

30 gennaio 2020
Giornata Europea della Protezione dei Dati Personali

Sicurezza informatica: i nuovi dati
Rapporto CLUSIT
Osservatorio Information Security & Privacy
Politecnico di Milano



GABRIELE FAGGIOLI



- *Presidente CLUSIT (Associazione Italiana per la Sicurezza Informatica)*
- *Adjunct Professor MIP-Politecnico di Milano*
- *Responsabile scientifico dell'Osservatorio Security & Privacy del Politecnico di Milano*
- *Già Membro del Group of Expert in Cloud Computing Contract della Commissione Europea*
- *CEO di p4i – Partners4Innovation*



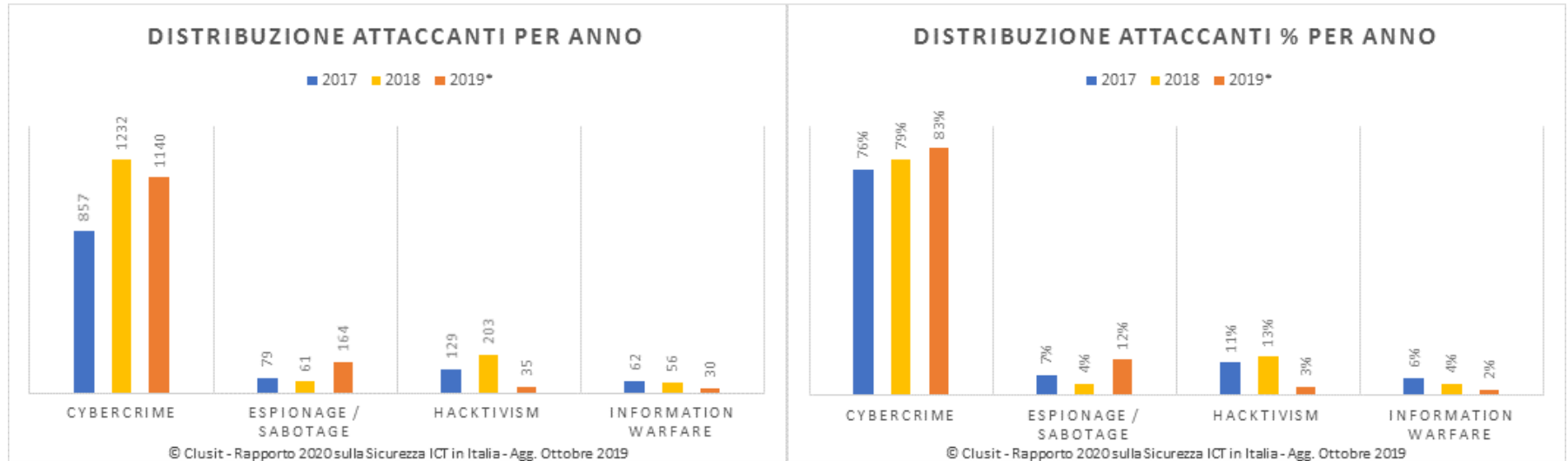
Anteprima sui dati del Rapporto del CLUSIT

Gli attaccanti (2019 - 10 mesi)

ATTACCANTI	2017	2018	2019*	2017%	2018%	2019*%	Totale
Cybercrime	857	1232	1140	76%	79%	83%	3229
Espionage / Sabotage	79	61	164	7%	4%	12%	304
Hacktivism	129	203	35	11%	13%	3%	367
Information warfare	62	56	30	6%	4%	2%	148
TOTALE	1127	1552	1369				4048

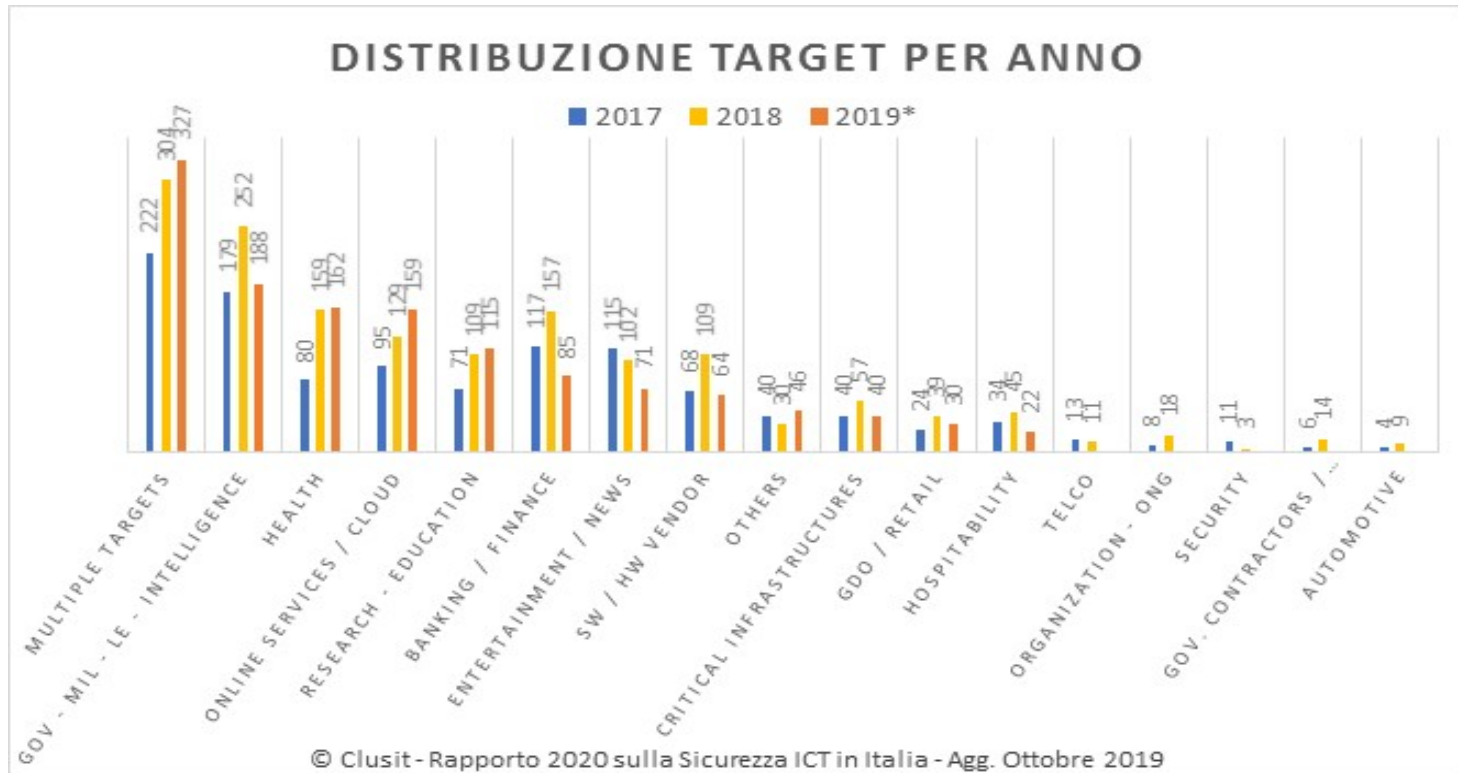
- L'analisi comprende un campione complessivo di 4.048 attacchi.
- Gli attacchi sono in prevalenza di natura Cybercrime (80% del totale).
- Le tecniche più utilizzate nel periodo sono Malware (40%) e Unknown / Data breach (24%).

Attaccanti (2019 - 10 mesi)



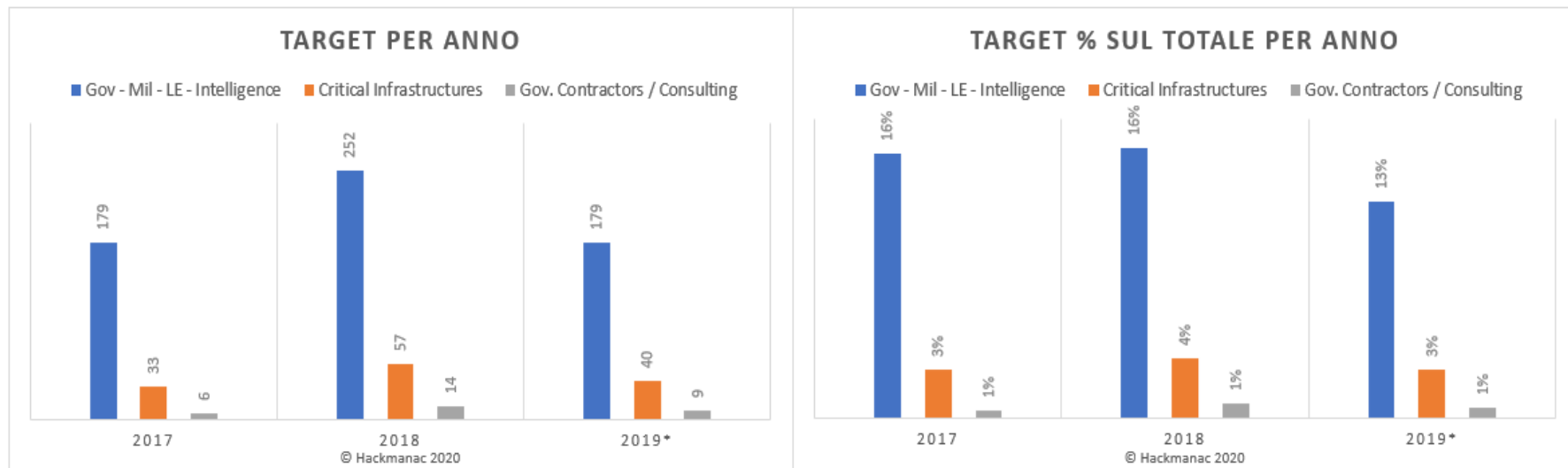
L'analisi mostra una crescita notevole del Cybercrime (dal 76% del 2017 all'83% del 2019) e dell'Espionage / Sabotage (dal 4% nel 2018 al 12% nel 2019).

Distribuzione target per anno (2019 - 10 mesi)



Focus GOV – critical: analisi dei target

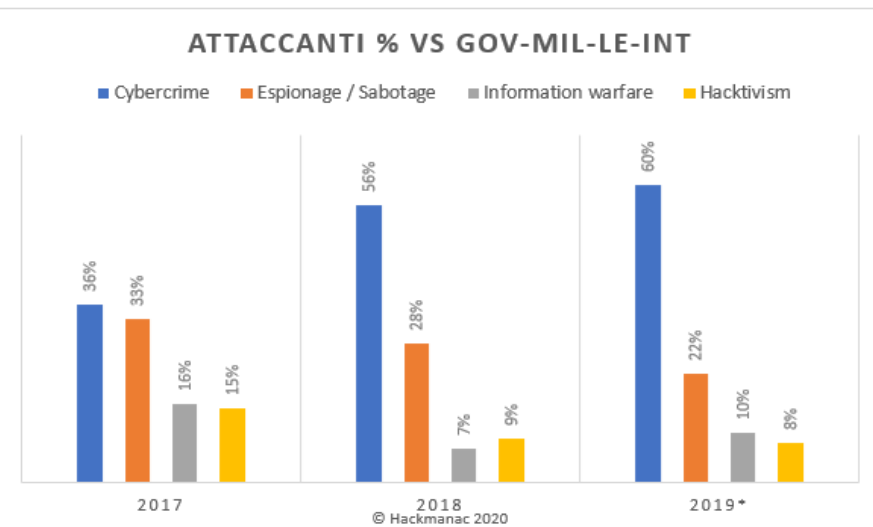
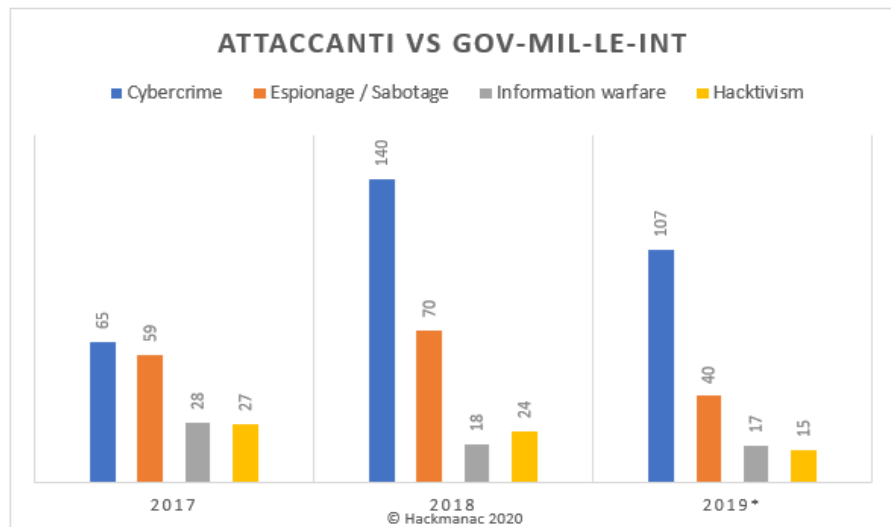
Target per anno



Il campione riguarda bersagli rilevanti dal punto di vista della sicurezza nazionale, ovvero vengono considerati gli attacchi diretti ad Enti Governativi, ad Infrastrutture Critiche e a Gov. Contractors con severity critica ed alta.

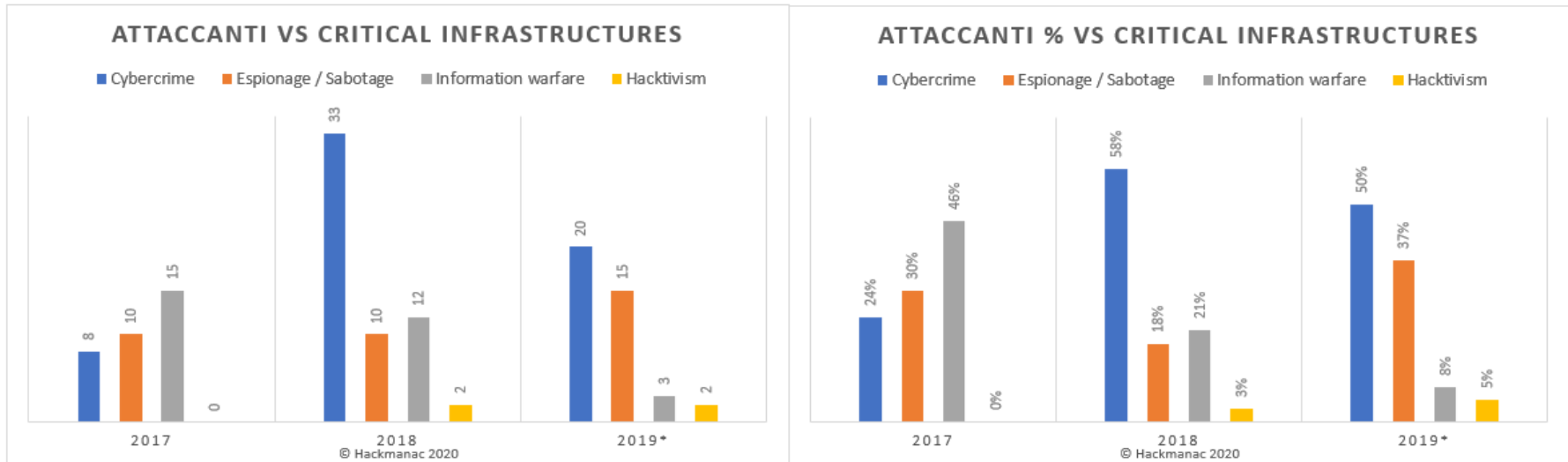
Focus GOV – critical: analisi degli attaccanti

Attaccanti vs GOV – MIL – LE – INT



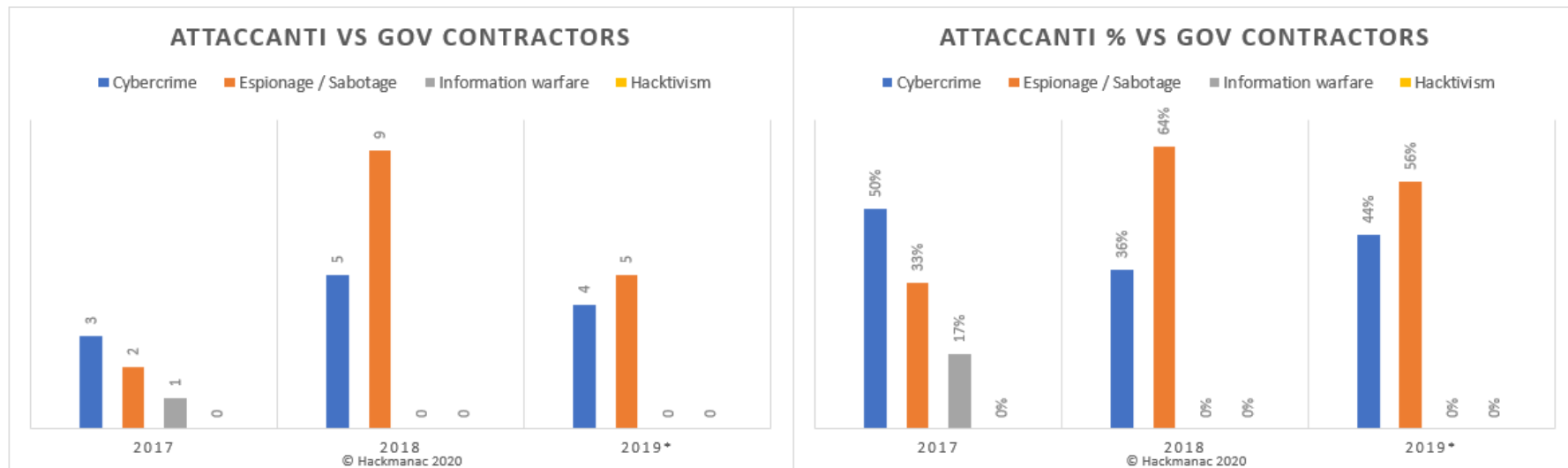
Sebbene in termini numerici assoluti la distribuzione mostri apparentemente una decrescita, l'analisi percentuale evidenzia invece una crescita degli attacchi dovuti a Cybercrime diretti ad enti governativi (passati dal 36% nel 2017 al 60% nel 2019).

Attaccanti vs critical infrastructures



Mentre sembrano diminuire gli attacchi dovuti a Cybercrime e Information warfare, l'Espionage / Sabotage verso Infrastrutture Critiche è in forte crescita (dal 24% nel 2017 al 37% nel 2019).

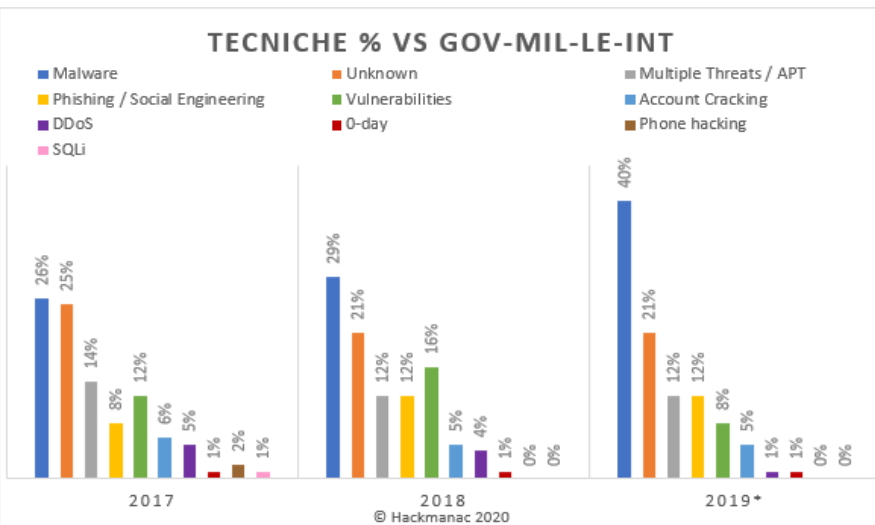
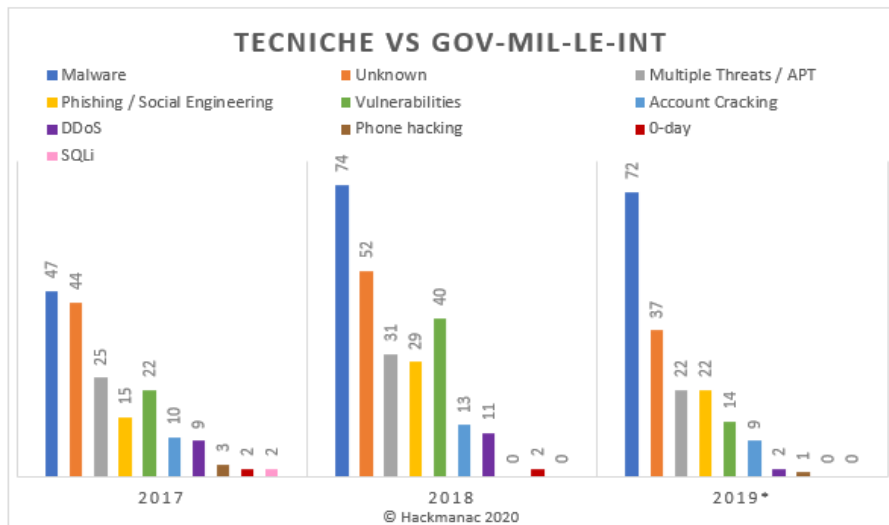
Attaccanti vs GOV Contractors



- Gli attacchi di stampo Cybercrime verso Gov. Contractors sono in crescita rispetto all'anno scorso (dal 36% del 2018 al 44% del 2019).
- Nel 2018 e 2019 non si sono verificati attacchi di Information warfare e Hacktivism.

Focus GOV – critical: analisi delle tecniche di attacco

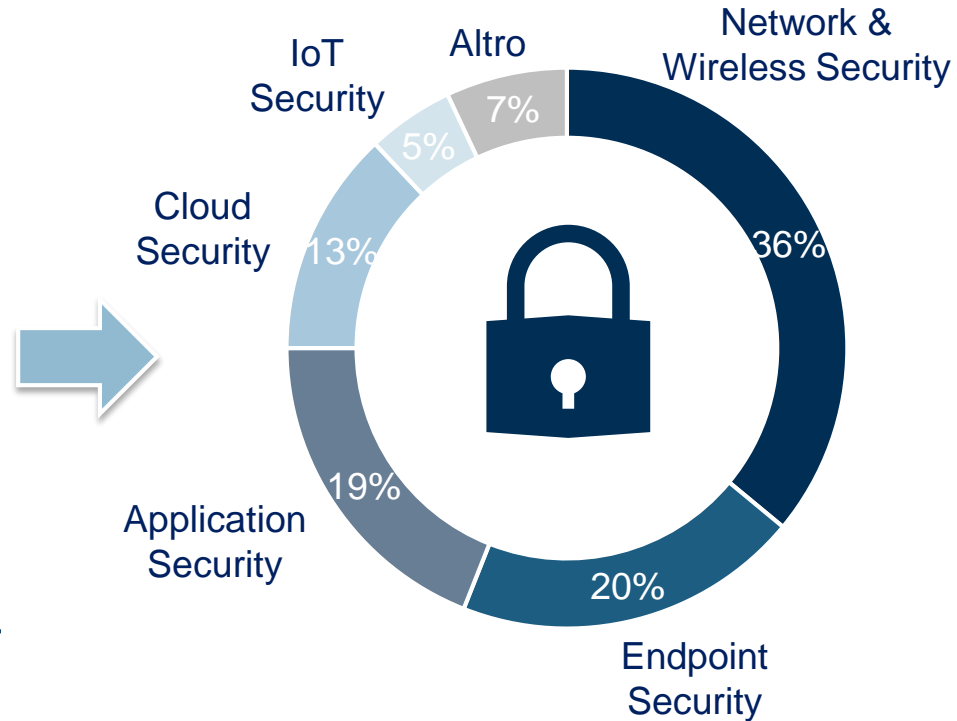
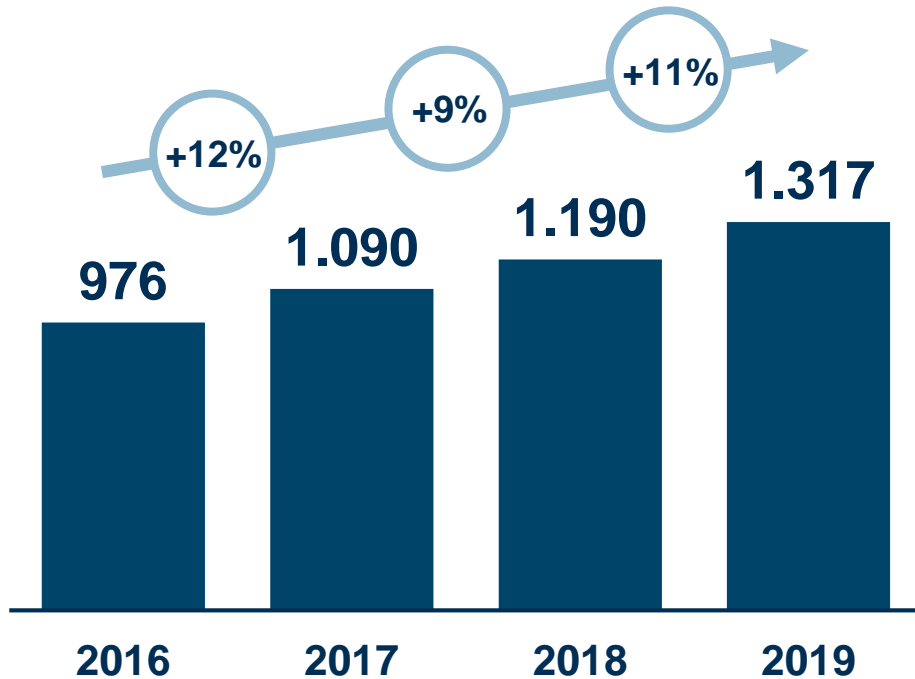
Tecniche vs GOV – MIL – LE -INT



L'analisi degli attacchi diretti verso Enti Governativi ed Infrastrutture Critiche nel campione preso in esame mostra una forte crescita nell'utilizzo di Malware (da 26% nel 2017 a 40% nel 2019).

Anteprima sui dati dell'Osservatorio Information Security & Privacy del Politecnico di Milano

Il mercato information security 2019



Campione: 698 organizzazioni italiane (dati in k€)

Qual è il trend degli investimenti in sicurezza informatica



Il mercato dell'information security cresce di circa l'11% e si attesta a 1.3 miliardi di euro

Il 51% delle grandi aziende ha dichiarato di aver aumentato il budget a fronte del solo 2% che ha dichiarato di averlo ridotto

Per la protezione delle risorse in cloud il 55% delle grandi aziende ha dichiarato di aver aumentato il budget

Fonte: Osservatorio Information Security & Privacy Politecnico Milano – Ricerca 2020

Le scelte organizzative

Nel 40% delle organizzazioni non esiste una specifica funzione Information Security (dato ancora fortemente negativo)

Oltre la metà delle organizzazioni ritiene che il modello organizzativo adottato non rappresenti una configurazione ottimale per un'efficace gestione dell'information security

In particolare, il grado di insoddisfazione raggiunge un picco del 65% tra le aziende in cui la funzione Information Security riporta all'IT

Il 90% delle organizzazioni che hanno adottato il modello nel quale il CISO è a riporto del Board ritiene che tale configurazione sia ottimale

Fonte: Osservatorio Information Security & Privacy Politecnico Milano – Ricerca 2020

Il fattore umano

Nel 55% dei casi, esiste un piano di formazione pluriennale, che coinvolge tutta l'organizzazione, dal Top Management alle Business Line.



Nel 25% del campione vi è un piano di formazione indirizzato nello specifico a funzioni con maggiore sensibilità alle tematiche di information security e data protection, quali IT, Risk Management e Compliance



Il 20% delle aziende gestisce le iniziative di formazione in modo spot, senza un piano strutturato

Di cosa hanno paura le aziende nel mondo industriale (Industry 4.0)

Fermo parziale o totale della produzione (54%), che può sia costituire l'obiettivo diretto e primario di un eventuale attacco sia rappresentare invece una ripercussione secondaria

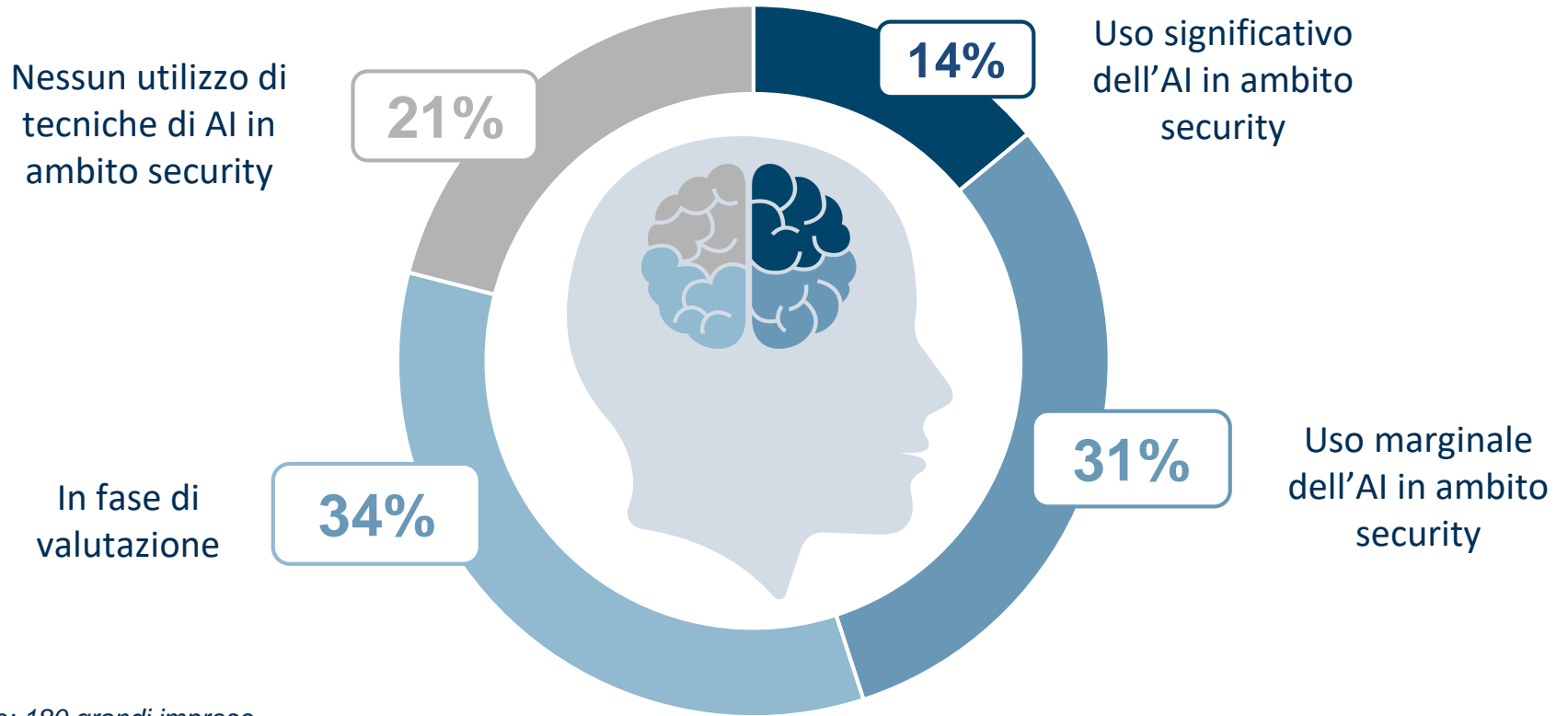


Tra le conseguenze più rilevanti si trova poi la safety (20%), requisito reso particolarmente critico dall'interazione sempre più diretta tra operatori e macchine (es. robotica collaborativa)

Possibile alterazione o modifica della produzione (16%), con motivazioni riconducibili al sabotaggio

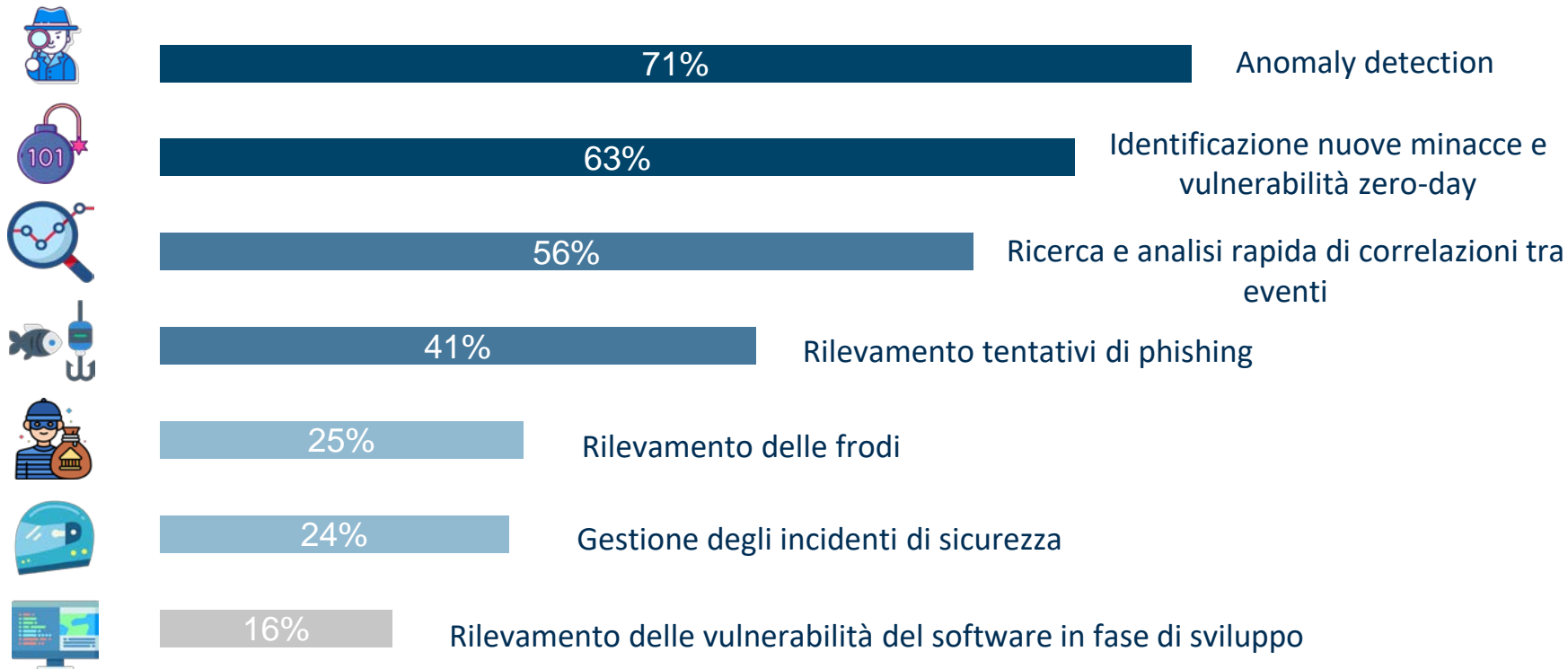
È invece considerata meno rilevante in questo ambito la possibilità di furto, perdita o divulgazione di dati confidenziali (10%), principalmente riguardanti la proprietà intellettuale.

L'utilizzo dell'AI in ambito security



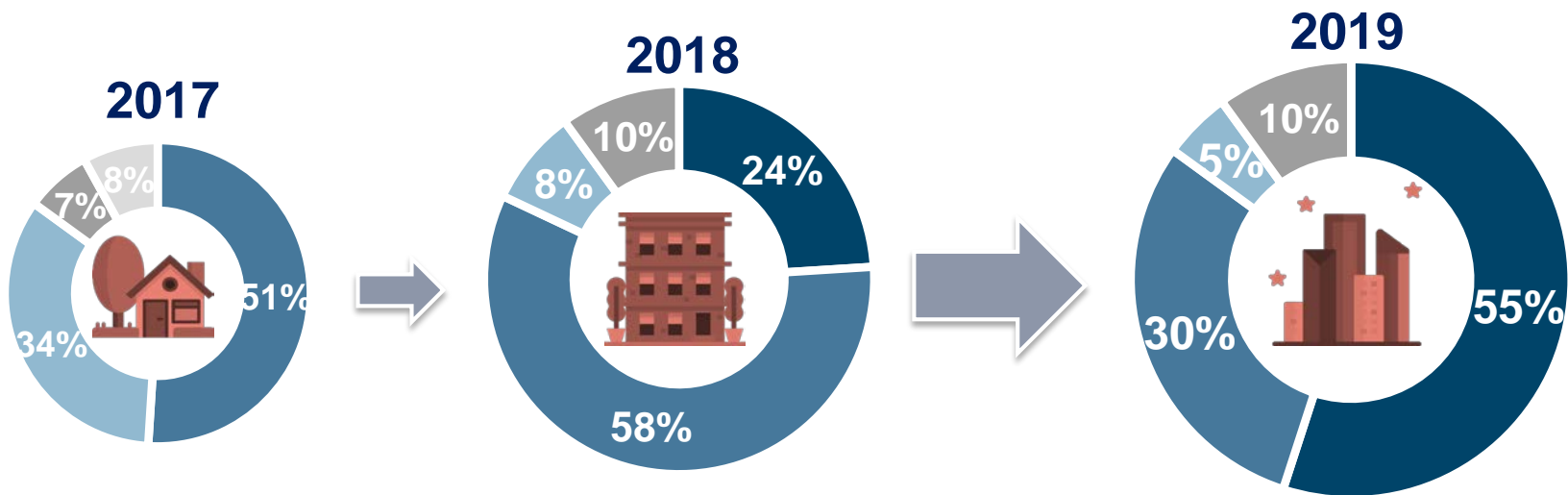
Campione: 180 grandi imprese

Le funzionalità dell'AI in ambito security



Campione: 180 grandi imprese

GDPR: il percorso di adeguamento

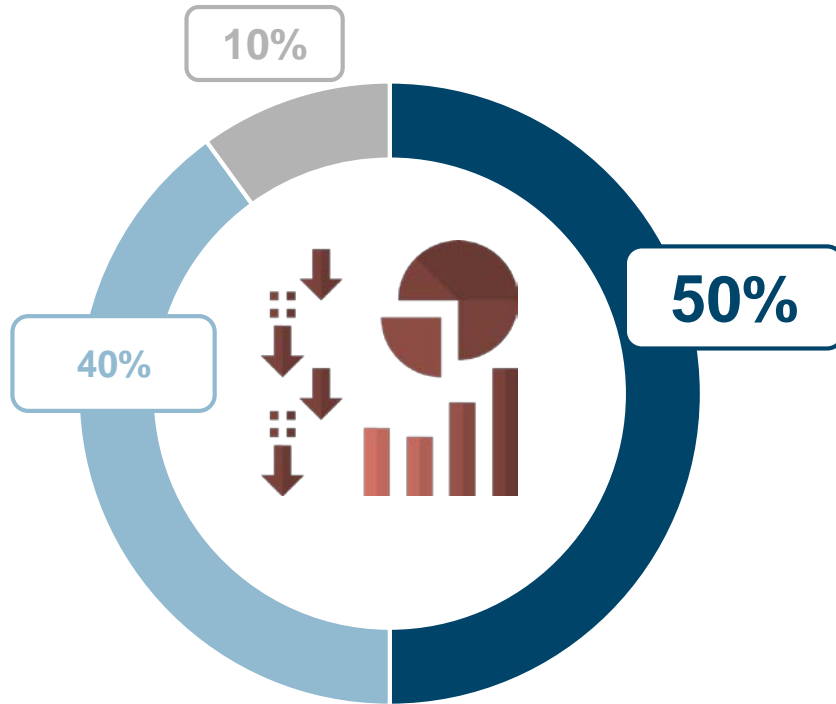


- I progetti di adeguamento al GDPR sono stati completati
- È in corso un progetto strutturato di adeguamento alla normativa

- È in corso un'analisi dei requisiti richiesti e dei piani di attuazione possibili
- Le implicazioni sono note nelle funzioni specialistiche ma il tema non è all'attenzione del vertice
- Le implicazioni del GDPR non sono note in dettaglio

Campione: 180 grandi imprese

La gestione del rischio cyber



■ Il rischio cyber viene gestito all'interno di un processo integrato di Risk Management aziendale

■ Il rischio cyber viene gestito come rischio a sé stante all'interno della funzione IT o di un'altra singola funzione (es. Security, Legal & Compliance, ecc.)

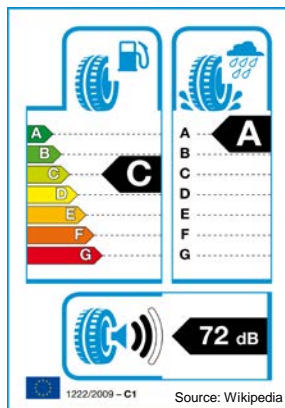
■ Il rischio cyber non viene monitorato costantemente

Campione: 180 grandi imprese

La sicurezza nasce dentro al progetto

Sicurezza fin dalla progettazione

- Perché l'azienda/utente finale si deve porre il problema di valutare la sicurezza dei prodotti che utilizza?
- Perché centinaia di migliaia di aziende devono rivalutare gli stessi prodotti, per arrivare alle stesse conclusioni?



Quale
modello
adottare?



L'evoluzione normativa e la filiera

- Gli obblighi previsti dal GDPR per i Responsabili obbligano tutta la filiera ad adeguarsi ai requisiti posti Titolare
- Se NIS riguarda pochi attori, il perimetro cibernetico rischia (ma ne siamo entusiasti) di imporre gli stessi requisiti a tutta la filiera, indipendentemente che siano OSE o dalla loro dimensione aziendale
- Il Cybersecurity Act obbligherà anche i piccoli produttori a soddisfare requisiti minimi di sicurezza
- **La protezione di sé è parte della protezione dell'ecosistema, nella stessa logica dell'igiene pubblica**

Tutto questo ha un impatto importante:

- Sui Titolari che dovrebbero assicurare il rispetto delle proprie esigenze su una catena di fornitura su cui ha un controllo limitato
- Sui fornitori, che dovrebbero adattarsi ai requisiti posti da ciascun cliente di cliente di cliente...

La non compliance impedirà sempre più spesso di far parte della filiera produttiva

Azione 1: certificazioni efficaci e uniformi

E' necessario che il sistema Paese e le istituzioni si facciano carico della necessità di adeguare l'intera filiera produttiva agli standard di sicurezza e di compliance che il presente richiede e che il futuro richiederà sempre di più

I diversi stakeholder dovrebbero collaborare con ENISA per assicurare che le certificazioni di sicurezza siano disegnate in modo da permettere valutazioni «graduali» e non disomogenee fra settori e normative, che permettano alle aziende produttrici di semplificare il processo di certificazione senza ridurne l'efficacia.



Azione 2: adozione di logiche di certificazione vincolanti e potenziamento del controllo

Le autorità di controllo dovrebbero definire le norme tecniche in modo da accettare queste stesse certificazioni come dimostrazione misure adeguate.

Allo stesso tempo, queste certificazioni dovrebbero essere richieste per l'accesso a mercati rilevanti a livello europeo (es. tutte le PA dell'Unione).

ENISA, o corrispondenti autorità nazionali, potrebbero avere un ruolo di audit delle certificazioni da un punto di vista non formale, per garantire l'efficacia sostanziale del processo.



Il trattamento massivo di dati da parte dei governi

Cina: il «Social Credit System»



- Da quest'anno in Cina dovrebbe diventare obbligatorio il «*Social Credit System*», un meccanismo attraverso il quale verrà assegnato a ciascun cittadino un punteggio di **affidabilità sociale**.
- Dal punteggio dipenderanno: **l'accesso al credito, a polizze assicurative e previdenziali, a molte professioni, a prestazioni di welfare, etc.**
- Ad assegnare i punteggi sarà insindacabilmente il Governo, sulla base di un **algoritmo** alimentato da **masse di dati** che in buona parte saranno forniti dai **grandi operatori del web**.

Fonte: *il Sole24Ore*

USA: le nostre foto sui social e sul web usate per il riconoscimento facciale

ANSA^{it} **Hi-tech**

Polizia Usa e Fbi usano potente app riconoscimento facciale

Nyt, può mettere fine a privacy, dietro c'è una start up

The New York Times

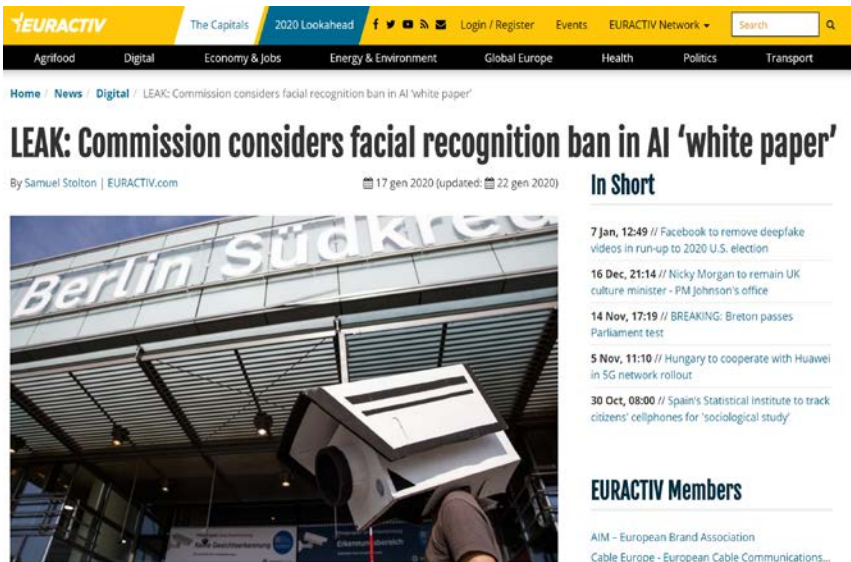
The Secretive Company
That Might End Privacy
as We Know It

A little-known start-up helps law enforcement match photos of unknown people to their online images — and “might lead to a dystopian future or something,” a backer says.

Fonte: ansa.it; nytimes.com

- Una start-up americana, «*Clearview AI*», ha sviluppato un'applicazione che, dall'immagine di un volto, consente di risalire a **tutte le foto pubbliche dell'interessato/a, inclusi i link ove reperirli.**
- Negli Stati Uniti tale applicazione sarebbe **già in uso**, non solo da parte della polizia, ma anche dall'**FBI** e dal **Dipartimento per la Sicurezza Nazionale.**
- A far discutere, rispetto ai sistemi di riconoscimento tradizionali, è soprattutto la possibilità di utilizzare algoritmi di **artificial intelligence** che sfruttano **l'enorme mole di dati presente sul web**, spesso **forniti volontariamente dagli utenti.**

Europa: al bando i sistemi di riconoscimento facciale



The screenshot shows the Euratectiv website interface. At the top, there's a navigation bar with 'EURACTIV' logo, 'The Capitals', '2020 Lookahead', and various utility links like 'Login / Register', 'Events', and 'EURACTIV Network'. Below this is a secondary navigation bar with categories: 'Agrifood', 'Digital', 'Economy & Jobs', 'Energy & Environment', 'Global Europe', 'Health', 'Politics', and 'Transport'. The main content area features a headline: 'LEAK: Commission considers facial recognition ban in AI 'white paper'' by Samuel Stolton, dated 17 Jan 2020. Below the headline is a photo of a person holding a large cardboard box in front of a building with 'Berlin Südkreuz' signage. To the right of the photo is an 'In Short' section with several news snippets, including one about Facebook removing deepfake videos and another about Nicky Morgan remaining UK culture minister.

Fonte: Euractive.com

- La Commissione europea starebbe valutando la possibilità di **vietare l'uso del riconoscimento facciale nelle aree pubbliche** per un periodo di almeno cinque anni.
- L'atteggiamento è prudenziale: **prendere tempo, per valutare le criticità e i possibili abusi di tale tecnologia.** Eccezioni al divieto potrebbero essere fatte per progetti di sicurezza e di ricerca e sviluppo.
- Sul punto, la Commissione avrebbe preparato un white paper (in via di pubblicazione) ove propone nuove regole per implementare la normativa *privacy* esistente e **linee guida per gli sviluppatori e gli utenti di sistemi di intelligenza artificiale.**

La frammentazione normativa

Asimmetria Regolamentare

Data Protection

1995

Direttiva
95/46/CE c.d.
«Data protection
Directive»

2002

Direttiva 2002/58/CE
(«Direttiva e-
Privacy»)

2003

D.lgs. 196/2003
Codice Privacy

2018

Reg. (UE) 2016/679
(«GDPR»)

2018

Codice Privacy
(«novellato») coordinato
con il D.lgs. 101/2018

Gli stati membri hanno individuato a livello locale le disposizioni europee → 28 normative differenti

Interessi dello Stato

2016

Direttiva 2016/1148 Network &
Information Security c.d. «NIS»
(recepita in Italia dal D.Lgs.
65/2018).

2019

Reg. (UE) 2019/881
c.d. «Cybersecurity
Act»

2019

L. 18 novembre 2019 n. 133 di conversione in legge, con
modificazioni, del D.L. 21 settembre 2019, n. 105, recante
«**Disposizioni urgenti in materia di perimetro di sicurezza
nazionale cibernetica**». Ulteriori modifiche sono state apportate
dall'art. 27 del Decreto-legge 30 dicembre 2019, n. 162 (decreto
Milleproroghe).

La sicurezza come elemento comune

In questo scenario che vede la protezione dei dati personali da un lato e gli interessi dello Stato dall'altro, il tema della SICUREZZA è sicuramente l'elemento comune.

DATA PROTECTION

La sicurezza è un tema ricorrente nel GDPR, principio fondamentale, che il Titolare deve tenere sempre in considerazione per trattare i dati personali e proteggerli (art.5, par.1, lett. f) del GDPR).

La sicurezza deve essere garantita:

1. A livello organizzativo:

- Nella scelta dei fornitori;
- Nelle verifiche periodiche volte al controllo (audit);
- Nella valutazione del rischio nell'ambito dei processi (privacy by design e by default);
- Nell'adozione di misure di sicurezza fisiche;
- Nell'adozione di procedure volte alla gestione dei data breach.

2. A livello informatico:

- Nell'adozione di misure di sicurezza adeguate a proteggere le reti;
- Nell'adozione di misure di sicurezza informatiche e logiche.

Interessi dello Stato

Il tema della sicurezza ricorre anche in questo ambito, con il fine di:

1. Direttiva NIS

- Uniformare la strategia della sicurezza per la gestione dei rischi;
- Proteggere contro i cyber attacchi;
- Individuare incidenti di cyber sicurezza;
- Ridurre l'impatto degli incidenti di cyber sicurezza

2. Cybersecurity Act

- Creare un sistema di certificazione di riferimento che assicuri una protezione adeguata di tutti i prodotti e servizi digitali (security by design e by default)

3. Perimetro nazione di sicurezza cibernetica

- Gestire e individuare eventuali vulnerabilità di prodotti e servizi ICT sin dalla fase di procurement (ad esempio il ruolo di Cvcn);
- Definire le modalità e le tempistiche associate agli obblighi di notifica in relazione all'esercizio di poteri speciali.

I rischi della frammentazione

Finalità e asset
tutelati

Nonostante l'elemento comune possa essere identificato nel concetto di Sicurezza, gli asset messi in sicurezza sono differenti:

- Da un lato i DATI PERSONALI (GDPR)
- Dall'altro lato GLI INTERESSI DELLA NAZIONE (direttiva NIS, Cyber Security Act, Perimetro nazionale).

Rischi

Ciò comporta il rischio per cui mettere in atto finalità condivise ma strumenti diversi rende complicato per le imprese fronteggiare questa situazione.

La difficoltà risiede soprattutto nei confronti delle piccole imprese e si manifesta nel:

- Incapacità nel fronteggiare costi eccessivi;
- Incremento dell'incapacità organizzativa a causa del complesso panorama;
- Aumento degli adempimenti a causa dei differenti asset tutelati (come nel caso delle notifiche in caso di data breach nel settore bancario).

Possibili soluzioni

Sfruttare gli strumenti messi a disposizione: es. codici di condotta che aiutino ad applicare correttamente il regolamento europeo ma che allo stesso tempo riescano a semplificare gli oneri in capo alle imprese.

Stimolare la crescita organizzativa promuovendo strutture a più livelli con il compito di accrescere il loro ecosistema.

Promuovere il ruolo delle aziende Capofila.

Key messages

Key messages

Non ci può essere trasformazione digitale senza sicurezza

Servono maggiori investimenti

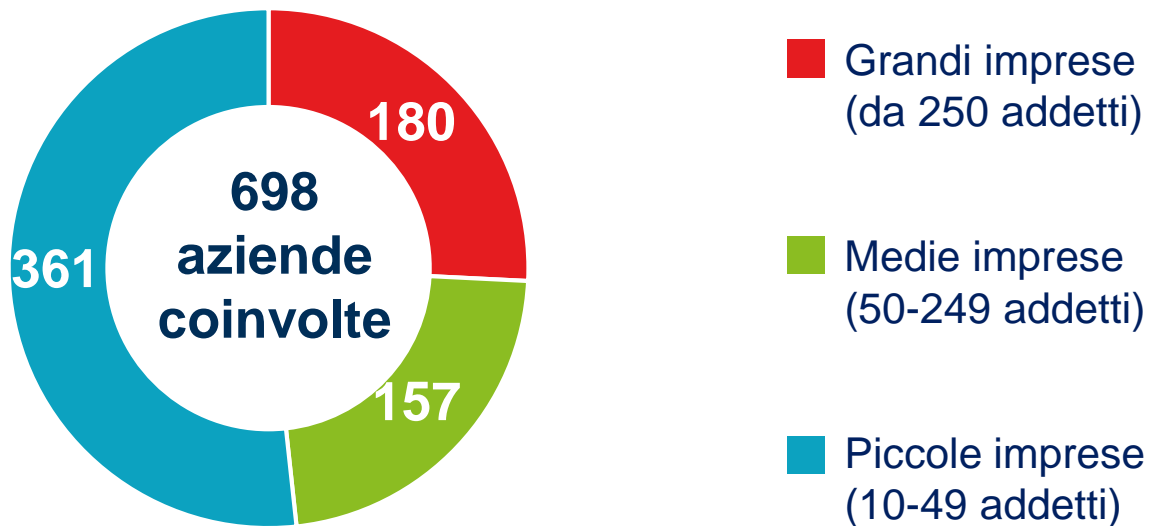
Serve maggiore e più efficiente organizzazione interna negli enti (priorità: adozione di un modello integrato di indirizzo e governo della security che permetta di garantire l'adozione e logiche di intervento operative uniformi a ogni livello e di supervisionare in maniera completa e affidabile le fonti di minaccia)

Serve maggiore consapevolezza e formazione

Nota metodologica

Il campione – Ricerca 2019

La scomposizione per dimensione



Il campione – Grandi imprese

La scomposizione per settore

