

Cybersecurity: nuove sfide per l'applicazione del GDPR in ambito sanitario

Pisa, 23 marzo 2018

Attacchi informatici e CyberDifese

Giuseppe Augiero

© 23 marzo 2018 - Giuseppe Augiero - talk@augiero.it - Apihm - Aula Magna Facoltà di Economia - Università di Pisa



Attacchi informatici -> Criminalità



Il punto di vista è errato



Irresponsabilità degli utenti



Non è un data breach

“il ricercatore che ha creato l'app ha ottenuto i dati da utenti che hanno scelto di iscriversi alla app e chiunque è stato coinvolto era consenziente”



Cambia la geografia del potere



Proteggere il bene più prezioso: le informazioni



Cultura digitale

1) Oggetto

Il servizio oggetto dell'esternalizzazione consiste nell'espletamento della **funzione di Responsabile della protezione dei dati personali (Data Protection Officer)**, prevista dal Regolamento (UE) 2016/679 del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), sezione 4, articoli 37-39.

In particolare il servizio oggetto dell'esternalizzazione prevede l'erogazione delle seguenti prestazioni ed interventi:

- informare e consigliare il titolare o il responsabile del trattamento in merito agli obblighi derivanti dal regolamento europeo e conservare la documentazione relativa a tale attività e alle risposte ricevute;
- vigilare sull'attuazione e sull'applicazione delle politiche del titolare o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la formazione del personale che partecipa ai trattamenti e gli audit connessi;
- verificare l'attuazione e l'applicazione del Regolamento europeo, con particolare riguardo ai requisiti concernenti la protezione della privacy fin dalla sua progettazione (privacy by design); la protezione di default di dati e sistemi (privacy by default); la sicurezza dei dati; il riscontro alle richieste degli interessati di esercitare i diritti riconosciuti dal Regolamento;
- garantire la conservazione della documentazione relativa ai trattamenti effettuati dal titolare;
- controllare che le violazioni dei dati personali siano documentate, notificate e comunicate;
- controllare che il titolare o il responsabile del trattamento effettui la valutazione d'impatto sulla protezione dei dati e richieda l'autorizzazione preventiva o la consultazione preventiva nei casi previsti;
- fungere da punto di contatto per il Garante per la protezione dei dati personali oppure, eventualmente, consultare il Garante di propria iniziativa;
- controllare che sia dato seguito alle richieste del Garante per la protezione dei dati personali e, nell'ambito delle sue competenze, cooperare di propria iniziativa o su richiesta dell'Autorità.

2) Durata e compenso

Il servizio avrà durata dalla firma del contratto sino al 31.12.2019 e prevede un importo massimo annuo di € 1.000,00 lordi e onnicomprensivi.

3) Requisiti

La funzione di RPD può essere esercitata indifferentemente da una persona fisica - in possesso di Partita Iva - o da persona giuridica.

La triste situazione Italiana



Cavallo di Troia



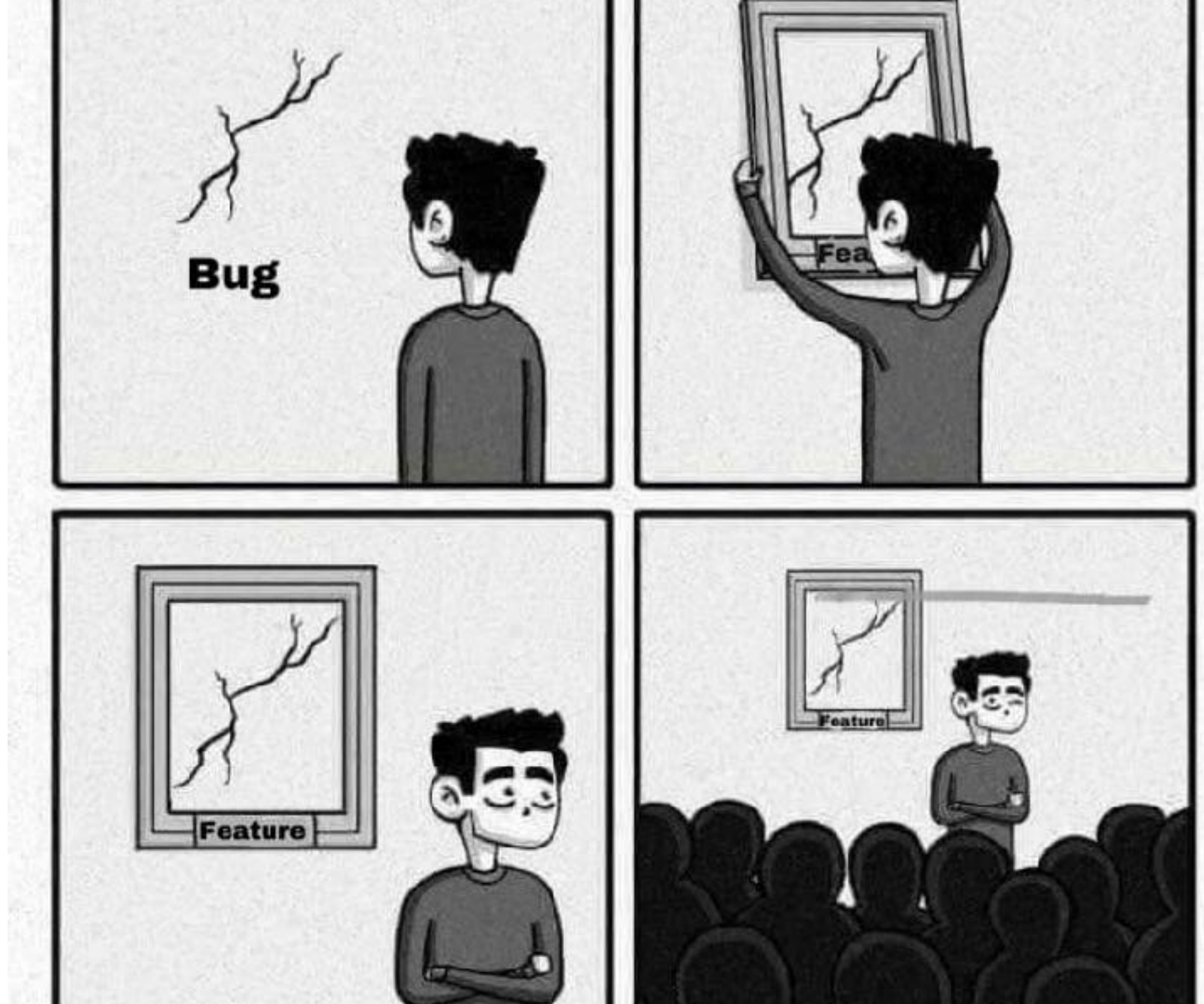
La mia banca è differente



Bug Bounty



Centro Unico Prenotazioni



Feature



Manca la percezione del rischio



**La cybersecurity non si implementa
con un dispositivo.**



Paura fa rima con marketing



Reputazione



**I dati sono degli utenti.
Dobbiamo averne cura.**

Cybersecurity: nuove sfide per l'applicazione del GDPR in ambito sanitario

Pisa, 23 marzo 2018

Attacchi informatici e CyberDifese

Giuseppe Augiero

Email: talk@augiero.it
Twitter: [GiuseppeAugiero](https://twitter.com/GiuseppeAugiero)
Web: www.augiero.it

© 23 marzo 2018 - Giuseppe Augiero - talk@augiero.it - Apihm - Aula Magna Facoltà di Economia - Università di Pisa