ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI AVELLINO

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI SALERNO

CORSO PREPARATORIO AGLI ESAMI DI STATO

II sessione 2023

ETICA E PRATICA PROFESSIONALE DELL'INGEGNERE

9-13 novembre 2023

Relatore: Ing. Luca Del Pizzo

I dati preoccupanti…

Ulteriore crescita degli attacchi cyber

I dati sono preoccupanti e in crescita costante, ecco perché il **45,1%** delle imprese medio-grandi italiane ha stipulato un'assicurazione contro gli incidenti e attacchi informatici (*dati ISTAT*). La stessa cosa vale per il **14,4%** delle PMI.

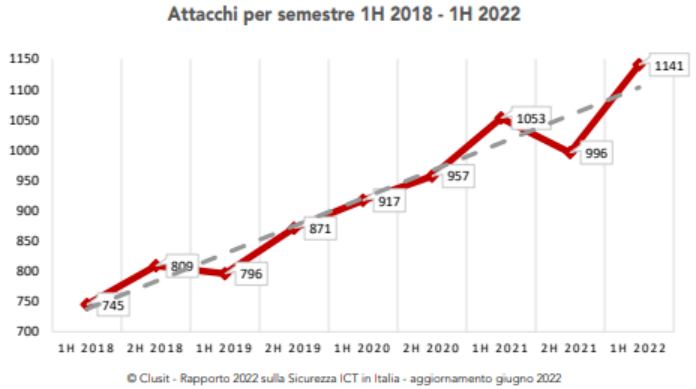
Nel 2022 l'Italia ha speso per prodotti e servizi di sicurezza informatica un miliardo e ottocentocinquanta milioni: **solo la metà di Germania, Francia, Canada e Giappone e di un terzo di Stati Uniti e Regno Unito**.

Ing. Luca Del Pizzo, Ph.D.
ing.lucadelpizzo@gmail.com

I dati preoccupanti…

- la Polizia Postale ha registrato un **incremento del 138% di attacchi in un anno** ad infrastrutture IT di aziende, privati e PA in Italia. Erano oltre 5000 i casi nel 2021 e quasi **13.000 nel 2022**.
- L'escalation di tensioni causate dal conflitto russo-ucraino ha scatenato una vera e **propria guerra digitale** negli Stati ostili.
  - adottando **sofisticati attacchi informatici per minare la stabilità economica, effettuare attività di spionaggio e violazione di dati di industrie, privati e istituzioni**.

Sui tentativi di intrusione tramite **servizi Mail** dove **il principale vettore d'attacco**, in crescita dell'11%, è l'utilizzo di URL malevoli che vengono impiegati nell'87% dei casi.



Ing. Luca Del Pizzo, Ph.D.
ing.lucadelpizzo@gmail.com

I dati preoccupanti…

- In base all'indice DESI (Digital Economy and Society Index) della Commissione Europea sui 27 Paesi membri dell'Unione Europea, **è ventesima per livello di digitalizzazione complessiva**.
- E' **terzultima per popolazione con competenze digitali almeno di base** (42%), contro una media UE del 56%.
- E' **quartultima per competenze digitali avanzate** (22%), contro una media UE del 31%.

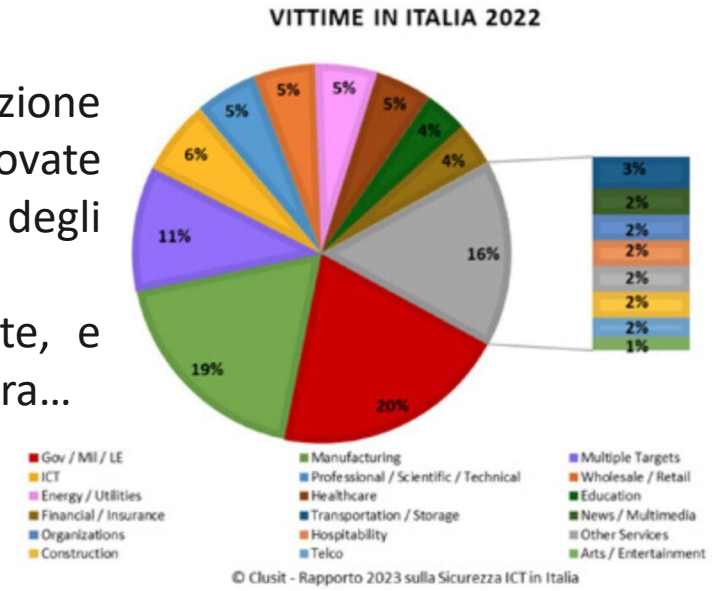
INVESTIRE NELLA DIGITALIZZAZIONE SENZA INCLUDERE PROGRAMMI DI SICUREZZA INFORMATICA RAPPRESENTA UNA POLITICA NON IN GRADO DI FAR FRONTE ALLE REALI ESIGENZE: LA RECENTE CRONACA LO DIMOSTRA.

Ing. Luca Del Pizzo, Ph.D.
ing.lucadelpizzo@gmail.com

I dati preoccupanti…

- Le vittime preferite dagli “attaccanti” sono le Pubbliche Amministrazioni. In particolare il 20% degli attacchi informatici sferrati in Italia nel 2022 è stato indirizzato verso le organizzazioni di tipo governativo.

Complice la pandemia e la conseguente accelerazione verso il digitale, diverse PP.AA. si sono trovate impreparate a sostenere la crescente pressione degli attacchi informatici.
Mancanza di investimenti (adeguati) da una parte, e scarsità di competenze informatiche (di base) dall’altra…



Ing. Luca Del Pizzo, Ph.D.
ing.lucadelpizzo@gmail.com

Alcuni numeri sulle soluzioni adottate…

- Una soluzione fondamentale come l'**Autenticazione Multifattoriale**, si pensi, è stata scelta solo dal 27,1% delle aziende ed il **Backup** solo all'**80%**. Il 20% delle aziende, quindi, non possiede una copia dei propri dati in caso di violazioni, condannandosi ad una fine quasi certa in caso di attacchi o incidenti informatici.
- Ancora meno adottati i sistemi di **Penetration Test** per la verifica costante dei sistemi IT (poco più del 30%) e della **Crittografia dei dati** (circa il 20%).
- Quasi il 42% invece ha deciso di adottare le reti **VPN** per connessioni più sicure anche da remoto.

Ing. Luca Del Pizzo, Ph.D.
ing.lucadelpizzo@gmail.com

Alcune soluzione…

- Avere sempre una copia dei dati da recuperare in caso di attacchi: **Backup & Disaster Recovery**
- Proteggere la navigazione in rete e l'utilizzo del traffico dati: **Firewall**
- Controllare e gestire gli accessi a dati e sistemi: **Data Security & Governance**
- Misurare la sicurezza continuamente: **Penetration Test Continuativo**
- Identificare l'identità di coloro che accedono ai dati e sistemi: **Autenticazione Multifattoriale**
- Verificare se i propri dati sono stati violati e pubblicati per adottare opportune contromisure: **DarkWeb Scan**

Ing. Luca Del Pizzo, Ph.D.
ing.lucadelpizzo@gmail.com

Obbligo della formazione

- La PREVENZIONE passa anche attraverso la formazione sulla cybersecurity dei propri dipendenti, che ogni giorno – sia durante la giornata lavorativa che nella vita privata – sono costantemente a rischio di subire un attacco informatico.
  - **diffusione di programmi strutturati di Awareness**
- Ed è proprio per questo motivo che all'interno del programma di formazione, l'Ordine degli Ingegneri della provincia di Salerno, per il tramite della Commissione «Trasformazione digitale e sicurezza delle informazione», ha inserito diversi interventi dedicati alla sicurezza informatica e alla protezione dei dati personali…

Ing. Luca Del Pizzo, Ph.D.
ing.lucadelpizzo@gmail.com

GDPR

Il "Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016", ha l'obiettivo di garantire una disciplina sulla protezione dei dati personali uniforme ed omogenea in tutta la UE

24 maggio 2016

Il **Regolamento entra in vigore;** i Paesi dell'Unione Europea avranno **due anni per porre in essere gli adeguamenti richiesti dalla normativa** in questione alle proprie politiche per la protezione ed il trattamento dei dati personali

25 maggio 2018

Il **Regolamento è definitivamente applicabile in via diretta in tutti i Paesi UE**, considerato che **non vi è la necessità di recepimento con atti nazionali** (anche se non poche disposizioni lasciano liberi gli Stati Membri - o richiedono agli stessi - di introdurre ulteriori regole e condizioni)

1. Definizioni
2. Ambito di applicazione territoriale
3. Autorità di controllo
4. Comitato europeo protezione dei dati
5. Principi applicabili al trattamento
6. Interessato
7. Diritti dell'interessato
8. Titolare del trattamento
9. Principio di accountability
10. Privacy by design e by default
11. Contitolari del trattamento
12. Responsabile del trattamento
13. Persone autorizzate al trattamento
14. Certificazioni
15. Sicurezza del trattamento
16. Data breach
17. Registri delle attività di trattamento
18. Valutazione impatto protezione dei dati (PIA)
19. Responsabile della protezione dei dati (DPO)
20. Trasferimento di dati extra UE
21. Nuovi diritti: Diritto all'oblio, Data portability
22. Cooperazione e coerenza
23. Mezzi di ricorso
24. Diritto al risarcimento e responsabilità
25. Disposizioni relative a specifiche situazioni di trattamento
26. Disposizioni finali
27. Sanzioni amministrative pecuniarie

Ing. Luca Del Pizzo, Ph.D.
ing.lucadelpizzo@gmail.com

GDPR

Il Regolamento UE 2016/679 **unifica** e **rafforza** la protezione dei dati personali tra i paesi membri dell'Unione Europea, introducendo **novità sostanziali** rispetto alle precedenti normative.

Accountability

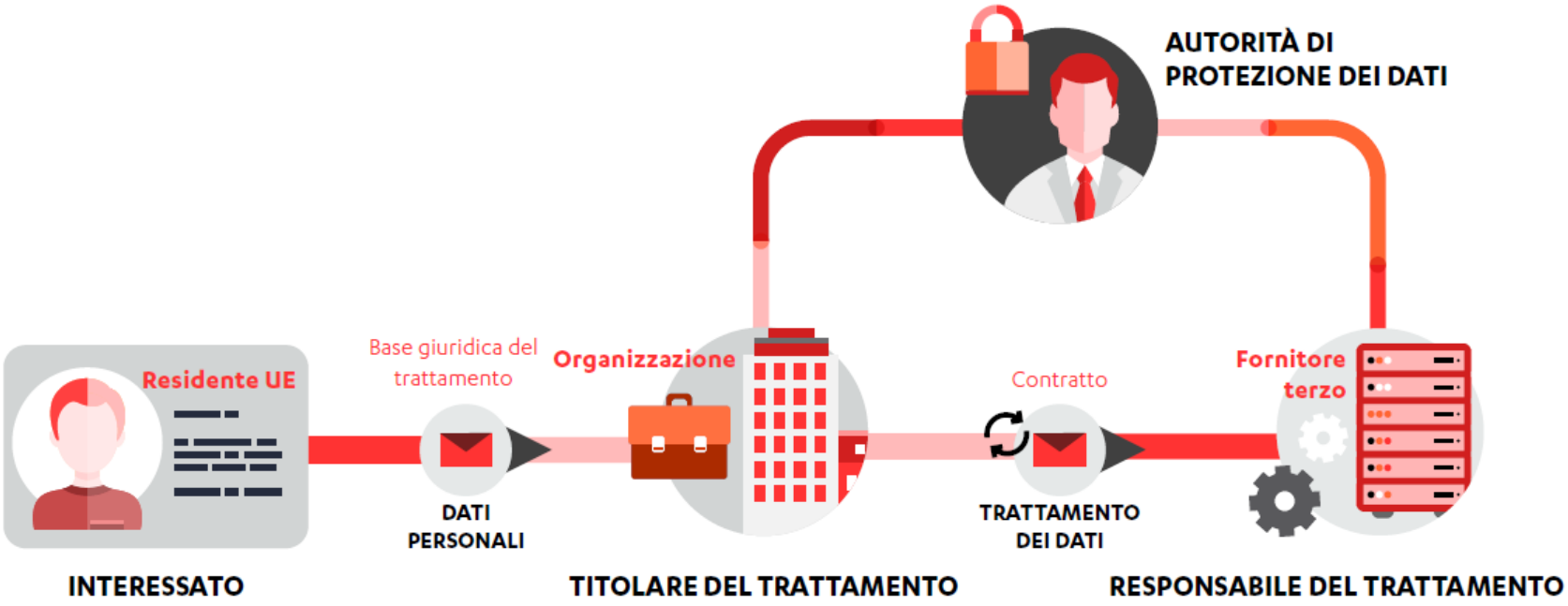
*Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per **garantire**, ed essere in grado di **dimostrare**, che il trattamento è effettuato in **conformità** al presente regolamento.*

Approccio Risk-Based

*Per la protezione dei dati personali si passa dal concetto di **misure minime** a quello di **misure adeguate ai rischi** del trattamento, aventi probabilità e gravità diverse per i **diritti e le libertà** delle persone fisiche.*

Ing. Luca Del Pizzo, Ph.D.
ing.lucadelpizzo@gmail.com

Definizioni



Ing. Luca Del Pizzo, Ph.D.
ing.lucadelpizzo@gmail.com

Accountability
Responsabilità del Titolare (art. 24)

Tenuto conto

- della natura
- dell'ambito di applicazione
- del contesto
- delle finalità del trattamento
- dei rischi per i diritti e le libertà delle persone fisiche

Il titolare mette in atto misure

- tecniche e
- organizzative

adeguate per

- garantire
- ed essere in grado di dimostrare

che il trattamento è effettuato conformemente al regolamento.

Misure tecniche ed organizzative

Ing. Luca Del Pizzo, Ph.D.
ing.lucadelpizzo@gmail.com

Misure tecniche e organizzative

- Il Regolamento sebbene non elenchi in modo tassativo le **misure minime**, individua una serie di misure (dalla **pseudonimizzazione** alla **resilienza** dei sistemi, alle procedure di **back-up** e **disaster recovery**, a varie attività di **testing**) che ribadiscono la natura prettamente informatica del concetto di sicurezza riferito ai dati personali.

- L'intero impianto del Regolamento, tuttavia, è costruito attorno ad un principio che va ben oltre la mera sicurezza del dato in sé e che riguarda, invece, la **sicurezza dei diritti e delle libertà delle persone fisiche**.

Misure tecniche e organizzative

- Il concetto emerge anche nel già menzionato **art.32**, nella parte in cui prescrive al titolare di mettere in atto **misure tecniche ed organizzative adeguate** a garantire un livello di sicurezza adeguato al **rischio**, tenuto conto dello
  - **stato dell'arte** e
  - dei **costi** di attuazione,
  - della **natura**,
  - **dell'oggetto**,
  - del **contesto** e
  - delle **finalità** del trattamento nonché
  - del "***rischio*** *di varia* ***probabilità*** *e* ***gravità*** *per i diritti e le libertà delle persone fisiche*".

Misure tecniche e organizzative

Articolo 24 - Responsabilità del titolare del trattamento (C74-C78)

- 1. Tenuto conto della **natura**, dell'**ambito di applicazione**, del **contesto** e delle **finalità** del trattamento, nonché dei **rischi** aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il **titolare** del trattamento mette in atto **misure tecniche e organizzative** adeguate per garantire, ed **essere in grado di dimostrare**, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono **riesaminate** e **aggiornate** qualora necessario.
- 2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di **politiche adeguate** in materia di protezione dei dati da parte del titolare del trattamento.

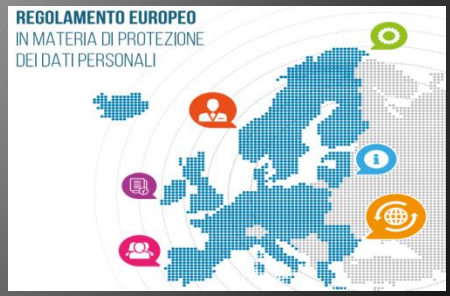
Misure tecniche e organizzative

Art. 25 comma 1

- **Tenendo conto** dello **stato dell'arte** e dei **costi di attuazione**, nonché della **natura**, **dell'ambito di applicazione**, del **contesto** e delle **finalità** del trattamento, come anche dei **rischi** aventi probabilità 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**.

Data Breach
(cons. 85-88, artt. 4.12, art. 33, 34)

Notifica delle violazioni di dati personali



Ing. Luca Del Pizzo, Ph.D.
ing.lucadelpizzo@gmail.com

Data breach – Considerando 85 (art. 33)

artt. 33-34
Notifica al Garante di una violazione di dati personali e comunicazione all'interessato

Linee guida Gruppo Art. 29 in materia di notifica delle violazioni di dati personali (data breach notification) del 3/10/2017

Violazione dei dati personali
«Violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati»

Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di DIMOSTRARE che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche