Itamhar Daniel Barrios Castro

Actividad 1: Análisis de brechas de datos **UNIDAD 2**

Existen varios casos de fallas de grandes corporaciones en la protección de la información como son:

1. Falla de Sony PlayStation network (Abril de 2011)

2. Drobpox (Agosto de 2012)

3. Ashley Madison (2015)

4. UIDAI (Aadhaar)

Consultar en internet qué sucedió en cada caso y discutir las siguientes preguntas:

¿Qué información se expuso?

En abril de 2011, la **PlayStation Network (PSN)** de Sony fue víctima de un ciberataque que comprometió la información de millones de usuarios. El 20 de abril, Sony suspendió todos los servicios de PSN y Qriocity en todo el mundo debido a una intrusión externa. Se estima que la filtración afectó a 77 millones de usuarios, incluyendo nombres, direcciones y posiblemente datos de tarjetas de crédito.

En agosto de 2012, **Dropbox** experimentó una brecha de seguridad que comprometió las contraseñas de más de 68 millones de usuarios. Los piratas informáticos robaron las credenciales de un empleado, lo que permitió el acceso a las cuentas de los usuarios. La compañía confirmó la brecha y recomendó a los usuarios que cambiaran sus contraseñas

En julio de 2015, el sitio web de citas **Ashley Madison** (plataforma para relaciones extramatrimoniales) fue hackeado por un grupo llamado "The Impact Team". Los atacantes robaron 37 millones de registros de usuarios, incluyendo datos sensibles, y los filtraron públicamente en agosto de 2015 bajo la amenaza de cerrar el sitio. La filtración expuso no solo información personal, sino también prácticas engañosas de la empresa.

Aadhaar es el mayor sistema de identificación biométrica del mundo, gestionado por la Autoridad de Identificación Única de la India (UIDAI). Para 2018, almacenaba datos de 1,100 millones de indios. Durante este periodo, los datos confidenciales y confidenciales de cientos de millones de personas fueron descifrados y expuestos, posteriormente agregados a diversas listas de la dark web para su venta. Ciberataques maliciosos y protocolos de ciberseguridad laxos provocaron nuevamente filtraciones masivas de información personal en 2018, la mayor de las cuales fue la de Aadhaar, en India.

¿Cómo afectó la filtración a la empresa y a sus clientes?

Empresas:

- Pérdidas económicas de $171 millones por multas y compensaciones. Sony PlayStation
- Suspensión del servicio durante 23 días, afectando ventas y reputación. Sony PlayStation
- Demandas legales colectivas por negligencia en protección de datos. Sony PlayStation
- Obligación de resetear 68 millones de contraseñas. Dropbox.
- Daño reputacional al admitir el uso de hashing débil (SHA-1). Dropbox.
  Multa de $11.2 millones por prácticas engañosas (perfiles falsos). Ashley Madison

Itamhar Daniel Barrios Castro

- Pérdida del 80% de sus usuarios tras el escándalo. Ashley Madison
- Crisis de confianza en el sistema de identificación nacional. UIDAI (Aadhaar).
- Inversión de $1,100 millones en reparaciones. UIDAI (Aadhaar).

Clientes:

- Robo de identidades y fraudes con tarjetas de crédito vinculadas a PSN. Sony PlayStation
- Ataques de phishing masivos aprovechando los correos expuestos. Sony PlayStation
- Cuentas vulnerables a ataques de fuerza bruta. Dropbox.
  Reutilización de contraseñas expuestas en otros servicios (efecto dominó). Dropbox.
- Extorsiones y chantajes con datos íntimos. Ashley Madison
- Casos reportados de divorcios y suicidios (ej: pastor John Gibson). Ashley Madison
- 8,000 casos de fraudes con subsidios gubernamentales. Aadhaar
- Robo de fondos bancarios vinculados a Aadhaar (ej: Vijay Mandloi perdió ₹45,000).

¿Qué impacto tuvo la perdida de datos?

- Social: Desconfianza en plataformas de gaming en línea. Sony PlayStation
- Legal: Multada por violar leyes de protección de datos en EE.UU. y la UE. Sony PlayStation
- Técnico: Reveló la falta de cifrado en contraseñas y datos financieros. Sony PlayStation
- Técnico: Demostró los riesgos de algoritmos de hashing obsoletos. Dropbox.
- Legal: Dropbox firmó un acuerdo con la FTC para mejorar su seguridad. Dropbox.
- Ético: Debate global sobre privacidad en plataformas sensibles. Ashley Madison
- Legal: Nueva regulación en Canadá (Ley PIPEDA) para protección de datos. Ashley Madison
- Social: Protestas masivas contra la obligatoriedad de Aadhaar.
- Técnico: Exposición de datos biométricos irrevocables (huellas/iris). Aadhaar.

¿Qué se podía hacer para evitar tales fallas en los datos?

Para sony

- Implementar cifrado AES-256 para todos los datos sensibles.
- Segmentar redes internas para aislar bases de datos críticas.
- Auditorías de seguridad para detectar vulnerabilidades.

Para Dropbox

- Usar bcrypt o PBKDF2 para hashing de contraseñas.
- Implementar autenticación multifactor (MFA) obligatoria.
- Auditorías de seguridad para detectar vulnerabilidades.

Para Ashley Madison

- Cifrado de extremo a extremo para mensajes y perfiles.
- Eliminar datos antiguos (principio de mínima retención).

Para UIDAI (Aadhaar).

- Tokenización en lugar de almacenar biométricos crudos.
- Arquitectura zero-trust para limitar accesos internos.
- Tokens y APIs con autenticación estricta.
- Auditorías de seguridad para detectar vulnerabilidades.