RISORSE DI SICUREZZA PER L'UTILIZZO DEGLI SMART CONTRACT NELL'IOT

LA SICUREZZA DEI NUOVI MODELLI DI BUSINESS IoT-ORIENTED

18 LUGLIO 2017 – UNIVERSITA' DELLA CALABRIA

LA SICUREZZA DEI NUOVI MODELLI DI BUSINESS IoT-ORIENTED

LE TECNOLOGIE EMERGENTI

DODICI TECNOLOGIE CHE CAMBIERANNO LA VITA, GLI AFFARI E L'ECONOMIA GLOBALE

SICUREZZA E PRIVACY

NUOVI MODELLI DI BUSINESS

GRANDI OPPORTUNITA' MA ANCHE GRANDI RISCHI

Fonte: McKinsey Global Institute, Disruptive technologies: Advances that will transform life, business, and the global economy, May 2013

LA SICUREZZA DEI NUOVI MODELLI DI BUSINESS IoT-ORIENTED

CONVERGENZA TRA MONDO VIRTUALE E MONDO FISICO

L'INTERNET OF THINGHS E' UN FENOMENO DI CONVERGENZA DEL MONDO VIRTUALE INTERNET E QUELLO REALE DI OGGETTI FISICI INTELLIGENTI, LA CUI AFFERMAZIONE STA TRASFORMANDO IL MODELLO DI COMUNICAZIONE GLOBALE INIZIALMENTE PENSATO PER GLI UOMINI CON L'INCLUSIONE DELLE MACCHINE

TECNOLOGIE, STANDARD E PROTOCOLLI CHE CONSENTONO A OGGETTI FISICI INTELLIGENTI DI INTERAGIRE CON LA RETE

L'INTERAZIONE CON LA RETE INTERNET CONSENTE DI SCAMBIARE GRANDE QUANTITA' DI DATI

GLI OGGETTI AVRANNO L'INTELLIGENZA PER SVOLGERE COMPITI SEMPRE PIU' COMPLESSI

DA UN MODELLO DI CONNETTIVITA' PER TUTTI AD UN MODELLO DI CONNETTIVITA' PER OGNI COSA

Fonte: Osservatorio Internet of Things Politecnico di Milano

LA SICUREZZA DEI NUOVI MODELLI DI BUSINESS IoT-ORIENTED

NUOVI MODELLI DI BUISNESS IOT-ORIENTED

AMBITI APPLICATIVI

Smart City & Smart Environment
Monitoraggio e gestione degli elementi di una città (es. mezzi per il trasporto pubblico, lampioni) e dell'ambiente circostante per migliorarne la vivibilità, sostenibilità e competitività

Smart Home
Gestione automatica di impianti e sistemi (es. illuminazione, climatizzazione). I dispositivi (es. elettrodomestici) «parlano» tra loro e agiscono autonomamente in un'ottica di risparmio energetico

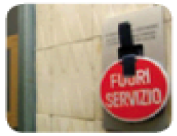
Smart Metering & Smart Grid
Reti elettriche e contatori intelligenti per il livellamento del carico della rete, la gestione della produzione distribuita e della mobilità elettrica nonché la corretta fatturazione dei consumi

Smart Building
Gestione automatica di impianti e sistemi (es. illuminazione, climatizzazione). Monitoraggio degli ambienti interni in un'ottica di risparmio energetico, comfort e sicurezza delle persone (ad esempio, in impianti industriali)

eHealth
Monitoraggio real time di parametri vitali da remoto riducendo il ricorso all'ospedalizzazione, a fini diagnostici e di cura. Localizzazione pazienti (es. malati di Alzheimer)

Smart Logistics
Soluzioni per la tracciabilità di filiera, la protezione del brand e il monitoraggio della catena del freddo, per la sicurezza in poli logistici complessi e per la gestione delle flotte (tracciabilità del mezzo e delle sue condizioni)

Smart Factory
Implementazione di nuove logiche di gestione della produzione grazie all'uso di macchine sensibili al contesto in cui operano, in grado di rilevare informazioni in tempo reale, comunicare tra loro e prendere decisioni



Smart Asset Management
Gestione in remoto di asset di valore (es. dispositivi elettrobiomedicali, vending machine) ai fini di rilevazione guasti e manomissioni, localizzazione, tracciabilità e gestione inventariale

Smart Agricolture
Monitoraggio parametri ambientali a supporto dell'agricoltura per migliorare la qualità dei prodotti, ridurre le risorse utilizzate e l'impatto ambientale

Smart Car
Connessione tra veicoli o tra questo e l'infrastruttura circostante (es. guardrail) per la prevenzione e rilevazione di incidenti. Offerta di nuovi modelli assicurativi e/o di informazioni geo-referenziate su viabilità e situazione del traffico

FATTORI ABILITANTI

PROTOCOLLI DI COMUNICAZIONE

DIVERSI PROTOCOLLI DI COMUNICAZIONE - TRA WI-FI, 3G, LTE, RFID, NFC, E BLUETOOTH I DISPOSITIVI RISCHIANO DI NON RIUSCIRE PIÙ A COMUNICARE TRA DI LORO PERCHÈ PARLANO LINGUE TROPPO DIVERSE.

ALFABETIZZAZIONE INFORMATICA

PER L'INTERNET OF THINGS È NECESSARIA UNA DOVUTA ALFABETIZZAZIONE INFORMATICA DELL'UTENTE. LE NUOVE APPLICAZIONI SVILUPPATE SONO SEMPRE PIÙ USER FRIENDLY.

BANDA TRASMISSIVA

E' NECESSARIO DISPORRE DI BANDA ADEGUATA PER ABILITARE L'INTERNET DELLE COSE – ANCHE ATTRAVERSO UN ADEGUAMENTO DELLA CAPACITà INFRASTRUTTURALE.

SICUREZZA

LA SICUREZZA È INVECE UNA CONSEGUENZA DEL CONTROLLO: SE QUALUNQUE OGGETTO PUÒ ESSERE COMANDATO A DISTANZA, POTREBBE ANCHE ESSERE ATTACCATO DA CRIMINALI INFORMATICI.

PRIVACY

LA PRIVACY È UNA CONSEGUENZA DEL MONITORAGGIO. SE UN OGGETTO IoT PRODUCE DATI, QUESTI POTREBBERO ESSERE RELATIVI A PERSONE E AL LORO UTILIZZO. LA MANIPOLAZIONE DI QUESTE INFORMAZIONI RICADREBBE NEL DISCUSSO CAMPO DELLA TRASPARENZA E TRATTAMENTO DEI DATI PERSONALI.

LA SICUREZZA DEI NUOVI MODELLI DI BUSINESS IoT-ORIENTED

SICUREZZA E PRIVACY

SICUREZZA E PRIVACY

DEVICE MANUFACTURE

- PRODUTTORI DI DISPOSTIVI IOT, CHE SI PREOCCUPANO DI REALIZZARE DISPOSITIVI A BASSO COSTO E NUOVE FUNZIONALITA' NON CONSIDERANDO IN MANIERA DEGUATA GLI ASPETTI DI SICUREZZA E PRIVACY.
- DISPOSITIVI HEADLESS CON CAPACITA' COMPUTAZIONALE LIMITATA E SISTEMI OPERATIVI EMBEDDED, PER CUI NON E' POSSIBILE DOTARLI DI CLIENT DI SICUREZZA E SPESSO NON POSSONO ESSERE AGGORNATI O DOTATI DI PATCH
- PROTOCOLLI INSUFFICIENTI DI AUTENTICAZIONE E AUTORIZZAZIONE
- FIRMWARE DOTATI DI BACKDOOR CODIFICATE PER INTERAGIRE DA REMOTO
- POSSIBILITA' LIMITATE DI CONFIGURAZIONE DEL DISPOSITIVO

SERVICE PROVIDER

- POLITICHE PER LO SVILUPPO SICURO DEI SISTEMI DI BACK-END E DELLE APPLICAZIONI MOBILI
- ANALISI DEL RISCHIO (NON SOLO PER GLI ASPETTI DI SICUREZZA MA ANCHE PER LA POSSIBILITÀ CHE I DISPOSITIVI INTERCONNESSI POSSANO RACCOGLIERE, IN MANIERA NON DEL TUTTO TRASPARENTE PER L'UTENTE, INFORMAZIONI DA CONDIVIDIRE CON ALTRI SOGGETTI - ES. VENDOR DI PRODOTTI, SOCIETÀ DI MARKETING, ETC.
- VULENRABILITY ASSESSMENT E PENETRATION TEST SUI DISPOSITIVI IOT, L'INFRASTRUTTURA DI BACK-END E L'END DEVICE
- ICT GOVERNANCE – ADEGUAMENTO DELL'INFRASTRUTTURA ICT: STORAGE, GESTIONE BIG DATA E DI ANALAISI DEI DATI, CAPACITA' DELLA RETE, DISPONIBILITA' DEL SERVIZIO, SCALABILITA', ETC.

END DEVICE & CONSUMER

- SPESSO NON EFFETTUA LE CONFIGURAZIONI MINIMALI PER L'USO CORRETTO DEI DISPOSITIVI IoT (ES. PERCHE' NON E' POSSIBILE CAMBIARE LE PASSWORD DI DEFAULT, OPPPURE E' POSSIBILE CAMBIARLA MA NON IMPOSTANDOLA CON CARATTERISTICHE DI ROBUSTEZZA, ETC.)
- SCARSA CONSAPEVOLEZZA DEGLI ASPETTI DI SICUREZZA NELL'UTILIZZARE I DISPOSITIVI – ES. USO DI DISPOSTIVI MOBILI COMPROMESSI (ROOTING, JAILBREAKING) PER L'INTERAZIONE CON I DISPOSITIVI IoT O CON LIVELLI DI SICUREZZA INADEGUATI (ASSENZA DI AV\FW)

I GRANDI "PLAYER" DEL MERCATO DOVRANNO CREARE QUELLA SANA E GIUSTA PRESSIONE NEI CONFRONTI DEI PRODUTTORI PERCHE' DEFINISCANO STANDARD SICURI PER LA REALIZZAZIONE DI DISPOSITIVI IOT, UTILIZZANDO IL CONCETTO DI SICUREZZA E PRIVACY BY DESIGN GIA' NELLA FASE DI PROGETTAZIONE; ANALOGAMENTE DOVRANNO CREARE LE CONDIZIONI PER RENDERE SEMPRE PIU' CONSAPEVOLI GLI UTILIZZATORI FINALI SULLE MODALITA' DA ADOTTARE PER UN USO SICURO DEI PROPRI DISPOSITIVI UTILIZZATI.

LA SICUREZZA DEI NUOVI MODELLI DI BUSINESS IoT-ORIENTED
CONCLUSIONI

PER UN SANO E CONCRETO SVILUPPO DEL PARADIGMA DELL'INTERNET OF THINGS E' NECESSARIO:

- "SECURITY BY DESIGN" NEGLI SMART OBEJECT
- SVILUPPO E CONSOLIDAMENTO DEGLI STANDARD DI SICUREZZA PER L'INTERNET OF THINGS
- "PRIVACY BY DESIGN" E "PRIVACY BY DEFAULT" NEGLI SMART OBEJECT
- NORMATIVA PER LA PROTEZIONE DEI DATI (ARMONIZZAZIONE E MIGLIORAMENTO DELLE REGOLE DI PROTEZIONE DEI DATI TRATTAI NELL'INTERNET OF THINGS)
- COSTRUIRE UNA RELAZIONE DI FIDUCIA TRA LE DIVERSE ENTITA' CHE REALIZZANO L'INTERNET OF THINGS PER GARANTIRE LA TUTELA DEL CONSUMATORE E LO SVILUPPO DEL BUSINESS