Associazione Italiana Strumentisti

ISA Italy Section

«LE DIMENSIONI DELLA SICUREZZA INDUSTRIALE»
I percorsi della sicurezza industriale dagli standard ISA/IEC 62443 ai temi della cybersecurity

Milano, 30 Maggio 2018

Auditorio TECNIMONT

Cybersecurity e Hardware: che cosa prevede il GDPR

ReD OPEN
BICOCCA RESEARCH GROUP

1998-2018
20 UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA
VENTESIMO ANNIVERSARIO

Stefano Ricci, PhD
stefano.ricci@unimib.it
stefano.ricci@uninsubria.it

Stefano Ricci

Avvocato Foro di Milano

Professore a contratto di informatica giuridica presso l'Uninsubria

Fondatore ReD Open - Bicocca Research Group

PhD in materia Global Privacy Standard presso l'Università di Milano Bicocca

Socio del BisLab dell'Università di Milano Bicocca

Agenda

1. *Il GDPR in generale*
2. *Il GDPR in 9 punti*
3. *Cybersecurity e minacce hardware*

Il GDPR

Ricordare tre aspetti fondamentali

Il GDPR disciplina il trattamento di dati personali e si applica a tutti i soggetti (anche extra UE) che offrono servizi a cittadini UE.

“

Il titolare del trattamento deve dimostrare la propria compliance – cd. Accountability – responsabilizzazione e rendicontazione

“

Sono previste sanzioni sino al 4% del fatturato annuo e sino a 20 milioni di euro che coinvolgono sia i titolari del trattamento sia i loro fornitori

“

Il GDPR è direttamente applicabile dal 25 maggio 2018

“

micatwitto
@micatwitto

Ho letto tutta l'Informativa sulla Privacy.
Alla fine lui muore.

25/05/18, 18:56

1.175 Retweet **3.202** Mi piace

“

Il GDPR

Illustrato in nove aspetti essenziali

1

I ruoli

Titolare, responsabile, sub-responsabile, amministratore di sistema, soggetti autorizzati

2

Il registro dei trattamenti

Il censimento dei dati trattati

3

La sicurezza dei dati

La sicurezza informatica

4

Il data breach

Gli obblighi di comunicazione in caso di attacco informatico

5

Il data protection officer

Il nuovo soggetto, anche esterno, che garantisce la compliance aziendale

6

Il privacy impact assessment

La valutazione di impatto dei trattamenti più delicati

7

Privacy by design e by default

L’impostazione sin dall’inizio del trattamento dei principi fondamentali in materia

8

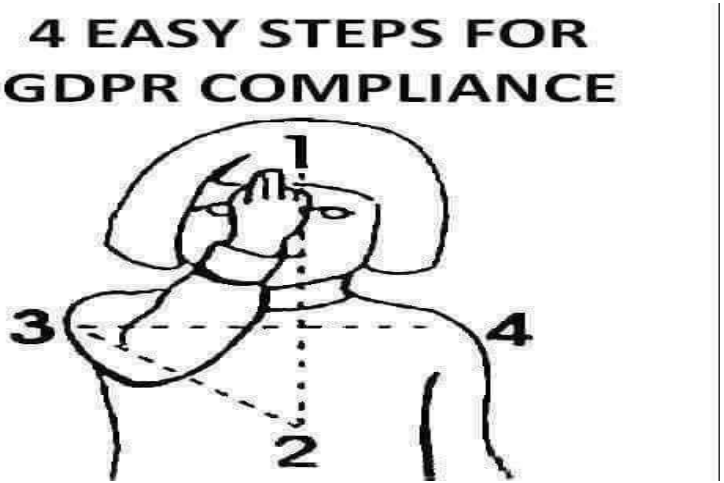
I diritti degli interessati

In materia di portabilità, profilazione, diritto all’oblio

9

Le sanzioni

Amministrative (sino al 4% del fatturato o 20 milioni di euro) ma anche civili e penali


4 EASY STEPS FOR
GDPR COMPLIANCE
1
2
3
4

“

Cybersecurity

Focus: hardware

La Gestione della Sicurezza dei Dati Personali Trattati nell'Organizzazione - (*art. 32 e c. 83 del Gdpr*)

Affinché sia garantito un livello di sicurezza dei Dati personali trattati, il Gdpr impone al Titolare ed al Responsabile del Trattamento di porre in essere delle **misure tecniche organizzative adeguate al rischio** che presenta un determinato tipo di Trattamento.

La Gestione della Sicurezza dei Dati Personali Trattati nell'Organizzazione - (*art. 32 e c. 83 del Gdpr*)

Le misure di sicurezza devono essere adottate tenendo conto dello stato dell'arte e dei relativi costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento.

La Gestione della Sicurezza dei Dati Personali Trattati nell'Organizzazione - (*art. 32 e c. 83 del Gdpr*)

Particolare rilievo assume, inoltre, l'analisi dei rischi che può presentare il trattamento.

Tale analisi deve essere svolta su base individuale dal Titolare del Trattamento e dal Responsabile del Trattamento.

La Gestione della Sicurezza dei Dati Personali Trattati nell'Organizzazione - *(art. 32 e c. 83 del Gdpr)*

L'**art. 32** del Gdpr elenca alcune delle **misure di sicurezza** che possono essere adottate dall'organizzazione:

La Gestione della Sicurezza dei Dati Personali Trattati nell'Organizzazione - (*art. 32 e c. 83 del Gdpr*)

la pseudonimizzazione e la cifratura dei Dati personali;

La Gestione della Sicurezza dei Dati Personali Trattati nell'Organizzazione - *(art. 32 e c. 83 del Gdpr)*

la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di Trattamento;

La Gestione della Sicurezza dei Dati Personali Trattati nell'Organizzazione - *(art. 32 e c. 83 del Gdpr)*

la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

La Gestione della Sicurezza dei Dati Personali Trattati nell'Organizzazione - *(art. 32 e c. 83 del Gdpr)*

una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del Trattamento.

Minacce hardware

Focus: COTS

Le Minacce - Interne ed esterne - Software e hardware

"*The challenge with supply chain attacks is that a sophisticated adversary might narrowly focus on particular systems and make manipulation virtually impossible to discover*" - Cyberspace Policy Review 2011

Le Minacce - Interne ed esterne - Software e hardware

Problema - COTS commercial off-the-shelf

Più economici, facilmente integrabili, impossibili da controllare

Le Minacce - Interne ed esterne - Software e hardware

Problema - condivisione delle minacce

Impossibilità di condividere dati di “intelligence”

Le Minacce - Interne ed esterne - Software e hardware

Problema - servizi aggiuntivi

Servizi di manutenzione dei sistemi

Le Minacce - Interne ed esterne - Software e hardware

Gestione del rischio - individuare i sistemi critici

Concentrare gli sforzi su quelli

Le Minacce - Interne ed esterne - Software e hardware

Gestione del rischio - analisi del fornitore

In particolare misure di sicurezza utilizzate

Le Minacce - Interne ed esterne - Software e hardware

Il rischio di intrusione hardware non può essere eliminato - può essere solo gestito

Thanks!

Any questions ?

You can find me at

- @stefanoricci
- ricci@htlaw.it