Universidad Francisco de Vitoria
Centro de Documentación Europea
UFV Madrid

Diseño de sistemas de cumplimiento normativo

Héctor Ramírez López

Índice

Caso 1-Ataque externo (Mitm-Man in the middle)

1.1 Analizar Incidente

Como CCO, la tarea inicial sería comprender que un ataque Man in the Middle (MitM) consiste en la interceptación de las comunicaciones entre dos individuos sin que ellos lo sepan, este tipo de ataque puede poner en riesgo información crítica, como datos personales, financieros y empresariales lo que genera problemas para la privacidad y la integridad de la información.

1.2 Normativa a aplicar

Como CCO es esencial conocer y asegurar el cumplimiento de las normativas que aseguran la protección de datos y la seguridad de la información en este caso las principales normativas aplicables serían:

- **RGPD (Reglamento general de protección de datos)**
  - **Notificación de brecha de seguridad (art.33)**
    En caso de que se vean afectados datos personales como información bancaria o datos sensibles de los usuarios el RGPD establece que hay que informar a la Autoridad de Protección de Datos en un plazo de 72 horas. Esto debe contener un relato preciso del incidente, los datos implicados y las acciones correctivas que se han tomado.

  - **Notificación a los afectados (art.34)**
    Si el incidente supone un grave riesgo para las personas afectadas como el robo de datos financieros, la entidad debe comunicarlo a los afectados de forma clara e indicarles las medidas que deben seguir para reducir el efecto (como actualizar contraseñas y vigilar sus cuentas bancarias)

- **ENS (esquema nacional de seguridad)**
  - **Confidencialidad de la información**
    El ENS pide que las comunicaciones sean seguras y estén bien protegidas. Un ataque MitM puede significar que el cifrado que se ha establecido pueden no ser suficiente.

  - **Plan de respuesta**
    El ENS pide que las empresas tengan un plan para responder a incidentes con el objetivo de reconocer, manejar y reducir los peligros que surgen de un ataque a la seguridad.

- **ISO 27001**
  - **Gestión de riesgos:**
    Indica que hay que tener un procedimiento para examinar y manejar los peligros de seguridad. Un ataque de tipo MitM tenía que haber sido detectado en la evaluación de riesgos.

  - **Controles de Acceso y Seguridad en las Comunicaciones**:
    El cifrado y la verificación de las comunicaciones sirven para prevenir ataques como este.

1.3 Medidas que se deben tomar

Como CCO debo asegurar que la empresa respete la normativa legal. Las medidas a implementar son tanto para resolver el problema como acciones proactivas para que no vuelva a pasar. Aquí se explican las principales acciones a realizar:

- **Notificación del incidente**: a la autoridad de protección de datos dentro de 72 horas.
- **Notificación a los afectados**: si se ha expuesto información sensible.
- **Auditorias**: después del ataque se debería realizar una auditoría interna para evaluar si las medidas de seguridad actuales son efectivas.

Caso 2-Ataque interno (insider)

2.1 Analizar Incidente

Un trabajador ha robado información protegida, aunque los datos están protegidos el hecho de que el trabajador con acceso a esta información haya cometido este acto genera problemas sobre las políticas de acceso, la seguridad de los datos y las obligaciones legales de la empresa como CCO es esencial tratar este incidente desde la normativa y el cumplimiento.

2.2 Normativa a aplicar

- **RGPD (Reglamento general de protección de datos)**
  - **Principios de tratamiento de datos (art.5)**
    El robo de información cifrada puede implicar una violación del principio de integridad y confidencialidad.

  - **Seguridad del tratamiento (art.32)**
    establece la obligación de aplicar medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos personales.

- **Ley de delitos informáticos**
  - **Responsabilidad penal**
    Si el robo de la información infringe la ley penal (delitos informáticos), el empleado podría enfrentarse a acciones legales penales.

- **ISO 27001**
  - **Control de acceso (A.9.1)**
    establece que los accesos a los datos deben estar restringidos según las necesidades laborales y que debe garantizarse el principio de mínimo privilegio.

2.3 Medidas que se deben tomar

Como CCO la organización debe tomar una serie de medidas clave para manejar el robo de información cifrada de manera efectiva, garantizar el cumplimiento de las normativas legales y normativas (como el RGPD y la ISO 27001):

- **Notificación del incidente**: a la autoridad de protección de datos dentro de 72 horas.
- **Notificación a los afectados**: si se ha expuesto información sensible.
- **Auditorias**: después del ataque se debería realizar una auditoría interna para evaluar si las medidas de seguridad actuales son efectivas.
- **Investigación forense:** Una vez detectado el robo de información cifrada hay que realizar un análisis forense para determinar el alcance del incidente y las causas que permitieron el acceso no autorizado.
- **Revisión de control de acceso**: Es necesario implementar medidas para reforzar la protección de los datos cifrados.
- **Acciones legales**: Si se confirma que el empleado ha actuado de forma malintencionada y ha violado las políticas de la empresa deben tomarse medidas disciplinarias y acciones legales.

Caso 3-Datos personales

Como CCO la decisión de borrar todos los datos para evitar gestionar su tratamiento posteriormente entra en conflicto con el Reglamento General de Protección de Datos (RGPD)

- **RGPD**
  - **Principio de limitación del tratamiento (art.5.1. e)** establece que los datos personales deben ser almacenados durante el tiempo necesario para los fines para los que se han recogido (Si se borra todo sin tener en cuenta el propósito original del tratamiento y la duración mínima de conservación no se estaría cumpliendo)

3.1 Medidas que se deben tomar

- **Notificación del incidente**: a la autoridad de protección de datos dentro de 72 horas.
- **Notificación a los afectados**: si se ha expuesto información sensible.
- **Responsabilidad proactiva**
- **Auditoria inmediata**
- **Revisión de control de acceso**: Es necesario implementar medidas para reforzar la protección de los datos cifrados.

Universidad Francisco de Vitoria
Centro de Documentación Europea
UFV Madrid