PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 26 - numero 5637 di Lunedì 10 giugno 2024

Due importanti iniziative per la protezione degli apparati IoT

Gli apparati IoT offrono soddisfacenti garanzie di protezione da possibili attacchi di malviventi informatici? Ecco due importanti iniziative, che mostrano come gli esperti di sicurezza sappiano reagire a certe categorie di rischi informatici.

Gli apparati IoT hanno raggiunto ormai un livello di diffusione estremamente elevato e, di conseguenza, sono cresciute le preoccupazioni dei responsabili della sicurezza informatica, circa il fatto che possano offrire soddisfacenti garanzie di protezione da possibili attacchi di malviventi informatici.

Il Regno Unito è il primo paese al mondo che ha ufficialmente proibito l'introduzione di parole chiave di default su apparati IoT.

La legge del 2022 sulla sicurezza dei prodotti e delle infrastrutture di telecomunicazione introduce dei nuovi livelli minimi di sicurezza, da parte dei fabbricanti, introducendo inoltre delle indicazioni sulla durata minima della garanzia di ricevere aggiornamenti informatici sugli apparati IoT.

Poiché anche negli Stati Uniti, in particolare in California, era stata attivata un'iniziativa similare, oggi molti fabbricanti di apparati IoT devono costruire apparati che possono essere venduti in California e nel Regno Unito, ed apparati che possono essere venduti nel resto d'Europa e del mondo. Se i fabbricanti rimuovono le parole chiave di default, gli apparati possono essere venduti in tutto il mondo.

In particolare, il dispositivo legislativo britannico afferma che le parole chiave devono essere scelte dall'utente, oppure devono essere uniche per lo specifico apparato. Inoltre, queste parole chiave non possono essere prodotte con degli algoritmi, che possano facilitare al malvivente la individuazione della parola chiave.

In parallelo, un'altra interessante iniziativa è stata portata a termine dal prestigioso istituto ETSI European Telecommunication Standard istitute, con sede ad Antibes, in Francia. Questo ente ha pubblicato la norma EN 303645, dal titolo: sicurezza informatica per apparati IoT, destinati agli utenti.

La norma stabilisce tutt'una serie di misure di sicurezza e protezione dei dati per tutti gli apparati che sono connessi ad infrastrutture di rete, sia a livello Internet, sia a livello di rete domestica.

In particolare, questa norma si applica a:

- giocattoli per i bambini,
- rivelatori di fumo, serrature elettroniche e sensori alle finestre,
- telecamere intelligenti,
- dispositivi sanitari indossabili,
- sistemi di automazione d'allarme per uso domestico,
- elettrodomestici collegati in rete, come ad esempio frigoriferi e lavatrici, ed infine
- gli assistenti per la smart home.

Come i lettori possono ben capire, si tratta di un elenco non limitativo, che include, in pratica, tutti gli apparati domestici, che potrebbero esser attaccati da criminali informatici, creando significativi problemi agli utenti e proprietari di questi apparati.

La norma in particolare proibisce l'uso di parole chiave di default, impone la adozione di sistemi di individuazione di possibili anomalie e metodologie di aggiornamento del software.

Il fabbricante deve garantire che i dati personali eventualmente presenti sul dispositivo siano protetti in modo adeguato e che eventuali cadute di rete non portino ad un abbassamento del livello delle misure di sicurezza.

Ci auguriamo che i produttori di apparati IoT prendano buona nota di questa norma e comincino al più presto a rispettare le preziose indicazioni della norma stessa. Nel frattempo, è bene che gli acquirenti di questi dispositivi comincino a verificare, in fase di acquisto, il livello di sicurezza di questi dispositivi e, in particolare, il rispetto di specifiche norme di sicurezza, a tutela dei dati e degli utenti.

ETSI EN 303 645 V2.1.1 - Cyber Security for Consumer Internet of Things: Baseline Requirements (pdf)

Adalberto Biasiotti