Adesione Geovision TAICS

L'organizzazione per gli standard europei rilascia lo standard di sicurezza informatica IoT

Geovision,
GVision Italia
13/02/21

Via Prealpi 13
20833 Giussano MB
Italy

www.gvision.it
info@gvision.it

L'European Telecommunications Standards Institute (ETSI) unitamente al consorzio **TAICS**, ha rilasciato ETSI TS 103 645, uno standard per la sicurezza informatica “Internet of Things” , per stabilire una base di sicurezza per i prodotti di consumo connessi a Internet e fornire una base per i futuri schemi di certificazione IoT.

Man mano che più dispositivi domestici si connettono a Internet, la sicurezza informatica dell'Internet of Things (IoT) sta diventando una preoccupazione crescente. Le persone affidano i propri dati personali a un numero crescente di dispositivi e servizi online.
Inoltre, i prodotti e gli apparecchi tradizionalmente offline sono ora connessi e devono essere progettati per resistere alle minacce informatiche. Prodotti scarsamente protetti minacciano la privacy del consumatore e alcuni dispositivi vengono sfruttati per lanciare attacchi informatici su larga scala DDoS (Distributed Denial of Service).

La norma TAICS e TS 103 645

La nuova specifica ETSI, TS 103 645 , affronta questo problema e specifica disposizioni di alto livello per la sicurezza dei dispositivi di consumo connessi a Internet e dei loro servizi associati.
I prodotti IoT includono: Telecamere di sicurezza intelligenti, giocattoli per bambini e baby monitor collegati in rete, prodotti rilevanti per la sicurezza come rilevatori di fumo e serrature delle porte, telecamere intelligenti, TV e altoparlanti, rilevatori di salute indossabili, sistemi di automazione e allarme domestici, elettrodomestici collegati in rete (ad es. Lavatrici , frigoriferi) o assistenti domestici intelligenti.
TS 103 645 richiede agli implementatori di rinunciare all'uso di password predefinite universali, che sono state la fonte di numerosi problemi di sicurezza.
Richiede inoltre l'implementazione di una politica di divulgazione delle vulnerabilità per consentire ai ricercatori della sicurezza e ad altri di segnalare problemi di sicurezza.
Richiede che tutte le credenziali e i dati sensibili alla sicurezza siano archiviati in modo sicuro all'interno dei servizi e sui dispositivi e che non vengano utilizzate credenziali codificate nel software del dispositivo.

I produttori di dispositivi e i fornitori di servizi devono fornire ai consumatori informazioni chiare e trasparenti su come i loro dati personali vengono utilizzati, da chi e per quali scopi, per ciascun dispositivo e servizio. Ciò vale anche per le terze parti che possono essere coinvolte, compresi gli inserzionisti ", le note sulle specifiche.
Il consenso del consumatore deve essere ottenuto in modo "Chiaro" e può essere revocato in qualsiasi momento.
Lo standard include molte altre disposizioni, alcune delle quali sono requisiti obbligatori e altre semplici raccomandazioni.

Tra questi ultimi ci sono:
Comunicazioni protette (crittografia, chiavi gestite in modo sicuro)
Minimizzare l'esposizione agli attacchi (porte chiuse non utilizzate, software in esecuzione con il privilegi non necessari, ecc.)
Integrità del software garantita (avvio sicuro, rilevamento modifiche non autorizzato).

Poiché molti dispositivi e servizi IoT elaborano e archiviano dati personali, questa specifica può contribuire a garantire che siano conformi al Regolamento generale sulla protezione dei dati (GDPR).

Le parti interessate a tutti i livelli hanno lavorato insieme per assicurarsi che le specifiche fossero incentrate sui risultati, piuttosto che prescrizioni, offrendo alle organizzazioni la flessibilità necessaria per innovare e implementare soluzioni di sicurezza adeguate ai loro prodotti

Questa garanzia è necessaria dato che da tempo riteniamo che alcuni fallimenti del mercato (come le backdoor sui prodotti di videosorveglianza) possano essere affrontati solo attraverso i giusti quadri normativi e incentivi.

A seguito dell'imminente introduzione della tecnologie 5G l'adesione agli standard di sicurezza TAICS diventa prioritaria. Oltre 90 membri aziendali hanno aderito a TAICS come : Geovision, Vodafone, Telecom Italia, AT&T, China Mobile, Chunghwa Telecom, Korea Telecom, NTT DOCOMO, Orange, Singtel, SK Telecom, T-Mobile,, Verizon e Vodafone ecc. dalla sua istituzione nel luglio 2015 con l'obiettivo di integrare gli standard tecnologici internazionali e promuovere la cooperazione.

Man mano che la standardizzazione globale avanza, i produttori di ogni paese devono adeguarsi e non trarre giustificazioni da una catena di approvvigionamento internazionale.