PROGETTARE SECONDO IL PARADIGMA DEL "SECURITY BY DESIGN"

Francesco Violante, Francesco De Lucci, Michele Caringella

ITALPAGHE s.r.l., Viale Paolo Borsellino e Giovanni Falcone, 17, 70125 Bari BA
info@italpaghe.net

SOMMARIO

Il "*Security by Design*" è un approccio innovativo nello sviluppo di sistemi software e hardware, mirato a garantire la sicurezza fin dalle prime fasi della progettazione. A differenza delle metodologie tradizionali che considerano la sicurezza come un'aggiunta successiva, il *Security by Design* integra la sicurezza come componente fondamentale durante tutto il ciclo di vita del prodotto, dall'ideazione alla dismissione. Questo approccio è diventato sempre più cruciale con l'aumento delle minacce informatiche e la crescente complessità delle tecnologie digitali. L'articolo esplora l'importanza del *Security by Design* non solo per la protezione dei dati e delle applicazioni aziendali, ma anche per la sicurezza di infrastrutture critiche e servizi essenziali, come la gestione dei trasporti pubblici, le reti energetiche e i servizi sanitari. In questo asrticolo Inoltre, si discute l'applicazione del *Security by Design* nello sviluppo di tecnologie innovative come gli *smart contract*, con un focus sul modulo PACO-Smart-Contract sviluppato durante il progetto ACROSS da Italpaghe srl. Vengono illustrati i principi fondamentali del *Security by Design*, tra cui la riduzione della superficie d'attacco, il privilegio minimo, la *privacy by default* e la difesa in profondità. L'articolo descrive anche le fasi dell'implementazione, che includono l'analisi delle esigenze degli utenti, la valutazione dei rischi informatici, la definizione delle specifiche di sicurezza, la progettazione dell'architettura sicura, il *testing* e la verifica, nonché la manutenzione e l'aggiornamento continui. L'adozione del *Security by Design* offre numerosi vantaggi, tra cui una protezione più efficace dei dati sensibili, la riduzione dei costi di sicurezza, la conformità normativa e una maggiore affidabilità del sistema.

1. INTRODUZIONE

Il "*Security by Design*" garantisce la sicurezza sin dalle prime fasi della progettazione. Contrariamente alle metodologie tradizionali che affrontano le questioni di sicurezza come un'aggiunta successiva, il *Security by Design* integra la sicurezza come componente fondamentale del ciclo di vita del prodotto, dall'ideazione fino alla dismissione. Questo paradigma è diventato sempre più rilevante con l'aumento delle minacce informatiche e la crescente complessità delle tecnologie digitali. L'approccio del Security by Design è di fondamentale importanza non solo per la protezione dei dati e delle applicazioni aziendali, ma anche per la sicurezza di infrastrutture critiche e servizi essenziali. Questi includono la gestione dei trasporti pubblici, le reti energetiche, i servizi sanitari e molti altri settori vitali per il funzionamento della società moderna. L'integrazione della sicurezza fin dalla fase di progettazione in questi ambiti è cruciale per prevenire interruzioni di servizio, attacchi cyber e danni potenziali alle persone e alle economie. Un esempio significativo dell'importanza del *Security by Design* si trova nella gestione dei trasporti pubblici. Le reti di trasporto pubblico sono sempre più interconnesse e dipendono da sistemi informatici per il loro funzionamento quotidiano, come i sistemi di bigliettazione elettronica, i segnali di traffico e le comunicazioni di emergenza. Un attacco informatico a questi sistemi potrebbe causare disservizi massicci, mettere a rischio la sicurezza dei passeggeri e causare gravi danni economici. Integrare la sicurezza fin dalla progettazione di questi sistemi aiuta a proteggere contro tali minacce. Molti studi in letteratura sostengono che l'adozione di pratiche di Security by Design può migliorare la resilienza delle reti di trasporto pubblico delle città, riducendo significativamente i tempi di inattività e i costi associati agli attacchi informatici [1]. Anche la digitalizzazione dei servizi sanitari, inclusa la gestione delle cartelle cliniche elettroniche e i sistemi di monitoraggio remoto dei pazienti, richiede un'attenzione particolare alla sicurezza. Gli attacchi informatici in questo settore possono avere conseguenze devastanti, compromettendo la privacy dei pazienti e la disponibilità dei servizi sanitari critici. Un articolo scientifico del 2023 discute l'implementazione del *Security by Design* nei sistemi sanitari, proponendo una metodologia di gestione della sicurezza che permette di ridurre significativamente gli incidenti di sicurezza e migliorare la protezione dei dati dei pazienti [2]. Tra i settori fondamentali e critici, quindi, è da evidenziare anche la distribuzione di energia elettrica. Le reti energetiche, composte da sistemi di distribuzione e gestione dell'energia, sono un altro settore critico dove il Security by Design gioca un ruolo essenziale. Con l'espansione delle *smart grids* e l'integrazione di tecnologie IoT, le reti energetiche sono diventate bersagli attraenti per i cyber-attacchi. Un attacco riuscito potrebbe interrompere l'erogazione di energia, causando *blackout* diffusi e compromettendo la sicurezza nazionale. Un esempio pratico è il caso dell'attacco informatico alla rete elettrica ucraina nel 2015, che ha lasciato senza corrente più di 200.000 persone. Le *smart grid* in Italia sono

caratterizzate da un'infrastruttura avanzata che integra vari componenti tecnologici per migliorare l'efficienza e la sicurezza del sistema energetico. Un elemento chiave di questa infrastruttura è l'*Advanced Metering Infrastructure* (AMI), che collega le abitazioni dei consumatori con la rete di comunicazione, utilizzando contatori intelligenti per trasmettere dati di utilizzo energetico e guasti ai fornitori di servizi *cloud*. Essendo uno dei primi paesi per lo sviluppo dell'infrastruttura di misurazione intelligente, l'Italia ha distribuito contatori intelligenti a quasi tutti i clienti con la tecnologia PLC per trasferire i dati dei contatori intelligenti al concentratore dati più vicino situato nella sottostazione MT/BT. Quindi questi dati vengono inviati ai data center del DSO (Distribution System Operator) per la registrazione e l'analisi dei dati [3]. Questo approccio permette una gestione più efficiente e reattiva delle risorse energetiche. In Italia, l'implementazione delle *smart grid* ha visto l'adozione di tecnologie di comunicazione sia cablate che wireless. Le tecnologie cablate includono *Power Line Communication* (PLC), fibra ottica ed Ethernet, mentre le tecnologie wireless comprendono reti cellulari, WiMAX, Zigbee, Zwave, satelliti e comunicazioni ottiche in spazio libero. Queste tecnologie facilitano la raccolta e la trasmissione dei dati dai contatori intelligenti ai centri di elaborazione dati, migliorando l'efficienza operativa e la stabilità della rete. Le tecnologie delle *smart grid* offrono numerosi vantaggi rispetto alle reti tradizionali, inclusi miglioramenti nella gestione, controllo e operazioni. Questi benefici rendono la *smart grid* una scelta più attraente rispetto ai sistemi di rete tradizionali. Adottare un approccio di *Security by Design* nella progettazione delle *smart grids* può prevenire incidenti gravi, come quello accaduta in Ucraina nel 2015, garantendo una protezione robusta contro le intrusioni e le manipolazioni dei sistemi [4]. Inoltre, il *Security by Design* trova applicazione anche nello sviluppo di tecnologie innovative come gli *smart contract*. Gli *smart contract* sono protocolli informatici che verificano e applicano automaticamente la negoziazione di un contratto. Utilizzando la tecnologia blockchain, questi contratti garantiscono transazioni sicure e trasparenti, eliminando la necessità di intermediari. Negli ultimi anni, l'aumento dei prezzi dell'energia ha destato preoccupazioni globali. Nel 2022, l'Unione Europea ha registrato prezzi energetici storicamente elevati, come riportato dal Consiglio dell'UE. Questo incremento è stato attribuito a una maggiore domanda di energia in seguito alla pandemia di COVID-19, alla guerra in Ucraina e all'accelerazione dei cambiamenti climatici. In particolare, la decisione della Russia di sospendere le forniture di gas alla maggior parte degli Stati membri dell'UE ha aumentato significativamente i prezzi del gas e dell'elettricità. Tra gennaio 2021 e gennaio 2023, i prezzi dell'energia per i produttori industriali domestici sono aumentati del 127%, mentre i prezzi per i consumatori sono aumentati del 63,5%. Considerando l'elevata volatilità dei prezzi dell'energia e il fatto che il settore energetico sta attraversando una trasformazione digitale, la tecnologia blockchain e gli *smart contract* offrono il potenziale per rivoluzionare questo settore fornendo una piattaforma sicura, trasparente ed efficiente per le transazioni energetiche. La blockchain è una tecnologia di registro distribuito che consente transazioni *peer-to-peer* (P2P) senza autorità centrale o organo di controllo [5]. Questa tecnologia può essere utilizzata sia per supportare transazioni energetiche complesse tra consumatori e produttori di energia, sia per sviluppare nuovi modelli di business, come le transazioni energetiche *peer-to-peer*. L'uso della *blockchain* nel settore energetico ha guadagnato slancio negli ultimi anni grazie alla sua capacità di garantire transazioni sicure, trasparenti ed efficienti. Le aziende energetiche possono ridurre i costi associati ai processi tradizionali di trading energetico, come le commissioni di transazione e i costi amministrativi [6]. Inoltre, la tecnologia *blockchain* può contribuire a migliorare l'accuratezza e l'affidabilità dei dati energetici, portando a decisioni migliori e a un miglior servizio clienti. In questo contesto, l'adozione del paradigma del *Security by Design* negli *smart contract* diventa cruciale. Integrare la sicurezza fin dalle prime fasi della progettazione degli *smart contract* permette di prevenire vulnerabilità e garantire la robustezza delle transazioni energetiche digitali. Questo approccio è essenziale per proteggere i dati sensibili e garantire la fiducia tra le parti coinvolte nelle transazioni energetiche basate su blockchain.

Un esempio concreto di applicazione del *Security by Design* nel contesto degli *smart contract* è il modulo PACO-Smart-Contract, sviluppato durante il progetto ACROSS da Italpaghe srl . Questo modulo è stato progettato per facilitare la contrattualizzazione e la gestione dei consulenti da parte delle aziende, integrando misure di sicurezza robuste per proteggere i dati e garantire la correttezza delle transazioni. Di seguito verranno esplorate le basi teoriche del *Security by Design*, illustrando i principi chiave che guidano questo approccio e gli *step* necessari per la sua implementazione pratica.

2. PRINCIPI DEL *SECURITY BY DESIGN*

L'introduzione del Regolamento Generale sulla Protezione dei Dati (GDPR) [7] e della Direttiva NIS sulla sicurezza delle reti e dei sistemi informativi [8] ha significativamente influenzato l'adozione del *Security by Design* in Europa. Il GDPR, in particolare, enfatizza l'importanza della protezione dei dati personali e impone che le misure di sicurezza siano integrate nei processi di trattamento dei dati fin dalla fase di progettazione. L'articolo 25 del GDPR stabilisce che i titolari del trattamento devono implementare misure tecniche e organizzative adeguate per garantire che, per impostazione predefinita, siano trattati solo i dati personali necessari per ciascuna specifica finalità del trattamento. Contrariamente alle metodologie tradizionali, il "*Security by Design*" integra la sicurezza come componente fondamentale del ciclo di vita del prodotto, dall'ideazione fino alla dismissione. Questo paradigma è diventato sempre più rilevante con l'aumento delle minacce informatiche e la

crescente complessità delle tecnologie digitali. Il *Security by Design* si basa su una serie di principi fondamentali volti a creare un ambiente sicuro e resiliente. Tra questi, i più rilevanti sono:

1. la riduzione della superficie d'attacco: minimizzare i punti di ingresso vulnerabili riducendo la complessità del sistema e limitando le funzionalità esposte agli utenti esterni. Questo principio si focalizza sull'eliminazione delle potenziali vie di accesso per gli attaccanti, rendendo il sistema meno suscettibile alle minacce;
2. il privilegio minimo: assegnare agli utenti solo i permessi strettamente necessari per svolgere le loro attività. Questo principio limita l'accesso ai dati e alle risorse critiche, riducendo il rischio di abuso o di compromissione delle informazioni sensibili;
3. la privacy by default: implementare impostazioni di sicurezza predefinite che proteggano i dati personali degli utenti senza richiedere interventi manuali da parte loro. Questo principio assicura che le misure di protezione siano attive fin dall'inizio, riducendo il rischio di configurazioni errate o inadeguate;
4. la difesa in profondità: adottare un approccio multilivello alla sicurezza, implementando diverse linee di difesa per proteggere i dati e i sistemi. Questo principio prevede l'utilizzo di più livelli di protezione, come firewall, sistemi di rilevamento delle intrusioni e crittografia, per creare un ambiente sicuro e resistente agli attacchi.

3. IMPLEMENTAZIONE DEL *SECURITY BY DESIGN*

L'implementazione del *Security by Design* richiede un approccio strutturato e metodico che coinvolga diverse fasi del ciclo di vita dello sviluppo del software. Queste fasi includono:

1. l'analisi delle esigenze degli utenti: identificazione dei requisiti di sicurezza specifici degli utenti e delle applicazioni. Questo passaggio è cruciale per garantire che le misure di sicurezza siano allineate con le necessità operative e i rischi specifici del sistema;
2. la valutazione dei rischi informatici: analisi delle potenziali vulnerabilità e minacce che potrebbero compromettere la sicurezza del sistema. Questa fase prevede la conduzione di valutazioni di rischio per identificare le aree critiche e determinare le contromisure appropriate;
3. la definizione delle specifiche di sicurezza: stabilire i requisiti di sicurezza dettagliati per il sistema, basati sui risultati della valutazione dei rischi. Questi requisiti devono essere chiaramente documentati e integrati nel processo di sviluppo;
4. la progettazione dell'architettura sicura: rappresenta uno degli aspetti fondamentali del *Security by Design*. Questa fase prevede la creazione di un sistema che integri i principi di sicurezza fin dalle prime fasi di progettazione, garantendo che ogni componente del sistema sia progettato tenendo conto delle potenziali vulnerabilità e minacce. La definizione di interfacce sicure è un passaggio cruciale nella progettazione dell'architettura di un sistema. Le interfacce rappresentano i punti di contatto tra diverse componenti del sistema o tra il sistema e l'esterno, e come tali, possono essere potenziali punti di ingresso per attacchi informatici. Assicurare che queste interfacce siano progettate in modo sicuro significa implementare controlli di accesso rigorosi, autenticazione robusta e meccanismi di verifica dell'integrità dei dati. Inoltre, è essenziale utilizzare protocolli di comunicazione sicuri che proteggano i dati in transito da intercettazioni e manomissioni. La segmentazione delle reti è un altro elemento chiave nella progettazione di un'architettura sicura. Questo principio prevede la suddivisione della rete in segmenti più piccoli e isolati, limitando così il movimento laterale di un attaccante in caso di compromissione di una parte del sistema. La segmentazione può essere attuata attraverso l'uso di VLAN, firewall interni e altre tecniche di isolamento delle reti. Questo approccio non solo riduce la superficie d'attacco, ma migliora anche la gestione e il monitoraggio del traffico di rete, facilitando l'identificazione di attività sospette.
   L'implementazione di misure di crittografia è fondamentale per proteggere la riservatezza e l'integrità dei dati sia a riposo che in transito. La crittografia assicura che i dati non possano essere letti o alterati da soggetti non autorizzati. Nella progettazione di un'architettura sicura, è essenziale utilizzare algoritmi di crittografia robusti e aggiornati, e gestire le chiavi crittografiche in modo sicuro. La crittografia deve essere applicata non solo ai dati sensibili memorizzati nei database, ma anche alle comunicazioni tra utenti e server, tra server e applicazioni, e tra dispositivi all'interno della rete. Oltre a questi elementi, un'architettura sicura deve prevedere l'implementazione di controlli di accesso granulari. Questo significa definire chiaramente i permessi per utenti e applicazioni, assicurando che ogni entità abbia accesso solo alle risorse necessarie per le sue funzioni. I controlli di accesso possono includere l'uso di autenticazione multifattore (MFA), politiche di accesso basate sui ruoli (RBAC) e monitoraggio continuo delle attività di accesso per rilevare e rispondere a comportamenti anomali.
5. il *testing* e la verifica: esecuzione di test di sicurezza, come il *penetration testing* e il *vulnerability assessment*, per identificare e correggere eventuali vulnerabilità nel sistema. Questa fase è essenziale per garantire che le misure di sicurezza implementate siano efficaci e funzionino come previsto;
6. la manutenzione e l'aggiornamento ovvero il monitoraggio continuo del sistema e l'aggiornamento delle misure di sicurezza per affrontare minacce e vulnerabilità emergenti. La sicurezza deve essere considerata un processo continuo e adattativo e non un obiettivo statico.

4. *SECURITY TESTING*

Il *Security Testing* è una componente cruciale del *Security by Design*, finalizzata a identificare e correggere le vulnerabilità e le minacce potenziali nei sistemi informatici e nelle applicazioni software. Questa attività è fondamentale per garantire che le misure di sicurezza implementate siano efficaci e che il sistema sia protetto contro una vasta gamma di minacce. Il *Security Testing*, in particolare, è un processo continuo e iterativo che non si limita a un'unica fase del ciclo di vita del sistema, ma che deve essere integrato in tutte le fasi, dalla progettazione iniziale alla manutenzione operativa. Solo attraverso un approccio sistematico e comprensivo al *Security Testing* è possibile garantire che un sistema sia veramente sicuro e in grado di resistere alle minacce in continua evoluzione del panorama digitale moderno.

Una delle tecniche principali utilizzate nel *Security Testing* è il *Penetration Testing*. Questo metodo simula attacchi reali per valutare la resistenza del sistema alle intrusioni esterne. Attraverso il *Penetration Testing*, gli esperti di sicurezza cercano di identificare le vulnerabilità che potrebbero essere sfruttate da attaccanti malintezionati. Durante questi test, vengono utilizzati vari strumenti e tecniche per tentare di compromettere il sistema, simulando le strategie che un vero hacker potrebbe adottare. Questo tipo di test non solo aiuta a identificare le debolezze del sistema, ma fornisce anche una valutazione del potenziale impatto che un attacco riuscito potrebbe avere sull'organizzazione. I risultati del *Penetration Testing* permettono di sviluppare strategie di mitigazione efficaci e di rafforzare le difese del sistema. Il *Vulnerability Assessment* è un altro strumento fondamentale nel *Security Testing*. Questo processo prevede l'identificazione e la valutazione delle vulnerabilità all'interno di un sistema o di un'applicazione attraverso un'analisi dettagliata del codice, delle configurazioni e delle architetture. A differenza del *Penetration Testing*, che si focalizza sull'imitazione degli attacchi, il *Vulnerability Assessment* è più orientato alla scoperta di potenziali debolezze che potrebbero essere sfruttate in futuro. Gli strumenti di *vulnerability* scanning esaminano automaticamente il sistema per individuare configurazioni errate, *patch* mancanti e altre vulnerabilità note. Questo processo aiuta a determinare le aree che necessitano di miglioramenti di sicurezza, consentendo ai team IT di prendere provvedimenti correttivi prima che le vulnerabilità possano essere sfruttate da attaccanti. Il Se*curity Auditing* rappresenta un ulteriore aspetto critico del *Security Testing*. Questo processo implica un esame approfondito della conformità del sistema o dell'applicazione con le policy di sicurezza, gli standard e le *best practice*. Gli audit di sicurezza sono essenziali per garantire che tutte le misure di protezione siano implementate correttamente e siano efficaci. Durante un audit di sicurezza, vengono valutati vari aspetti del sistema, tra cui l'accesso degli utenti, la gestione delle password, la configurazione del firewall, e la protezione dei dati sensibili. Gli audit possono essere interni, condotti da personale dell'azienda, o esterni, realizzati da enti terzi indipendenti per garantire un'analisi obiettiva. I risultati dell'audit offrono una panoramica delle aree di conformità e delle potenziali lacune, fornendo raccomandazioni dettagliate per migliorare la postura di sicurezza del sistema.

5. ESEMPIO DI IMPLEMENTAZIONE: IL CASO DEL MODULO PACO-SMART-CONTRACT

Durante il progetto ACROSS, sviluppato dalla Italpaghe srl, è stato previsto lo sviluppo di un modulo per la gestione degli smart contract denominato "PACO-Smart-Contract". Lo sviluppo di tale modulo rappresenta un esempio concreto di applicazione del paradigma del *Security by Design*. Questo modulo è stato progettato per facilitare la contrattualizzazione e il pagamento dei *freelance* tramite l'uso di *smart contract* basati su *blockchain*. Gli *smart contract* sono protocolli informatici che verificano e applicano la negoziazione di un contratto in modo automatico e sicuro. Essi consentono di gestire gli accordi tra acquirenti e venditori, riducendo la necessità di intermediari e migliorando la fiducia tra le parti coinvolte.

Il principale obiettivo del modulo PACO-Smart-Contract è creare una piattaforma più trasparente ed efficiente per la gestione dei contratti e dei pagamenti nel mercato dei consulenti aziendali. Questo sistema mira a risolvere i problemi comuni associati alle piattaforme centralizzate, come le elevate commissioni di transazione, i ritardi nei pagamenti e la mancanza di trasparenza. Gli *smart contract* sono programmi che si eseguono automaticamente quando vengono soddisfatte determinate condizioni predefinite. Nel contesto dei mercati dei consulenti aziendali, gli *smart contract* possono essere utilizzati per gestire in modo sicuro e automatico gli accordi tra datori di lavoro e consulenti. I vantaggi degli *smart contract* includono l'automazione dei processi di pagamento, la riduzione del rischio di mancato pagamento e la garanzia della correttezza delle transazioni. L'implementazione del modulo PACO-Smart-Contract ha seguito un approccio sistematico che ha integrato i principi del *Security by Design* in ogni fase del processo. Di seguito una panoramica delle principali attività svolte durante la progettazione e lo sviluppo del modulo:

1. la prima fase ha coinvolto l'identificazione delle specifiche esigenze di sicurezza degli utenti finali e la definizione delle specifiche dell'applicazione. Questo passaggio è cruciale per garantire che le misure di sicurezza siano allineate con le necessità operative e i rischi specifici del sistema;
2. sono stati studiati i principali servizi per l'utilizzo della *blockchain*, valutando la fattibilità per la creazione di un servizio di *blockchain* ad hoc per l'applicativo. Questo ha permesso di determinare le soluzioni tecniche più adatte per integrare gli *smart contract*;
3. la metodologia di creazione e gestione degli *smart contract* è stata progettata per garantire la protezione

dei dati e la correttezza delle transazioni. Gli *smart contract* sono stati scritti in un linguaggio di programmazione specifico per la *blockchain* e implementati utilizzando strumenti come *Ganache* per il *testing* locale;

4. sono state identificate le potenziali vulnerabilità e modellate le minacce applicabili agli oggetti coinvolti nel sistema. Questa fase ha incluso la conduzione di valutazioni di rischio per determinare le contromisure appropriate da adottare;
5. sono stati eseguiti test di sicurezza sia in modalità *black box* che *white box* per garantire che il sistema fosse robusto e resistente agli attacchi.

L'adozione del paradigma del *Security by Design* è stata integrata in ogni fase della progettazione e sviluppo del modulo PACO-Smart-Contract. Ogni componente del sistema è stato progettato tenendo conto delle potenziali vulnerabilità e minacce, garantendo che le misure di sicurezza fossero implementate fin dalle prime fasi. Questo approccio ha permesso di creare un ambiente digitale sicuro e resiliente, capace di proteggere efficacemente i dati sensibili e di garantire la fiducia tra datori di lavoro e *freelance*.

6. CONCLUSIONI

L'adozione del paradigma del *Security by Design* offre numerosi vantaggi, rendendo questo approccio essenziale per affrontare le sfide della sicurezza informatica nel mondo moderno. Integrando la sicurezza fin dalle prime fasi di progettazione, si garantisce una protezione più efficace dei dati sensibili e delle informazioni personali, riducendo significativamente il rischio di violazioni. Questo approccio non solo migliora la protezione dei dati, ma è anche economicamente vantaggioso. Implementare misure di sicurezza durante la fase di progettazione è generalmente meno costoso rispetto all'adozione di soluzioni correttive postume, riducendo i costi di sicurezza complessivi per l'organizzazione. Adottare il *Security by Design* aiuta inoltre a soddisfare i requisiti normativi e a mantenere la conformità con le leggi sulla protezione dei dati, come il GDPR e la Direttiva NIS. La conformità normativa non solo evita potenziali sanzioni, ma contribuisce anche a costruire e mantenere la fiducia degli utenti e dei clienti. Un sistema progettato con principi di sicurezza integrati è più robusto e affidabile, riducendo il rischio di interruzioni operative e violazioni della sicurezza. Questa maggiore affidabilità del sistema si traduce in una riduzione dei tempi di inattività e delle perdite associate, migliorando l'efficienza operativa complessiva. Il *Security by Design* non è solo una pratica tecnica, ma un approccio strategico che richiede una collaborazione tra diversi settori dell'organizzazione. La progettazione di un'architettura sicura deve incorporare i principi di sicurezza in ogni fase del ciclo di vita del sistema, dalle prime fasi di analisi e definizione dei requisiti, passando per la progettazione e lo sviluppo, fino al testing e alla manutenzione continua. Questo include la definizione di intefacce sicure, la segmentazione delle reti, l'implementazione di misure di crittografia e l'adozione di controlli di accesso granulari. La progettazione di un'architettura sicura rappresenta uno degli aspetti fondamentali del *Security by Design*. Creare un sistema che integri i principi di sicurezza fin dalle prime fasi di progettazione garantisce che ogni componente del sistema sia progettato tenendo conto delle potenziali vulnerabilità e minacce. La definizione di interfacce sicure assicura che i punti di contatto tra diverse componenti del sistema o tra il sistema e l'esterno siano protetti da controlli di accesso rigorosi, autenticazione robusta e meccanismi di verifica dell'integrità dei dati. La segmentazione delle reti riduce la superficie d'attacco e migliora la gestione e il monitoraggio del traffico di rete, limitando il movimento laterale di un attaccante in caso di compromissione di una parte del sistema. L'implementazione di misure di crittografia protegge la riservatezza e l'integrità dei dati sia a riposo che in transito, utilizzando algoritmi robusti e aggiornati. Inoltre, i controlli di accesso granulari definiscono chiaramente i permessi per utenti e applicazioni, assicurando che ogni entità abbia accesso solo alle risorse necessarie per le sue funzioni.

BIBLIOGRAFIA

[1] Z. Xu and S. S. Chopra, "Interconnectedness enhances network resilience of multimodal public transportation systems for Safe-to-Fail urban mobility," Nat. Commun., vol. 14, no. 1, p. 4291, Jul. 2023.

[2] A. Almalawi, A. I. Khan, F. Alsolami, Y. B. Abushark, and A. S. Alfakeeh, "Managing Security of Healthcare Data for a Modern Healthcare System," Sensors, vol. 23, no. 7, p. 3612, Mar. 2023.

[3] A. Bahmanyar et al., "Emerging smart meters in electrical distribution systems: Opportunities and challenges," in 2016 24th Iranian Conference on Electrical Engineering (ICEE), Shiraz, 2016, pp. 1082–1087.

[4] J. Ding, A. Qammar, Z. Zhang, A. Karim, and H. Ning, "Cyber Threats to Smart Grids: Review, Taxonomy, Potential Solutions, and Future Directions," Energies, vol. 15, no. 18, p. 6799, Sep. 2022.

[5] R. Ramadoss, "Blockchain technology: An overview," IEEE Potentials, vol. 41, no. 6, pp. 6–12, Nov. 2022.

[6] H. Muhsen, A. Allahham, A. Al-Halhouli, M. Al-Mahmodi, A. Alkhraibat, and M. Hamdan, "Business Model of Peer-to-Peer Energy Trading: A Review of Literature," Sustainability, vol. 14, no. 3, p. 1616, Jan. 2022.

[7] G. D. P. R. GDPR, "General data protection regulation," URL Httpsgdpr-Infoeu, 2018.

[8] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, vol. 194. 2016.