LA GUIDA "SECURITY GUIDANCE FOR EARLY ADOPTERS ON THE INTERNET OF THINGS (IOT)" APRILE 2015

A cura del gruppo di Lavoro Mobile Working Group di CSA Cloud Security Alliance

Enzo M. Tieghi,
Coordinatore Area di Ricerca Internet of Things di CSA Italy

Il documento "Security Guidance for Early Adopters on the Internet of Things (IoT)" è il prodotto del gruppo di lavoro CSA Mobile - IoT Initiative (del quale fa parte anche Alberto Manfredi, Presidente di CSA Italy Chapter), pubblicato ad Aprile 2015: il documento è stato creato utilizzando input di un gruppo di esperti di sicurezza e di mobilità provenienti da diversi settori industriali.
Sono inseriti nella Guida riferimenti e informazioni provenienti da linee guida già esistenti, al fine di evitare duplicazioni e favorire l'allineamento con il lavoro di altri organismi del settore. Inoltre questo documento è stato realizzato in modo tale da consentire utilizzo cross-industry: questo è stato ottenuto esaminando architetture utilizzati in molteplici settori e la selezione di controlli di sicurezza che possano essere espressione in ogni settore.

L'IMPORTANZA DI TERMINOLOGIA E DEFINIZIONI

All'inizio, questo documento riporta terminologia e definizioni necessarie in una guida per lo sviluppo sicuro di sistemi basati su Internet of Things (IoT).
Si prende in prestito la terminologia dallo report ITU-T Y.2060 per definire i vari aspetti della IoT. In particolare ITU-T Y.2060 da una definizione di IoT: "infrastruttura globale per la società dell'informazione, che permette servizi avanzati tramite l'interconnessione di cose (fisiche e virtuali) basandosi su tecnologie dell'informazione e della comunicazione (ICT) interoperabili esistenti ed in evoluzione. "
Inoltre ITU-T Y.2060 fornisce anche le seguenti definizioni:

- **Device**/ dispositivo: ... "una apparecchiatura con le funzionalità obbligatorie di comunicazione e le funzionalità opzionali di rilevamento, attuazione, acquisizione, archiviazione e elaborazione di dati."
- **Thing**/Cosa: ... "un oggetto del mondo fisico (cose fisiche) o il mondo informazioni (cose virtuali), che può essere identificato e integrato in reti di comunicazione."

LE SFIDE E MERCATI DELL'IOT

Innanzitutto questa guida è un documento per aiutare gli sviluppatori nell'arduo compito di mettere in piedi ed utilizzare al meglio l'IoT in modo sicuro, in quanto le soluzioni di sicurezza enterprise tradizionali non rispondono sufficientemente alle esigenze di sicurezza IoT.
L'IoT presenta nuove sfide, tra le quali:

- Aumento di preoccupazioni sulla privacy, un tema che spesso rimane poco chiaro
- Sicurezza limitata da vincoli della piattaforma stessa, che rende una sfida i controlli di sicurezza di base
- La mobilità estesa, che rende complessi il monitoraggio e la gestione degli asset
- Volumi, che fanno delle operazioni di aggiornamento e manutenzione di routine una sfida
- Operazioni basate su Cloud che rendono il perimetro di sicurezza meno efficace.

SCOPI DIFFERENTI PER IOT DIFFERENTI

L'IoT è già una realtà nel mondo "consumer" con l'adozione da parte dei consumatori di molti prodotti/servizi già diffusi: oggetti IoT indossabili, elettrodomestici "Smart", abitazioni "smart", negozi "smart", musei, pubblicità, entertainment, ecc.
Ma IoT è anche nel mondo B2B, Industria e nel settore Infrastrutture pubbliche: energia, trasporti, produzione industriale, grande distribuzione, banche, assicurazioni, pagamenti, salute, difesa, ecc.
Nella figura 2 vediamo alcuni tipici esempi di IoT già disponibili oggi.

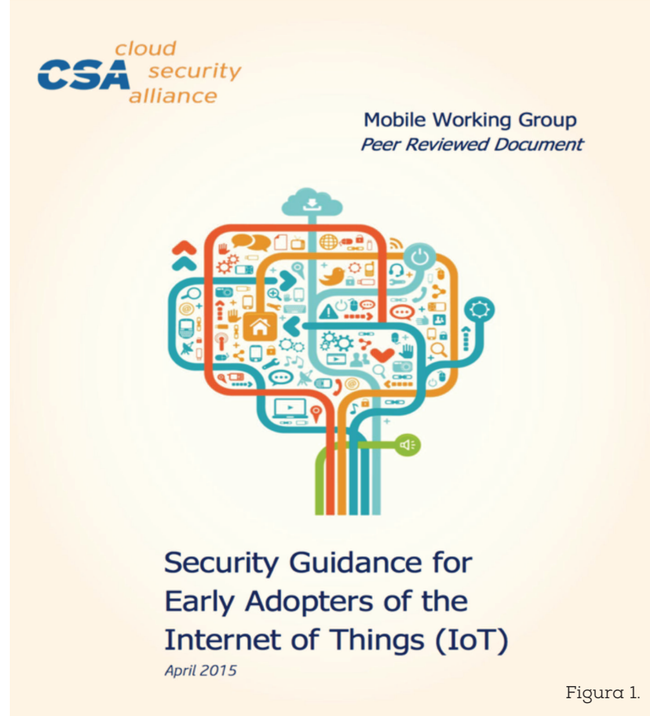


Figura 1.

SVILUPPARE SISTEMI IOT "SICURI"

In questa guida della Cloud Security Alliance (CSA) vengono descritte alcune sfide connesse con l'adozione della IoT e si illustra una serie di raccomandazioni che possono essere seguiti da utenti-

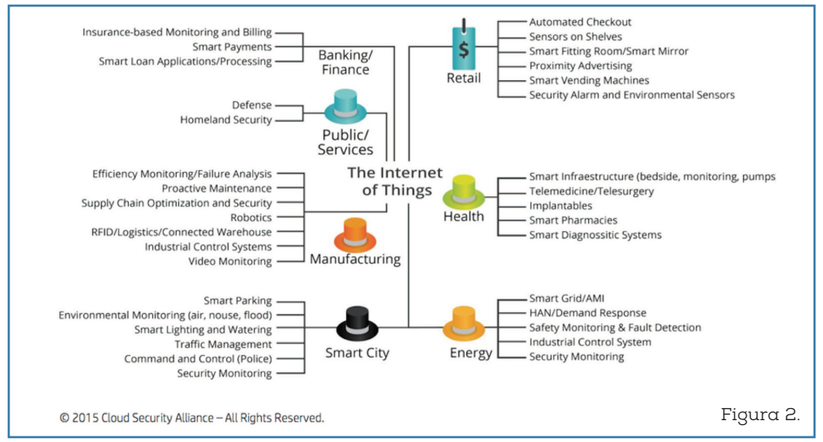


Figura 2.

Enzo Maria Tieghi, imprenditore, informatico, milanese, da oltre 30 anni si occupa di software per automazione e controllo di impianti, di security e compliance a standard e normative dei diversi settori industriali, utility e delle infrastrutture in cui opera. Tieghi è A.D. di ServiTecno (Milano), che dal 1985 distribuisce e supporta software di GE Digital per sistemi ICT industriale, SCADA, Industrial Internet, IIoT, Plant Intelligence e tool per protezione di reti e sistemi nell'industria ed utility. Socio in CSA Italy, ove coordina l' Area di Ricerca Internet of Things, tiene lezioni e partecipa come speaker ad eventi specialistici sia in Italia che all'estero, oltre a contribuire con articoli e memorie a riviste specializzate e conferenze internazionali.

pionieri dell'IoT per soddisfare i seguenti obiettivi:

- mantenere riservatezza e integrità di dati personali e di business raccolti all'interno dell'IoT attraverso l'utilizzo di crittografia, autenticazione e protezione dell'integrità dell'infrastruttura IoT
- Comprendere ed affrontare i temi della privacy dei soggetti interessati prima della implementazione dell'IoT effettuando una valutazione globale dell'impatto sulla privacy
- Salvaguardare l'infrastruttura dagli attacchi che colpiscono la IoT come vettore con destinazione gli asset di un'organizzazione, attraverso l'uso di controlli del ciclo di vita del dispositivo IoT e un approccio di security a strati (layered security)
- Avviare un approccio globale per la lotta contro le minacce alla sicurezza attraverso la condivisione di informazioni all'interno della community con fornitori di security, colleghi del settore industriale e la Cloud Security Alliance.

Ecco quindi cosa valutare per rendere uno "sviluppo IoT sicuro":

- Molti sistemi dell'IoT sono mal progettati e implementati perché usano protocolli e tecnologie diversi che portano a configurazioni complesse
- La mancanza nell'IoT di tecnologie mature e di processi di business consolidati
- Scarse linee guida per la manutenzione del ciclo di vita e la gestione dei dispositivi IoT
- La IoT introduce problemi di sicurezza fisica ancora da valutare
- Preoccupazioni sulla privacy IoT sono complesse e non sempre immediatamente evidenti
- Scarsità di Best Practice disponibili per gli sviluppatori IoT
- Mancanza di Standard per l'autenticazione e l'autorizzazione di dispositivi IoT.
- Mancanza di Best Practice per Incident Management e Response nell'IoT
- Standard di Audit e di Logging non definiti per i componenti dell'IoT
- Disponibilità limitata di interfacce tra dispositivi IoT, SIEM, IAM e applicazioni di Security. Ancora non sono pronti metodi di identificazione e di situational awareness per la postura di security riguardo agli asset IoT
- Norme di security per le configurazioni per piattaforme virtualizzate IoT e multi-tenancy non ancora mature.

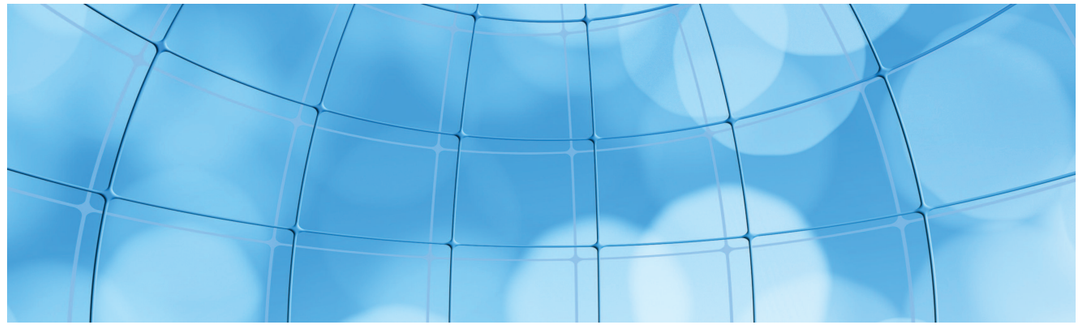
CONTROLLI DI SECURITY DA TENERE PRESENTI NELL'IOT

I seguenti controlli di sicurezza sono raccomandati per le organizzazioni che intendono dotarsi o utilizzare l'IoT: sono stati adattati alle specifiche caratteristiche dell'IoT, per consentire ai primi che adottano la IoT di mitigare alcuni dei rischi più evidenti associati a questa nuova tecnologia.

1. Analizzare l'impatto sulla privacy per i soggetti interessati e adottare un approccio "Privacy-by-Design" nello sviluppo e deployment dell'IoT.
2. Applicare un approccio "Secure Systems Engineering" in fase di disegno e sviluppo dell'IoT.
3. Adottare protezioni e security a più livelli per difendere beni IoT.
4. Implementare Best-Practice per la protezione dei dati e delle informazioni sensibili.
5. Definire i controlli per tutto il ciclo di vita dei dispositivi IoT.
6. Definire e sviluppare un framework di autenticazioni/autorizzazioni per l'ecosistema IoT.
7. Definire e attuare un quadro di Audit/Logging per l'ecosistema IoT.

ALCUNE CONSIDERAZIONI ED AREE DA GUARDARE CON ATTENZIONE PER LA SICUREZZA IOT

- Al momento c'è ancora un po' di confusione sia su ruolo dell'IoT che su modelli di business ed architetture: ad esempio c'è chi parla di IoT "personali/consumer" e chi di "Industrial IoT". Proviamo a pensare alle differenze tra "Smart Home" e "Smart City", tra Health Care, Utility, Manufacturing, trasporti, veicoli connessi, droni, veicoli a guida assistita, dispositivi indossabili, gaming e vending machines, POS, ecc.
- Differenze insite in sistemi semplici e complessi allo stesso tempo, senza



Standard condivisi all'interno dello stesso ecosistema IoT: protocolli, sistemi operativi, tipologia di dati e messaggi, piattaforme, organizzazione e modelli di business.

- Pensiamo a differenti "cicli di vita" per diverse applicazioni e target di mercato: ad esempio un prodotto consumer è destinato ad essere attivo ed utilizzato anche solo per alcune settimane/mesi (a volte quanto dura il dispositivo stesso, e non per questo meno "importante" a livello di privacy e di PII, Personally Indentifiable Information). Un device per l'industria o utility ha un ciclo di vita di anni/lustri: proviamo a pensare ai lampioni di un centro abitato o stazioni di pompaggio di un acquedotto. Come metteremo mano agli aggiornamenti di firmware/software o gestiremo le configurazioni? Come "spegneremo" dispositivi obsoleti, "dimenticati" ed abbandonati che potranno rappresentare future backdoor per accesso alle reti di domani?
- Che protezione "fisica" possiamo ipotizzare per dispositivi sul territorio che potrebbero rappresentare porte di ingresso alla rete?
- Qual è la linea di demarcazione tra la rete dell'IoT e la rete dell'organizzazione che la gestisce? Dove finiscono i sistemi I.T. dell'azienda e dove inizia la IoT che utilizza e/o fa confluire dati ai quei sistemi I.T.? Proviamo a pensare all'impatto che ha già oggi la "BYOD".
- Valutiamo la Privacy by Design, in quanto applicazioni IoT che non hanno impatti sulla privacy, messe insieme, potrebbero avere grossi impatti sulla privacy: anche utilizzando crittografia ed altri controlli una qualsiasi traccia potrebbe far risalire una specifica transazione ad una specifica persona.
- Sappiamo che alcuni protocolli e dispositivi IoT oggi disponibili non sono stati pensati fin dall'inizio per essere sicuri, e a volte vincoli di capacità di elaborazione e di banda non permettono l'implementazione di tecniche di autenticazione e crittografia evoluti e necessari agli scopi della Security
- Oggi ci sono poche esperienze, poche persone formate e poche best practice sul tema IoT Security e sugli impatti che possano esserci nello sviluppare applicazioni "non sicure". E questo è vero anche per la gestione di eventuali incidenti dovuti ai problemi di security su reti IoT.

In conclusione, questa guida fornisce alcuni buoni input per fare in modo di avere dei livelli di sviluppo e gestione accettabili già oggi per mettere in piedi IoT più sicure. ■

BIBLIO E RIFERIMENTI

https://cloudsecurityalliance.org/media/news/csa-launches-new-security-guidance-for-early-adopters-of-the-iot

https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf

http://www.itu.int/itu-t/recommendations/rec.aspx?rec=Y.2060

http://www.iiconsortium.org/wc-security.htm