Position Paper SBA Italia

Cybersecurity, digital risk management e data privacy

Summit For Territories

Roma – 11.09.2024

Ing. Luca Girodo

1. Scopo

Il nostro obiettivo è fornire una panoramica completa delle sfide e delle opportunità legate alla cybersecurity degli edifici, offrendo linee guida pratiche per la protezione delle infrastrutture moderne per così garantire la sicurezza informatica degli edifici, preservando la sicurezza, la privacy e la resilienza delle nostre comunità.
Il progetto verte sulla realizzazione e progettazione di una infrastruttura di comunicazione sicura tra appartamenti ed edifici, utilizzando un Edge Computer - cioè una centralina elettronica programmata come un computer ma con comandi molto più semplici - per raccogliere i dati di un appartamento e poi convogliarli in un Edge Computer di edificio che si interfaccia con l'esterno.

Questa centralina serve a far girare più applicazioni diverse, incrementando l'interoperabilità, la sicurezza e diminuendo di costi.

2. Contesto

L'integrazione delle tecnologie informatiche negli edifici ha trasformato radicalmente il concetto stesso di infrastruttura. Gli edifici moderni - residenziali, commerciali o industriali - sono per la maggior parte dotati di sistemi avanzati di automazione e controllo che ne ottimizzano l'efficienza energetica, ne migliorano la sicurezza fisica e ne aumentano il comfort per gli occupanti.
Attualmente gli edifici intelligenti, o smart buildings, si basano su una vasta rete di dispositivi interconnessi, dai sensori IoT (Internet of Things come ad esempio i comandi di domotica per le tapparelle elettriche, la programmazione dei climatizzatori degli appartamenti) ai sistemi di gestione centralizzati, che monitorano e controllano vari aspetti operativi, come l'illuminazione, la climatizzazione, la videosorveglianza e l'accesso fisico,
Per aumentare la sicurezza verso le cyber minacce è opportuno creare dei singoli punti di raccolta dei dati – gli Edge Computer - con lo scopo di renderli più facilmente difendibili e aggiornabili.

3. Posizione

Tutte le connessioni, da e verso gli edifici, devono essere progettate con standard di sicurezza elevati e criptazione dei dati.
All'interno dell'edificio è necessario utilizzare l'impianto multiservizi – già obbligatorio per legge nelle nuove costruzioni dal 2015 - per sfruttare le qualità di sicurezza e le performance della fibra ottica (vedi Gpon). Tutti i fornitori potranno raggiungere l'interfaccia Edge Computer per installare l'App ed erogare i servizi, così da creare uno standard di prodotto.

L’aumento dei servizi erogabili attraverso questa modalità non comporterebbe modifiche all’infrastruttura che invece risulterebbe adeguata e adeguabile facilmente e per diverso tempo.

Le connettività tra le centraline, o Edge Computer, all’interno di un edificio saranno sviluppate con la medesima tecnologia in modo di poter garantire un facile interscambio di dati tra l’appartamento e l’edificio.
Le connessioni devono essere sempre protette al fine di garantire sia la sicurezza dei dati che la privacy dei dati degli appartamenti e degli edifici.

La creazione di una simile infrastruttura che condividerà protocolli trasmissivi, regole di Cybersecurity e di crypting e di anonimizzazione del dato, porterà alla creazione di uno standard certificato, grazie al quale sarà possibile creare un MarketPlace - con regole certe e sicure - dove i fornitori potranno sviluppare delle App per l’offerta dei propri servizi a livello di edificio/appartamento.
L’offerta diventerà così facilmente modulabile in base alle necessità dell’utilizzatore. I servizi verranno venduti come App che si installeranno sull’Edge Computer. I dati generati dalle singole App resteranno di proprietà del singolo cittadino, mentre altri dati una volta anonimizzati e criptati potranno essere resi disponibili alle reti collettive per gli usi necessari (come statistiche di vendita, forecasting, etc).

Il dato diventerà il “materiale economico” dell’infrastruttura essendo anonimizzato, criptato e certificato dalla catena blockchain

4. Proposte e soluzioni

La certificazione dei dati attraverso la blockchain rappresenta un metodo sicuro per garantire l'integrità e l'autenticità delle informazioni. La blockchain è una tecnologia di “registro distribuito“ che consente di registrare i movimenti dei dati in modo sicuro, trasparente e immutabile.

Il processo inizia con la creazione del dato che si desidera certificare. Questo dato può essere qualsiasi tipo di informazione, come documenti o dati di sensori IoT.
Una funzione criptografica viene applicata al dato originale per generare un'impronta digitale unica chiamata hash. Questa funzione produce un valore univoco di lunghezza fissa, indipendentemente dalla dimensione del dato originale. Anche una minima modifica nel dato originale produrrà un hash completamente diverso, il che rende l'hash stesso un indicatore affidabile dell'integrità del dato.

L'hash così generato, viene registrato su una blockchain. Questo comporta l'inclusione dell'hash in un blocco della blockchain. Ogni blocco contiene un insieme di dati e un riferimento crittografico al blocco precedente, formando una catena di blocchi.

Una volta che un blocco viene aggiunto alla blockchain e confermato dai nodi della rete stessa, diventa praticamente immutabile. Questo significa che l'hash del dato certificato è ora permanentemente registrato sulla blockchain e non può essere alterato senza modificare tutti i blocchi successivi.

Per verificare l'integrità del dato certificato, si può semplicemente ricalcolare l'hash del dato attuale e confrontarlo con l'hash registrato sulla blockchain. Se gli hash coincidono, si può essere certi che il dato non è stato alterato. Se gli hash non coincidono, significa che il dato è stato modificato.

I vantaggi della certificazione del dato blockchain sono:

1. **Immutabilità** → una volta registrato, l'hash del dato non può essere modificato, garantendo l'integrità del dato certificato
2. **Trasparenza** → la blockchain è pubblica e trasparente, permettendo a chiunque di verificare la certificazione dei dati in qualsiasi momento
3. **Decentralizzazione** → non esiste un punto centrale di controllo, riducendo il rischio di manipolazione da parte di attori malintenzionati
4. **Sicurezza** → l'uso di tecniche crittografiche avanzate rende estremamente difficile la falsificazione dei dati

La blockchain offre un metodo robusto per la certificazione dei dati, assicurando che le informazioni rimangano autentiche e non alterate, fornendo così una base solida per la fiducia digitale.

5. Conclusioni

La realizzazione di una infrastruttura tramite gli Edge Computer, che raccolgono i dati i e li certificano tramite la blockchain, ci consente di realizzare una piattaforma aperta a tutti dove erogare i servizi del futuro.

Facilità d'uso, di installazione, di manutenzione e di aggiornamento rendono e renderanno la piattaforma un luogo dove erogare servizi sempre più "ad personam".

Il rinnovo tecnologico continuo sarà l'opportunità per migliorare quanto già realizzato.

Il dato diventerà quindi il "materiale economico" dell'infrastruttura essendo anonimizzato, criptato e certificato dalla catena blockchain.

Garantiremo così la privacy dell'individuo, la sicurezza dei dati e la capacità di interscambio tra individuo, condomino e rete.