Universidad Francisco de Vitoria
Centro de Documentación Europea
UFV Madrid

UD01-Tarea-1-3

Héctor Ramírez López

INDICE

1. Comprensión del problema y puesta por escrito del mismo

Air Europa sufrió un ataque en el que los atacantes lograron acceder al entorno de pagos de su web, como consecuencia robaron varios datos como:

- datos de tarjetas de crédito de los clientes: número de tarjeta, fecha de caducidad y código CVV.
- Air Europa informó que podrían haberse comprometido datos personales de los clientes: nombres, fechas de nacimiento, nacionalidad, pasaporte y otros documentos de identidad.
- La empresa comunicó que no hay evidencias de que los datos robados se hayan usado para fraude.
- Es posible que el origen del ataque esté vinculado a un ataque de “skimming” en la web o a modificación de código en la pasarela de pago.

1.1 Saber y conocer lo qué es opinión de los medios de lo qué es problema.

Después de buscar información nos damos cuenta de las distintas opiniones de los medios, El Confidencial califica el ataque como **“gravísimo”** al haberse filtrado datos de tarjetas, incluidos los CVV, lo que es altamente sensible y **“casi impensable”** en una empresa que dice cumplir estándares de tarjeta de pago, otro medio dice que **“más de 100.000 clientes”** podrían estar afectados lo que amplifica la dimensión del problema. En Alemania algunos medios dicen que alrededor de **110.000 datos de tarjetas** habrían sido extraídos y que las asociaciones de consumidores critican que Air Europa no había adoptado suficientemente medidas antes del incidente, también la empresa indico a sus clientes que bloquearan sus tarjetas de crédito.

1.2 Soluciones adoptadas por Air Europa.

Las soluciones tomadas por Air Europa fueron las siguientes:

- Air Europa informó a los clientes afectados y les recomendó que cancelaran o bloquearan sus tarjetas bancarias para prevenir fraudes.
- La empresa comunicó que había “bloqueado la brecha de seguridad” y que sus sistemas estaban funcionando con normalidad.
- Se notificó a las entidades bancarias emisoras y según algunos informes la empresa contrató empresas externas para realizar análisis forenses del incidente.
- La empresa emitió nuevas comunicaciones para informar que también podrían estar comprometidos otros datos personales, no solo tarjetas.

2. Propuestas de acción como ComplianceOfficer.

Como Compliance Officer de Air Europa, estas serían mis propuestas

2.1 Alternativas.

Llevar a cabo una evaluación completa de la seguridad y el cumplimiento (**esto conlleva el rediseño de la estructura de pagos, la división de redes, la sustitución de la pasarela de pago, la certificación de cumplimiento con PCI-DSS y auditorías de terceros)** más una mejora en la comunicación pública para restaurar la confianza.

2.2 Fortalezas debilidades.

- **Fortalezas**: más robusta, mayor mitigación del riesgo a largo plazo puede restaurar reputación.
- **Debilidades**: costosa y mayor tiempo de implementación.

3. Resolución como ComplianceOfficer.

Como *Compliance Officer* de Air Europa la resolución del incidente requiere el uso de herramientas tanto técnicas como organizativas para garantizar el cumplimiento normativo y fortalecer la seguridad de la información.

3.1 Herramientas a utilizar.

- **RGPD**: para aplicar medidas técnicas y organizativas adecuadas y garantizar la notificación a la AEPD en un plazo máximo de 72 h.
- **LOPDGDD**: es para la adaptación del RGPD a la normativa española especialmente en los derechos de los afectados.
- **PCI-DSS:** es un cumplimiento obligatorio para las empresas que procesan pagos con tarjeta.
- **ISO 27001 e ISO 27701**: Es un marco de referencia para la gestion de la seguridad y privacidad de la información.

3.2 Medidas.

- **Revisión de la arquitectura de red y separación**: separar los entornos de desarrollo, pruebas y producción.
- **No almacenar CVV ni información sensible de pago:** cumpliendo estrictamente con PCI-DSS.
- **Implantación de cifrado completo:** para los datos personales y financieros.
- **Certificación externa PCI-DSS e ISO 27001:** para demostrar el cumplimiento ante reguladores y socios comerciales.
- **Implementar un SOC (centro de operaciones):** interno o contratado para la monitorización 24/7.
- **Programa de concienciación:** En ciberseguridad para todos los empleados.
- **Auditorías anuales externas:** para comprobar que toda valla bien.
- **Creación de un Comité de Seguridad de la Información:** con representación del área técnica, legal y de cumplimiento.
- **Contratación de un seguro de ciber-riesgos:** que cubra costes de respuesta, recuperación y sanciones regulatorias.

3.3 Mejoras respecto a las soluciones adoptadas.

Aspecto	Medida actual	Mejora propuesta
Gestión de incidentes	Comunicación a clientes tras detectar la brecha.	Establecer un plan de respuesta proactivo y formación interna.
Protección de datos	Bloqueo de la brecha y análisis forense.	Certificación PCI-DSS e implementación de cifrado.
Comunicación	Aviso general a los clientes.	Comunicación transparente, implementar canales de ayuda y seguimiento personalizado.
Reputación	Defensa pública limitada.	Publicación de un informe de ciberseguridad y auditorías externas.
Normativa	Cumplimiento básico del RGPD	sistema de cumplimiento integral y preventivo

4. Coordinación con la parte de Tecnología.

Como *Compliance Officer* mi función principal tras el incidente es coordinar las acciones con el departamento tecnológico para garantizar que todas las medidas adoptadas cumplen con el RGPD y los estándares de seguridad aplicables (como PCI-DSS).

4.1 Insiders.

En el caso de los insiders, se tiene que trabajar con el CISO y el equipo de IT para revisar los registros de acceso y determinar si existió participación de personal interno. Se debería aplicar el principio de *mínimo privilegio,* monitorización para prevenir y se debe implementar la formación de los empleados en seguridad y protección de datos para reducir riesgos derivados del error humano.

En este caso no hubo ataque por parte de insiders.

4.2 Outsiders.

Respecto a los outsiders, se trabajará con los equipos técnicos y las autoridades para identificar el ataque utilizado por los ciberdelincuentes externos. En este caso se reforzo la seguridad, se realizaron auditorías forenses, y se verificó el cumplimiento del estándar **PCI-DSS**, dado que el ataque afectó a datos de tarjetas de crédito. También se revisaron los contratos con proveedores externos para garantizar que todos aplicaran las medidas de seguridad adecuadas y notificaran incidentes de inmediato.

En este caso el ataque fue realizado por outsiders.

4.2 Coordinación con el jefe del Dato (CDO).

Tras el ciberataque sufrido por Air Europa, mi responsabilidad como *Compliance Officer* seria coordinarme con el **jefe del Dato (CDO)** para evaluar la magnitud del robo de información, identificar los tipos de datos comprometidos, determinar su ubicación actual y analizar el impacto sobre los clientes afectados.

4.2.1 ¿Robo de datos?

Si hubo robo de datos

4.2.2 Datos personales.

Sí, el ataque afectó principalmente a los datos personales y financieros de clientes, concretamente a la información de las tarjetas de crédito y débito utilizadas en el sistema de pagos.
Esto supone una violación de los artículos **32 y 33 del RGPD**, relacionados con la seguridad del tratamiento y la obligación de notificar brechas de datos personales.

4.2.3 Datos empresariales.

No se detectó acceso directo a información corporativa confidencial (como contratos, acuerdos comerciales o información interna). Durante la investigación se vigiló los sistemas críticos de gestión interna y se revisaron posibles movimientos inusuales en bases de datos de reservas y proveedores.

4.2.4 ¿Dónde están? Investigación.

- Se realizó una **investigación forense** para rastrear el punto de acceso y determinar si los datos robados habían sido exfiltrados o publicados en foros delictivos.
- Se notificó el incidente a la **Agencia Española de Protección de Datos (AEPD)** y a las **entidades bancarias afectadas**, siguiendo los plazos y procedimientos del RGPD.
- Se identificó que los datos sustraídos provenían del **entorno de la pasarela de pagos**, lo que sugiere una brecha en la seguridad de ese sistema o de un proveedor externo vinculado.
- Se implementaron medidas para **revocar accesos, bloquear flujos de datos vulnerables y reforzar los controles de seguridad** en la infraestructura afectada.

4.2.5 Análisis del impacto de los datos vs clientes.

El robo de datos personales tiene un impacto sobre los clientes principalmente:

- **Riesgo financiero**: se pueden usar en un fraude las tarjetas robadas.
- **Riesgo de reputación**: pérdida de confianza en los sistemas de pago de la compañía.
- **Riesgo de privacidad**: se expone información que puede identificar a los pasajeros.

4.3 Coordinación con el jefe de personal (HR).

Tras el ciberataque sufrido por Air Europa, resulta fundamental coordinarme con el **jefe de Personal** para abordar cualquier implicación del incidente desde el punto de vista del **personal interno**, tanto para investigar posibles riesgos como para garantizar la protección de los datos de los empleados.

4.3.1 Origen del ataque.

- El ataque fue realizado por **outsiders (agentes externos)**, no por personal interno.
- Sin embargo, parte de la investigación con HR consistió en revisar **accesos y responsabilidades del personal interno** para descartar cualquier participación interna (insiders) que pudiera haber facilitado el ataque.
- Esto incluyó la revisión de logs de accesos a sistemas críticos, permisos y políticas de control de cuentas de usuario.

4.3.2 Información personal (circunstancias).

- Durante la investigación, se revisaron datos de los empleados, principalmente aquellos con acceso a sistemas críticos.
- Se evaluó que no hubo exposición de datos sensibles de empleados (números de DNI, nóminas, datos médicos, etc.) y que el ataque afectó únicamente a datos de clientes.
- Como Compliance Officer, trabajé con HR para garantizar confidencialidad y que la revisión del personal se realizara cumpliendo el **RGPD** y la **LOPDGDD**, evitando cualquier filtración de información interna.

4.3.3 Formación.

Coordiné junto con HR un programa de formación obligatoria sobre ciberseguridad, protección de datos y responsabilidad legal para todos los empleados, especialmente aquellos con acceso a sistemas críticos.

La formación incluyó:

- Prevención de phishing y ataques de ingeniería social.
- Buenas prácticas para el manejo de información sensible de clientes y la empresa.
- Procedimientos de respuesta ante incidentes de seguridad.

4.3.4 Documento ético y responsabilidad.

Se reforzó la firma y aceptación de un documento de ética y responsabilidad para todos los empleados que incluyo:

- Responsabilidad personal en el manejo seguro de información interna y de clientes.
- Compromiso de cumplimiento del RGPD, PCI-DSS y políticas internas de seguridad.
- Responsabilidad de informar sobre incidentes o actitudes sospechosas

  Este documento funciona como una medida preventiva para disminuir riesgos de empleados internos y aumentar la cultura de cumplimiento dentro de la organización.

4.4 Coordinación con el jefe de marketing (CMO).

Tras el ataque a Air Europa, la coordinación con el área de Marketing y Comunicación fue fundamental para gestionar la información pública sobre el incidente, equilibrando transparencia, cumplimiento legal y protección de la reputación de la empresa.

Como Compliance Officer, definí las siguientes reglas para cualquier comunicación externa:

- **Cumplimiento normativo:**
    a. Toda información debe respetar el RGPD y la LOPDGDD, evitando divulgar datos personales de clientes afectados.
    b. Las declaraciones públicas deben alinearse con los requisitos de notificación de brechas de seguridad ante la AEPD.
- **Transparencia controlada:**
    a. Se debe informar a los medios de manera veraz, evitando generar alarma innecesaria.
    b. Se prioriza la información general sobre el incidente (tipo de ataque, medidas adoptadas, canales de asistencia al cliente), sin revelar vulnerabilidades técnicas que puedan ser explotadas.
- **Coherencia corporativa:**
    a. Mensajes alineados con los comunicados oficiales del CEO.
    b. Coordinación estrecha con IT y DPO para confirmar que lo comunicado refleja la realidad del incidente y la situación legal.

Universidad Francisco de Vitoria
Centro de Documentación Europea
UFV Madrid