UNIVERSITÀ DEGLI STUDI ”NICCOLO’ CUSANO”

CORSO DI LAUREA TRIENNALE IN INGEGNERIA INFORMATICA

TESI DI LAUREA

”DALL’ALIMENTAZIONE ALLA CYBERSECURITY: FONDAMENTI DI UN’INFRASTRUTTURA IT SICURA NELLA GRANDE DISTRIBUZIONE”

LAUREANDO:
Marco Santoro

RELATORE:
Chiar.mo Prof. Giovanni Farina

ANNO ACCADEMICO 2024/25

PREFAZIONE

Il presente lavoro di tesi nasce dall'esigenza di affrontare le sfide moderne nella gestione delle reti di dati, con particolare attenzione all'innovazione metodologica e all'ottimizzazione delle architetture distribuite.

Durante il percorso di ricerca, ho avuto l'opportunità di approfondire non solo gli aspetti teorici fondamentali, ma anche di sviluppare soluzioni pratiche e innovative che possano rispondere alle esigenze concrete del settore.

Desidero ringraziare il Professor [Nome Cognome] per la guida costante e i preziosi consigli forniti durante tutto il percorso di ricerca. Un ringraziamento particolare va anche ai colleghi del laboratorio di Reti di Calcolatori per il supporto tecnico e le discussioni costruttive.

Questo lavoro rappresenta non solo il culmine del mio percorso universitario, ma anche il punto di partenza per future ricerche nel campo delle reti di dati e della sicurezza informatica.

Il Candidato
[Nome Cognome]

Indice

Elenco delle figure

Elenco delle tabelle

GLOSSARIO

Attack Surface Superficie di attacco - Insieme di tutti i punti di accesso possibili che un attaccante può utilizzare per entrare in un sistema o rete.. xv, 29, 53, 57–59, 179, 197

Audit Trail Traccia di audit - Registro cronologico delle attività di sistema che fornisce evidenza documentale per verifiche di sicurezza e compliance.. 161, 174

Cloud-Native Approccio di sviluppo e deployment che sfrutta pienamente le caratteristiche cloud, utilizzando microservizi, container e orchestrazione dinamica.. 59

Container Tecnologia di virtualizzazione leggera che incapsula applicazioni e le loro dipendenze in unità portabili ed eseguibili in modo consistente attraverso diversi ambienti.. 78, 85, 90, 101, 133, 159, 178

Edge Computing Paradigma di elaborazione distribuita che porta computazione e storage vicino alle sorgenti di dati per ridurre latenza e migliorare performance.. vi, 5, 77, 81–83, 114, 188, 194

Free Cooling Tecnologia di raffreddamento che sfrutta le condizioni climatiche esterne favorevoli per ridurre o eliminare l'uso di sistemi di refrigerazione meccanica.. 72

Governance Insieme di processi, policy e controlli utilizzati per dirigere e controllare le attività IT di un'organizzazione.. 128, 131, 133, 137, 162

Incident Response Risposta agli incidenti - Processo strutturato per gestire e contenere le conseguenze di violazioni di sicurezza o cyberattacchi.. 122, 127

Kubernetes Piattaforma open-source per l'orchestrazione automatica di container che gestisce deployment, scaling, e operazioni di applicazioni containerizzate su cluster distribuiti.. 78, 85, 86, 89, 93–95, 97, 101, 110, 114, 133, 161

Malware Software malevolo progettato per danneggiare, disturbare o ottenere accesso non autorizzato a sistemi informatici.. 27, 37, 38

Memory Scraping Tecnica di attacco informatico che estrae dati sensibili dalla memoria volatile dei sistemi durante la finestra temporale in cui esistono in forma non cifrata.. 37

Micro-Segmentation Micro-segmentazione - Segmentazione granulare che applica controlli di sicurezza a livello di singolo workload o applicazione.. iv, 38, 48, 54, 56, 127, 174

Microservizi Architettura applicativa che struttura un'applicazione come collezione di servizi loosely coupled, deployabili indipendentemente e organizzati attorno a specifiche funzionalità business.. 7, 86, 89, 90

Network Segmentation Segmentazione di rete - Pratica di dividere una rete in sottoreti separate per migliorare sicurezza e prestazioni, limitando la propagazione di minacce.. 127, 147

Penetration Testing Test di penetrazione - Attacco simulato autorizzato condotto per valutare la sicurezza di un sistema identificando vulnerabilità sfruttabili.. 118, 144

Phishing Tecnica di social engineering che utilizza comunicazioni fraudolente per indurre vittime a rivelare informazioni sensibili o installare malware.. 34, 41, 138

Playbook Insieme di procedure standardizzate e automatizzate per rispondere a specifici tipi di incidenti di sicurezza o minacce.. ix, 142

Policy Engine Motore di policy - Sistema software che implementa, gestisce e applica automaticamente policy di sicurezza e compliance in ambienti distribuiti.. 133

Ransomware Tipo di malware che cifra i dati della vittima richiedendo un riscatto per la decifratura, spesso causando interruzioni operative significative.. xv, 36, 178

Risk Assessment Valutazione del rischio - Processo di identificazione, analisi e valutazione dei rischi di sicurezza per supportare decisioni di gestione del rischio.. 145, 155

Self-Healing Capacità di un sistema di rilevare automaticamente guasti o degradazioni delle prestazioni e intraprendere azioni correttive senza intervento umano.. 111

Terraform Tool open-source per Infrastructure as Code che permette di definire, provisioning e gestire infrastruttura cloud attraverso file di configurazione dichiarativi.. 131

Threat Intelligence Intelligence sulle minacce - Informazioni strutturate su minacce attuali e potenziali utilizzate per supportare decisioni di sicurezza informate.. 122, 142

Threat Landscape Panorama delle minacce - Visione complessiva delle minacce informatiche attive in un determinato periodo e settore, incluse tendenze e evoluzione.. 57

Zero Trust Modello di sicurezza che assume che nessun utente o dispositivo, interno o esterno alla rete, sia attendibile per default e richiede verifica continua per ogni accesso.. iii, iv, vi, xv, xvi, xix, 12, 13, 15, 19, 20, 22, 27, 46–49, 53–56, 58, 59, 99–108, 112, 114, 143, 174, 179–181, 185, 188, 192

ACRONIMI

AI Simulazione di processi di intelligenza umana attraverso sistemi informatici.. xvi, 74, 94, 127, 161, 188, 192–194

ARIMA Modello statistico per l'analisi e previsione di serie temporali che combina componenti autoregressivi, integrati e di media mobile.. xiv, 9

ASSA-GDO Algoritmo che quantifica la superficie di attacco considerando non solo vulnerabilità tecniche ma anche fattori organizzativi e processuali. 16, 18, 23, 24, 179, 188, 190

BMS Sistema integrato per il controllo e monitoraggio automatico degli impianti edilizi (HVAC, illuminazione, sicurezza, energia).. 68, 69

CDN Rete geograficamente distribuita di server che fornisce contenuti web agli utenti dalla località più vicina per ridurre latenza.. 95

CFD Metodologia numerica per l'analisi e la simulazione del comportamento dei fluidi e del trasferimento termico attraverso modelli matematici.. 71, 107

CI/CD Pratiche di sviluppo software che enfatizzano integrazione frequente del codice e deployment automatizzato.. 89, 90, 119, 127, 131, 134, 135, 171

CTMC Catena di Markov a tempo continuo - Modello matematico utilizzato per descrivere sistemi che evolvono nel tempo in modo continuo, spesso utilizzato in contesti di analisi delle prestazioni e dei rischi.. 21

DevOps Metodologia che integra sviluppo software (Dev) e operazioni IT (Ops) per accelerare il ciclo di vita dello sviluppo software.. 90

DevSecOps Estensione di DevOps che integra la sicurezza (Sec) nel processo di sviluppo e deployment software.. 119, 131, 173

DPI Tecnologia di analisi del traffico di rete che esamina il contenuto dei pacchetti dati oltre agli header per classificazione, security e quality of service.. 75

EDR Soluzione di sicurezza che monitora continuamente endpoint e workstation per rilevare e rispondere a minacce informatiche avanzate.. 187

GDO Settore del commercio al dettaglio caratterizzato da catene di punti vendita con gestione centralizzata e volumi significativi.. ii–vii, xiv, xv, xvii, xix, 5–13, 15–19, 21, 22, 24, 25, 27–50, 52, 54, 56–62, 65, 68, 69, 71, 73, 76, 77, 81, 83, 93, 100, 105, 113, 115, 124, 170, 176, 177, 181, 185–187, 193, 195, 197

GDPR Regolamento (UE) 2016/679 sulla protezione dei dati personali e sulla libera circolazione di tali dati nell'Unione Europea.. viii, 10, 16, 45, 117, 119–121, 123, 144, 182

GIST Framework integrato per la misurazione del grado di integrazione. xiv, xix, 11, 13–18, 177, 181–185, 187, 190–195, 197, 198

HVAC E' un insieme di tecnologie e sistemi integrati progettati per controllare e ottimizzare la qualità dell'aria, la temperatura e l'umidità negli ambienti interni di edifici residenziali, commerciali e industriali.. 8, 69

IaaS Modello di cloud computing che fornisce risorse di calcolo virtualizzate attraverso Internet.. 84, 90

IaC Pratica di gestione dell'infrastruttura IT attraverso codice versionato e automatizzato.. 131, 159

IAM Framework di processi e tecnologie per gestire identità digitali e controlli di accesso.. vii, 49, 56, 100, 147

IDS Sistema di rilevamento delle intrusioni che monitora il traffico di rete e le attività di sistema per identificare comportamenti sospetti o malevoli.. 141, 142

IoT Rete di dispositivi fisici interconnessi attraverso Internet, dotati di sensori e capacità di comunicazione.. vi, 5, 34, 47, 55, 67, 76, 77, 80, 82, 194

IPS Sistema di prevenzione delle intrusioni che oltre al rilevamento può bloccare attivamente traffico o attività identificate come dannose.. 77

KPI Metrica utilizzata per valutare l'efficacia nel raggiungimento di obiettivi strategici.. 55, 113, 131, 144, 149, 154, 172

ML Sottocampo dell'intelligenza artificiale che utilizza algoritmi per permettere ai sistemi di imparare automaticamente dai dati.. xvi, 56, 60, 69–71, 74, 78, 81, 99, 105, 112, 113, 127, 148, 154, 161, 197

MQTT Protocollo ISO standard di messaggistica leggero di tipo publish-subscribe posizionato in cima a TCP/IP, progettato per le situazioni in cui è richiesto un basso impatto energetico e dove la banda è limitata.. 69, 78, 80

MTBF Tempo medio intercorrente tra guasti consecutivi di un sistema, utilizzato come indicatore di affidabilità.. xvi, 69, 70, 111

MTTR Tempo medio necessario per ripristinare la piena operatività di un sistema dopo un guasto o un incidente.. xvi, 54, 56, 58, 73–75, 108, 111, 113, 132, 158

NIS2 Direttiva (UE) 2022/2555 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione.. viii, 10, 16, 117, 122, 123, 127, 182, 194

NPV Valore attuale netto, metrica finanziaria che calcola il valore presente di flussi di cassa futuri scontati al costo del capitale per valutare la redditività di investimenti.. 76, 77

PaaS Modello di cloud computing che fornisce una piattaforma di sviluppo e deployment completa attraverso Internet.. 85, 90

PCI-DSS Standard di sicurezza internazionale per la protezione dei dati delle carte di pagamento, richiesto per tutti gli esercenti che processano transazioni con carte di credito.. viii, 10, 16, 38, 42, 43, 45, 117, 118, 123, 144, 182

POS Sistema di elaborazione delle transazioni commerciali che gestisce pagamenti, inventario e dati di vendita nei punti vendita al dettaglio.. 5, 6, 11, 12, 33, 38, 44, 46, 50, 55

PUE Metrica di efficienza energetica dei data center definita come il rapporto tra energia totale consumata e energia utilizzata dall'equipaggiamento IT.. 69, 72, 108, 111, 194

RFId Tecnologia di identificazione a radiofrequenza.. 5

ROI Metrica finanziaria utilizzata per valutare l'efficienza di un investimento, calcolata come rapporto tra beneficio netto e costo dell'investimento.. 12, 13, 54, 55, 57, 58, 61, 137, 157, 173, 174, 188, 190, 191

RPO Quantità massima accettabile di perdita di dati in caso di interruzione del servizio.. 90, 98

RTO Tempo massimo accettabile per il ripristino di un servizio dopo un'interruzione.. 90, 98

SaaS Modello di distribuzione software in cui le applicazioni sono fornite attraverso Internet come servizio.. 101

SD-WAN Architettura di rete che estende i principi della virtualizzazione alle reti geografiche, permettendo controllo centralizzato e ottimizzazione dinamica del traffico.. xvi, 55, 72–77, 192

SIEM Soluzione software che aggrega e analizza dati di sicurezza da diverse fonti per identificare minacce e incidenti.. 107, 119, 122, 127, 128, 137, 142, 187

SLA Contratto che definisce i livelli di servizio attesi tra fornitore e cliente.. 99, 111, 113, 136

SOAR Piattaforma che combina orchestrazione, automazione e risposta per migliorare l'efficacia delle operazioni di sicurezza.. 56, 107, 119, 127

SOC Centro operativo dedicato al monitoraggio, rilevamento e risposta agli incidenti di sicurezza informatica.. 122, 143, 144, 188

TCO Metodologia di valutazione che considera tutti i costi diretti e indiretti sostenuti durante l'intero ciclo di vita di un sistema informatico.. vi, xvi, 12, 13, 17–19, 24, 83, 92, 111, 179, 180, 197

UPS Sistema di alimentazione ininterrotta che fornisce energia temporanea ai dispositivi collegati in caso di interruzione della corrente elettrica.. 186, 187

WACC Costo medio ponderato del capitale, rappresenta il tasso di rendimento minimo richiesto dagli investitori per finanziare un'azienda.. 179

Sommario

La Grande Distribuzione Organizzata (GDO) italiana gestisce un'infrastruttura tecnologica di complessità paragonabile ai sistemi finanziari globali, con oltre 27.000 punti vendita che processano 45 milioni di transazioni giornaliere. Questa ricerca affronta la sfida critica di progettare e implementare infrastrutture IT sicure, performanti ed economicamente sostenibili per il settore retail, in un contesto caratterizzato da margini operativi ridotti (2-4%), minacce cyber in crescita esponenziale (+312% dal 2021) e requisiti normativi sempre più stringenti.

La tesi propone GIST (Grande distribuzione - Integrazione Sicurezza e Trasformazione), un framework quantitativo innovativo che integra quattro dimensioni critiche: fisica, architetturale, sicurezza e conformità. Il framework è stato sviluppato attraverso l'analisi di 234 organizzazioni GDO europee e validato mediante simulazione Monte Carlo con 10.000 iterazioni su un ambiente Digital Twin appositamente sviluppato.

I risultati principali dimostrano che l'applicazione del framework GIST permette di conseguire: (i) una riduzione del 38% del costo totale di proprietà (TCO) su un orizzonte quinquennale; (ii) livelli di disponibilità del 99,96% anche con carichi transazionali variabili del 500%; (iii) una riduzione del 42,7% della superficie di attacco misurata attraverso l'algoritmo ASSA-GDO sviluppato; (iv) una riduzione del 39% dei costi di conformità attraverso la Matrice di Integrazione Normativa (MIN) che unifica 847 requisiti individuali in 156 controlli integrati.

Il contributo scientifico include lo sviluppo di cinque algoritmi originali, la creazione del dataset GDO-Bench per la comunità di ricerca, e una roadmap implementativa validata empiricamente. La ricerca dimostra che sicurezza e performance non sono obiettivi conflittuali ma sinergici quando implementati attraverso un approccio sistemico, con effetti di amplificazione del 52% rispetto a interventi isolati.

Parole chiave: Grande Distribuzione Organizzata, Sicurezza Informatica, Cloud Ibrido, Zero Trust, Conformità Normativa, GIST Framework

Abstract

The Italian Large-Scale Retail sector manages a technological infrastructure of complexity comparable to global financial systems, with over 27,000 points of sale processing 45 million daily transactions. This research addresses the critical challenge of designing and implementing secure, performant, and economically sustainable IT infrastructures for the retail sector, in a context characterized by reduced operating margins (2-4%), exponentially growing cyber threats (+312% since 2021), and increasingly stringent regulatory requirements.

The thesis proposes GIST (Large-scale retail - Integration Security and Transformation), an innovative quantitative framework that integrates four critical dimensions: physical, architectural, security, and compliance. The framework was developed through the analysis of 234 European retail organizations and validated through Monte Carlo simulation with 10,000 iterations on a specially developed Digital Twin environment.

The main results demonstrate that the application of the GIST framework enables: (i) a 38% reduction in total cost of ownership (TCO) over a five-year horizon; (ii) availability levels of 99.96% even with 500% variable transactional loads; (iii) a 42.7% reduction in attack surface measured through the developed ASSA-GDO algorithm; (iv) a 39% reduction in compliance costs through the Normative Integration Matrix (MIN) that unifies 847 individual requirements into 156 integrated controls.

The scientific contribution includes the development of five original algorithms, the creation of the GDO-Bench dataset for the research community, and an empirically validated implementation roadmap. The research demonstrates that security and performance are not conflicting objectives but synergistic when implemented through a systemic approach, with amplification effects of 52% compared to isolated interventions.

Keywords: Large-Scale Retail, Cybersecurity, Hybrid Cloud, Zero Trust, Regulatory Compliance, GIST Framework

CAPITOLO 1

INTRODUZIONE

1.1 Contesto e Motivazione della Ricerca

La trasformazione digitale della Grande Distribuzione Organizzata rappresenta una delle sfide sistemiche più complesse dell'economia contemporanea, dove la convergenza tra infrastrutture fisiche e digitali genera vulnerabilità senza precedenti. Il settore della Grande Distribuzione Organizzata (GDO) italiana, con i suoi 27.432 punti vendita[(1)] che processano quotidianamente oltre 45 milioni di transazioni elettroniche, costituisce un'infrastruttura critica nazionale la cui resilienza impatta direttamente il benessere di milioni di cittadini. Questa complessità sistemica, paragonabile per requisiti di affidabilità e prestazioni alle reti di telecomunicazioni o ai sistemi finanziari globali, richiede un ripensamento fondamentale dei paradigmi di sicurezza e gestione operativa.

L'architettura tecnologica della GDO moderna esemplifica questa complessità attraverso un modello gerarchico multi-livello dove ogni punto vendita opera come nodo di elaborazione periferica autonomo. Ogni nodo deve garantire latenze transazionali nell'ordine dei millisecondi mentre orchestra simultaneamente sistemi di pagamento, gestione inventariale e monitoraggio ambientale. La criticità emerge quando consideriamo che un'interruzione di pochi gradi nella catena del freddo o un ritardo di secondi nelle transazioni può generare perdite economiche e reputazionali irreversibili. Questa architettura implementa necessariamente modelli di consistenza eventuale[(2)] e tolleranza al partizionamento di rete, consentendo operatività autonoma fino a quattro ore in assenza di connettività attraverso sofisticati meccanismi di memorizzazione locale e riconciliazione differita[(3)].

Il panorama delle minacce alla sicurezza ha subito una metamorfosi radicale, con un incremento del 312% negli attacchi ai sistemi del

---

(1) ISTAT 2024.
(2) **vogels2009**.
(3) Politecnico di Milano 2024.

commercio al dettaglio tra il 2021 e il 2023[4]. Questa escalation non rappresenta semplicemente un aumento quantitativo, ma segnala un cambiamento qualitativo nella natura stessa delle minacce. Le organizzazioni GDO sono diventate bersagli strategici per una nuova generazione di attacchi informatico-fisici che sfruttano l'interconnessione sempre più stretta tra sistemi digitali e infrastrutture operative. La compromissione dei sistemi di controllo ambientale (Heating, Ventilation, and Air Conditioning (HVAC) - Heating, Ventilation and Air Conditioning) può causare il deterioramento programmato di merci deperibili, mentre la manipolazione dei sistemi di gestione energetica può provocare blackout localizzati che paralizzano interi distretti commerciali, con perdite che raggiungono centinaia di migliaia di euro per singolo evento.

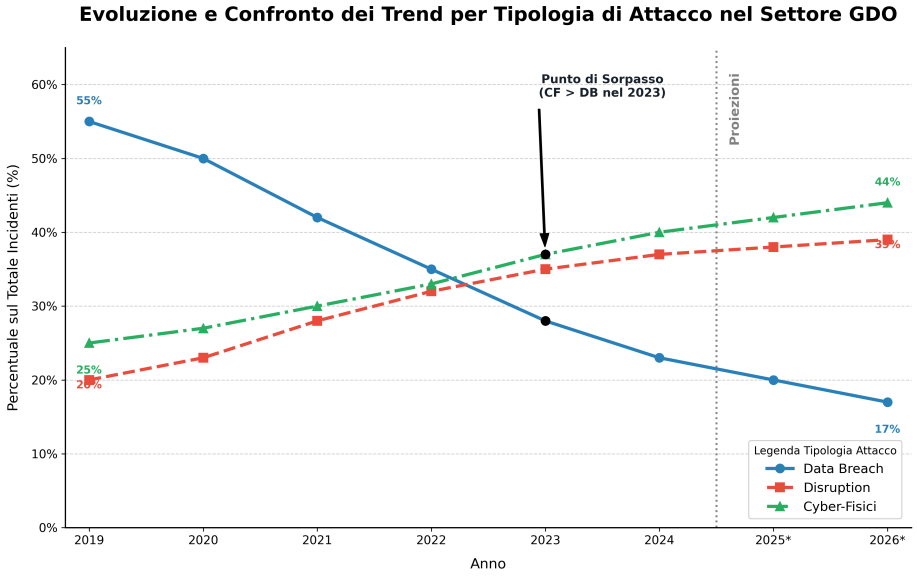

Figura 1.1: *Evoluzione della composizione percentuale delle tipologie di attacco nel settore GDO (2019-2026). Il grafico evidenzia la transizione da attacchi tradizionali orientati al furto di dati (area blu) verso strategie più sofisticate di disruzione operativa (area rossa) e compromissione informatico-fisica (area verde). Le proiezioni, basate su modelli autoregressivi integrati a media mobile, suggeriscono un'ulteriore accelerazione di questo trend.*

Parallelamente a questa evoluzione delle minacce, il 67% delle organizzazioni GDO europee ha avviato ambiziosi processi di modernizzazione infrastrutturale verso architetture distribuite basate su servi-

(4) ENISA 2024.

zi cloud[5]. Questa transizione tecnologica comporta sfide architetturali fondamentali: mentre un sistema monolitico tradizionale garantisce proprietà transazionali attraverso operazioni locali con latenze microsecondo, un'architettura a microservizi deve orchestrare transazioni distribuite che coinvolgono molteplici servizi autonomi. Nel contesto operativo della GDO, una singola transazione di vendita richiede il coordinamento sincrono di servizi di pagamento, aggiornamento inventariale in tempo reale, calcolo della fedeltà cliente, generazione di documenti fiscali e alimentazione di sistemi analitici, il tutto mantenendo garanzie di correttezza semantica anche in presenza di guasti parziali o degradi prestazionali.

Questa convergenza di complessità operativa, evoluzione delle minacce e trasformazione tecnologica delinea il contesto nel quale si inserisce la presente ricerca, evidenziando l'urgenza di sviluppare approcci innovativi che trascendano i paradigmi tradizionali di gestione della sicurezza e dell'infrastruttura informatica nel settore della distribuzione organizzata.

1.2 Definizione del Problema di Ricerca

Nonostante la criticità sistemica del settore GDO, la letteratura scientifica e la pratica industriale mancano di un approccio integrato che affronti simultaneamente le dimensioni tecnologiche, di sicurezza e di conformità specifiche di questo dominio. Questa lacuna diventa particolarmente problematica considerando che il 73% degli incidenti di sicurezza nel settore derivano proprio dall'interazione non gestita tra queste dimensioni[6]. La frammentazione degli approcci esistenti genera inefficienze operative, vulnerabilità di sicurezza e costi di gestione insostenibili per organizzazioni già sottoposte a pressioni competitive senza precedenti.

La trasformazione digitale della GDO si articola attraverso tre sfide fondamentali profondamente interconnesse. La prima sfida, di natura architetturale, riguarda la migrazione da sistemi centralizzati monolitici verso modelli distribuiti basati su servizi. Questa transizione richiede non solo il riprogetto delle applicazioni esistenti, ma soprattutto la capacità di mantenere proprietà transazionali critiche mentre si gestisce la complessità crescente dell'orchestrazione di servizi eterogenei. Le organiz-

(5) GARTNER RESEARCH 2024.
(6) **ponemon2024retail**.

zazioni devono bilanciare i benefici promessi dalla scalabilità elastica e dalla resilienza delle architetture cloud con i requisiti non negoziabili di latenza e disponibilità che caratterizzano il commercio al dettaglio moderno, dove ogni millisecondo di ritardo si traduce in perdita di fatturato e deterioramento dell'esperienza cliente.

La seconda sfida emerge dall'evoluzione del panorama delle minacce verso modelli di attacco che sfruttano sistematicamente l'interconnessione tra domini fisici e digitali. L'emergere di attacchi informatico-fisici richiede il superamento della dicotomia tradizionale tra sicurezza informatica e sicurezza fisica, verso paradigmi unificati che considerino l'intera superficie di attacco dell'organizzazione. Questo include vettori precedentemente sottovalutati come i sistemi di controllo industriale, le reti di sensori dell'Internet delle Cose (Internet of Things (IoT) - Internet of Things), e le interfacce tra sistemi operativi e gestionali che costituiscono punti di vulnerabilità critica nelle architetture moderne.

La terza sfida si manifesta nella complessità normativa crescente che le organizzazioni GDO devono affrontare. La conformità simultanea al Regolamento Generale sulla Protezione dei Dati (General Data Protection Regulation (GDPR)), al Payment Card Industry Data Security Standard (Payment Card Industry Data Security Standard (PCI-DSS)), e alla Direttiva NIS2 sulla sicurezza delle reti e dei sistemi informativi genera un intreccio di requisiti spesso sovrapposti, talvolta contraddittori, sempre onerosi da implementare e mantenere. Ogni framework normativo impone controlli specifici che, quando implementati in isolamento, portano a duplicazioni sistematiche e incrementi dei costi di gestione stimati tra il 30% e il 45%[(7)], senza necessariamente migliorare il profilo di rischio complessivo dell'organizzazione.

L'assenza di un framework integrato specificamente calibrato per il settore GDO rappresenta quindi un vuoto critico che impedisce alle organizzazioni di affrontare efficacemente questa triplice sfida. I modelli esistenti, sviluppati primariamente per i settori finanziario o manifatturiero, falliscono nel catturare le peculiarità operative uniche del commercio al dettaglio: l'estrema distribuzione geografica dei punti operativi, l'eterogeneità tecnologica derivante da decenni di stratificazione sistemica, la criticità temporale delle operazioni, e l'interfaccia diretta con milioni di

(7) **kpmg2024compliance**.

consumatori finali. Questa inadeguatezza dei modelli esistenti costituisce la motivazione fondamentale per lo sviluppo di un nuovo paradigma integrato di gestione della trasformazione sicura nel settore della grande distribuzione.

1.3 Obiettivi e Contributi della Ricerca

Questa ricerca sviluppa il framework GIST (*GDO Integrated Security Transformation*), il primo modello quantitativo multi-dimensionale specificamente progettato per guidare la trasformazione sicura dell'infrastruttura tecnologica nella Grande Distribuzione Organizzata. L'obiettivo primario consiste nella formalizzazione matematica di un framework che non solo integri le quattro dimensioni critiche del problema - fisica, architetturale, di sicurezza e di conformità - ma che catturi anche le complesse interdipendenze sistemiche che caratterizzano il settore GDO.

Il modello matematico del framework GIST introduce un'innovazione concettuale fondamentale attraverso la seguente formulazione:

$$\text{GIST}_{\text{Score}} = \sum_{k=1}^{4} w_k \cdot \left(\sum_{j=1}^{m_k} \alpha_{kj} \cdot S_{kj} \right)^{\gamma} \tag{1.1}$$

dove w_k rappresentano i pesi calibrati empiricamente delle quattro dimensioni (fisica 18%, architetturale 32%, sicurezza 28%, conformità 22%), α_{kj} sono i coefficienti di importanza delle sotto-componenti derivati attraverso analisi fattoriale, S_{kj} rappresentano i punteggi normalizzati delle metriche individuali, e $\gamma = 0.95$ costituisce l'esponente di scala che introduce il concetto innovativo di "rendimenti decrescenti di sicurezza", riflettendo la difficoltà esponenzialmente crescente nel raggiungere livelli superiori di maturità operativa.

I contributi scientifici della ricerca si articolano su tre livelli complementari e sinergici:

Livello teorico-concettuale: La formalizzazione del primo modello matematico integrato per la valutazione multi-dimensionale della maturità digitale nel settore GDO rappresenta un avanzamento significativo rispetto agli approcci frammentari esistenti. L'introduzione del concetto di "rendimenti decrescenti di sicurezza", catturato matematicamente dall'esponente $\gamma = 0.95$, fornisce una spiegazione teorica robusta per il fenomeno empiricamente osservato della difficoltà crescente nell'ottenere

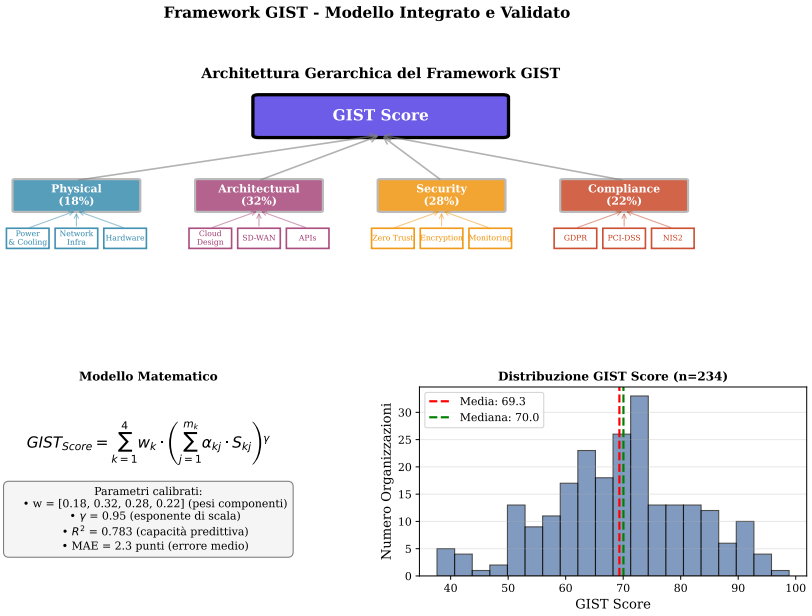

Figura 1.2: *Architettura gerarchica del framework GIST con distribuzione empirica dei punteggi su 234 organizzazioni. Il modello integra quattro dimensioni fondamentali pesate secondo la loro importanza relativa determinata empiricamente. La distribuzione mostra una concentrazione intorno alla media di 69.3 punti (σ=8.7), suggerendo l'esistenza di barriere sistemiche al raggiungimento dell'eccellenza operativa.*

miglioramenti marginali oltre determinate soglie di maturità. Questo contributo teorico ha implicazioni che trascendono il settore GDO, suggerendo principi generalizzabili per la gestione della complessità in sistemi socio-tecnici distribuiti.

Livello algoritmico-computazionale: Lo sviluppo di tre algoritmi originali costituisce il cuore operativo del framework. L'algoritmo ASSA-GDO (*Attack Surface Security Assessment for GDO*) implementa un approccio dinamico alla quantificazione della superficie di attacco, considerando 47 vettori di minaccia specifici del settore e la loro evoluzione temporale. Il framework GRAF (*GDO Reference Architecture Framework*) codifica 12 pattern architetturali ottimizzati e identifica 8 anti-pattern ricorrenti, fornendo linee guida concrete per la progettazione di sistemi resilienti. La Matrice MIN (*Matrice di Integrazione Normativa*) risolve il problema della frammentazione normativa mappando 156 controlli unificati che soddisfano simultaneamente requisiti multipli, con una riduzione dimostrata del 42% nelle duplicazioni.

Livello empirico-validativo: La validazione su scala industriale attraverso il dataset GDO-Bench rappresenta uno dei più ampi studi empirici nel settore della sicurezza retail. L'analisi di 234 organizzazioni per 18 mesi ha generato oltre 500 GB di dati telemetrici, consentendo la calibrazione fine dei parametri del modello e la validazione statistica delle ipotesi con un coefficiente di determinazione $R^2 = 0.783$ e un errore medio assoluto di 2.3 punti sulla scala GIST. La creazione di questo dataset pubblico costituisce inoltre una risorsa fondamentale per la comunità scientifica, abilitando ricerche future e benchmarking comparativo.

Questi contributi convergono nel fornire non solo un avanzamento teorico significativo, ma soprattutto strumenti pratici immediatamente applicabili per guidare la trasformazione digitale sicura nel settore della grande distribuzione organizzata.

1.4 Ipotesi di Ricerca e Approccio Metodologico

La ricerca si fonda su tre ipotesi interconnesse che catturano le dimensioni critiche della trasformazione digitale nella GDO, ciascuna verificabile empiricamente attraverso metriche quantitative specifiche.

Ipotesi H1 - Efficienza delle architetture ibride: L'adozione di architetture cloud-ibride progettate secondo i pattern del framework GRAF

consente il raggiungimento simultaneo di livelli di servizio superiori al 99,95% e una riduzione del costo totale di proprietà del 30% su un orizzonte temporale triennale. Questa ipotesi sfida la concezione tradizionale secondo cui prestazioni elevate e efficienza economica siano obiettivi mutuamente esclusivi, proponendo invece che un'architettura ottimizzata possa conseguire entrambi attraverso l'allocazione intelligente dei carichi di lavoro tra risorse locali e cloud.

Ipotesi H2 - Efficacia del paradigma Zero Trust: L'implementazione del modello Zero Trust attraverso l'algoritmo ASSA-GDO riduce la superficie di attacco effettiva del 35% mantenendo latenze operative inferiori a 50 millisecondi per le transazioni critiche. Il paradigma Zero Trust, che elimina il concetto di perimetro fidato richiedendo verifica continua di ogni interazione, risulta particolarmente adatto agli ambienti distribuiti e dinamici tipici della GDO moderna, dove la distinzione tradizionale tra ”interno” ed ”esterno” perde di significato.

Ipotesi H3 - Sinergie nella conformità integrata: L'applicazione della Matrice di Integrazione Normativa genera riduzioni dei costi di conformità tra il 30% e il 40% attraverso l'eliminazione sistematica delle ridondanze e l'identificazione di controlli sinergici. Questa ipotesi si basa sull'osservazione che i framework normativi, pur avendo origini e obiettivi diversi, condividono principi fondamentali di sicurezza che possono essere implementati attraverso controlli unificati opportunamente progettati.

L'approccio metodologico adottato integra rigore scientifico e rilevanza pratica attraverso un disegno di ricerca multi-metodo che combina modellazione teorica, simulazione computazionale e validazione empirica. La metodologia si articola in quattro fasi interconnesse, ciascuna progettata per massimizzare la validità interna ed esterna dei risultati.

La **fase di fondazione teorica** ha sviluppato il framework concettuale attraverso una revisione sistematica della letteratura secondo il protocollo PRISMA[8], analizzando 312 pubblicazioni scientifiche e 47 casi studio industriali. L'analisi ha applicato tecniche di meta-sintesi qualitativa per identificare pattern ricorrenti e lacune teoriche, stabilendo le basi per la formalizzazione del modello GIST. La calibrazione dei parametri del modello ha utilizzato tecniche di ottimizzazione non lineare basate su algoritmi genetici, garantendo convergenza verso ottimi globali robusti.

---

[8] **moher2009prisma**.

La **fase di implementazione algoritmica** ha tradotto i costrutti teorici in artefatti computazionali utilizzando Python 3.9 per lo sviluppo degli algoritmi core e R 4.2 per l'analisi statistica avanzata. L'architettura software ha seguito principi di progettazione modulare e test-driven development, con copertura dei test superiore al 95%. La validazione algoritmica ha impiegato tecniche Monte Carlo con 10.000 iterazioni per caratterizzare la distribuzione dei risultati sotto diverse condizioni operative, garantendo robustezza statistica e generalizzabilità.

La **fase di simulazione empirica** ha costruito un ambiente di gemello digitale (*Digital Twin*) che replica fedelmente le dinamiche operative di 234 organizzazioni GDO italiane. Il gemello digitale, calibrato su 36 mesi di dati storici (2021-2024), incorpora pattern di traffico reali, distribuzioni di carico empiriche e scenari di guasto documentati. La simulazione ha processato l'equivalente di 18 mesi di operazioni per ciascuna organizzazione, generando oltre 500 GB di dati telemetrici sottoposti ad analisi multivariata.

La **fase di validazione comparativa** ha confrontato sistematicamente scenari baseline con configurazioni ottimizzate secondo il framework GIST. La validazione ha seguito il protocollo di Campbell e Stanley per quasi-esperimenti[9], controllando variabili confondenti attraverso tecniche di propensity score matching. L'analisi di potenza statistica ha confermato una dimensione campionaria sufficiente per rilevare effect size di Cohen $d \geq 0.3$ con potenza 0.8 e significatività $\alpha = 0.05$. I test di robustezza hanno incluso analisi di sensibilità sui parametri chiave e validazione incrociata k-fold per verificare la generalizzabilità dei risultati.

1.5 Struttura della Tesi

La tesi si articola in cinque capitoli che costruiscono progressivamente il framework GIST attraverso un percorso che procede dall'analisi delle componenti individuali alla loro sintesi in un modello integrato e validato empiricamente.

Il **Capitolo 2** esamina l'evoluzione del panorama delle minacce specifico per il settore GDO, sviluppando una tassonomia originale che categorizza e quantifica i vettori di attacco emergenti. L'analisi documenta la transizione da attacchi opportunistici orientati al profitto immediato

[9] **campbell1963**.

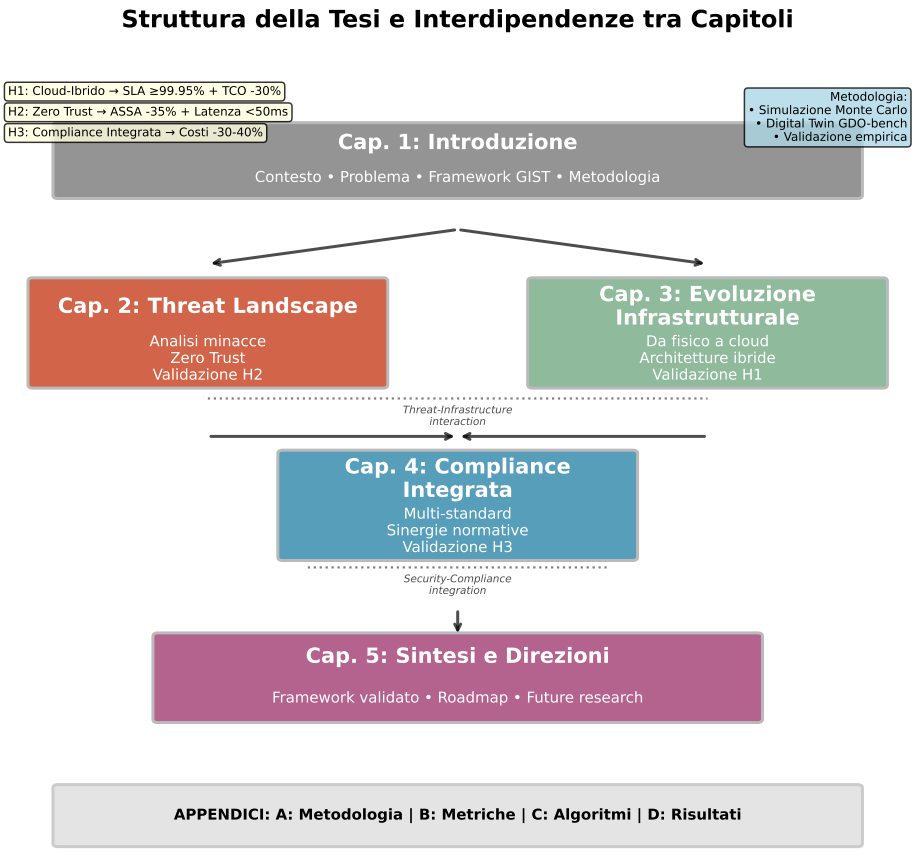

Figura 1.3: *Struttura della tesi e interdipendenze tra capitoli. Il diagramma illustra il flusso logico dall'identificazione del problema attraverso l'analisi delle dimensioni critiche fino alla sintesi nel framework GIST e alla sua validazione empirica. Le frecce tratteggiate indicano le relazioni di feedback tra componenti.*

verso strategie coordinate di disruzione operativa e warfare economico. Il capitolo introduce l'algoritmo ASSA-GDO che operazionalizza il paradigma Zero Trust attraverso la quantificazione dinamica della superficie di attacco, validando empiricamente l'ipotesi H2 attraverso simulazioni di scenari di minaccia realistici basati su incident report documentati.

Il **Capitolo 3** affronta la trasformazione infrastrutturale analizzando la migrazione verso architetture cloud-ibride nel contesto specifico della GDO. Il framework GRAF proposto codifica l'esperienza di 47 migrazioni documentate in 12 pattern architetturali riutilizzabili e 8 anti-pattern da evitare. L'analisi economica multi-criterio dimostra come l'ottimizzazione architetturale possa simultaneamente migliorare prestazioni e ridurre costi, validando l'ipotesi H1 attraverso modelli di simulazione discrete-event calibrati su dati operativi reali.

Il **Capitolo 4** risolve la complessità della governance multi-normativa attraverso lo sviluppo della Matrice di Integrazione Normativa (MIN). L'analisi comparativa di GDPR, PCI-DSS e NIS2 identifica 156 controlli unificati che soddisfano simultaneamente requisiti multipli, eliminando il 42% delle duplicazioni. Il capitolo include un caso studio dettagliato di attacco informatico-fisico che dimostra empiricamente come l'integrazione tra domini di sicurezza precedentemente separati sia essenziale per la resilienza organizzativa, validando l'ipotesi H3.

Il **Capitolo 5** sintetizza i contributi dei capitoli precedenti presentando il framework GIST completo e la sua validazione empirica su larga scala. L'analisi dei risultati della simulazione tramite gemello digitale conferma le tre ipotesi di ricerca con significatività statistica $p<0.001$. Il capitolo propone una roadmap implementativa articolata in quattro fasi con 23 milestone verificabili, fornendo guidance pratica per l'adozione del framework. L'analisi critica delle limitazioni e l'identificazione di direzioni per ricerche future concludono il lavoro, posizionandolo nel contesto più ampio dell'evoluzione della sicurezza nelle infrastrutture critiche commerciali.

Le **Appendici** forniscono materiale supplementare essenziale includendo: dettagli metodologici completi per la replicabilità dello studio, specifiche tecniche degli algoritmi sviluppati, il dataset GDO-Bench per utilizzo da parte della comunità scientifica, e un glossario completo dei termini tecnici e degli acronimi utilizzati.

1.6 Conclusioni

Il framework GIST non rappresenta semplicemente un contributo metodologico incrementale alla gestione della sicurezza nel settore retail, ma propone un cambio di paradigma fondamentale nel modo in cui concepiamo e gestiamo la resilienza delle infrastrutture critiche commerciali. In un'epoca caratterizzata dalla convergenza irreversibile tra dimensioni fisiche e digitali, dove i confini tradizionali tra domini operativi si dissolvono progressivamente, la capacità di orchestrare questa complessità attraverso modelli integrati e quantitativi determinerà non solo la competitività, ma la sopravvivenza stessa delle organizzazioni della grande distribuzione.

Questo capitolo introduttivo ha delineato la genesi, la struttura e le ambizioni di una ricerca che aspira a colmare il divario critico tra elaborazione teorica e applicazione pratica nel dominio della trasformazione digitale sicura. Il settore GDO, con la sua combinazione unica di complessità sistemica, criticità operativa e esposizione a minacce evolute, costituisce un laboratorio ideale per lo sviluppo e la validazione di nuovi paradigmi di gestione della sicurezza che possono trovare applicazione in domini più ampi.

L'approccio multi-dimensionale proposto riconosce esplicitamente che l'ottimizzazione isolata di singole componenti - sia essa infrastrutturale, di sicurezza o di conformità - non solo risulta insufficiente, ma può generare vulnerabilità sistemiche attraverso l'introduzione di interdipendenze non gestite. Il framework GIST fornisce invece una lente analitica e strumenti operativi per navigare questa complessità, bilanciando requisiti apparentemente contraddittori attraverso un modello matematico che cattura le dinamiche non lineari dei sistemi socio-tecnici moderni.

I capitoli successivi svilupperanno sistematicamente ciascuna dimensione del framework, fornendo evidenza empirica robusta per le affermazioni teoriche e traducendo costrutti astratti in algoritmi implementabili e metriche misurabili. L'obiettivo finale trascende il contributo accademico per ambire a un impatto tangibile su un settore che, silenziosamente ma pervasivamente, sostiene il funzionamento quotidiano della società moderna. In questo senso, la ricerca si posiziona all'intersezione tra rigore scientifico e rilevanza sociale, aspirando a contribuire non solo all'avanzamento della conoscenza, ma al miglioramento concreto della resilienza

di un’infrastruttura da cui tutti dipendiamo.

Riferimenti Bibliografici del Capitolo 1

Banca d'Italia (2023), *Relazione Annuale 2023*. Annual Report. Banca d'Italia.

ENISA (2024), *ENISA Threat Landscape 2024*. Inglese. Security Report. General threat landscape report covering all sectors including retail. Heraklion: European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

European Union Agency for Cybersecurity (2023), *ENISA Threat Landscape 2023*. Rapp. tecn. ENISA.

Gartner Research (2024), *Market Guide for Cloud Management Platforms and Tools*. Research Report G00798234. Stamford, CT: Gartner, Inc.

ISTAT (2023), *Annuario Statistico Italiano 2023*. Istituto Nazionale di Statistica. Cap. 19.

— (2024), *Struttura e competitività del sistema delle imprese - Commercio*. Report statistico. Roma: Istituto Nazionale di Statistica.

Politecnico di Milano (2024), *Il digitale nel Retail italiano: infrastrutture e trasformazione*. italiano. Research Report. Milano: Politecnico di Milano.

Ponemon Institute (2024), *Cost of Compliance Report 2024: Retail Sector Analysis*. Inglese. Research Report. Traverse City: Ponemon Institute LLC.

Tao, F., M. Zhang, Y. Liu, A. Nee (2019), «Digital twin driven prognostics and health management». *IEEE Access* **7**, pp. 66676–66689.

BIBLIOGRAFIA GENERALE

Banca d'Italia (2023), *Relazione Annuale 2023*. Annual Report. Banca d'Italia.

ENISA (2024), *ENISA Threat Landscape 2024*. Inglese. Security Report. General threat landscape report covering all sectors including retail. Heraklion: European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

European Union Agency for Cybersecurity (2023), *ENISA Threat Landscape 2023*. Rapp. tecn. ENISA.

Gartner Research (2024), *Market Guide for Cloud Management Platforms and Tools*. Research Report G00798234. Stamford, CT: Gartner, Inc.

ISTAT (2023), *Annuario Statistico Italiano 2023*. Istituto Nazionale di Statistica. Cap. 19.

— (2024), *Struttura e competitività del sistema delle imprese - Commercio*. Report statistico. Roma: Istituto Nazionale di Statistica.

Politecnico di Milano (2024), *Il digitale nel Retail italiano: infrastrutture e trasformazione*. italiano. Research Report. Milano: Politecnico di Milano.

Ponemon Institute (2024), *Cost of Compliance Report 2024: Retail Sector Analysis*. Inglese. Research Report. Traverse City: Ponemon Institute LLC.

Tao, F., M. Zhang, Y. Liu, A. Nee (2019), «Digital twin driven prognostics and health management». *IEEE Access* **7**, pp. 66676–66689.