Seguridad Forense

- La clave conservar la integridad de los datos y no contaminarlos.
- Esto es porque el profe dijo que quiere que ojalá pueda venir alguien a dar una clase de esto.

Token

- Ver como se usan en un ámbito transaccional, supongo que relacionado a los bancos, ya que él tiene experiencia ahi.

Caso: Aplicar la matriz de requerimientos de seguridad en un SaaS

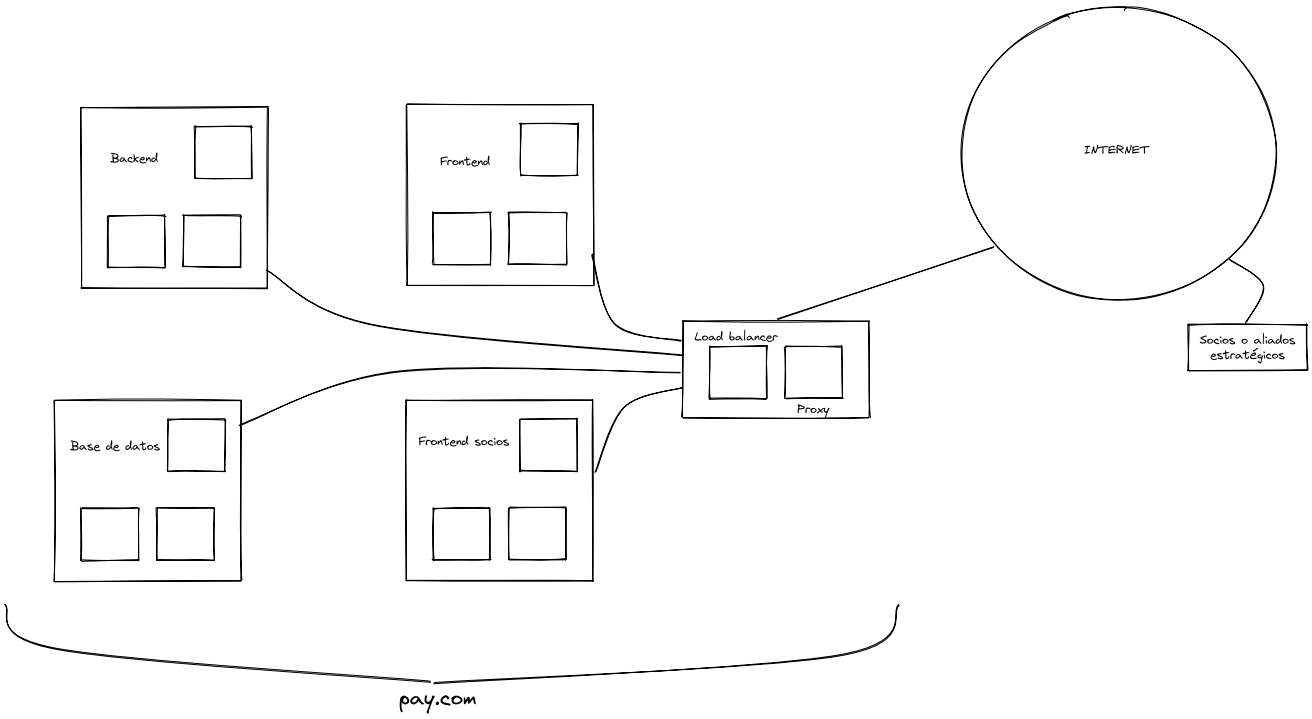
1. ¿El proveedor lleva a cabo regularmente evaluaciones de riesgo sobre sus instalaciones y servicios para evitar posibles incidentes de seguridad asociados a vulnerabilidades, fallas de proceso o incumplimientos legales, regulatorios y/o contractuales?
2. ¿El proveedor de servicios realiza regularmente evaluaciones internas sobre sus políticas, procedimientos y disponibilidad de sus métricas de control?
3. ¿El proveedor realiza las auditorías periódicas de sus procesos internos?
4. ¿El proveedor cuenta con reportes SOC 1 Tipo 2 (ISAE 3402/SSAE 18) u otros informes de auditoría similares hechas por terceros? Especificar cuáles.
    1. ***Check***: artículo sobre SOC (SOC).
    2. ***SOC***: surge por los fraudes esos de hace banda (creo que fue el escándalo de Lockheed Corporation). Se alinea con la ISO 27001.
    3. ***ISO 17799***: relacionada con la ISO 27001, da las recomendaciones concretas para técnicas de seguridad, tanto física, de la información y las personas. Acá es donde habla de **cómo** se **implementa** la 27001. ISO 17799:2007
5. ¿El proveedor posee certificación ISO 27001? De ser así, especifique declaración de alcance.
    1. **SLA**: Service Level Agreement. → Un contrato que fija qué nivel de servicio va a tener asegurado el cliente/usuario, que soporte va a tener y que van a haber métodos para poder cumplir con dicho nivel. Se tratan requerimientos como la disponibilidad o velocidad o almacenamiento, etc.
    2. Desde el área de sistemas que servicios le brinda a cada uno de las demás gerencias.
        1. Data de reportes (BI) → Ventas.
        2. Gestor curriculums → RRHH.

6. ¿El proveedor realiza con regularidad pruebas de penetración de sus aplicaciones en la nube, según lo prescrito por las mejores prácticas de industria?
7. ¿El proveedor permite que sus clientes realicen evaluaciones de vulnerabilidad independientes?
8. ¿El proveedor tiene la capacidad de segmentar lógicamente o cifrar los datos del cliente de tal manera que los datos puedan ser accedidos solo por ese cliente, sin tener acceso inadvertido a los datos de otro cliente?
9. ¿El proveedor tiene la capacidad de segmentar y recuperar lógicamente los datos de un cliente específico en caso de una falla o pérdida de datos? **HASTA ACÁ LLEGAMOS**
10. En caso de corresponder con el servicio que brinda ¿El proveedor cumple requisitos legales y regulatorios tales como (p.e., EU Data Directive, PCAOB AS5, PCI DSS, HIPAA, LPDP, GDPR)? Cuáles?
11. ¿El proveedor tiene políticas y procedimientos que describen qué controles existen para proteger la propiedad intelectual de los Clientes?
12. ¿El proveedor puede proporcionar el storage de los datos en un país/región a acordar con el cliente?
13. ¿El proveedor tiene la capacidad de acordar esquemas de retención que se adecuen a las políticas de retención de datos de los clientes?
14. ¿El proveedor acepta una cláusula en el contrato que especifique el mecanismo de entrega de los datos del cliente al mismo ante necesidades puntuales o decisión del contrato, manteniendo la integridad de los mismos, así cómo el borrado de la información en sus sistemas al finalizar el servicio?
15. ¿El proveedor posee algún mecanismo o proceso para evitar la fuga de información, detectar y prevenir violaciones de datos, filtraciones o destrucción no deseada de datos del cliente?

Cuando te auditan lo primero por lo que parten es entender cuál es tu negocio, qué haces y cuál es tu objetivo.

Caso 'pay.com'

Infraestructura:



Cosas a ver en una auditoria de seguridad de comunicación: Integridad, confidencialidad, autenticidad y no repudio.

- Ver https.
- Ver qué onda los certificados.
  - ¿Son emitidos por pay.com?
  - ¿Quién es su versificador?
  - ¿Qué algoritmos usa?
- Ver puertos abiertos.
- Inyección SQL.
- Ver comunicación de la API.
- Certificación PCI-DSS (***P**ayment **C**ard **I**ndustry **D**ata **S**ecurity **S**tandard*) → se exige para operar en bolsa y a las empresas que guardan datos de tarjetas. (PCI DSS)
- Principios de mínimo privilegio.
- Mapas de infraestructura (como están los microservicios desplegados).
- Estrategias de escalabilidad (documentación) → Crecimiento elástico.
- Subdivisión de redes.
- Staging → dev, test, prod.
- Analizar políticas de acceso de la información.
  - ¿La lógica programada hace que se cumpla?
- Trazabilidad → Logs y su control de integridad (del log).

Investigar

- SOC2 aplicado a la nube → SOC
- API vs WebService → API vs WebService
- ¿Cuánto sale un certificado SSL/TLS? → Dependiendo del agente emisor

    - GoDaddy: $1906 - $17820.
    - DonWeb: $100.
    - Puede ser gratis → emitido por uno mismo.
- PCI DSS → PCI DSS

Continúa en 2022-09-30