Basque CyberSecurity Centre

Manejo seguro de redes sociales corporativas

Checklist

- ☐ Abrir un servidor que escuche un puerto determinado.
- ☐ Identificar los dispositivos desde los que se administran las cuentas.
- ☐ Controlar proveedores con acceso a las cuentas.
- ☐ Monitorizar continuamente las cuentas de redes sociales de la organización para detectar comportamientos inusuales.
- ☐ Mantener concienciadas a las personas que administren las cuentas, haciéndolas conscientes del papel que juegan en la reducción de riesgos.
- ☐ Establecer un plan de respuesta a incidentes:
  - ☐ Incluir acciones esperadas a tomar ante determinadas situaciones, como accesos o publicaciones no autorizados, dispositivos comprometidos y la divulgación de comunicaciones privadas.
  - ☐ Incluir orientación sobre cómo reportar un incidente a las autoridades competentes.
  - ☐ Incluir información de contacto de las plataformas de redes sociales adecuadas en caso de que se produzca una infracción.
- ☐ Gestionar de forma segura las cuentas y credenciales:
  - ☐ Utilizar la autenticación multifactor (MFA).
  - ☐ Limitar las personas con control administrativo.
  - ☐ Si la red social o la herramienta utilizada para gestionarla lo permite, que cada usuario acceda con sus propias credenciales.
  - ☐ Comprobar con regularidad la lista de personas con rol de administración. Revisar con más detalle en momentos de mayor sensibilidad para la organización.
  - ☐ Analizar los eventos de inicio y cierre de sesión, cambios de permisos o cualquier otra actividad inusual.
  - ☐ Limitar el acceso de aplicaciones de terceros a las cuentas de redes sociales, ya que pueden solicitar privilegios excesivos y exponer información privada.
  - ☐ Comprobar que ninguna aplicación innecesaria pueda acceder a las cuentas de la organización.
  - ☐ Gestionar los tokens que utilizan las API de forma segura, ya que podrían permitir interactuar con la cuenta sin requerir nombres de usuario o contraseñas.
  - ☐ Asegurar que las contraseñas y los tokens siguen las mejores prácticas en cuanto a longitud y complejidad.
  - ☐ Mantener una política para la modificación periódica de contraseñas y tokens. No compartir ni escribir las credenciales.
  - ☐ Modificar las credenciales de inmediato si existe algún indicio o sospecha de que una contraseña o un token puede haber sido comprometido.
- ☐ Definir y mantener una política de redes sociales que considere al menos las cuestiones planteadas en este documento y cualquier otra protección que la organización considere necesaria para ayudar a proteger las cuentas de redes sociales

Para conocer más información sobre cómo protegerte puedes visitar **https://www.basquecybersecurity.eus/es/**

Si necesitas asesoramiento profesional, puedes consultar el catálogo de proveedores de ciberseguridad de Euskadi disponible en la web.