Università degli Studi di Bari “Aldo Moro”

Dipartimento di Informatica

Corso di laurea in   
**Informatica e Tecnologie per la Produzione del Software**

Tesi di laurea in

**Cybersecurity**

**Definizione di Metodi e Tecniche per la Gestione del Rischio**

Relatori:

**Chiar.mo Prof. Danilo CAIVANO**

**Dott.ssa Vita Santa BARLETTA**

Laureando:

**Nicola BALZANO**

Anno Accademico 2023/2024

**Indice**

[Capitolo I – Stato dell’Arte 4](#_Toc162107974)

[Introduzione 4](#_Toc162107975)

[1.1 Internet of Things – Un mondo interconnesso 6](#_Toc162107976)

[1.2 Cybersecurity – Cos’è e di cosa si occupa 6](#_Toc162107977)

[1.3 Attacchi Cyber – Analisi delle tendenze 7](#_Toc162107978)

[1.4 NIS2 – L’ultima normativa nel mondo cyber 10](#_Toc162107979)

[1.5 Cyber Kill Chain – Cos’è e come usarla 11](#_Toc162107980)

[1.6 MITRE ATT&CK Framework 14](#_Toc162107981)

[1.7 MITRE ATLAS – Nuove tecnologie e nuove minacce 15](#_Toc162107982)

[Capitolo II 16](#_Toc162107983)

[Nuova Privacy Knowledge Base 16](#_Toc162107984)

[2.1 Privacy Design Pattern 17](#_Toc162107986)

[Bibliografia 18](#_Toc162107987)

# Capitolo I – Stato dell’Arte

Introduzione

Nell'era digitale in cui viviamo, **l'informatica** e la **cybersecurity** sono diventate componenti fondamentali della nostra **esistenza** **quotidiana**. Questo legame inscindibile tra tecnologia e sicurezza informatica è al centro della presente tesi, che esplora non solo come l'informatica ha plasmato il mondo moderno, ma soprattutto come la cybersecurity è diventata una materia indispensabile per proteggere i dati e le infrastrutture che sostengono la nostra società. Il mondo sta andando incontro all’evoluzione, giorno dopo giorno, mese dopo mese, anno dopo anno. L’**evoluzione** però non è solo positiva: ogni scoperta può essere interpretata sia come un progresso benefico, sia come una possibilità di impiego dannoso.

Nell'ambito della sicurezza informatica, la distinzione tra uso **legittimo** e **malintenzionato** delle nuove tecnologie è delineata da una linea estremamente sottile. Per anticipare, identificare e difendere efficacemente le infrastrutture digitali dalle minacce emergenti, diventa cruciale adottare un approccio proattivo, che sia costantemente aggiornato. In questo contesto, ciò che distingue l'uso legittimo da quello malevolo non è tanto la **conoscenza** in sé, quanto piuttosto gli **intenti** che guidano il suo impiego. Le tecniche di attacco evolvono di pari passo con le tecnologie di difesa, generando un **ciclo** **continuo** di sfide e risposte. Questa dinamica impone agli esperti di sicurezza informatica di andare oltre la semplice reazione agli incidenti, spingendoli a prevedere e prevenire attivamente le potenziali minacce.

Adottare tale approccio multidisciplinare, che integra una profonda comprensione delle **tattiche**, **tecniche** e **procedure** (**TTP**) impiegate dagli aggressori con l'uso di strumenti all'avanguardia come l'**analisi** **comportamentale**, la **threat** **intelligence** e l'**apprendimento** **automatico**, consente di anticipare e neutralizzare le minacce informatiche prima che queste si trasformino in attacchi concreti e dannosi. La capacità di rilevare precocemente le anomalie e i potenziali pericoli, analizzando e interpretando i segnali deboli all'interno del vasto mare di dati generati dalle attività di rete, rappresenta un pilastro fondamentale nella costruzione di un ecosistema digitale resiliente e sicuro.

In questo contesto, l'obiettivo primario della presente tesi è esattamente quello di esplorare e delineare l'importanza di un approccio proattivo nella sicurezza informatica, attraverso l'analisi dettagliata delle strategie offensive e difensive, insieme all'**implementazione** **di soluzioni innovative per la prevenzione e il rilevamento** di ogni possibile minaccia conosciuta.

## Internet of Things – Un mondo interconnesso

Per acquisire una piena comprensione del panorama della cybersecurity bisogna conoscere l’ambiente in cui ormai l’uomo da anni si muove.

Il concetto dell’**Internet delle Cose** [1] (**IoT**[[1]](#footnote-1)) è alla base della vita smart[[2]](#footnote-2) che l’uomo vive ogni giorno, descrive dispositivi dotati di sensori, capacità di elaborazione, software e altre tecnologie che collegano e scambiano dati con altri dispositivi e sistemi su Internet o altre reti di comunicazione.

La riflessione su chi detenga la vera conoscenza, se **siamo noi a esplorare il mondo o** se **è il mondo a scrutarci dettagliatamente**, assume un rilievo particolare nell'era attuale, dominata dalla presenza capillare di dispositivi connessi. Questi strumenti, progettati per agevolare la nostra esistenza, entrano nella sfera della nostra **privacy** per nostra stessa scelta, sollevando interrogativi imprescindibili: quali dati raccolgono su di noi? Con quale precisione possono anticipare i nostri interessi e desideri di acquisto? E come fanno a mappare così accuratamente le nostre routine quotidiane? Ancor più cruciale è comprendere le potenziali implicazioni legate alla divulgazione di queste informazioni personali.

Il compito della materia d’argomento di questo elaborato è proprio quello di rispondere all’ultima domanda.

## Cybersecurity – Cos’è e di cosa si occupa

La **Cybersecurity** [2]è una materia che ha il compito di **proteggere**, nel senso più ampio del termine, **infrastrutture** **digitali** come sistemi, reti e programmi software da attacchi informatici, finalizzati all’ottenimento, trasformazione, distruzione, di informazioni sensibili e/o interruzione di processi aziendali.

Al cuore della cybersecurity vi è la triade **CIA** [3] (Confidentiality, Integrity, Availability) che funge da pilastro per la sicurezza delle informazioni. Questo modello si prefigge di garantire la **riservatezza** (**Confidentiality**) proteggendo le informazioni sensibili dall'accesso non autorizzato, l'**integrità** (**Integrity**) assicurando che i dati non vengano alterati o distrutti in modo improprio, e la **disponibilità** (**Availability**) mantenendo l'accesso continuo e ininterrotto alle informazioni e ai sistemi per gli utenti autorizzati.

Insieme, questi principi formano il framework su cui si basano le strategie di difesa contro gli attacchi informatici, che puntano a violare queste fondamenta per infliggere danni o trarre vantaggi illeciti.

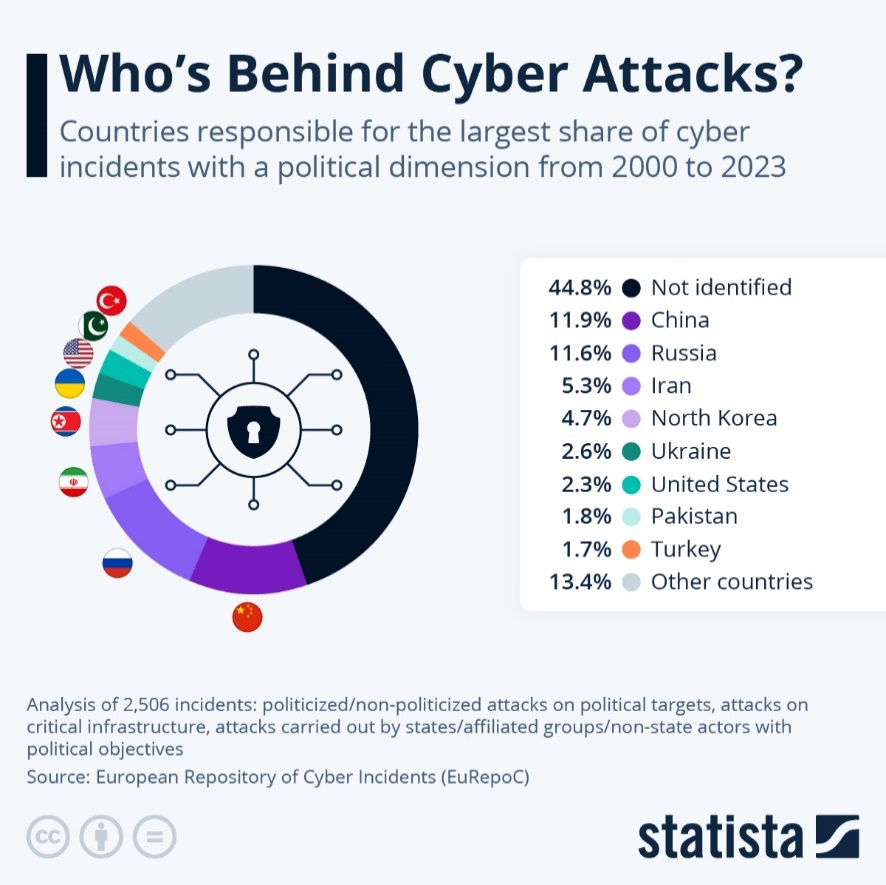
## Attacchi Cyber – Analisi delle tendenze

Negli ultimi anni, il panorama globale ha testimoniato l'urgente richiesta di avanzamenti tecnologici nel campo della difesa informatica, volti a proteggere dati, procedure e infrastrutture critici. Un'**indagine comparativa** recente [4], che confronta i dati relativi agli attacchi informatici noti fino al Q2[[3]](#footnote-3) 2022 e quelli registrati nel Q2 2023, ha evidenziato un incremento esponenziale nella media settimanale degli attacchi informatici a livello globale, interessando diversi settori industriali. Questo trend allarmante sottolinea non solo la crescente sofisticatezza e frequenza delle minacce informatiche, ma anche l'impellente necessità per le organizzazioni di ogni ambito di rafforzare le loro misure di sicurezza per contrastare efficacemente tali pericoli.

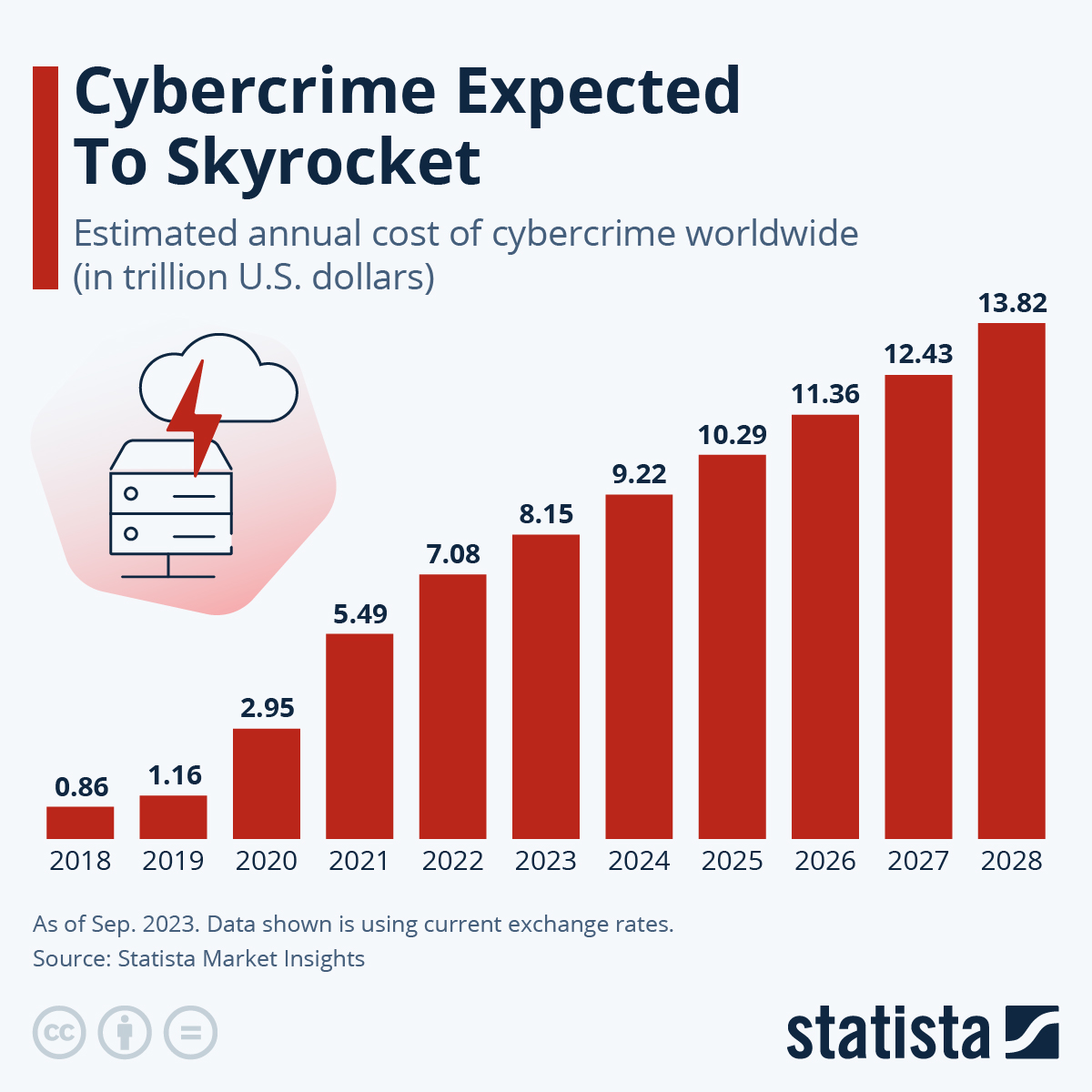


I dati allarmanti emersi dallo studio mostrano un incremento significativo degli attacchi informatici, con particolare enfasi sui settori delle consulenze, bancario e sanitario. Tra questi, il **settore** **sanitario** emerge come particolarmente **critico**, non solo perché rappresenta il terzo settore più colpito al mondo da questa ondata di attacchi, ma anche per l'ampia quantità di introiti che genera a livello globale e per il **vasto** **volume** **di** **informazioni** **sensibili** che gestisce. Questa situazione mette in luce l'urgenza con cui il settore sanitario deve affrontare le sfide legate alla cybersecurity, sottolineando l'importanza di implementare misure di protezione avanzate per salvaguardare dati di vitale importanza.

Un altro grande problema dilemma è dovuto alla provenienza di questi attacchi. Uno studio [5] in cui sono coinvolte la Cybersecurity and Infrastructure Security Agency (**CISA**), la National Security Agency (**NSA**) e il Federal Bureau of Investigation (**FBI**) evidenzia che circa il 45% di questi attacchi ha origine ignota, perciò la **tracciabilità** e l'**identificazione** **degli aggressori** rappresentano ancora sfide significative nel contrasto alle minacce informatiche.



Basandosi sulle valutazioni della fonte che ha fornito i dati menzionati in precedenza, il **costo annuale globale associato alla mitigazione dei crimini informatici** [6] nei prossimi 4 anni è destinato ad aumentare in maniera lineare di circa **1,5 trilioni di dollari statunitensi** all’anno.



## NIS2 – L’ultima normativa nel mondo cyber

Il mondo ha iniziato a mobilitarsi per rispondere alle minacce derivanti dalla evolutiva sfera informatica, molto sono state le normative che hanno coinvolto questo dominio di conoscenza.

La direttiva più recente è la cosiddetta **NIS2** (**Network and Information Systems 2**), entrata in vigore nel 17 gennaio 2023, rappresenta un passo significativo verso il rafforzamento della resilienza e della sicurezza delle reti e dei sistemi informativi all'interno dell'**Unione Europea**, dove gli stati membri dovranno incorporare questa normativa entro il 17 ottobre 2024. Questa nuova direttiva si propone di aggiornare e ampliare l'ambito di applicazione della antesignana direttiva **NIS1**, per porre rimedio all’aumento del tasso digitalizzazione in tutti i Paesi membri, il quale ha inasprito la superfice di attacco informatico.

La normativa rende più stringenti:

* **requisiti di governance**, in modo che gli organi di gestione di una struttura economica approvino misure per la *gestione dei rischi* dell’Organizzazione e una *formazione* *periodica* su tematiche di cybersicurezza;
* **gestione dei rischi**, inserendo l’obbligo di *valutare* *i* *rischi* e attuare le necessarie *misure* *tecniche* *e* *organizzative* anche nell’ambito della supply chain e rapporti con i propri fornitori**;**
* **segnalazione** **di** **incidenti** **avvenuti**, notificandoli ai rispettivi *CSIRT[[4]](#footnote-4)* o *autorità* *nazionale* entro 24 ore dall’evento.

La NIS2 mira a **stabilire** un livello comune elevato di sicurezza delle reti e dei sistemi informativi tra gli Stati membri, promuovendo al contempo una **maggiore** **cooperazione** e condivisione delle informazioni sulle minacce informatiche all'interno dell'UE. Tra le novità più rilevanti, la direttiva prevede l'istituzione di punti di contatto nazionali per la cybersecurity, l'obbligo di notifica degli incidenti informatici e l'introduzione di **sanzioni** significative **per** **le** **violazioni**, pari ad un massimo di 10.000.000 EUR.

Implementando misure come queste, la NIS2 non solo cerca di proteggere le infrastrutture critiche europee, ma anche di creare un ambiente digitale più sicuro per cittadini, imprese e governi. L'**obiettivo** è di anticipare, prevenire e rispondere efficacemente agli attacchi informatici, assicurando così la continuità dei servizi essenziali su cui la società moderna si affida profondamente.

## Cyber Kill Chain – Cos’è e come usarla

Per poter prevenire che accada qualsiasi tipo di incidente in natura di sicurezza informatica, bisogna comprendere a pieno come questi vengono messi in atto. Il modello che descrive le fasi con cui avviene un cyber-attacco è stato concretizzato e definito come **Cyber Kill Chain** [8].

È fondamentale analizzare e capire in dettaglio la Cyber Kill Chain per implementare efficacemente misure di prevenzione e difesa. Questo modello, sviluppato per descrivere le fasi sequenziali di un attacco informatico, offre agli esperti di sicurezza una visione strutturata dei processi attraverso cui un aggressore pianifica e esegue un attacco.



Le *fasi* di cui è composta la Cyber Kill Chain sono:

1. **Reconaissance**: volta a ottenere informazioni sulla vittima al fine di capire le modalità con cui agire successivamente. Può essere svolta in due modalità:
   1. ***Passiva***: utilizza metodi che non permettono all’individuo/organizzazione target di essere individuati (es. Domain Names, whois, Social Network).
   2. ***Attiva***: permette di ottenere un profilo del target più specifico ma potrebbe mettere in allerta la vittima (es. Port scanning and Services).
2. **Weponaize**: ha lo scopo di progettare il metodo con cui agire, tramite le informazioni ottenute precedentemente, progettando e sviluppando due componenti:
   1. ***RAT***: *Remote Acces Tool*, è la parte di software che permette di ottenere l’accesso al sistema target quando viene eseguita sul sistema target, solitamente anche chiamata *payload of cyber-weapon*.
   2. ***Exploit***: è lo script che permette di eseguire il RAT utilizzando vulnerabilità dei sistemi/software target, tramite l’utilizzo di *CVE*[[5]](#footnote-5).
3. **Delivery**: la parte critica della catena per un attacker[[6]](#footnote-6), l’*alto rischio* è dovuto alle possibili tracce che vengono lasciate dal cyber criminale. Nessun metodo permette di ottenere il 100% di successo in questa fase, ma anche un tentativo andato male permette di ottenere rilevanti informazioni sul target.
4. **Exploitation**: è la fase in cui vengono sfruttate le CVE per eseguire lo script sviluppato precedentemente, molte volte non è sufficiente un solo *exploit*, bensì si utilizzano *exploit kit[[7]](#footnote-7)*.
5. **Installation**: prevede l’istallazione del RAT eludendo tutti i sistemi di sicurezza della vittima (ad es. Anti-Virus, Anti-Debugger, Anti-Emulation), tramite l’utilizzo di *Rootkit* e *Bootkit*, rendendo l’accesso ai sistemi della vittima persistente.
6. **Command & Controll (C2)**: in questa fase l’attacker riesce a comunicare con i sistemi infetti, negli anni sono nate differenti strutture per portare a termine questo step:
   1. ***Struttura Centralizzata***: classica *struttura client-server*, la limitazione consiste nel numero di risorse hardware/software disponibili nel *C2 Server*.
   2. ***Struttura Decentralizzata*:** prevede l’utilizzo della modalità di *comunicazione peer-to-peer*, la quale permette alta scalabilità e tolleranza verso gli errori di trasmissione.
   3. ***Struttura basata sui Social Network***: permette di passare le informazioni tramite l’utilizzo di social network (es. *Taidoor*)
7. **Act on Objective**: l'ultima fase della Cyber Kill Chain, implica *il raggiungimento dell'obiettivo* *prefissato* dall'aggressore. Dopo aver stabilito una presenza solida all'interno del sistema e aver ottenuto il controllo necessario tramite le fasi precedenti, l'attaccante esegue le azioni finali che possono variare a seconda delle sue intenzioni. Queste possono includere il furto di dati sensibili, la distruzione di informazioni critiche o asset aziendali o qualsiasi altro obiettivo malevolo (ad es. Ransoware, BOTNets, DDos, ZeroDay, Data exfiltration).

## APT -

## MITRE ATT&CK Framework

## MITRE ATLAS – Nuove tecnologie e nuove minacce

# Capitolo II

Nuova Privacy Knowledge Base



## Privacy Design Pattern

sium

# Bibliografia

[1] *Cisco* (2022).   
https://www.cisco.com/c/it\_it/products/security/what-is-cybersecurity.html

[2] *Wikipedia* (2024, marzo 11). https://it.wikipedia.org/wiki/Internet\_delle\_cose

[3] *Cisco* (2023).   
https://www.learncisco.net/courses/iins/common-security-threats/information-security-and-common-threats.html

[4] *Check Point* (2023, luglio ). https://blog.checkpoint.com/security/average-weekly-global-cyberattacks-peak-with-the-highest-number-in-2-years-marking-an-8-growth-year-over-year-according-to-check-point-research/

[5] *Statista* (2024, febbraio 23). https://www.statista.com/chart/31805/countries-responsible-for-the-largest-share-of-cyber-incidents/

[6] Statista (2024, febbraio 22). https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/

[7] *Agenda Digitale Eu* (2024, gennaio 25). https://www.agendadigitale.eu/sicurezza/obblighi-di-cyber-sicurezza-come-adeguarsi-alla-direttiva-nis2/

[8] Tauran Yadav, Rao Arvind Mallari (2016, giugno 10).  
Technical Aspect of Cyber Kill Chain

1. Acronimo del neologismo **Internet of Things**. [↑](#footnote-ref-1)
2. Si riferisce a uno stile di vita reso più efficiente e comodo attraverso l'uso di dispositivi connessi e tecnologie intelligenti. [↑](#footnote-ref-2)
3. Secondo semestre [↑](#footnote-ref-3)
4. **Computer Security Incident Response Team**, gruppo di sicurezza governativo con il compito di regolamentare le cooperazioni con il settore privato nella sfera della cybersicurezza. [↑](#footnote-ref-4)
5. Common Vulnerabilities and Exposures, falle di sicurezza rese pubbliche. [↑](#footnote-ref-5)
6. Colui che svolge l’attacco. [↑](#footnote-ref-6)
7. Combinazione di exploit (es. per attacchi a sistemi web questi coprono l’eventualità di utilizzo di CVE in base ai di differenti Browser esistenti) [↑](#footnote-ref-7)