DATA BREACH

difficoltà pratiche di una procedura apparentemente semplice

Leader

Marta Colonna

(DPO del Team per la Trasformazione Digitale
della Presidenza del Consiglio dei Ministri)

Part one
- *Use Case*

Part two
- *Problematiche principali*

Part three
- *Tips*

Part four
- *Risultanze emerse*

Part One

USE CASE

DP innovation

Caso 1: Data Breach & social engineering

Misure di sicurezza tecniche vs organizzative

Anche quando il sistema centrale è protetto e sicuro, si possono verificare violazioni per l'inosservanza da parte di chi ne ha accesso di alcune regole basilari sulla sicurezza. Il rischio aumenta quanto più il sistema è «condiviso». Quali misure adottare per prevenire il rischio?

Caso 2: Data Breach & Vulnerability Assessment

Accesso autorizzato vs accesso abusivo

Lo svolgimento di vulnerability assessment risulta essere un efficace strumento di protezione dei sistemi informatici. Ma può esserci un accesso «abusivo» e al tempo stesso «autorizzato»?

Part Two

PROBLEMATICHE PRINCIPALI

DP innovation

- **Case 1**: Come individuare misure organizzative efficienti? Le nomine a incaricato, i webseminar, i corsi tailorizzati per dipartimento, sanzioni disciplinari. Come responsabilizzare e diffondere la cultura della privacy e della cybersecurity?

- **Case 2**: Come gestire attività di vulnerability assessments in conformità con il GDPR? Ambienti di test, test in locale, programmi che prevedono la previa registrazione dei ricercatori?

Part Three

TIPS

DP innovation

Part Three| Tips

- Provvedimento del Garante Privacy n. 106 del 30 aprile 2019
- Cybersecurity act
- Guidelines on Personal data breach notification under Regulation 2016/679 WP250
- Personal Data breaches Information Commissioner's Office

Part Four

RISULTANZE EMERSE

DP innovation

Part Four| Risultanze emerse

Misure di sicurezza tecniche vs organizzative

- ✓ Corsi di formazione specifici e tailor-made (no corsi generici no webinar)
- ✓ Coinvolgimento dal basso *bottom up* (es. raccogliere domande, proposte, casi pratici, soluzioni)
- ✓ Attività che coinvolgono il personale incaricato (tranelli, giochi, esercitazioni) per sensibilizzare le persone sul valore dei dati
- ✓ Lavorare insieme ai team e prendere parte alle loro attività (es. campagna «Adotta un DPO»)
- ✓ Diversificare la formazione ed incrementare le misure organizzative (nomine *ad hoc*) per soggetti che svolgono attività critiche
- ✓ Richiedere competenze privacy fin dalla selezione per alcune funzioni aziendali (es. nella job description)

Data Breach & Vulnerability Assessment

- ✓ Importanza di clausole contrattuali nella contrattualizzazione dei fornitori che effettuano i penetration test
- ✓ Ambiti di test il più possibile sicuri ed epurati da dati
- ✓ Rispetto dell'art. 28 GDPR e requisiti di onorabilità
- ✓ Trasparenza e comunicazione delle azioni di vulnerability assessment ai titolari quando i dati sono trattati per conto di un altro soggetto