Alcune analisi tecniche su casi di data breach

Prof. Antonio Lioy

< lioy @ polito.it >

Politecnico di Torino

Dip. Automatica e Informatica

Statistiche sui primi mesi di GDPR

- **(source: DLA Piper)**
- **dati del periodo da 25/5/2018 (entrata in vigore GDPR) a International Data Protection Day 28/1/2019**
- **notifiche totali**
  - in testa: NL, DE, UK con 15.400, 12.600 e 10.600
  - Italia = 610
  - in coda: LI, IS, CY con 15, 25 e 35
- **notifiche pro-capite (#breach per 100.000 persone)**
  - in testa NL, IE, DK con 89.8, 74.9 e 53.3
  - in coda: GR, IT, RO con 0.6, 0.9 e 1.2
- **dati non forniti da SK, BG, HR, EE, LT**

Hospital do Barreiro

- **ottobre 2018, 400.000 Euro di multa**
- **una delle prime grosse multe GDPR**
- **dati sanitari dei pazienti accessibili a tutti gli utenti del sistema IT, non solo ai medici**
  - 985 utenti con accesso ai dati
  - … ma solo 269 medici!
- **ispezione, non data breach**
  - insufficiente sistema di autorizzazione
  - carenze nel sistema di creazione degli account (richiesta via mail senza ulteriori controlli)
  - nessuna indicazione dei ruoli ospedalieri dell'utente

Equifax

- **luglio 2019, multa di 575-700M $ da FTC a Equifax**
  - per non avere preso misure di sicurezza adeguate
  - "failure to take reasonable steps to secure its network”
- **data breach di mag'17**
  - milioni di cittadini USA, UK e CA = multa anche da UK
  - Social Security Number, data di nascita e record di pagamenti … utili per furto d'identità
- **“This settlement requires that the company take steps to improve its data security going forward, and will ensure that consumers harmed by this breach can receive help protecting themselves from identity theft and fraud”**

British Airways

- **21/8-5/9/2018 attacco al sistema IT di British Airways**
- **copiati dati personali e finanziari relativi a 380.000 transazioni di acquisto**
- **denuncia dell'accaduto entro 24 ore**
  - è in accordo col GDPR ma è sufficiente?
- **un'intrusione informatica è sempre segno di una debolezza del sistema**
  - errata progettazione (security by design!)
  - … o errata gestione (stato dell'arte!)

Marriott: un'eredità scomoda

- **dal 2014 al 10 settembre 2019**
- **stima dei dati copiati**
  - 383 M di record personali di ospiti in chiaro
  - 5,25 M di passaporti in chiaro e 20,3 M cifrati
  - 8,6 M di carte di credito (cifrate)
- **accesso permanente al DB di Starwood, catena acquisita da Marriot nel 2016 anche per i suoi clienti**
- **lezione da imparare: in un'acquisizione, la "due diligence" richiede di valutare anche la sicurezza dei dati e le relative modalità di gestione**
- **… per evitare di comprare anche un APT**

Unicredit

- **accesso non autorizzato a tre milioni di dati di clienti italiani**
- **dati in un file generato nel 2015 (!)**
  - nome, cognome, mail, telefono, indirizzo
  - non intrinsecamente critici … ma sfruttabili per attacchi fingendo di essere la banca (perché a conoscenza di tali dati)
- **evento scoperto ad ott'19 da analisi del dark web**
  - clienti prontamente informati in modo dettagliato
  - … ma nessuna informazione su cause e rimedi
  - … è una buona strategia?

Un ministero italiano

- **ottobre 2019**
- **codice fiscale, mail, numero di cellulare e CV di un gruppo di esperti raccolti in un albo online**
  - accessibile a chiunque
  - senza il consenso degli interessati
  - documento di consenso non più disponibile
  - … ma numeri di cellulare rimossi dal 7/11/2019
- **anche se c'era il consenso bisogna sempre pensare a proporzionalità, finalità e minimizzazione dei dati**

Un po' di tecnologia

- **FIDO = Fast IDentity Online**
- **autenticazione forte:**
  - basata su firma digitale (sfida asimmetrica)
  - … con unlinkability (!) perché usa una chiave diversa per ogni sito web su cui l'utente è registrato
- **con supporto (opzionale) per biometria**
  - privacy perché biometria locale del dispositivo utente
- **anti-phishing (no fake server, no MITM)**
  - la firma include il nome del server a cui è destinata
- **anti-replay**
  - la firma include i dati della transazione