Implementación de autenticación multifactor (MFA) 2. Establecer y hacer cumplir políticas de contraseñas seguras 3. Realizar el mantenimiento del firewall periódicamente   MFA requiere que los usuarios utilicen más de una forma de identificar y verificar sus credenciales antes de acceder a una aplicación. Algunos métodos MFA incluyen escaneos de huellas dactilares, tarjetas de identificación, números PIN y contraseñas.  Las políticas de contraseñas se pueden refinar para incluir reglas sobre la longitud de la contraseña, una lista de caracteres aceptables y un descargo de responsabilidad para desalentar el intercambio de contraseñas. También pueden incluir reglas que rodean los intentos fallidos de inicio de sesión, como que el usuario pierda el acceso a la red después de cinco intentos fallidos.  El mantenimiento del firewall implica verificar y actualizar las configuraciones de seguridad periódicamente para anticiparse a posibles amenazas. | |
|

| **Recomendaciones** |
| --- |
| Hacer cumplir la autenticación multifactor (MFA) agrega una capa adicional de seguridad más allá de una contraseña. Reducirá la probabilidad de que un actor malintencionado pueda acceder a una red mediante un ataque de fuerza bruta o relacionado, ya que se requiere un esfuerzo adicional para autenticarse en más de una forma. MFA también puede reducir la probabilidad de que las personas compartan contraseñas. Dado que el destinatario de la contraseña compartida necesitaría poseer autenticación adicional además de una contraseña, MFA hace que sea menos útil compartir contraseñas, lo que hace que sea menos probable que se compartan.  Crear y hacer cumplir una política de contraseñas dentro de la empresa hará que sea cada vez más difícil para los actores malintencionados acceder a la red. Políticas como suspender la cuenta después de un cierto número de inicios de sesión pueden evitar ataques de fuerza bruta exitosos. El aumento de la complejidad de las contraseñas, la necesidad de actualizarlas con más frecuencia y el no permitir que se reutilicen también ayudan a evitar que actores maliciosos se infiltren en la red.  El mantenimiento del firewall debe realizarse con regularidad. Los administradores de red deben asegurarse de que existan reglas de firewall que reflejen los estándares más actualizados para el tráfico permitido y denegado. El tráfico procedente de fuentes sospechosas debe incluirse en una lista de tráfico denegado. Las reglas del firewall deben actualizarse cada vez que ocurre un evento de seguridad, especialmente un evento que permite el ingreso de tráfico de red sospechoso a la red. Esta medida se puede utilizar para protegerse contra diversos ataques DoS y DDoS. |