Cybersecurity e Data Protection: prospettive e scenari per il 2024?

Francesco Capparelli

Chief Cyber Security Specialist

Avvocato, Certified Ethical Hacker – Auditor/Lead Auditor ISO/IEC 27001, ISO 22301, ISO 37001 and ISO/IEC 20000-1, ISO 9001

Milano - Bologna - Roma – Amsterdam – Atene - Helsinki - Madrid – Lagos - Melbourne

Direttiva NIS 2 & AI Act

L'Italia avanza decisa nel panorama digitale: dalla robustezza della cybersecurity all'innovazione responsabile nell'AI

La Direttiva NIS2 rappresenta un passo decisivo nella normativa UE sulla sicurezza cibernetica. Inserita nel contesto di nuove regolamentazioni europee, introduce obblighi aggiornati e misure per assicurare la resilienza delle infrastrutture critiche e una protezione ottimale dei dati.

L’AI Act mira a stabilire un quadro giuridico uniforme per lo sviluppo, la commercializzazione e l'uso dell'intelligenza artificiale (IA) in conformità ai valori dell'Unione.

L’Evoluzione del Panorama Cibernetico - ENISA THREAT LANDSCAPE 2023

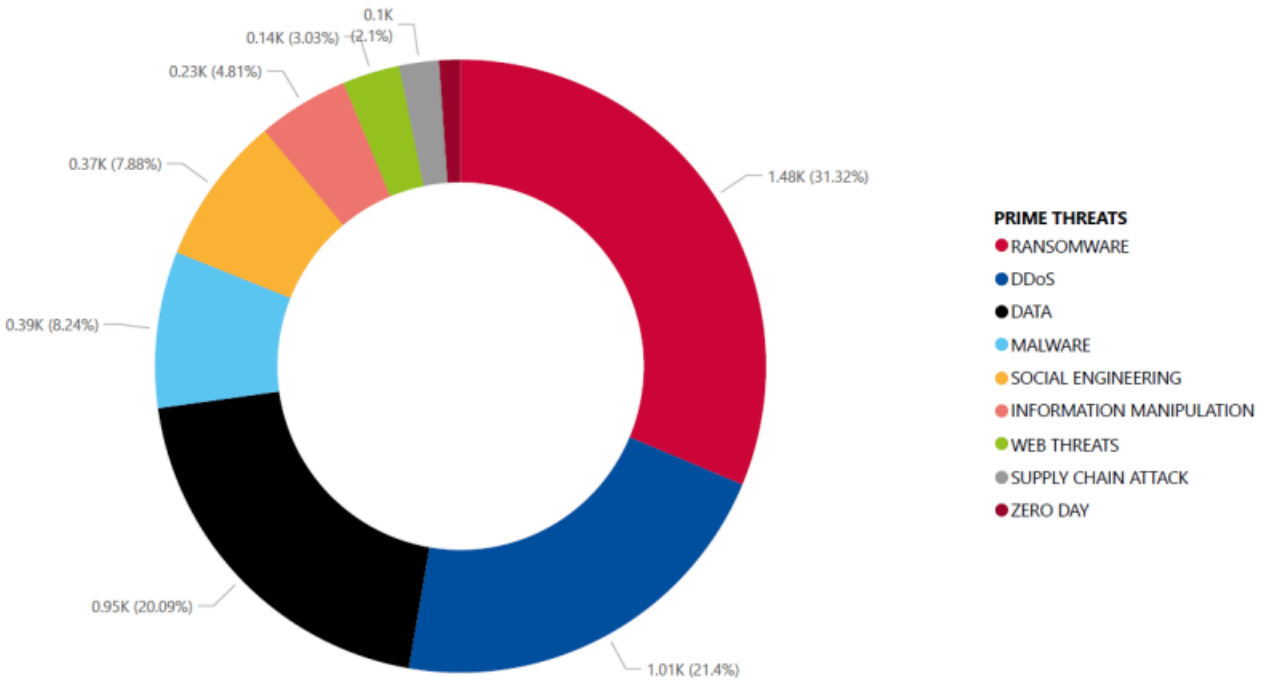
Il 2023 ha visto una rapida evoluzione delle minacce cibernetiche

Mentre il mondo diventa sempre più digitalizzato, la necessità di proteggere le nostre infrastrutture e i nostri dati diventa sempre più critica.

Gli attacchi cibernetici nel 2022-2023 hanno dimostrato che nessun settore rimane immune

La crescente interconnessione digitale ha ampliato il perimetro degli attacchi, rendendo essenziale una protezione cibernetica robusta in tutti i settori

Figure 2: Breakdown of analysed incidents by threat type (July 2022 till June 2023)

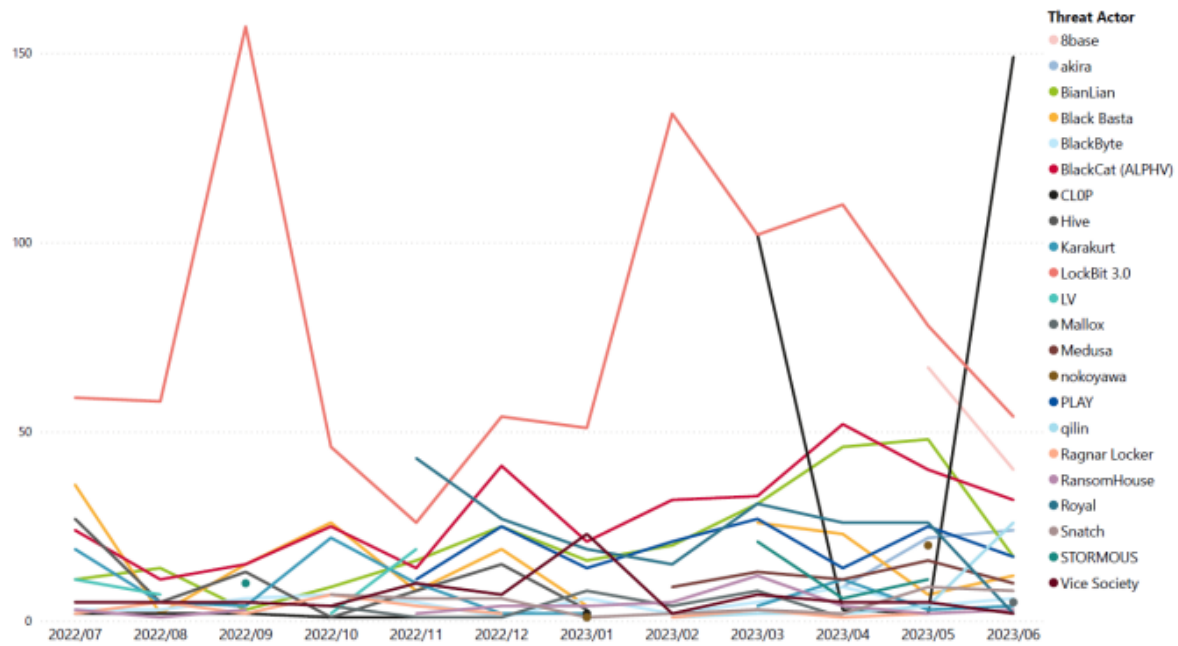


L’Evoluzione del Panorama Cibernetico - ENISA THREAT LANDSCAPE 2023

Nel 2023, il panorama della cybersecurity ha registrato un incremento significativo degli attacchi ransomware

Marzo 2023 ha stabilito un record con 459 attacchi ransomware, mostrando un aumento del 91% rispetto al mese precedente e del 62% rispetto a marzo 2022

Figure 21: Timeline of the 20 most active Ransomware groups during the reporting period



L’Evoluzione del Panorama Cibernetico – ENISA THREAT LANDSCAPE 2023

Pubblica Amministrazione: 19% degli eventi totali. Maggiormente colpita da ransomware, DDoS e malware. 21% degli attacchi alla catena di fornitura.

Salute: 8% degli eventi totali. 13% degli attacchi ransomware e 10% delle minacce legate ai dati.

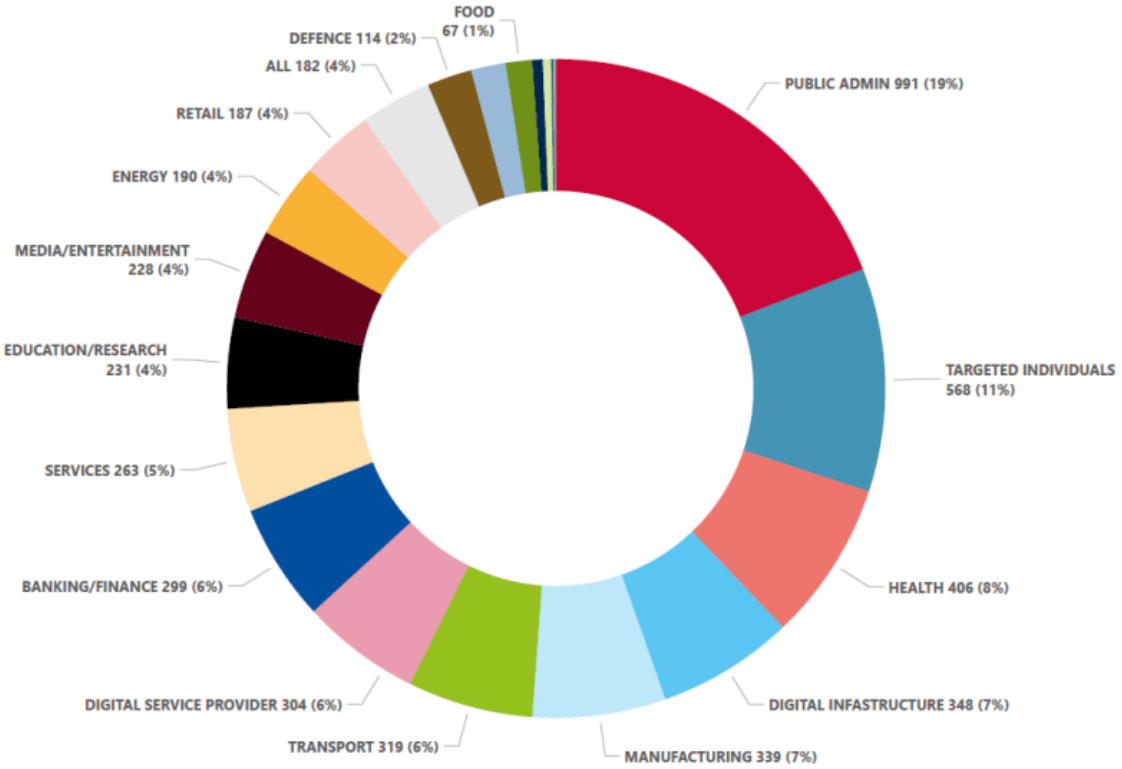
Infrastruttura Digitale: 7% degli eventi totali. Colpita da malware (13%) e minacce alla disponibilità di Internet (28%).

Fornitori di Servizi Digitali: 6% degli eventi totali. Colpiti da malware (7%) e minacce alla disponibilità di Internet (10%).

Individui Target: 11% degli eventi totali. Maggiormente colpiti da campagne di manipolazione delle informazioni (47%) e minacce legate ai dati (15%).

Servizi: Includono consulenza, servizi legali, ospitalità e sono raggruppati sotto la categoria 'Servizi'. 9% degli attacchi ransomware.

Figure 6: Targeted sectors per number of incidents (July 2022 - June 2023)



NIS 2

- **NIS1**: la Direttiva (UE) 2016/1148, nota con l'acronimo NIS (Network Information System) ha introdotto una serie di regole (di stampo tecnico e organizzativo) per le Organizzazioni che possiedono determinate caratteristiche di criticità sotto il profilo della postura di cybersicurezza, c.d. "infrastrutture critiche". Essa delinea un sistema coordinato, omogeneo, organico e integrato di regole in tema di cybersecurity, armonizzando quanto più possibile, a livello paneuropeo, la disciplina in materia di sicurezza informatica per gli Operatori di servizi pubblici essenziali (c.d. OSE), sulla base del presupposto che gli impatti di un eventuale incidente che coinvolgessero tali tipologie di soggetti giuridici potrebbero avere ripercussioni non indifferenti sull'intero sistema-Paese.

- **NIS2**: la successiva Direttiva 2022/2555 procede ad un aggiornamento della disciplina in esame, in particolare ampliando l'ambito soggettivo di applicazione. Ciò, in quanto in quanto il panorama delle minacce preso in considerazione nel 2016 non teneva conto delle nuove esigenze di tutela in settori di più recente sviluppo (e.g., le tecnologie 5G) nonché del legame, oramai indissolubile, dell'economia dell'Unione con l'utilizzo di apparati, sistemi e reti ICT.

NIS 2

La Direttiva stabilisce una scadenza chiara: gli Stati membri devono adottare le misure necessarie entro il 17 ottobre 2024 e iniziare ad applicarle dal 18 ottobre 2024;

Le organizzazioni potrebbero dover rivedere e potenziare le loro infrastrutture di sicurezza per rispondere alle nuove disposizioni.

La formazione del personale, la sensibilizzazione e l'aggiornamento diventeranno essenziali per garantire che tutti siano a conoscenza delle nuove responsabilità e obblighi.

NIS 2

- Anticipazione e Pianificazione: Le organizzazioni dovrebbero iniziare a valutare e pianificare le modifiche necessarie ben prima della scadenza del 2024
- Formazione continua: La formazione e l'aggiornamento del personale non sono solo essenziali, ma fondamentali. La comprensione delle nuove disposizioni favorirà la transizione verso il nuovo regime giuridico
- Collaborazione e Condivisione: La collaborazione tra settori e la condivisione delle migliori pratiche possono facilitare l'adozione delle nuove norme e rafforzare la postura di sicurezza complessiva

NIS 2

La Direttiva NIS 2 supera la distinzione tra OSE e FSD prevista dalla NIS 1.
Al loro posto, introduce alcuni criteri uniformi per identificare le due nuove categorie di soggetti che saranno soggette agli obblighi della direttiva ossia:

- *Soggetti "essenziali"*
- *Soggetti "importanti"*

Tali soggetti devono essere individuarsi nei settori ritenuti "essenziali", che comprendono sia i settori già individuati dalla Direttiva NIS 1, sia un ulteriore elenco di settori "**ad alta criticità**" (es. servizi sanitari, servizi postali, settore alimentare e di macchinari/apparecchiature, ulteriori servizi digitali).

Viene inoltre applicato un criterio dimensionale, che esclude dall'ambito di applicazione le piccole e medie imprese, salve alcune eccezioni che dipendono dalla criticità del servizio fornito (es. comunicazione elettronica o servizi fiduciari).

NIS 2 e GDPR

Cosa hanno in comune?

Attenzione alle terze parti ovvero mitigazione supply chain incident

Audit di seconda parte possono diventare lo strumento di compliance integrata tra art. 28 GDPR, obblighi derivanti da DORA, NIS 2 e Perimetro di Sicurezza Nazionale Cibernetica e anche standard di certificazione volontaria quali ISO/IEC 27001:2022

AI ACT

Regolamentazione sull'Intelligenza Artificiale nell'Unione Europea

L'AI Act nasce con l'obiettivo di creare un ambiente sicuro per l'innovazione tecnologica, assicurando al contempo che l'uso dell'intelligenza artificiale rispetti i diritti fondamentali delle persone.
Questo non si limita solo a guardare il prodotto finale; è essenziale prendere in considerazione l'intero processo, dalla concezione all'implementazione, assicurando che ogni tassello rispetti gli standard previsti.

L'AI Act si concentra sulla protezione dei diritti fondamentali, la sicurezza e l'assicurazione che l'IA sia usata in modo sicuro e conforme alla legge.
Il regolamento interagisce con altre normative dell'UE, garantendo la libera circolazione transfrontaliera di beni e servizi basati sull'IA.

AI ACT

Regolamentazione sull'Intelligenza Artificiale nell'Unione Europea

1. L'AI Act si concentra sui sistemi di IA che possono comportare rischi alti per i diritti fondamentali e la sicurezza.
2. Stabilisce requisiti di qualità elevata dei dati, documentazione, tracciabilità, trasparenza, sorveglianza umana, precisione e robustezza.
3. L'AI Act prevede l'istituzione di strutture e meccanismi di governance per coordinare l'utilizzo dell'IA in tutti gli Stati membri.
4. Norme e strumenti di sostegno per l'orientamento e la conformità forniranno assistenza a fornitori e utenti ai fini del rispetto dei requisiti stabiliti.
5. L'AI Act mira a garantire una concorrenza leale nel mercato dell'IA, evitando limitazioni contrarie al trattato sul funzionamento dell'Unione.
6. I fornitori di IA dovrebbero trarre beneficio da una serie minima ma chiara di requisiti, con certezza del diritto e assicurano l'accesso all'intero mercato unico.
7. Gli utenti IA dovrebbero beneficiare della certezza del diritto in merito al fatto che i sistemi di IA ad alto rischio che essi acquistano rispettano le normative.

THANKS FOR WATCHING!

We are available to answer your questions