Università degli Studi di Milano
Facoltà di Scienze e Tecnologie
Corso di Laurea in Sicurezza dei Sistemi e delle Reti Informatiche

SICUREZZA DELL'INFRASTRUTTURA AWS IN UNA STARTUP FINTECH

Relatore: Prof. Claudio Agostino Ardagna

Correlatore: Lorenzo Perotta, Andrea Pasini, Simone Cortese

Tesi di:
Andrea Ferraboli
Matricola: 09985A

Anno Accademico 2024-2025

dedicato a chi mi vuole bene, a chi mi stima e ai miei compagni di viaggio, vi voglio bene

Indice

ii

1 Introduzione **1**
1.1 Principi di sicurezza olistici per un'infrastruttura tech 6
1.1.1 Introduzione 6
1.1.2 Principi di cybersecurity 7

2 Compliance a standard internazionali e framework di sicurezza **13**
2.1 NIST Cybersecurity Framework (CSF) 14
2.1.1 Identify (Identifica) 15
2.1.2 Protect (Proteggi) 15
2.1.3 Detect (Individua) 16
2.1.4 Respond (Rispondi) 16
2.1.5 Recover (Recupera) 17
2.2 ISO/IEC 27001 e Sistemi di Gestione della Sicurezza (ISMS) 17
2.3 NIST SP 800-53 – Catalogo di Controlli di Sicurezza 18
2.4 Architettura Zero Trust (ZTA) 20
2.5 Sicurezza OT (Tecnologie Operative) – NIST SP 800-82 20
2.6 Sicurezza delle Password e Gestione delle Identità – NIST SP 800-63B 21
2.7 Difesa Perimetrale Avanzata e Soluzioni di Next-Gen Firewall – Check Point Quantum 21
2.8 Best practice e strategie di mitigazione 22

3 Fondamenti di Sicurezza su AWS **23**
3.1 Modello di responsabilità condivisa di AWS 23
3.2 Best practice di sicurezza specifiche per startup fintech 23
3.3 Panoramica dei principali servizi di sicurezza di AWS 23
3.3.1 AWS Identity and Access Management (IAM) 23
3.3.2 AWS Key Management Service (KMS) 23
3.3.3 AWS CloudTrail e Amazon CloudWatch (servizi concorrenti) . 23

3.3.4 AWS GuardDuty, Amazon Inspector e Amazon Macie (alternativa valida) . . . 23
3.3.5 Altri servizi rilevanti (es. AWS WAF, VPC) . . . 23

4 Gestione delle Identità e degli Accessi (IAM) 24
4.1 Implementazione del principio del minimo privilegio . . . 24
4.2 Creazione e gestione di utenti, gruppi e ruoli IAM . . . 24
4.3 Utilizzo di policy IAM per concedere permessi granulari . . . 24
4.4 Configurazione dell'autenticazione a più fattori (MFA) . . . 24
4.5 Gestione delle credenziali (es. utilizzo di IAM Roles per EC2) . . . 24
4.6 Audit e monitoraggio degli accessi IAM . . . 24

5 Monitoraggio e Logging della Sicurezza 25
5.1 Configurazione di AWS CloudTrail per tracciare le attività degli utenti 25
5.2 Implementazione di Amazon CloudWatch per monitorare le metriche di sistema . . . 25
5.3 Creazione di allarmi per eventi specifici e attività sospette . . . 25
5.4 Utilizzo di AWS GuardDuty per il rilevamento automatico di minacce 25
5.5 Integrazione con sistemi SIEM (Security Information and Event Management) . . . 25
5.6 Gestione e analisi dei log . . . 25

6 Protezione dei Dati Sensibili e Conformità Normativa 26
6.1 Crittografia dei dati a riposo e in transito . . . 26
6.2 Gestione delle chiavi di crittografia con AWS KMS o CloudHSM . . . 26
6.3 Implementazione di meccanismi per la protezione dei dati in S3 . . . 26
6.4 Misure per la conformità a PCI DSS (se rilevante) . . . 26
6.5 Misure per la conformità al GDPR e protezione dei dati personali . . . 26
6.6 Valutazione e gestione del rischio di perdita di dati . . . 26

7 Casi Studio e Implementazione Pratica 27
7.1 Esempio di architettura di sicurezza AWS per una startup fintech (proposta) . . . 28
7.2 Implementazione delle best practice descritte nei capitoli precedenti . . . 28
7.3 Test di penetrazione e valutazione della sicurezza dell'ambiente . . . 28
7.4 Analisi dei risultati e confronto con le best practice . . . 28
7.5 Integrazione di strumenti di sicurezza terzi (es. SentinelOne) . . . 28
7.6 Infrastruttura di base AWS, integrazione codice e infrastruttura di un sistema honeypot . . . 28
7.7 Deadcode per confondere malware (Capitolo 7) . . . 28
7.8 Autenticazione con chiavi pubbliche (Capitolo 8) . . . 28

7.9 Progettazione e implementazione di una Virtual Private Cloud (VPC) isolata 28
7.9.1 Creazione di subnet pubbliche e private 28
7.9.2 Utilizzo di gruppi di sicurezza e ACL per controllare il traffico di rete 28
7.9.3 Implementazione di Network Address Translation (NAT) e VPN/Direct Connect 28
7.9.4 Configurazione di load balancer per alta disponibilità e scalabilità 28
7.9.5 Utilizzo di container (es. ECS o EKS) per una maggiore sicurezza e scalabilità 28

8 Discussione e Conclusioni **29**
8.1 Rielaborazione delle domande di ricerca iniziali e discussione dei risultati 29
8.2 Riflessioni sulle sfide e opportunità per la sicurezza di AWS nelle startup fintech 29
8.3 Prospettive future per la ricerca e l'innovazione 29
8.4 Raccomandazioni per la creazione di un modello di cybersecurity resiliente per startup fintech 29

Capitolo 1

Introduzione

La Cybersecurity nelle Startup Fintech: Sfide, Vulnerabilità e Strategie di Protezione in un Ecosistema in Rapida Evoluzione

Il settore fintech rappresenta oggi una delle aree più dinamiche e innovative dell'ecosistema startup, con investimenti globali che hanno raggiunto i 115 miliardi di dollari, in crescita esponenziale rispetto ai 53.2 miliardi del 2018 [1]. Questo rapido sviluppo, caratterizzato dall'implementazione di tecnologie emergenti per i servizi finanziari, porta con sé non solo opportunità senza precedenti ma anche significative sfide in termini di sicurezza informatica. Le startup fintech, che si trovano all'intersezione tra finanza tradizionale e innovazione tecnologica, gestiscono dati estremamente sensibili diventando bersagli privilegiati per i cybercriminali. Questa tesi esplora le vulnerabilità specifiche di queste realtà, analizza le principali minacce che affrontano e propone strategie di sicurezza efficaci anche in contesti di risorse limitate, evidenziando come un approccio proattivo alla cybersecurity non rappresenti un costo ma un investimento strategico fondamentale per il successo a lungo termine di una startup fintech.

Definizione di Fintech

Nell'ambito economico-finanziario, con il termine **fintech** (contrazione di "financial technology") si indica l'**innovazione nei servizi finanziari** resa possibile dalle moderne tecnologie digitali [2]. Una **startup fintech** è quindi una **nuova impresa** che opera nel settore della tecnologia finanziaria, basando il proprio modello di business sulle tecnologie ICT più avanzate e contrapponendosi agli approcci tradizionali degli operatori finanziari consolidati [3].

Queste giovani aziende ad alta componente tecnologica mirano a migliorare l'accessibilità, l'efficienza e la qualità dei servizi finanziari, e stanno svolgendo un ruolo cruciale nella **digitalizzazione del mercato finanziario italiano** [2].

Tra i servizi e le soluzioni tipicamente offerti dalle startup fintech vi sono:

- **Pagamenti digitali** (ad esempio tramite app mobili)
- Trasferimenti di denaro **peer-to-peer**
- **Prestiti diretti tra privati** (social lending)
- **Finanziamento partecipativo** (crowdfunding)
- Servizi assicurativi innovativi legati all'**insurtech**
- Impiego di tecnologie come la **blockchain** e le **criptovalute** per abilitare nuovi servizi finanziari

In linea con la crescita globale del fenomeno, in Italia si contavano oltre **600 startup fintech e insurtech** attive nel 2023 [3], a testimonianza di un ecosistema in rapido sviluppo.

Il Contesto delle Startup Fintech: Un Ecosistema Dinamico e Sfidante

Le startup fintech operano in un ambiente caratterizzato da elevata incertezza, risorse limitate e necessità di crescita rapida, fattori che influenzano profondamente le decisioni in ambito IT e sicurezza informatica [4]. A differenza delle istituzioni finanziarie tradizionali, queste realtà innovative non dispongono generalmente di strutture gerarchiche complesse o budget consistenti dedicati alla sicurezza, dovendo invece adottare approcci agili e flessibili.

Il contesto finanziario in cui operano le startup fintech impone pressioni significative sulle decisioni di spesa. Ogni investimento, compreso quello per l'infrastruttura IT e la sicurezza, deve essere attentamente valutato in termini di ritorno immediato e benefici a lungo termine [4]. Questa ottimizzazione dei costi rappresenta una sfida continua, poiché la sicurezza informatica richiede investimenti costanti, spesso non producendo risultati immediatamente visibili, la cui assenza può comportare conseguenze catastrofiche. In questo equilibrio delicato, le startup fintech devono trovare il giusto compromesso tra la necessità di scalare rapidamente e l'implementazione di solide misure di protezione.

La Distinzione tra Cybersecurity Bancaria e Fintech

Un aspetto fondamentale da considerare è la sostanziale differenza tra l'approccio alla cybersecurity nel settore bancario tradizionale e nelle startup fintech. Mentre le banche operano in un contesto fortemente regolamentato, con obblighi legali precisi in materia di sicurezza e protezione dei dati, le fintech hanno tradizionalmente goduto di una maggiore flessibilità normativa [5]. Le grandi istituzioni bancarie investono ingenti risorse nel testare costantemente le proprie misure di sicurezza, consapevoli che anche il minimo incidente può comportare la perdita di migliaia di clienti e sanzioni finanziarie significative.

Le fintech, spesso costituite da piccole startup in rapida espansione, possono fungere da "overlay" per le banche, facilitando la fornitura di servizi finanziari innovativi ma operando inizialmente con regolamentazioni meno stringenti [5]. Questa differenza normativa sta tuttavia diminuendo, soprattutto per quelle fintech che si trasformano gradualmente in vere e proprie banche, sottoponendosi così a un maggiore scrutinio regolamentare. La sfida per le startup fintech consiste quindi nel bilanciare l'agilità operativa con l'adozione di standard di sicurezza elevati, anticipando l'evoluzione normativa del settore.

Sfide Principali per le Startup Fintech in Ambito Cybersecurity

Le startup fintech affrontano sfide specifiche nel campo della sicurezza informatica, che derivano dalla loro natura innovativa e dalle caratteristiche distintive del loro modello di business [4]. La prima e più evidente sfida è rappresentata dal budget limitato per la sicurezza, che spesso costringe a difficili compromessi tra lo sviluppo di nuove funzionalità e l'implementazione di adeguate misure protettive. Questa limitazione finanziaria si riflette anche nella difficoltà di attrarre e mantenere personale specializzato in cybersecurity, un ambito in cui la domanda supera ampiamente l'offerta e le grandi aziende possono offrire compensi difficilmente pareggiabili da una startup.

La pressione per un rapido accesso al mercato rappresenta un'ulteriore sfida significativa. Nel settore fintech, essere i primi a offrire un servizio innovativo può fare la differenza tra il successo e il fallimento, ma questa corsa contro il tempo spesso porta a sottovalutare gli aspetti legati alla sicurezza [4]. Inoltre, la scalabilità dell'infrastruttura IT rappresenta una sfida tecnica considerevole: progettare sistemi che siano non solo sicuri ma anche in grado di crescere rapidamente al crescere dell'azienda richiede competenze specifiche e una pianificazione accurata.

L'adozione di tecnologie emergenti, caratteristica distintiva delle fintech, introduce nuove superfici di attacco e vulnerabilità potenziali [4]. Cloud computing, intelligenza artificiale, blockchain e API aperte offrono opportunità straordinarie ma richiedono

approcci di sicurezza specifici e aggiornati. Allo stesso tempo, la crescente interconnessione con partner, fornitori e piattaforme di terze parti amplia ulteriormente la superficie di attacco, rendendo la gestione del rischio ancora più complessa.

Non va sottovalutato, infine, il rischio rappresentato dalle minacce interne (insider threats). Nelle fasi iniziali di una startup, quando i controlli sono meno rigidi e le procedure di sicurezza meno formalizzate, il rischio legato a dipendenti negligenti o, in casi più rari, malintenzionati, aumenta considerevolmente [4]. La cultura della condivisione e dell'apertura, tipica delle startup, deve quindi essere bilanciata con adeguate politiche di accesso e controllo.

Minacce e Attacchi Informatici nel Settore Fintech

Il settore fintech, per la sua natura altamente tecnologica e la gestione di dati finanziari sensibili, è diventato uno dei bersagli preferiti dei cybercriminali [6]. Tra le minacce più diffuse e pericolose figurano gli attacchi di phishing, attraverso i quali i malintenzionati cercano di ottenere credenziali di accesso, dati personali o informazioni finanziarie utilizzando email, messaggi e siti web fraudolenti che imitano comunicazioni ufficiali [6]. Queste tecniche di social engineering sfruttano la fiducia degli utenti e le loro abitudini digitali per compromettere account e sistemi aziendali.

I malware e i ransomware rappresentano un'altra categoria di minacce particolarmente grave per le startup fintech. Questi software malevoli possono infiltrarsi nei sistemi attraverso vari vettori, bloccare l'accesso ai dati e richiedere un riscatto per ripristinarlo, causando danni finanziari diretti e interruzioni operative significative [6]. Le conseguenze di un attacco ransomware possono essere devastanti per una startup con risorse limitate, in quanto il riscatto diventa percentualmente troppo oneroso per le finanze aziendali.

Gli attacchi alle API (Application Programming Interfaces), sempre più utilizzate nel settore fintech per l'integrazione con servizi terzi, costituiscono un vettore di attacco in crescita [4]. Le API mal configurate o non adeguatamente protette possono diventare punti di ingresso privilegiati per i cybercriminali, consentendo l'accesso non autorizzato a dati sensibili e funzionalità critiche del sistema. Simile criticità presentano le configurazioni errate dei servizi cloud, che possono esporre involontariamente dati riservati o creare vulnerabilità sfruttabili.

Le startup fintech devono inoltre considerare il rischio di attacchi DDoS (Distributed Denial of Service), che mirano a rendere inaccessibili i servizi sovraccaricando i server con richieste fraudolente [4]. Questi attacchi, relativamente semplici da orchestrare ma potenzialmente molto dannosi, possono essere utilizzati sia come attacco diretto che come diversivo per mascherare altre attività malevoli più sofisticate.

Conseguenze degli Attacchi e Impatto sulle Startup Fintech

L'impatto di un attacco informatico su una startup fintech può essere multidimensionale e, in molti casi, esistenziale. A livello finanziario, oltre ai costi diretti per il ripristino dei sistemi e la gestione dell'incidente, vanno considerati i potenziali risarcimenti a clienti danneggiati, le sanzioni normative e l'aumento dei premi assicurativi [4]. Ma è forse l'impatto reputazionale a rappresentare la minaccia più grave: in un settore basato sulla fiducia come quello finanziario, una violazione dei dati può comprometterne irreparabilmente l'immagine, portando alla perdita di clienti attuali e potenziali.

L'interruzione operativa conseguente a un attacco può avere effetti a catena, influenzando non solo i clienti diretti ma anche partner commerciali e fornitori [4]. In un ecosistema interconnesso come quello fintech, l'interdipendenza tra diverse piattaforme e servizi amplifica ulteriormente l'impatto di un incidente di sicurezza, con effetti che possono estendersi ben oltre il perimetro aziendale immediato.

Importanza di un Approccio Proattivo alla Cybersecurity

Implementare una strategia di cybersecurity solida sin dalle prime fasi di sviluppo di una startup fintech non configura un semplice onere, bensì un investimento strategico di primaria importanza [4]. L'adozione del paradigma "security by design" permette infatti di integrare la sicurezza in maniera organica nei processi aziendali e nel ciclo di sviluppo del prodotto, contribuendo alla significativa riduzione dei costi a lungo termine e alla minimizzazione dei rischi potenziali. Al contrario, la mancata attenzione alla sicurezza nelle fasi iniziali comporta l'accumulo di "security debt", ovvero un debito tecnico in ambito sicurezza che, analogamente a un mutuo con tassi elevati, diventa progressivamente più oneroso da gestire e da ripagare nel tempo. Infine, la pressione derivante dalla necessità di accelerare lo sviluppo e di raggiungere rapidamente il mercato può portare a trascurare aspetti fondamentali della sicurezza, esacerbando ulteriormente tale debito tecnico.

Un approccio preventivo alla sicurezza risulta sempre più efficace ed economico rispetto a uno reattivo [4]. I costi per implementare misure di sicurezza di base sono generalmente inferiori rispetto a quelli necessari per rispondere a un incidente, che possono includere non solo il ripristino dei sistemi ma anche sanzioni, risarcimenti e danni reputazionali. La cybersecurity deve quindi essere considerata come parte integrante della strategia aziendale, non come un elemento accessorio o un costo da minimizzare.

Le startup fintech devono inoltre considerare che adeguati livelli di sicurezza rappresentano spesso un requisito fondamentale per attrarre investitori e partner commerciali [4]. Durante le fasi di due diligence, l'analisi delle misure di sicurezza implementate è diventata una componente standard, e lacune significative in questo ambito

possono compromettere opportunità di finanziamento o collaborazioni strategiche.

Approccio Metodologico della Tesi

Questa tesi si propone di affrontare le sfide della cybersecurity nelle startup fintech attraverso un approccio metodologico strutturato ma flessibile [4]. Pur concentrandosi su un caso studio pratico specifico, l'obiettivo è fornire principi e best practice di sicurezza generici e applicabili a qualsiasi startup fintech, indipendentemente dalla piattaforma tecnologica specifica utilizzata. L'approccio adottato riconosce le limitazioni di risorse tipiche delle startup e propone soluzioni scalabili che possono evolvere con la crescita dell'organizzazione.

La metodologia si basa su tre pilastri fondamentali: l'identificazione delle minacce specifiche per il modello di business fintech, la prioritizzazione degli interventi in base al rapporto rischio/beneficio e l'implementazione di controlli di sicurezza essenziali ma efficaci [4]. Questo approccio pragmatico consente di ottenere un livello di protezione adeguato anche con risorse limitate, concentrando gli sforzi sugli aspetti più critici.

1.1 Principi di sicurezza olistici per un'infrastruttura tech

1.1.1 Introduzione

Nell'analisi e nello studio dell'infrastruttura di una startup fintech, per comprendere le possibili implementazioni a livello di sicurezza dobbiamo prima delinare quali siano i principi di cybersecurity a cui ogni startup, fintech o meno, deve attenersi. In questo capitolo verranno analizzati i principi di cybersecurity più importanti e quali sono le principali sfide che un'azienda di piccole dimensione può affrontare all'inizio del proprio percorso nell'adozione delle medesime.Questo capitolo esplora i principi fondamentali di sicurezza informatica che ogni organizzazione dovrebbe implementare, con particolare attenzione alle sfide uniche che le startup fintech affrontano nell'adozione di tali pratiche. Il settore fintech, caratterizzato da rapida innovazione e gestione di dati finanziari sensibili, presenta un contesto particolarmente critico dove le best practice di sicurezza si scontrano spesso con le esigenze di velocità di sviluppo, risorse limitate e necessità di time-to-market accelerato.

1.1.2 Principi di cybersecurity

Triade CIA

La Triade CIA (Confidentiality, Integrity, Availability) rappresenta i pilastri fondamentali sui quali costruire qualsiasi strategia di sicurezza informatica robusta.

- **Confidentiality**: La riservatezza si concentra sul garantire che le informazioni siano accessibili solo a coloro che sono autorizzati a visualizzarle.[7] Questo principio viene generalmente rispettato tramite la crittografia dei dati, sia a riposo (stored data) che in transito (data in transit), controlli di accesso rigorosi, come liste di controllo degli accessi (ACL), autenticazione a più fattori (MFA) e Role-Based Access Control (RBAC). Nel contesto di una startup fintech, l'implementazione della riservatezza presenta sfide significative. L'accesso ai dati dei clienti e alle informazioni finanziarie deve essere rigorosamente controllato, ma i team piccoli e multifunzionali tipici delle startup spesso portano a una condivisione delle credenziali o all'assegnazione di privilegi eccessivi per "far funzionare le cose rapidamente". Ad esempio, durante lo sviluppo di un'API di pagamento, gli sviluppatori potrebbero avere accesso completo ai database di produzione contenenti dati sensibili dei clienti, invece di utilizzare dati anonimizzati o ambienti sandbox.

  La gestione delle chiavi di cifratura rappresenta un'ulteriore complessità: nelle startup dove i ruoli non sono chiaramente definiti, la responsabilità della gestione delle chiavi può essere ambigua, portando potenzialmente a compromissioni della sicurezza. L'implementazione di soluzioni robuste di Hardware Security Module (HSM) per la gestione delle chiavi può essere percepita come un costo eccessivo nella fase iniziale della startup, portando all'adozione di alternative meno sicure.

- **Integrity**: L'integrità garantisce che le informazioni rimangano accurate e affidabili durante il loro intero ciclo di vita. Mantenere l'integrità dei dati è essenziale per prevenire la diffusione di informazioni corrotte o ingannevoli, che potrebbero avere gravi ripercussioni in settori critici come quello sanitario o finanziario[7]Le tecniche utilizzate per preservare l'integrità includono:

  - Funzioni di hash crittografiche (es. SHA-256) per verificare che i dati non siano stati alterati.
  - Firme digitali per autenticare l'origine dei dati e garantirne la non modifica.
  - Controllo delle versioni per tracciare le modifiche e ripristinare versioni precedenti.
  - Checksum e meccanismi di rilevamento degli errori.

Nel contesto di una startup fintech, l'integrità dei dati è uno di quegli aspetti che va ad inficiare la brand reputation della startup stessa, in quanto la fiducia degli stakeholders si basa anche sulla capacità della startup di conservare i dati dei clienti senza distorsioni e di garantire l'accuratezza nelle transazioni di dati nella maniera più professionale possibile.

- **Availability**: assicurare che i dati siano sempre accessibili quando necessario.[7]Questo principio mira a prevenire interruzioni del servizio, sia dovute a guasti tecnici che ad attacchi malevoli come i Denial-of-Service (DoS) o Distributed Denial-of-Service (DDoS). L'indisponibilità può causare interruzioni operative, perdite economiche e danni alla reputazione. Le strategie per garantire un'elevata disponibilità comprendono:
  - Sistemi ridondanti (hardware, software, reti) per eliminare singoli punti di fallimento (Single Points of Failure - SPOF).
  - Backup regolari e piani di disaster recovery (DR) e business continuity (BCP).
  - Tecniche di bilanciamento del carico (load balancing) per distribuire il traffico di rete.
  - Misure di protezione contro attacchi DoS/DDoS.

  Nella maggior parte delle startup, l'infrastruttura di base viene sviluppata considerando una capacità di carico massimo limitato, in quanto nei primi periodo di vita dell'azienda non ci si aspetta un elevato numero di utenti. Proprio per questo motivo, l'infrastruttura presenta un punto vulnerabile che può essere sfruttato dagli attaccanti per mettere a repentaglio l'intero sistema, ad esempio con attacchi DoS/DDoS mirati al perimetro aziendale.La protezione contro attacchi DDoS richiede investimenti significativi in soluzioni di mitigazione che potrebbero non essere prioritarie nelle fasi iniziali. Inoltre, la natura delle startup spesso implica team ridotti con competenze concentrate su pochi individui, creando potenziali single point of failure umani: se l'unico ingegnere DevOps responsabile dell'infrastruttura non è disponibile durante un'emergenza, l'intera operatività potrebbe essere compromessa.

Difesa in Profondità (Defense in Depth)

Il principio di difesa in profondità prevede l'implementazione di multiple barriere protettive, così che se una viene compromessa, altre rimangono in piedi per proteggere le risorse. Questo approccio include strategie come autenticazione multi-fattore, segmentazione della rete, e rilevamento degli endpoint.

Nelle startup fintech, l'implementazione della difesa in profondità è spesso compromessa da vincoli di risorse e pressioni temporali. Ad esempio, mentre una soluzione di autenticazione a più fattori (MFA) è essenziale per proteggere l'accesso a dati finanziari sensibili, una startup potrebbe inizialmente implementare solo l'autenticazione basata su password per accelerare l'onboarding degli utenti, pianificando di aggiungere MFA "in un secondo momento" – un momento che potrebbe non arrivare prima che si verifichi un incidente di sicurezza.

La segmentazione della rete, fondamentale per contenere eventuali violazioni, richiede una progettazione accurata dell'infrastruttura. Tuttavia, nelle fasi iniziali, molte startup fintech operano con architetture di rete piatte per semplificare lo sviluppo e ridurre il sovraccarico operativo, oltre a non disporre del capitale umano competente per gestire una tale complessità. Questo approccio, sebbene comprensibile dal punto di vista dell'agilità, espone l'organizzazione a rischi significativi: un attaccante che ottiene accesso a un singolo segmento potrebbe muoversi lateralmente attraverso l'intera infrastruttura.

I test di vulnerabilità regolari, altro elemento chiave della difesa in profondità, sono spesso condotti in modo sporadico nelle startup a causa dei costi percepiti e dell'impatto sulle timeline di sviluppo. Una startup fintech potrebbe privilegiare il lancio rapido di nuove funzionalità rispetto a cicli di test di sicurezza approfonditi, esponendosi a vulnerabilità che potrebbero essere sfruttate da attaccanti motivati.

Principio del Minimo Privilegio

Questo principio stabilisce che ogni utente, processo o sistema debba operare utilizzando il set minimo di privilegi necessari per svolgere la propria funzione. Comprende pratiche come il controllo degli accessi basato sui ruoli e l'hardening dei sistemi.

Nelle startup fintech, applicare il principio del minimo privilegio (PoLP) presenta sfide uniche. La cultura focalizzata sulla velocità d'esecuzione spinge spesso a trascurare la sicurezza granulare degli accessi. È forte la tentazione di assegnare privilegi amministrativi ampi e generici per accelerare lo sviluppo, piuttosto che investire tempo nella configurazione di permessi specifici per ogni compito. Un esempio comune è concedere a tutti gli sviluppatori accesso completo al database di produzione durante la creazione di una nuova dashboard, invece di limitare ciascuno alle sole tabelle o operazioni strettamente necessarie. Sebbene sembri una scorciatoia efficiente, questa pratica crea vulnerabilità critiche: la compromissione di un singolo account può esporre una quantità sproporzionata di dati sensibili, amplificando enormemente i danni di una violazione. A complicare il quadro contribuisce l'alta mobilità interna tipica delle startup. I frequenti cambi di ruolo portano facilmente al "privilege creep", ovvero all'accumulo progressivo di accessi non più necessari, poiché mancano spesso processi formali di revoca. Anche la revisione periodica dei privilegi, fondamentale

per mantenere l'allineamento tra accessi e responsabilità correnti, viene spesso percepita come un intralcio burocratico e trascurata. Ulteriori difficoltà derivano dalle dimensioni ridotte dei team, dove i ruoli si sovrappongono, dalla rapida evoluzione delle responsabilità che rende obsoleti i permessi assegnati, e dalla complessa gestione degli accessi per fornitori e collaboratori esterni. Inoltre, trovare il giusto equilibrio tra sicurezza e produttività è cruciale: restrizioni eccessive possono rallentare il lavoro e spingere a cercare pericolose soluzioni alternative.

Separazione dei Compiti (Separation of Duties)

La separazione dei compiti prevede che nessun individuo possa controllare un processo critico dall'inizio alla fine, riducendo il rischio di frodi o errori. Si implementa attraverso processi di approvazione e controllo incrociato.

Nelle startup fintech, dove i team sono piccoli e i ruoli spesso sovrapposti, questo principio è particolarmente difficile da attuare. Ad esempio, in una startup che sviluppa una piattaforma di prestiti P2P, potrebbe esserci un solo ingegnere responsabile sia dell'implementazione del sistema di scoring del credito sia della configurazione dei controlli di sicurezza sullo stesso sistema. Questa concentrazione di responsabilità crea un rischio intrinseco: errori o azioni malevole potrebbero passare inosservati senza un secondo paio di occhi che verifichi il lavoro.

La pressione per l'efficienza operativa nelle startup può anche portare a scorciatoie nei processi di approvazione. Ad esempio, invece di richiedere approvazioni multiple per modifiche alla configurazione del sistema di pagamento, una startup potrebbe consentire a un singolo amministratore di implementare cambiamenti critici senza verifiche, aumentando il rischio di errori o frodi.

L'implementazione di controlli compensativi, come audit trail completi e revisioni post-implementazione, può mitigare parzialmente questi rischi quando la separazione completa dei compiti non è praticabile per vincoli di dimensione del team. Tuttavia, anche questi controlli richiedono disciplina e risorse dedicate che potrebbero non essere prioritarie nelle fasi iniziali della startup.

Zero Trust

Il modello Zero Trust si basa sul concetto di non fidarsi mai implicitamente di alcun utente, dispositivo o servizio, sia esso interno o esterno alla rete aziendale. Ogni richiesta di accesso a risorse (server, database, applicazioni) deve essere autenticata, autorizzata e verificata in base a criteri di identità, posture dei dispositivi e contesto operativo, indipendentemente dalla posizione di rete da cui proviene. L'architettura infrastrutturale tipica prevede micro-segmentazione dei carichi di lavoro, un sistema di controllo degli accessi basato su criteri dinamici e un monitoraggio continuo del comportamento e dello stato di sicurezza di utenti e dispositivi.

Per una startup fintech, l'adozione rigorosa del principio di Zero Trust può rivelarsi particolarmente gravosa. Nelle fasi iniziali, è frequente che l'intera infrastruttura sia gestita da una sola persona, con responsabilità sia di sviluppo sia di amministrazione di rete: questo crea un unico punto di falla, amplificando il rischio di errori di configurazione o di accesso non autorizzato. Inoltre, le limitate risorse economiche e umane possono rendere difficoltoso implementare soluzioni avanzate di micro-segmentazione, sistemi di Identity and Access Management (IAM) complessi e piattaforme di monitoraggio continuo. Infine, la mancanza di separazione dei compiti e di revisioni periodiche rende più probabile la persistenza di permessi eccessivi o non aggiornati, esponendo i sistemi a potenziali attacchi laterali e perdite di dati sensibili.

Secure by Design

Questo principio sostiene che la sicurezza debba essere integrata sin dall'inizio nel processo di sviluppo, piuttosto che aggiunta successivamente. Include pratiche come l'integrazione dei requisiti di sicurezza nelle prime fasi del progetto e lo sviluppo sicuro.

Per le startup fintech, l'adozione del principio "Secure by Design" rappresenta una tensione tra investimenti a lungo termine nella sicurezza e la necessità di velocità di sviluppo. Durante le fasi iniziali, quando l'obiettivo primario è dimostrare la validità del prodotto e acquisire i primi clienti, la tentazione di posticipare considerazioni di sicurezza è forte.

Ad esempio, una startup che sviluppa un'applicazione di gestione patrimoniale potrebbe concentrarsi inizialmente sull'esperienza utente e sulle funzionalità di investimento, lasciando per una fase successiva l'implementazione di controlli rigorosi per la protezione dei dati personali e finanziari. Questo approccio "security as an afterthought" può portare a vulnerabilità strutturali difficili da correggere successivamente, quando l'architettura del sistema è già consolidata.

L'integrazione della sicurezza nel processo di Continuous Integration/Continuous Deployment (CI/CD) rappresenta un'altra sfida: implementare scansioni di sicurezza automatizzate, analisi statica del codice e test di penetrazione come parte del pipeline di sviluppo richiede investimenti iniziali che potrebbero sembrare distrarre risorse dallo sviluppo delle funzionalità core. Tuttavia, l'automazione della sicurezza nel ciclo di vita dello sviluppo è fondamentale per identificare e correggere vulnerabilità prima che raggiungano l'ambiente di produzione.

Principio K.I.S.S. (Keep It Simple, Stupid)

Questo principio sostiene che sistemi più semplici tendono a essere più sicuri, poiché la complessità può introdurre vulnerabilità e rendere difficile per gli utenti seguire le procedure corrette.

Paradossalmente, nelle startup fintech, il principio K.I.S.S. viene spesso frainteso. Da un lato, c'è la tendenza a semplificare eccessivamente i controlli di sicurezza per ridurre l'attrito nell'esperienza utente o accelerare i processi interni. Dall'altro, la pressione per l'innovazione può portare a soluzioni tecnologiche complesse che introducono vulnerabilità non necessarie.

Un esempio tipico riguarda le politiche di password: una startup potrebbe implementare requisiti di complessità eccessiva (come cambi frequenti e regole complicate) che finiscono per incoraggiare comportamenti insicuri come l'annotazione delle password o il riutilizzo con piccole variazioni. Un approccio più equilibrato, basato su linee guida moderne come quelle del NIST, che privilegia la lunghezza rispetto alla complessità e riduce i cambi forzati, potrebbe essere più efficace e meno oneroso per gli utenti.

Analogamente, nell'architettura dei sistemi, l'adozione prematura di tecnologie emergenti senza una valutazione approfondita delle implicazioni di sicurezza può introdurre complessità e vulnerabilità. Una startup fintech che implementa una soluzione blockchain per il tracciamento delle transazioni senza una comprensione approfondita del modello di sicurezza sottostante potrebbe creare un sistema più vulnerabile rispetto a una soluzione tradizionale ben progettata e correttamente implementata.

Capitolo 2

Compliance a standard internazionali e framework di sicurezza

Nel settore fintech, la cybersecurity è una pietra angolare fondamentale per proteggere i dati sensibili e mantenere la fiducia degli utenti [8]. Le startup fintech operano in un contesto altamente digitale – con pagamenti elettronici, mobile banking, criptovalute e API aperte – che offre efficienze senza precedenti ma introduce anche rischi significativi [8]. Tra le minacce più comuni vi sono violazioni di dati finanziari, furti di identità, frodi sulle transazioni e attacchi informatici mirati ai sistemi di pagamento [8]. A differenza delle banche tradizionali, le fintech nascono spesso con minori vincoli normativi iniziali e un time-to-market aggressivo; ciò porta talvolta a trascurare gli aspetti di sicurezza nelle prime fasi di sviluppo [8]. Release frequenti e rapide possono indurre queste aziende a **omettere o posticipare misure di sicurezza** non ritenute immediatamente essenziali al business [8]. Ne risulta che molte soluzioni fintech, sebbene innovative, possono presentare controlli di sicurezza parziali o deboli, aumentando la probabilità di violazioni rispetto a istituzioni finanziarie più regolamentate.

Oltre alle minacce tecniche, le fintech affrontano rigorose sfide di **compliance normativa**. Se operano in ambito pagamenti, devono soddisfare standard come il **PCI DSS** (Payment Card Industry Data Security Standard) per la protezione dei dati delle carte, nonché normative sulla protezione dei dati personali come il **GDPR**. Studi di settore mostrano come molte fintech siano ancora in ritardo su questi fronti: ad esempio, il 62% dei siti web principali di aziende fintech esaminati non era conforme agli standard PCI DSS e il 64% non rispettava i requisiti GDPR [9]. Allo stesso tempo, regolamentazioni finanziarie come la PSD2 (Payment Services Directive 2) impongono requisiti di sicurezza (es. autenticazione forte del cliente) e le fintech

che offrono servizi analoghi a quelli bancari possono trovarsi sottoposte a verifiche di **sicurezza informatica e continuità operativa** tipiche del settore finanziario tradizionale.

In questo contesto complesso, diventa cruciale adottare **principi di cybersecurity strutturati** e basati su framework riconosciuti a livello internazionale. Questi framework forniscono un approccio sistematico per identificare i rischi, implementare controlli adeguati e garantire la resilienza dei sistemi. Nel seguito del capitolo verranno analizzati i principali framework e standard di sicurezza informatica – dal **NIST Cybersecurity Framework** all'ISO/IEC 27001, da linee guida NIST specifiche (SP 800-53, SP 800-82 per l'OT e SP 800-63B per le password) ai modelli di **Zero Trust** – illustrando come possano essere applicati nella pratica alla protezione dell'infrastruttura cloud di una startup fintech, con particolare riferimento ai server e ai dati ospitati su **Amazon Web Services (AWS)**. Verranno inoltre discusse **best practice e strategie di mitigazione** delle minacce più comuni, considerando le peculiarità degli ambienti cloud-native come AWS e l'importanza di un approccio di "difesa in profondità" integrato con i requisiti normativi di settore.

Prima di addentrarci nei framework, è fondamentale richiamare il modello di responsabilità condivisa nel cloud: **AWS è responsabile della sicurezza "of the cloud"**, ovvero della protezione dell'infrastruttura fisica e dei servizi di base (data center, hardware, rete, virtualizzazione), mentre **al cliente spetta la sicurezza "in the cloud"**, cioè la configurazione sicura dei propri ambienti virtuali, la gestione di accessi, rete, dati e applicazioni [10]. In altri termini, una fintech su AWS deve comunque implementare adeguati controlli di rete, cifratura, identity management, monitoring e così via, costruendo su un foundation sicuro fornito dal cloud provider ma senza delegare totalmente la responsabilità. Tenendo presente questo principio, esaminiamo ora i framework di sicurezza e come essi guidano l'implementazione di misure difensive su AWS.

2.1 NIST Cybersecurity Framework (CSF)

Il **NIST Cybersecurity Framework (CSF)**, sviluppato dal National Institute of Standards and Technology statunitense, è un framework di riferimento ampiamente adottato a livello globale come base per la gestione del rischio cyber in organizzazioni di qualsiasi settore o dimensione [11]. Nato per proteggere le infrastrutture critiche, il CSF è strutturato in cinque funzioni fondamentali – **Identify, Protect, Detect, Respond, Recover** – che rappresentano il ciclo continuo di gestione della sicurezza. Recentemente, con la versione 2.0 del 2024, è stata aggiunta una sesta funzione **"Govern"**, a sottolineare l'importanza delle attività organizzative e di governance nella gestione del rischio cyber [12]. Ciascuna funzione si articola in categorie e sottocategorie di controlli di sicurezza, fornendo così una tassonomia delle capacità di

cybersecurity che un'azienda dovrebbe sviluppare. Ad esempio, il CSF include categorie che coprono l'identificazione degli asset critici, la protezione tramite controlli di accesso e cifratura, il monitoraggio continuo degli eventi di sicurezza, la gestione degli incidenti e la resilienza operativa post-attacco.

Per una fintech che opera su AWS, il NIST CSF fornisce una **mappa concettuale** per implementare misure di sicurezza cloud in modo coerente e completo. AWS stessa riconosce il CSF come framework di riferimento e mette a disposizione linee guida su come allineare i servizi AWS alle diverse funzioni del CSF [12]. In pratica:

2.1.1 Identify (Identifica)

riguarda l'inventario e la classificazione di risorse, dati, software e flussi critici. Su AWS ciò implica mappare tutti i servizi in uso (istanze EC2, database RDS, bucket S3, ecc.), identificare i dati sensibili (es. dati finanziari dei clienti) e valutarne l'impatto in caso di compromissione. Strumenti come AWS Config e AWS Resource Explorer aiutano a mantenere la visibilità sugli asset cloud. È importante anche identificare le dipendenze da terze parti (ad es. API bancarie, servizi di pagamento) e i rischi di supply chain, in linea con l'enfasi posta dal CSF 2.0 sulla sicurezza della catena di fornitura [12].

2.1.2 Protect (Proteggi)

comprende tutte le misure volte a salvaguardare servizi e dati. In un'infrastruttura AWS, ciò include la **protezione della rete cloud** tramite VPC ben progettati e segmentati (suddividendo ambienti di produzione, staging, test in subnet isolate), l'uso di **security group** e **ACL di rete** per filtrare il traffico, e l'adozione di firewall applicativi e servizi come AWS WAF per difendersi da attacchi web. Possono essere integrate soluzioni di terze parti per rafforzare il perimetro, come vedremo con Check Point Quantum. La funzione Protect copre anche la **sicurezza dei dati**: su AWS è fondamentale cifrare i dati sia **a riposo** (es. tramite AWS KMS per chiavi di cifratura gestite e abilitando la crittografia su EBS, S3, RDS, etc.) sia **in transito** (usando protocolli TLS per API ed endpoint, e VPN/IPSec per connessioni private). Il controllo degli accessi ai dati va implementato con rigidi permessi IAM e politiche di bucket S3 che limitino l'accesso solo ai ruoli o servizi autorizzati. Un altro aspetto chiave è la **gestione delle identità e degli accessi (IAM)**: il CSF prescrive di implementare il principio del minimo privilegio e misure di robusta autenticazione. AWS IAM consente di definire ruoli e policy granulari, abilitare l'MFA sugli account (compreso l'account root) e centralizzare la gestione identitaria (ad esempio integrando provider SAML/SSO per gli utenti). L'uso di IAM Roles con credenziali temporanee

per servizi e applicazioni riduce il rischio di credenziali statiche esposte. Queste misure rispecchiano i **principi Zero Trust** di non fidarsi mai implicitamente di un'entità e di verificare ogni richiesta (vedi sezione 2.4). Infine, Protect include la **protezione dei sistemi e delle applicazioni**: ciò si traduce in hardening delle istanze (patching sistematico di sistemi operativi e middleware, disabilitazione di servizi inutili), utilizzo di servizi gestiti AWS (es. RDS, Lambda) che sollevano dall'onere di gestire direttamente server e riducono la superficie d'attacco, e impostazione di backup regolari e meccanismi di disaster recovery (snapshots, replicazione tra region, etc.) per garantire resilienza (quest'ultimo aspetto sconfina con la funzione Recover).

2.1.3 Detect (Individua)

il framework enfatizza la capacità di rilevare tempestivamente eventi anomali e possibili incidenti. Su AWS, **logging e monitoring** sono fondamentali. Ogni risorsa cloud dovrebbe generare log appropriati: AWS CloudTrail per tracciare tutte le chiamate API e attività nell'account, AWS CloudWatch per metriche di sistema e applicative con allarmi in caso di valori fuori soglia, AWS Config per cambiamenti di configurazione. Servizi avanzati come Amazon GuardDuty forniscono un monitoraggio continuo delle minacce analizzando pattern di traffico e log (identificando ad esempio comportamenti anomali indicativi di credenziali compromesse o istanze malevoli). Analogamente, Amazon Macie può rilevare eventuali esposizioni di dati sensibili su S3. L'aggregazione centralizzata dei log (magari in un servizio come Amazon S3 o CloudWatch Logs) e la loro correlazione tramite un SIEM (AWS offre AWS Security Hub per correlare avvisi da vari servizi) consente di **abilitare alerting in tempo reale** verso il team di sicurezza. Queste capacità rispondono all'esigenza di *traceability*: ogni azione o modifica nell'ambiente cloud deve essere tracciata e monitorata [13].

2.1.4 Respond (Rispondi)

definisce le attività di **gestione degli incidenti** nel momento in cui si verifica un problema di sicurezza. Una startup fintech dovrebbe avere un piano di incident response anche se piccola: procedure per analizzare gli eventi, contenere l'incidente (ad esempio isolando istanze compromesse, ruotando chiavi/API key esposte), eliminare la minaccia e ripristinare i servizi. AWS mette a disposizione strumenti che aiutano nella risposta: ad esempio, AWS CloudTrail facilita le indagini forensi permettendo di ricostruire le azioni compiute da un aggressore nell'account; servizi come AWS IAM Access Analyzer possono essere usati per verificare e chiudere eventuali accessi non intenzionali; AWS Systems Manager Incident Manager aiuta a orchestrare la risoluzione coordinando notifiche e runbook automatici. È buona prassi effettuare simulazioni

di incidenti e game-day per allenare il team a rispondere efficacemente, come raccomandato anche dal Well-Architected Framework [13]. Inoltre, bisogna considerare gli adempimenti di notifica: in caso di violazione di dati personali, ad esempio, il GDPR impone la comunicazione al Garante entro 72 ore, quindi il processo di incident response deve includere escalation manageriali e legali.

2.1.5 Recover (Recupera)

riguarda la **resilienza operativa** e la capacità di ripristinare rapidamente i servizi dopo un incidente o un guasto, minimizzando l'impatto sugli utenti e sui partner. In AWS, questo significa disporre di backup offline e piani di **disaster recovery** testati. Una fintech potrebbe mantenere backup crittografati dei database finanziari (ad esempio usando AWS Backup per centralizzare e automatizzare i backup di RDS, EBS, DynamoDB, etc.) e predisporre infrastrutture di ripristino in una regione secondaria per far fronte a eventi catastrofici sulla regione primaria. Servizi come Amazon S3 garantiscono durabilità elevatissima per i dati (11 9's) e possono versionare gli oggetti in modo da recuperare dati alterati o cancellati per errore. Il recover include anche comunicazioni post-incidente e miglioramento continuo: dopo il ripristino è importante condurre un post-mortem, capire le lezioni apprese e aggiornare i controlli di sicurezza per prevenire il ripetersi dell'incidente [12].

2.2 ISO/IEC 27001 e Sistemi di Gestione della Sicurezza (ISMS)

L'**ISO/IEC 27001** è lo standard internazionale di riferimento per stabilire, implementare e mantenere un *Information Security Management System* (**ISMS**), ovvero un sistema di gestione della sicurezza delle informazioni a 360 gradi. Si tratta di un framework gestionale che adotta un approccio basato sul rischio per garantire **riservatezza, integrità e disponibilità** delle informazioni aziendali attraverso un insieme di controlli di sicurezza organizzativi, fisici e tecnici. ISO 27001 è riconosciuto globalmente ed è applicato da organizzazioni in tutti i settori come **benchmark** di best practice per la sicurezza [14].

Cuore della norma è il ciclo PDCA (Plan-Do-Check-Act) applicato alla sicurezza: l'azienda deve condurre una valutazione dei rischi (identificando asset informativi, minacce, vulnerabilità e impatti), quindi adottare controlli adeguati (selezionati da una lista di riferimento nell'Annex A dello standard, che contiene 93 controlli suddivisi per tematiche nella versione 2022, tra cui politiche di sicurezza, sicurezza delle risorse umane, controllo accessi, criptografia, sicurezza fisica, sicurezza operativa, sicurezza

delle comunicazioni, controllo fornitori, gestione incidenti, continuità operativa, compliance, ecc.), monitorare e riesaminare periodicamente l'efficacia di tali controlli, e migliorare continuamente il sistema. La certificazione ISO 27001, rilasciata da un ente terzo accreditato, attesta che l'organizzazione segue questo processo e rispetta tutti i requisiti dello standard.

Per una startup fintech, ottenere la certificazione ISO 27001 può rappresentare un fattore abilitante di fiducia sul mercato – specialmente se si rivolge a clientela enterprise o bancaria – ma anche una sfida data la mole di processi e misure da implementare. L'adozione di servizi cloud AWS può tuttavia facilitare il raggiungimento della conformità ISO 27001. Innanzitutto, AWS stesso è certificato ISO/IEC 27001 per la propria infrastruttura globale di servizi cloud (oltre che per altri standard come ISO 27017 per i controlli cloud-specific e ISO 27018 per la privacy nel cloud), il che significa che i data center e i servizi AWS sono gestiti secondo controlli di sicurezza riconosciuti. Questo aiuta la fintech a concentrarsi sui controlli applicativi e organizzativi, sapendo che molti requisiti di base – ad esempio sulla protezione fisica dei server, il controllo degli accessi ai locali, la continuità elettrica e di rete – sono già coperti e attestati dalla piattaforma AWS. Tuttavia, la **responsabilità dell'implementazione** rimane al cliente per tutti i controlli relativi ai propri dati e configurazioni nel cloud (cfr. modello di responsabilità condivisa). Ad esempio, ISO 27001 richiede di controllare gli accessi logici: la fintech dovrà definire policy IAM, regole di password e uso di MFA in AWS per soddisfare tale controllo. Richiede di tenere registri degli eventi: la fintech dovrà configurare logging (CloudTrail, etc.) e conservarne le evidenze. Richiede di cifrare informazioni sensibili: la fintech dovrà abilitare la crittografia nei servizi AWS dove risiedono dati critici.

2.3 NIST SP 800-53 – Catalogo di Controlli di Sicurezza

Il framework NIST SP 800-53 fornisce un **catalogo completo di controlli di sicurezza e privacy** per sistemi informativi, originariamente sviluppato per le agenzie federali USA ma ormai adottato come riferimento anche da molte organizzazioni nel settore privato [14]. Si tratta quindi di uno standard più **prescrittivo e tecnico**, che copre aspetti di sicurezza logica, fisica, procedurale e del personale, organizzati in diverse famiglie di controlli. L'ultima revisione (Rev. 5) del NIST 800-53 contiene **20 famiglie di controlli** principali [14], tra cui ad esempio:

1. **AC – Access Control** (controllo degli accessi)
2. **IA – Identification and Authentication** (identificazione e autenticazione)

3. **SC – System and Communications Protection** (protezione dei sistemi e delle comunicazioni, es. cifratura, segregazione di rete)
4. **SI – System and Information Integrity** (integrità dei sistemi e delle informazioni, es. anti-malware, gestione vulnerabilità, monitoraggio)
5. **AU – Audit and Accountability** (audit e tracciabilità, es. logging)
6. **IR – Incident Response** (risposta agli incidenti)
7. **CP – Contingency Planning** (piani di emergenza e DR)
8. **PE – Physical and Environmental Protection** (sicurezza fisica)
9. **PS – Personnel Security** (sicurezza del personale, background check, ecc.)
10. **...** (oltre a **Risk Assessment**, **Security Assessment**, **Configuration Management**, **Training**, **Maintenance**, **Supply Chain Risk Management**, ecc.)

In totale, l'800-53 Rev.5 cataloga circa 1000 controlli di sicurezza, da cui vengono derivati dei **controlli di baseline** (Low, Moderate, High) in base al livello di impatto del sistema [14]. Ad esempio, un sistema *Moderate* (come potrebbe essere un sistema fintech con dati sensibili ma non classificati) deve implementare tutti i controlli del baseline Moderate, che sono un sottoinsieme di quelli totali, selezionati in base a un'analisi del rischio. Le organizzazioni possono poi *personalizzare* (tailor) il baseline aggiungendo o escludendo controlli a seconda delle esigenze specifiche e dei requisiti normativi applicabili [14].

Dal punto di vista di AWS, è importante notare che **l'infrastruttura AWS è già stata validata rispetto ai controlli NIST 800-53** (Rev.4) nell'ambito delle certificazioni FedRAMP Moderate/High per i servizi AWS [11]. Ciò significa che AWS ha superato audit di terza parte che attestano la presenza di controlli di sicurezza allineati a 800-53 per quanto riguarda la piattaforma cloud sottostante [11]. AWS ha ottenuto "Authority to Operate" FedRAMP per molte region (inclusa GovCloud) proprio in base a questi controlli [11]. Per la fintech cliente, questo non significa automaticamente essere conforme a 800-53, ma fornisce una base solida: ad esempio, i controlli di sicurezza fisica (PE) e ambientale, molti controlli di rete (SC), e parte di quelli di monitoraggio (SI) sono già soddisfatti dall'ambiente AWS stesso. Rimane al cliente implementare i controlli a livello di applicazione e configurazione cloud (ad es., definire ruoli IAM – controllo AC-2, o abilitare il versioning su S3 – parte di SC e SI, ecc.). AWS fornisce anche strumenti come **AWS Audit Manager** con regole predefinite per NIST 800-53, che consentono di valutare l'account AWS rispetto ai controlli di tale framework e collezionare evidenze in caso di audit [15].

2.4 Architettura Zero Trust (ZTA)

Tradizionalmente, la sicurezza informatica aziendale si basava su un modello di **difesa perimetrale**: si creava una rete aziendale considerata "fidata" all'interno, separata dall'esterno non fidato tramite firewall e altre barriere (il cosiddetto modello "castle and moat"). Tuttavia, con l'evoluzione delle minacce e soprattutto con la distribuzione di sistemi su cloud, utenti mobili, telelavoro e dispositivi personali, questo paradigma è diventato inefficace. Nasce così il concetto di **Zero Trust**, formalizzato anche dal NIST nel documento SP 800-207, che rivoluziona l'approccio: *non si deve mai implicitamente fidare di nulla, sia all'interno che all'esterno del perimetro, ma verificare esplicitamente ogni richiesta di accesso a risorse aziendali* [16]. In un'Architettura Zero Trust (**ZTA**), le difese non sono più incentrate su una rete interna considerata sicura, ma **sull'identità degli utenti e dei dispositivi, e sul contesto delle richieste**, indipendentemente dalla loro provenienza.

I principi cardine della Zero Trust, come delineati dal NIST, includono: **nessuna fiducia implicita basata su posizione di rete** (essere su una rete interna non concede privilegi di per sé) [16]; **autenticazione e autorizzazione continue** per ogni accesso, convalidando sia l'utente che il dispositivo prima di consentire comunicazioni [16]; **micro-segmentazione** delle risorse per minimizzare il movimento laterale – ovvero, anche all'interno dell'infrastruttura, segmentare applicazioni, servizi e database in piccole zone con regole di accesso rigorose; **principio del privilegio minimo dinamico**, adattando i permessi in base al contesto (orario, geolocalizzazione, integrità del dispositivo, comportamento anomalo); **monitoraggio e verifica costante** del traffico e dei comportamenti per rilevare eventuali compromissioni. In sintesi, Zero Trust "sposta" il confine di fiducia dal network all'entità che richiede l'accesso, in un modello in cui **ogni transazione è autenticata, criptata e validata** in modo robusto, come se provenisse da un ambiente non fidato, anche se in realtà avviene all'interno del sistema.

2.5 Sicurezza OT (Tecnologie Operative) – NIST SP 800-82

Nel dominio della cybersecurity aziendale, oltre all'IT tradizionale (server, applicazioni, dati), acquista importanza la protezione delle **tecnologie operative (OT)**, ossia quei sistemi digitali che interagiscono con il mondo fisico. Le aziende fintech, essendo principalmente nel settore finanziario digitale, generalmente non operano impianti industriali o infrastrutture OT su larga scala come farebbe una utility o una fabbrica. Tuttavia, è possibile che alcune componenti fisiche rientrino nel perimetro di una fintech: si pensi ad esempio agli **ATM/Bancomat**, ai dispositivi POS smart,

ai data center on-premises con sistemi di building automation, o a eventuali sensori IoT impiegati per servizi innovativi [17]. Il **NIST SP 800-82** fornisce linee guida specifiche per migliorare la sicurezza dei sistemi OT, tenendo conto dei loro requisiti unici di prestazioni, affidabilità e sicurezza fisica [17]. Tali sistemi presentano sfide peculiari: spesso operano in tempo reale, non possono subire interruzioni (disponibilità e sicurezza fisica prevalgono su confidenzialità), utilizzano protocolli proprietari o legacy, e possono avere cicli di vita molto lunghi con componenti non facilmente aggiornabili.

Per mettere in sicurezza ambienti OT, il framework NIST OT Security raccomanda di: **segmentare rigorosamente le reti OT dalle reti IT**, inserendo gateway e firewall industriali che limitino il traffico; **implementare controlli di accesso e monitoraggio specifici** per i protocolli OT; assicurare l'**integrità e l'affidabilità** dei comandi inviati ai dispositivi fisici; gestire patch e vulnerabilità OT in modo pianificato, compensando quando necessario; e predisporre piani di incident response OT che considerino anche scenari di sicurezza fisica e safety [17].

2.6 Sicurezza delle Password e Gestione delle Identità – NIST SP 800-63B

Le **password** rimangono tutt'oggi uno dei principali meccanismi di autenticazione, ma anche un punto debole sfruttato di frequente dagli attaccanti (tramite phishing, attacchi a dizionario, credential stuffing, ecc.). Per questo motivo, il NIST ha pubblicato il documento **NIST SP 800-63B** (Digital Identity Guidelines) che fornisce raccomandazioni aggiornate su come gestire in modo sicuro le password, ovvero i "memorized secrets" [18]. Le linee guida più recenti ribaltano alcuni concetti tradizionali a favore di un approccio più user-friendly e sicuro. In sintesi, il NIST suggerisce di privilegiare la lunghezza e la complessità "naturale" delle password rispetto a regole forzate e reset frequenti, integrando tali misure con verifiche di qualità e fattori aggiuntivi [18].

2.7 Difesa Perimetrale Avanzata e Soluzioni di Next-Gen Firewall – Check Point Quantum

Oltre ai framework e alle linee guida generali, è utile considerare l'adozione di **tecnologie specifiche** per potenziare la sicurezza dell'infrastruttura cloud. Nel panorama attuale, i firewall di nuova generazione e le piattaforme integrate di threat prevention giocano un ruolo chiave nel proteggere reti e workload, specialmente in scenari ibridi o multi-cloud. **Check Point Quantum** è un esempio di suite di sicurezza

che una fintech potrebbe adottare per migliorare la propria postura difensiva [19]. In particolare, Check Point Quantum Network Security offre una protezione scalabile e multi-livello contro minacce informatiche evolute, integrando moduli come SandBlast Threat Prevention e una console di gestione unificata [19].

2.8 Best practice e strategie di mitigazione

Attraverso l'analisi dei framework e delle soluzioni sopra esposte, emergono alcuni **principi trasversali di sicurezza** che dovrebbero guidare ogni fintech nella protezione della propria infrastruttura su AWS. Di seguito, le migliori pratiche e strategie di mitigazione più efficaci:

- **Identità solida e minimo privilegio**: Utilizzare account separati, applicare il principio del minimo privilegio e adottare MFA, come suggerito dal Well-Architected Framework [13].
- **Segmentazione e difesa in profondità**: Implementare controlli multipli a vari livelli, segmentando reti e isolando applicazioni, come indicato dal Well-Architected Framework [13].
- **Protezione dei dati critica**: Cifrare i dati a riposo e in transito, classificare le informazioni e implementare DLP, in accordo con le linee guida AWS [13].
- **Monitoraggio continuo e traceability**: Abilitare logging e correlare i dati tramite SIEM, come raccomandato dal Well-Architected Framework [13].
- **Automatizzare la sicurezza e l'infrastruttura come codice**: Utilizzare IaC e automatizzare controlli di sicurezza per ridurre errori umani [13].
- **Preparazione agli incidenti e resilienza**: Disporre di piani di incident response e di continuità operativa, testandoli regolarmente [13].
- **Formazione e cultura della sicurezza**: Investire nella formazione continua e adottare un approccio "Secure by Design" e "Shift Left" [8].
- **Compliance proattiva**: Integrare controlli normativi (es. PCI DSS, GDPR) nel ciclo di sicurezza per rafforzare l'ambiente [8].

Capitolo 3

Fondamenti di Sicurezza su AWS

3.1 Modello di responsabilità condivisa di AWS

3.2 Best practice di sicurezza specifiche per startup fintech

3.3 Panoramica dei principali servizi di sicurezza di AWS

3.3.1 AWS Identity and Access Management (IAM)

3.3.2 AWS Key Management Service (KMS)

3.3.3 AWS CloudTrail e Amazon CloudWatch (servizi concorrenti)

3.3.4 AWS GuardDuty, Amazon Inspector e Amazon Macie (alternativa valida)

3.3.5 Altri servizi rilevanti (es. AWS WAF, VPC)

Capitolo 4

Gestione delle Identità e degli Accessi (IAM)

4.1 Implementazione del principio del minimo privilegio

4.2 Creazione e gestione di utenti, gruppi e ruoli IAM

4.3 Utilizzo di policy IAM per concedere permessi granulari

4.4 Configurazione dell'autenticazione a più fattori (MFA)

4.5 Gestione delle credenziali (es. utilizzo di IAM Roles per EC2)

4.6 Audit e monitoraggio degli accessi IAM

Capitolo 5

Monitoraggio e Logging della Sicurezza

5.1 Configurazione di AWS CloudTrail per tracciare le attività degli utenti

5.2 Implementazione di Amazon CloudWatch per monitorare le metriche di sistema

5.3 Creazione di allarmi per eventi specifici e attività sospette

5.4 Utilizzo di AWS GuardDuty per il rilevamento automatico di minacce

5.5 Integrazione con sistemi SIEM (Security Information and Event Management)

5.6 Gestione e analisi dei log

Capitolo 6

Protezione dei Dati Sensibili e Conformità Normativa

6.1 Crittografia dei dati a riposo e in transito

6.2 Gestione delle chiavi di crittografia con AWS KMS o CloudHSM

6.3 Implementazione di meccanismi per la protezione dei dati in S3

6.4 Misure per la conformità a PCI DSS (se rilevante)

6.5 Misure per la conformità al GDPR e protezione dei dati personali

6.6 Valutazione e gestione del rischio di perdita di dati

Capitolo 7

Casi Studio e Implementazione Pratica

7.1 Esempio di architettura di sicurezza AWS per una startup fintech (proposta)

7.2 Implementazione delle best practice descritte nei capitoli precedenti

7.3 Test di penetrazione e valutazione della sicurezza dell'ambiente

7.4 Analisi dei risultati e confronto con le best practice

7.5 Integrazione di strumenti di sicurezza terzi (es. SentinelOne)

7.6 Infrastruttura di base AWS, integrazione codice e infrastruttura di un sistema honeypot

7.7 Deadcode per confondere malware (Capitolo 7)

7.8 Autenticazione con chiavi pubbliche (Capitolo 8)

7.9 Progettazione e implementazione di una Virtual Private Cloud (VPC) isolata

Capitolo 8

Discussione e Conclusioni

8.1 Rielaborazione delle domande di ricerca iniziali e discussione dei risultati

8.2 Riflessioni sulle sfide e opportunità per la sicurezza di AWS nelle startup fintech

8.3 Prospettive future per la ricerca e l'innovazione

8.4 Raccomandazioni per la creazione di un modello di cybersecurity resiliente per startup fintech

Bibliografia

[1] Gartner, *Rapporto sugli investimenti globali Fintech*, Investimenti globali in Fintech: crescita e trend, 2018.

[2] *Tecnofinanza - Wikipedia*, Accesso: 2023-10-01. indirizzo: `https://it.wikipedia.org/wiki/Tecnofinanza`.

[3] *Fintech: quali sono le startup e i numeri in Italia*, Accesso: 2023-10-01. indirizzo: `https://blog.osservatori.net/it_it/fintech-in-italia`.

[4] Anonimo, *Le sfide della cybersecurity nelle startup Fintech*, Rapporto sul rischio e le vulnerabilità in ambito Fintech, 2023.

[5] Anonimo, *Differenze tra Cybersecurity Bancaria e Fintech*, Analisi comparativa degli approcci di sicurezza, 2023.

[6] Anonimo, *Minacce informatiche nel settore Fintech*, Analisi delle tipologie di attacchi e delle vulnerabilità in ambito Fintech, 2023.

[7] D. Popescul, "The Confidentiality – Integrity – Accessibility Triad into the Knowledge Security. A Reassessment from the Point of View of the Knowledge Contribution to Innovation", vol. 4, pp. 978–, giu. 2011.

[8] Netguru. "Cybersecurity in Fintech. Why Is It Important? [2023 Update]". Accessed: 2025-03-10. indirizzo: `https://www.netguru.com/blog/cybersecurity-in-fintech`.

[9] S-PRO. "Fintech security and regulatory compliance best practices and checklists". Accessed: 2025-03-10. indirizzo: `https://s-pro.io/whitepapers/fintech-security-best-practices`.

[10] A. W. Services. "AWS Shared Responsibility Model". Accessed: 2025-03-10. indirizzo: `https://aws.amazon.com/marketplace/pp/prodview-noe2gzebdrqog`.

[11] A. W. Services. "NIST - Amazon Web Services (AWS)". Accessed: 2025-03-10. indirizzo: `https://aws.amazon.com/compliance/nist/`.

[12] A. W. Services. “Updated whitepaper available: Aligning to the NIST Cybersecurity Framework in the AWS Cloud”. Accessed: 2025-03-10. indirizzo: https://aws.amazon.com/blogs/security/updated-whitepaper-available-aligning-to-the-nist-cybersecurity-framework-in-the-aws-cloud/.

[13] A. W. Services. “Security - AWS Well-Architected Framework”. Accessed: 2025-03-10. indirizzo: https://wa.aws.amazon.com/wellarchitected/2020-07-02T19-33-23/wat.pillar.security.en.html.

[14] Hyperproof. “NIST SP 800-53 Compliance — Improve Your Security System”. Accessed: 2025-03-10. indirizzo: https://hyperproof.io/nist-800-53/.

[15] A. W. Services. “AWS Audit Manager: Automate Evidence Collection for Compliance”. Accessed: 2025-03-10. indirizzo: https://docs.aws.amazon.com/audit-manager/latest/userguide/NIST-Cybersecurity-Framework-v1-1.html.

[16] N. I. of Standards e Technology. “Zero Trust Architecture”. Accessed: 2025-03-10. indirizzo: https://www.nist.gov/publications/zero-trust-architecture.

[17] N. I. of Standards e Technology. “SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security”. Accessed: 2025-03-10. indirizzo: https://csrc.nist.gov/pubs/sp/800/82/r3/ipd.

[18] JumpCloud. “NIST 800-63 Password Guidelines at a Glance”. Accessed: 2025-03-10. indirizzo: https://jumpcloud.com/blog/nist-800-63-password-guidelines.

[19] A. W. Services. “AWS Marketplace: Check Point Quantum Network Security”. Accessed: 2025-03-10. indirizzo: https://aws.amazon.com/marketplace/pp/prodview-eu5dbipshnzkq.