filodiritto
APPROFONDISCI SEMPRE
Tribunale Bologna 24.07.2007, n.7770 - ISSN 2239-7752
Direttore responsabile: Antonio Zama

Sicurezza IOT

07 Luglio 2020
Gabriele Amato, Beatrice Amato, Mauro D'Ercole

Indice:

1. Introduzione

Semplicità d'uso, basso costo di acquisto e grande disponibilità di dati sono gli aspetti qualificanti della proposta IOT, l'aspetto della sicurezza è però da non sottovalutare nell'implementazione IOT. Proveremo ad esplorare rischi e possibili soluzioni connessi appunto alla sicurezza.

2. Criticità relative alla sicurezza in ambito IOT

La sicurezza dei dispositivi IOT e dei nostri dati da essi gestiti e postati in rete è un aspetto centrale e delicato sia per le aziende produttrici che per i consumatori siano essi privati cittadini, enti pubblici o aziende. È oggetto di dibattito ormai quotidiano su quale sia la migliore soluzione per stabilire standard di sicurezza e rispetto della privacy, soprattutto in vista dell'implementazione del sistema 5G. Negli USA entrerà in vigore nel corso di quest'anno una legge federale che prevederà l'adozione di standard minimi per tutti gli apparecchi utilizzati nell'ambito degli uffici pubblici. In Europa è già stato deliberato il GDPR che prevede al suo interno due concetti chiave: **LA "SECURITY BY DISIGN" E L'APPROCCIO "RISK BASED"**.

Il Gdpr, sigla di ***General data protection regulation***, è il regolamento europeo su privacy e dati che è operativo dal 25 maggio 2018. Ciò nonostante diversi utenti (e aziende produttrici)?sono in ritardo sulle proprie azioni di adeguamento. È probabile che il Garante per la privacy, l'autorità che vigila sul trattamento dei dati in Italia, conceda un ulteriore periodo di tolleranza, comportandosi in maniera più elastica sui casi di infrazione. Ma in cosa consiste, davvero, la Gdpr?

In estrema sintesi col **GDPR**:

- Si introduce il concetto di responsabilizzazione o accountability del titolare;
- Si introducono importi più elevati per le sanzioni amministrative pecuniarie che variano nel massimo a seconda delle disposizioni violate;
- Si introducono concetti di "privacy by design", nonché di approccio basato sul rischio e adeguatezza delle misure di sicurezza, di valutazione d'impatto e data breach;

- Regole più rigorose per la selezione e la nomina di un responsabile del trattamento e di eventuali sub-responsabili;
- Si introduce la previsione in alcuni casi tassativi di nomina obbligatoria di un Responsabile della protezione dei dati;
- Si introducono regole più chiare su informativa e consenso;
- Viene ampliata la categoria dei diritti che spettano all'interessato;
- Stabiliti criteri rigorosi per il trasferimento degli stessi al di fuori dell'Ue

In realtà, almeno in Italia, si stima che oltre la metà delle aziende ma anche tante Pubbliche Amministrazioni non sono ancora pronte ad allinearsi ai provvedimenti Ue in materia di data protection nonostante le severe sanzioni previste. Un aiuto in tal senso potrebbe venire dall'attuazione del Piano Industria 4.0 che permetterebbe alcune agevolazioni nell'investimento per avviare l'adeguamento al GDPR.

3. Gli aspetti da affrontare

Gli aspetti da affrontare sono di varia natura, prima di tutto la connettività ed il sistema di trasporto dei dati.
Con l'aumento dei dispositivi connessi aumenterà anche il numero dei punti di attacco da parte degli hacker e i dispositivi router e access point sono i primi punti deboli della catena della sicurezza, così come il trasporto dei dati dai dispositivi che avviene generalmente in modo wireless espone gli utenti a vulnerabilità.
Per la protezione degli standard di trasmissione prevede l'adozione di soluzioni di crittografia, più difficile da risolvere è il problema connesso all'hardware utilizzato nella trasmissione dati.
Le aziende produttrici non prevedono di default l'utilizzo di criteri di protezione adeguati e gli utenti, spesso, non hanno la sensibilità o le capacità per comprendere i rischi che si corrono nell'implementare un'infrastruttura debole. Il discorso è valido sia per le aziende che per l'utenza retail. In effetti pensiamo all'azienda che investe in macchinari che possono essere collegati alla rete ad esempio per la teleassistenza e diagnosi da remoto e all'utente retail che implementa un sistema di videosorveglianza per la propria abitazione. In generale l'azienda potrebbe rivolgersi ad uno dei tanti fornitori che vendono apparecchiature e soluzioni per la sicurezza (firewall, software specifici, servizi di configurazione e monitoraggio della rete IT), man mano che si "scende" verso l'artigiano o l'utente privato tale sensibilità non è riscontrabile, a volte addirittura la configurazione della sicurezza è ritenuta un optional. Sarebbe interessante conoscere quante persone che hanno installato un impianto di videosorveglianza della propria abitazione, magari ricorrendo ad ambienti in cloud per la memorizzazione delle registrazioni si sono avvalse di un esperto per configurare firewall, crittografia di trasmissione e così via.

4. I sistemi di home automation e la privacy

Il problema non è solo la sicurezza ma anche la privacy. L'implementazione di sistemi di home automation in grado di regolare le luci, climatizzare gli ambienti o videosorveglianza e l'introduzione dei cosiddetti assistenti vocali (ad esempio Apple/Siri o Google/Home o Amazon/Alexa) focalizza l'attenzione sul fatto che la mancanza di adeguate procedure di tutela non faccia altro che avvantaggiare le case produttrici in grado di profilare ogni minimo dettaglio delle nostre più intime abitudini. Gli **assistenti vocali** sono dispositivi "intelligenti" in grado di riconoscere il linguaggio naturale e sfruttano i principi di " **machine learning**" per perfezionare il loro **apprendimento** migliorando la conoscenza delle nostre abitudini con la capacità di ascolto. Le interazioni fra noi e questi dispositivi vengono registrate e riutilizzate per perfezionare i sistemi di apprendimento, un'indagine pubblicata da Bloomberg ha evidenziato che centinaia di dipendenti di un noto fornitore di queste apparecchiature avesse lo specifico compito di ascoltare i campioni di registrazione audio per migliorare le competenze del dispositivo offerto e quindi migliorare l'efficacia del prodotto. Questo ha suscitato una prevedibile polemica sul rispetto della privacy e sull'etica professionale.

5. Dispositivi smart home, applicazioni pubbliche ed industriali

Tutte queste considerazioni assumono un'importanza di grado diverso in funzione dell'applicazione e della tipologia di utente, ad esempio quando dai dispositivi smart home ci spostiamo ai sistemi di gestione del traffico, all'ambiente sanitario, alle applicazioni industriali.

In Italia circa un terzo dei veicoli circolanti è equipaggiato con "APP" che ne permettono la connessione ad Internet; recentemente un test effettuato dal CNR di Pisa ha dimostrato quanto sia semplice assumere il controllo remoto di un'automobile sfruttando una vulnerabilità nel sistema operativo Android Auto. Così come è stato dimostrato che sfruttando alcune vulnerabilità nel sistema operativo che gestisce la regolazione dei semafori è possibile modificare il traffico fino al congestionamento in alcune aree cittadine rispetto ad altre. Ancora più delicato è il settore sanitario con la crescente diffusione della telemedicina.

> **La tecnologia IoT a supporto degli ospedali sta cercando di migliorare la ricerca medica ed in molti casi abbattere i costi di gestione, è il caso dei dispositivi indossabili in grado di monitorare e trasmettere dati sulle pulsazioni cardiache o dei cerotti smart per pazienti diabetici che controllano il livello di glicemia nel sangue, cosa succederebbe se questi dispositivi potessero essere leggibili a distanza? In ambito industriale la crescente automazione con macchinari dotati di plc connessi alla rete espone l'azienda alla vulnerabilità dei propri processi di produzione e alla esposizione dei dati sensibili relativi al software di funzionamento delle macchine stesse.**

6. Standard per garantire sicurezza e privacy

La soluzione non è quella di limitare l'uso della tecnologia in ambito IOT, è necessario individuare un protocollo che possa contenere i rischi di intrusione aumentando la consapevolezza e l'attenzione a progettare sistemi di sicurezza e di rispetto della privacy. Tale atteggiamento dovrebbe costituire il primo passo nell'implementazione di sistemi IOT.

Un primo passo dovrebbe essere l'adozione di un protocollo in grado di definire le caratteristiche minime di sicurezza dei vari dispositivi e la modalità di trasmissione delle informazioni raccolte. Si tratta di integrare tecnologie indipendenti fra loro individuando i punti di possibile vulnerabilità. È una condizione preliminare all'adozione di qualsiasi soluzione e che renderebbe efficace l'uso dell'Internet of Things. Non trascuriamo il fatto che la prossima implementazione di sistemi di trasmissione molto più performanti (5G) da un lato rappresenterebbe un'ulteriore spinta alla diffusione dei sistemi connessi e dall'altro, senza adeguate protezioni, potrebbe significare l'esasperazione di scenari critici.

Un valido aiuto potrebbe venire dall'adozione delle norme sul **Cybersecurity Improvement Act** emanato di recente negli USA e che entrerà in vigore nel corso del 2020.

> **La norma prevede di definire standard minimi di sicurezza per tutti gli apparati presenti negli uffici pubblici, standard che devono garantire semplicità di aggiornamento e devono sfruttare protocolli comuni per la gestione della sicurezza delle informazioni. A questi si aggiungono le caratteristiche minime delle credenziali di primo accesso configurate di default sui sistemi.**

Resta un ultimo elemento da considerare, forse il più importante, sulla protezione dei dati personali. Non a caso il **GDPR** parla esplicitamente di "**security by design**" introducendo il concetto dell'approccio **"risk based"**, sarebbe sufficiente adottare nella pratica questi due concetti per ridurre ulteriormente i rischi connessi alla operatività dei sistemi di IoT.

TAG: *privacy, Sicurezza, GDPR*
