Roma, 9 Maggio 2019

Spunti Privacy

E' notizia di qualche giorno fa la violazione delle caselle di posta, da parte di soggetti non autorizzati, dell'ordine degli avvocati di Roma, compresa quella di alcuni esponenti governativi.

L'attività illecita da parte di soggetti non autorizzati non si arresta ma continua il suo percorso con lo scopo di creare danno o beneficio economico.

La sicurezza dei dati e delle informazioni, è un asset fondamentale e strategico per le organizzazioni. I dati, e la loro gestione, sono la parte più importante e più critica delle organizzazioni.

A circa due anni dall'entrata in vigore del regolamento europeo 2016/679 (GDPR) poche sono le organizzazioni che hanno recepito il regolamento e si sono adeguate.
I dati sono la linfa delle organizzazioni, delle aziende e nostra, essi sono perennemente e costantemente connessi.

I dati sono un assett strategico, la gestione dei quali consente un vivere quotidiano tranquillo.

Comunque a fronte di questa importanza, poche aziende, ad oggi, si sono dotate di adeguati strumenti di controllo e gestionali.

Il regolamento europeo (GDPR) 679/2016 ha introdotto una nuova visione in merito alla gestione e trattamento dei dati. L'ottica si è spostata su una consapevolezza maggiore del titolare su diversi fronti.

In particolare, nel caso di interesse, il regolamento europeo pone l'accento sui rischi che possono derivare dai trattamenti: infatti la parola rischio compare ben 83 volte.

Come ha osservato proprio il Presidente dell'Autorità garante per la protezione di dati personali, Antonello Soro: "*Il GDPR prevede l'incorporazione delle misure di protezione dati negli stessi sistemi e dispositivi, in modo che essi siano progettati e configurati in maniera da minimizzare l'uso di dati personali e proteggerli adeguatamente.Queste misure compensano quel deficit di consapevolezza nell'utilizzo di dispositivi intelligenti di uso quotidiano, la cui apparente innocuità ci induce a sottovalutarne la potenziale esposizione ad attacchi informatici o comunque la capacità di rivelare, tramite i dati raccolti, stili e tenore di vita, persino patologie o dipendenze.*

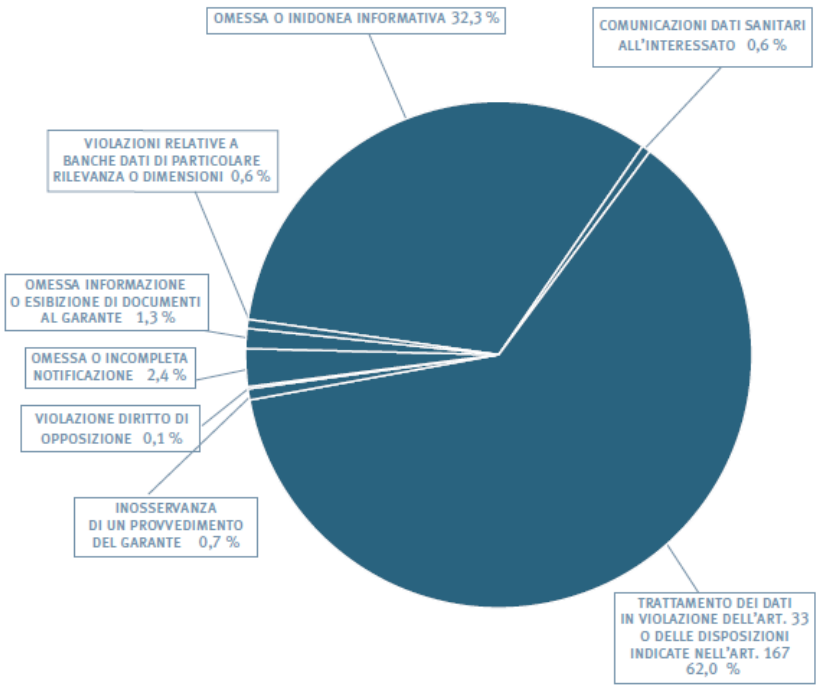
Inoltre, rispetto alla profilazione e al microtargeting che questi dispositivi possono incentivare, risultano determinanti il diritto di opposizione e quello di contestare la decisione automatizzata, nonché di ottenere l'intervento umano nel processo decisionale".

Il giorno 7 maggio, l'Autorità Garante Privacy ha presentato la sua relazione annuale della quale riportiamo alcuni punti.

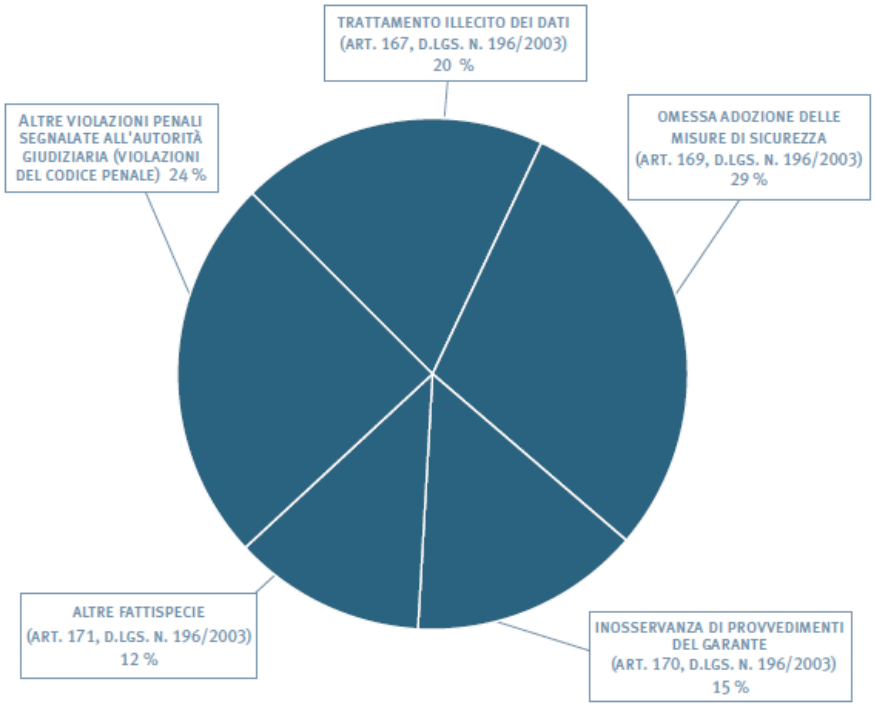
Il processo di accountability (rendicontazione) non è stato ancora compreso e recepito. La responsabilità della dimostrazione di aver intrapreso tutte le azioni necessarie è a carico del Titolare del trattamento.

Riportiamo anche alcuni grafici di sintesi.

Il primo riguarda le sanzioni amministrative contestate. E' eclatante il fatto che il 32% riguarda ancora l'omessa informativa al trattamento e il 62% il Data Breach (violazione) cioè il trattamento illecito da parte di persone non autorizzate.



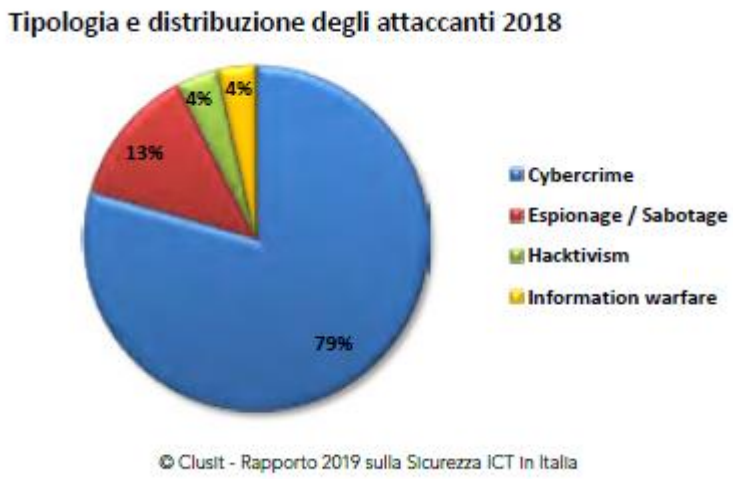
Il secondo grafico riguarda le sanzioni penali e le comunicazioni all'autorità giudiziaria.



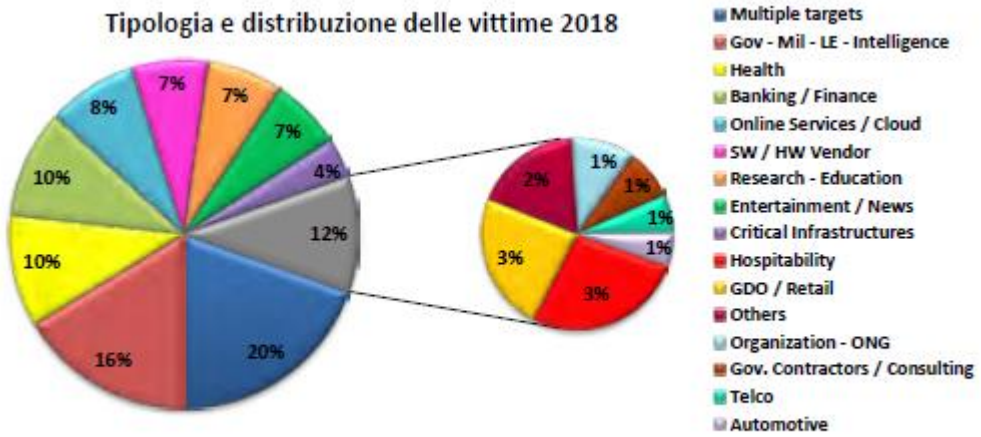
Anche in questo caso è sorprendente come il 29% riguardi l'adozione delle misure di sicurezza.

La sicurezza dei dati e delle informazioni è un processo trasversale che riguarda tutta l'organizzazione.

Dal rapporto del Clusit 2019 si evidenzia come gli attaccanti non risparmiano nessuno.



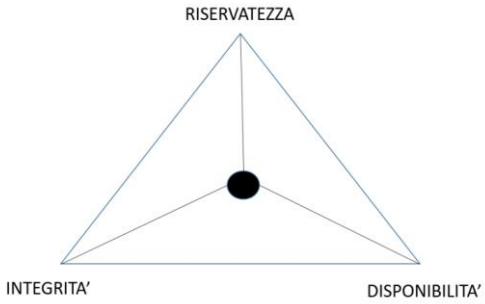
© Clusit - Rapporto 2019 sulla Sicurezza ICT in Italia



© Clusit - Rapporto 2019 sulla Sicurezza ICT in Italia

Valutare lo stato di questi sistemi risulta allora importante. E' possibile fare ciò attraverso dei momenti formali, audit, svolti all'organizzazione oppure coinvolgendo il personale dedicata attraverso una metodologia di autovalutazione e di confronto. Sia per la parte audit che per la parte di autovalutazione, che deve essere guidata ed approfondita, si possono utilizzare vari modelli basati però tutti sui su tre punti fondamentali:

- Riservatezza
- Integrità
- Disponibilità



Ci sono vari livelli di autovalutazione in funzione di cosa vogliamo misurare e con quale dettaglio.

Un esempio di una check list, di 15 punti, è riportato sotto, tratta dall'Italian Cybersucurity Report CIS Sapienza e laboratorio CINI del marzo 2017.

1	Esiste ed è mantenuto aggiornato un inventario dei sistemi, dispositivi, software, servizi e applicazioni informatiche in uso all'interno del perimetro aziendale.
2	I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc…) offerti da terze parti a cui si è registrati sono quelli strettamente necessari.
3	Sono individuate le informazioni, i dati e i sistemi critici per l'azienda affinché siano adeguatamente protetti.
4	È stato nominato un referente che sia responsabile per il coordinamento delle attività di gestione e di protezione delle informazioni e dei sistemi informatici.
5	Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in tema di cybersecurity che risultino applicabili per l'azienda.
6	Tutti i dispositivi che lo consentono sono dotati di software di protezione (antivirus, antimalware, ecc...) regolarmente aggiornato.
7	Le password sono diverse per ogni account, della complessità adeguata e viene valutato l'utilizzo dei sistemi di autenticazione più sicuri offerti dal provider del servizio (es. autenticazione a due fattori).
8	Il personale autorizzato all'accesso, remoto o locale, ai servizi informatici dispone di utenze personali non condivise con altri; l'accesso è opportunamente protetto; i vecchi account non più utilizzati sono disattivati.
9	Ogni utente può accedere solo alle informazioni e ai sistemi di cui necessita e/o di sua competenza.
10	Il personale è adeguatamente sensibilizzato e formato sui rischi di cybersecurity e sulle pratiche da adottare per l'impiego sicuro degli strumenti aziendali (es. riconoscere allegati e-mail, utilizzare solo software autorizzato, …). I vertici aziendali hanno cura di predisporre per tutto il personale aziendale la formazione necessaria a fornire almeno le nozioni basilari di sicurezza.
11	La configurazione iniziale di tutti i sistemi e dispositivi è svolta da personale esperto, responsabile per la configurazione sicura degli stessi. Le credenziali di accesso di default sono sempre sostituite.
12	Sono eseguiti periodicamente backup delle informazioni e dei dati critici per l'azienda (identificati al controllo 3). I backup sono conservati in modo sicuro e verificati periodicamente.
13	Le reti e i sistemi sono protetti da accessi non autorizzati attraverso strumenti specifici (es: Firewall e altri dispositivi/software anti-intrusione).
14	In caso di incidente (es. venga rilevato un attacco o un malware) vengono informati i responsabili della sicurezza e i sistemi vengono messi in sicurezza da personale esperto.
15	Tutti i software in uso (inclusi i firmware) sono aggiornati all'ultima versione consigliata dal produttore. I dispositivi o i software obsoleti e non più aggiornabili sono dismessi.

In questa autovalutazione è necessario definire però delle metriche e misurare la distanza (gap) o meglio l'applicazione del sistema di sicurezza IT.

Quindi oltre agli aspetti giuridici importanti da presidiare come le nomine, le informative, i registri, i trattamenti, le procedure, importantissimi sono gli aspetti relativi alla sicurezza dei dati. Queste sono prassi che ogni organizzazione deve intraprendere per non incappare in "spiacevoli incidenti" come visto sopra.

Cordiali saluti.

Dott. Stefano. Gorla
Governance e Compliance Team leader InTheCyber
DPO Certificato 001 FAC Certifica.