

Indice

Prefazione	1
Dedica	3
Ringraziamenti	4
1 Introduzione	1
1.1 La Cybersecurity nelle Startup fintech: Sfide, Vulnerabilità e Strategie di Protezione in un Ecosistema in Rapida Evoluzione	1
1.1.1 Definizione di fintech	1
1.1.2 Il Contesto delle Startup fintech: Un Ecosistema Dinamico e Sfidante	4
1.1.3 Banche Tradizionali vs. Startup fintech: Divergenze Strategiche in Tecnologia, Regolamentazione e Cybersecurity	5
1.1.4 Analisi delle Sfide di Cybersecurity per le Startup fintech	6
1.1.5 Principali Vettori di Attacco e Minacce Informatiche nel Contesto fintech	9
1.1.6 Conseguenze degli Attacchi e Impatto sulle Startup fintech	11
1.1.7 Importanza di un Approccio Proattivo alla Cybersecurity	11
1.1.8 Approccio Metodologico	12
2 Principi di cybersecurity olistici per un'infrastruttura fintech	13
2.1 Introduzione	13
2.2 Triade CIA: Il Nucleo della Sicurezza delle Informazioni	14
2.3 Difesa in Profondità (Defense in Depth)	16
2.4 Principio del Minimo Privilegio (Principle of Least Privilege - PoLP)	16
2.5 Separazione dei Compiti (Separation of Duties - SoD)	17
2.6 Zero Trust Architecture (ZTA)	17
2.7 Economia del Meccanismo	18
2.8 Impostazioni Sicure per Difetto (Fail-Safe Defaults)	18
2.9 Mediazione Completa	19

2.10	Resilienza Cibernetica (Cyber Resiliency)	20
2.11	Responsabilizzazione e Non-Ripudio (Accountability and Non-Repudiation)	20
2.12	Privacy by Design (PbD) e Privacy by Default	21
2.12.1	Conclusioni Preliminari del Capitolo	21
3	Principi dell'Infrastruttura Cloud e Scelta di AWS	23
3.1	Fondamenti di Cloud Computing	23
3.1.1	Modelli di servizio e distribuzione cloud	24
3.1.2	Cloud Computing vs Infrastrutture On-Premises	27
3.1.3	Perché le Startup Scelgono il Cloud	28
3.1.4	Introduzione ad Amazon Web Services (AWS)	30
3.1.5	Il Caso Specifico: AWS per la Startup fintech	31
3.1.6	Infrastruttura Globale AWS: Fondamenta per la fintech	33
3.1.7	Architettura Virtualizzata e Meccanismi di Scalabilità per la fintech	34
3.1.8	Modello di Responsabilità Condivisa: Implicazioni per la fintech	37
4	Progettazione e Implementazione Avanzata della Sicurezza delle Identità e degli Accessi (IAM) in AWS	39
4.1	Introduzione alla Gestione delle Identità e degli Accessi	39
4.1.1	Configurazione dell'infrastruttura AWS per la piattaforma <i>Finanz</i>	40
4.1.2	Implementazione del Modello Zero Trust e del Principio del Minimo Privilegio	41
4.1.3	Gestione delle Identità e degli Accessi (IAM) come Pilastro di Zero Trust in AWS	44
4.1.4	Valutazione dell'implementazione IAM corrente di <i>Finanz</i>	45
4.2	Implementazione delle Migliorie Proposte alla Gestione IAM	47
4.2.1	Ristrutturazione della Gerarchia degli Accessi	47
4.2.2	Sviluppo di un Modello Ibrido Aggiornato per la Gestione degli Accessi	51
4.2.3	Introduzione di un Break-Glass Account	58
4.2.4	Implementazione di un Workflow di Approvazione a Due Fasi (Opzionale)	61
4.3	Conclusioni sulla Sicurezza IAM	61
5	Architettura di Rete Sicura e Protezione dei Servizi Applicativi su AWS per Finanz	63
5.1	Introduzione alla Sicurezza dell'Infrastruttura	63
5.2	Progettazione di una Rete Sicura con Amazon VPC	63

5.2.1	Subnet Pubbliche e Private: Segmentazione Essenziale	64
5.2.2	Controllo Granulare del Traffico: Gruppi di Sicurezza e Network ACL	64
5.2.3	NAT Gateway per l'Accesso Controllato a Internet	65
5.2.4	VPC Endpoints per Comunicazioni Private con Servizi AWS	66
5.2.5	Connessioni Sicure verso Ambienti Esterni (Opzionale: VPN/Direct Connect)	66
5.3	Gestione Sicura delle Istanze EC2	67
5.3.1	Scelta delle AMI, Patching e Hardening del Sistema Operativo	67
5.3.2	Utilizzo Fondamentale di IAM Roles per le Istanze EC2 . . .	74
5.3.3	Scalabilità e Disponibilità con Auto Scaling Groups	74
5.4	Protezione dei Dati Sensibili: Un Imperativo per le fintech	75
5.4.1	Crittografia dei Dati: a Riposo (At Rest) e in Transito (In Transit)	75
5.4.2	Gestione Centralizzata delle Chiavi Crittografiche con AWS KMS	76
5.4.3	Strategie di Backup e Disaster Recovery (DR)	77
5.4.4	Misure di Sicurezza Specifiche per i Bucket S3	77
5.5	Monitoraggio Continuo, Logging e Alerting: Vedere per Proteggere	79
5.5.1	Abilitazione e Configurazione di AWS CloudTrail e Amazon CloudWatch	79
5.5.2	Configurazione di Allarmi CloudWatch Proattivi	80
5.5.3	Utilizzo di Servizi di Sicurezza Gestiti: AWS Security Hub e Amazon GuardDuty	81
5.6	Automazione e Coerenza con Infrastructure as Code (IaC)	82
5.7	Conclusioni sulla Sicurezza dell'Infrastruttura e dei Servizi	84
6	Implementazione di un Honeypot in un'Infrastruttura AWS per Startup fintech	85
6.1	Definizione e Utilità di un Honeypot	85
6.1.1	Che cos'è un Honeypot	85
6.1.2	Utilità nel Contesto di una Startup fintech	86
6.2	Tipologie di Honeypot	86
6.2.1	Classificazione per Livello di Interazione	86
6.2.2	Classificazione per Scopo	87
6.3	Vantaggi e Svantaggi degli Honeypot	88
6.3.1	Vantaggi	88
6.3.2	Svantaggi	88
6.4	Implementazione di un Honeypot in AWS	89
6.4.1	Pianificazione e Requisiti	89

6.4.2	Selezione del Tipo di Honeypot per una Startup fintech . . .	90
6.4.3	Implementazione Tecnica in AWS	90
6.4.4	Configurazioni di Sicurezza Aggiuntive	94
6.5	Analisi dei Costi per una Startup fintech	95
6.5.1	Stima dei Costi di Implementazione e Mantenimento	95
6.5.2	Valutazione Costo-Beneficio per una Startup fintech	95
6.6	Test di Verifica: Esperimento di Attacco Controllato	96
6.6.1	Progettazione dell'Esperimento	96
6.6.2	Software e Comandi Utilizzati (Esempi)	97
6.6.3	Risultati Ottenuti (Ipotetici)	99
6.6.4	Analisi dei Risultati (Ipotetica)	100
6.7	Considerazioni Finali e Raccomandazioni	100
6.7.1	Sintesi dei Risultati	100
6.7.2	Raccomandazioni per l'Implementazione	101
6.7.3	Sviluppi Futuri	101
7	Conclusioni	103