Cyber Resilience 'by design' e 'by default'

Luca Bechelli

Information & Cyber Security Advisor

Direttivo e Comitato Tecnico - Scientifico CLUSIT

Ci sono cose che non cambiano mai…

OWASP Top ten vulnerabilities 2017

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Primi 6 mesi del 2018

10%

di tutti gli attacchi registrati dal 2011

~~Privacy~~ Security by design

Search & replace

Descritta da sette principi, definiti negli anni '90 (in particolare nel 1995):

- Proactive not Reactive: The PbD approach attempts to anticipate and prevent privacy-invasive events before they happen.
- Privacy as the Default Setting: Ensure that personal data is automatically protected in any given IT system or business practice, ***so that if an individual does nothing, their privacy still remains intact***.
- Privacy Embedded into Design: Privacy should be embedded into the design and architecture of IT systems and business practices.
- Full Functionality – Positive-Sum, not Zero-Sum: PbD seeks to accommodate all legitimate interests and objectives in a "win-win" manner, balancing seemly opposing interests, such as security and privacy.
- End-to-End Security – Full Lifecycle Protection: PbD extends throughout the entire lifecycle of the data involved, from start to finish.
- Visibility and Transparency: It seeks to assure all stakeholders that component parts and operations remain visible and transparent, to users and providers alike.
- Respect for User Privacy – Keep it User-Centric: Above all, it puts the interests of the individual by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.

https://www.ipc.on.ca/privacy/protecting-personal-information/privacy-by-design/

Privacy by Design

- Art.25 – Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita:
  - tenendo conto dello stato dell'arte e dei costi di attuazione, nonche´della natura, dell'ambito di applicazione, del contesto e delle finalita`del trattamento, come anche dei **rischi aventi probabilita`e gravità** diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, **sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso** il titolare del trattamento **mette in atto misure tecniche e organizzative adeguate**, quali la pseudonimizzazione, **volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione**, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

By design e by default: obiettivi da perseguire

- **correttezza e trasparenza**: i dati saranno trattati in modo corretto e trasparente nei confronti dell'interessato, in particolare prevedendo informative adeguate prima di intraprendere qualsiasi trattamento e successive comunicazioni riguardo ad eventuali modifiche rispetto a quanto inizialmente indicato;

- **limitazione della finalità**: i dati saranno raccolti esclusivamente per finalità determinate, esplicite e legittime e successivamente trattati in modi che non siano incompatibili con tali finalità;

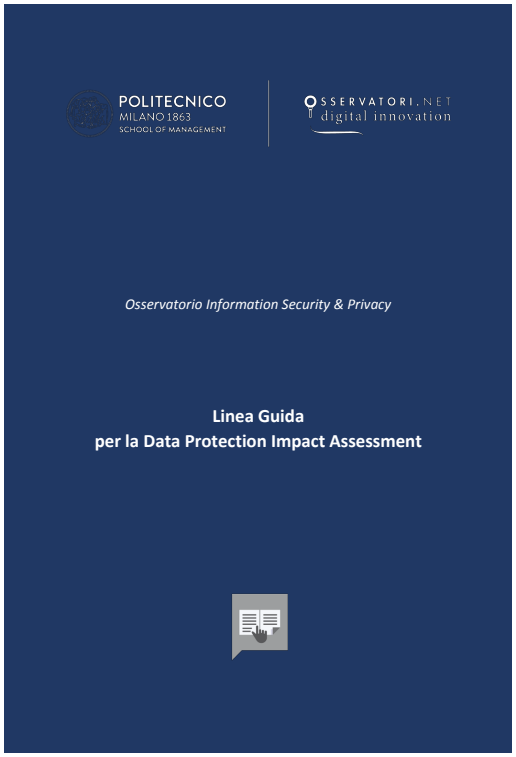
- **liceità**: i dati saranno raccolti e trattati, ad eccezione dei casi tassativi esplicitamente previsti dal Regolamento, solo in presenza di una o più delle condizioni di liceità da quest'ultimo identificate;

- **esattezza:** i dati devono essere mantenuti esatti e, se necessario, aggiornati. Pertanto, dovranno sussistere tutte le misure necessarie a cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;

- **minimizzazione dei dati**: i dati devono essere adeguati, pertinenti e limitati a quanto strettamente necessario alla realizzazione delle finalità per cui saranno raccolti;

- **limitazione della conservazione**: i dati saranno conservati in una forma che consentirà l'identificazione degli interessati per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono stati raccolti e trattati;

- **responsabilizzazione**: l'azienda dovrà essere in grado di comprovare l'adozione di misure e processi idonei a garantire il rispetto dei principi descritti ai punti che precedono, delle norme del GDPR (accountability) e delle misure individuate sulla base dell'analisi dei rischi.



https://www.osservatori.net/it_it/pubblicazioni/linea-guida-per-la-data-protection-impact-assessment

GRAZIE

Domande?

Luca Bechelli
Direttivo e Comitato Tecnico Scientifico Clusit
luca@bechelli.net
www.bechelli.net
https://twitter.com/luca_bechelli
https://www.facebook.com/bechelli.luca
http://www.linkedin.com/in/lucabechelli