TELETASK

trendsetter in domotics

INTERNET VEILIGHEID

HOE VEILIG IS HET OM UW HUIS/GEBOUW VIA HET INTERNET TE BESTUREN?

Geen enkele softwarebeveiliging biedt 100% garantie. Toch zijn er enkele beveiligingsmaatregelen die u kan nemen om te vermijden dat uw data in de verkeerde handen valt. TELETASK gebruikt daarom altijd minstens een TLS-versleuteling (ingebakken in onze TT Cloud-connecties) om zo een zeer hoge mate van beveiliging te bieden.

TLS-VERSLEUTELING

Bij TELETASK bestaat de volledige beveiliging uit een combinatie van verschillende technieken. De basisbeveiliging met daarboven een TLS-beveiligde verbinding maakt het mogelijk om ongewenste bezoeken zo goed als volledig te vermijden.

Wat doet een versleutelde TLS-verbinding? TLS codeert niet alleen gegevens, maar verifieert daarnaast ook elke verbinding om een hoge beveiliging te garanderen.

TELETASK-systemen maken intern in de woning gebruik van een bedraad bus-netwerk. Een bedrade oplossing is vaak niet alleen degelijker maar ook gemakkelijker te beveiligen. Er is bovendien maar één softconnectie naar het internet, die altijd minstens versleuteld wordt met TLS. Daarin ligt ook het verschil met een IoT-netwerk, waarbij elke individuele sensor of actor individueel met de cloud verbonden is. Dat verhoogt het risico op ongewenste toegang enorm. Daarom pakt TELETASK het anders aan.

Uw TELETASK-verbinding loopt in de woning via een bekabelde bus en Ethernet bekabelingsnetwerk. Uw installateur kan u ook daardoor extra beveiliging waarborgen. Op elk moment, op elk niveau.

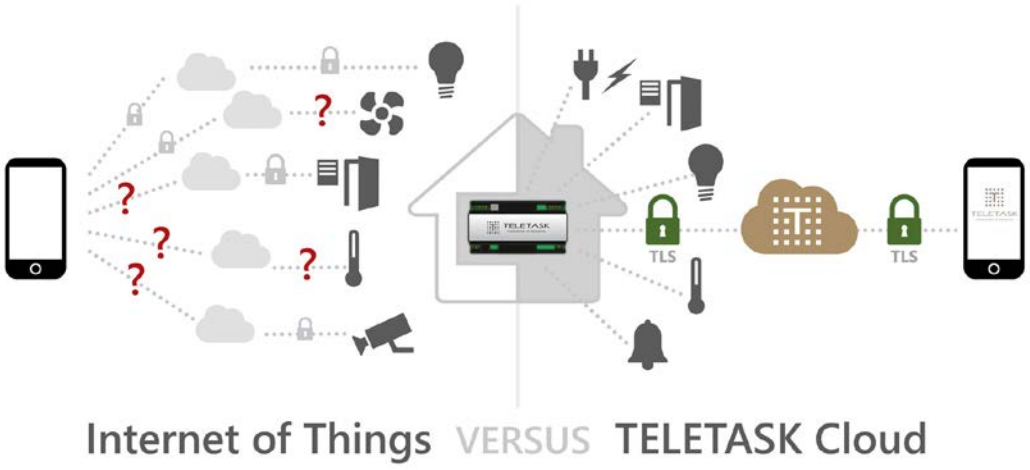
Vergeet trouwens ook niet dat men uw woning niet enkel via de elektronische weg, maar ook via de simpele mechanische weg kan betreden. Indien u zich wil beschermen tegen ongewenste toegang tot uw woning dient u ook te voorzien in kwalitatieve poorten, deuren, ramen, dak en dito glas- en sluitwerk. Een steen door een raam gooien is voor een inbreker namelijk veel makkelijker om toegang tot uw eigendom te krijgen dan een TLS-beveiligde verbinding hacken.

TTCLOUD-VERBINDINGEN

Ook de cloud-verbindingen (TTCloud) waarmee TELETASK smart homes en buildings op afstand aanstuurt, al dan niet via een applicatie op uw smartphone, desktop of tablet, zijn altijd minstens beveiligd met een TLS-encryptie. Zo bent u ook buiten

TELETASK

trendsetter in domotics



uw thuisnetwerk optimaal beschermd. Er is dan ook geen extra beveiliging nodig voor residentiële en professionele toepassingen.

De TTCloud laat gebruikers toe om zich overal ter wereld te verbinden met de TELETASK-app om hun domotica-toepassingen te controleren en te besturen. Daarnaast kan de systeemintegrator alle TELETASK-applicaties op afstand onderhouden en upgraden via de beveiligde "Remote Services".

LOKALE SETUP

U kan er bij TELETASK ook voor kiezen om enkel lokaal (in de woning/gebouw) te communiceren. Uw centrale is dan niet verbonden met de cloud en werkt dus enkel via uw lokaal netwerk. U behoudt zo 100% controle over de geïntegreerde toestellen en systemen zonder enige connectie met de buitenwereld.
Als u werkt met een lokale setup, dan kan u uw smart home-installatie niet vanop afstand besturen. Daarom gebruikt bijna elke klant de standaard volledig beveiligde smartphone app van TELETASK.

VPN EXTRA TIPS

Dankzij de TLS-versleuteling is het niet meer nodig om te werken met een VPN-verbinding. Als u toch een eigen cloudverbinding wil opzetten, dan kan u dit op twee manieren aanpakken:

1. U kunt uw router simpelweg configureren opdat hij zou werken met "port forwarding". Dit biedt echter GEEN BEVEILIGING! TELETASK keurt deze methode dan ook volledig af.

2. U kunt de router configureren opdat deze zou werken via een VPN-tunnel: hiermee kan ook, net zoals bij TTcloud van hierboven, een hoge veiligheidsgraad worden bereikt.

Als u dus toch graag met een VPN-verbinding werkt, dan raadt TELETASK u ten stelligste aan om te kiezen voor een beveiligde VPN en dus zeker geen "port forwarding" te gebruiken. De verantwoordelijkheid hiervoor ligt volledig bij de systeemintegrator die deze verbindingen opzet.

Wanneer u Wi-Fi gebruikt, gebruik hier dan minimaal de WEP bescherming. TELETASK adviseert anno 2016 het gebruik van WPA/PSK.

EXTRA TIPS

1. Zorg ervoor dat de TELETASK centrale eenheid en zijn LAN- toegang is geïnstalleerd in de beveiligde zone van uw project (security system protected area). De systeemintegrator dient ervoor te zorgen dat het niet mogelijk is om het beveiligingssysteem vanop afstand uit te schakelen.

2. De "remote management"-mogelijkheid van uw router (WAN-zijde) dient uitgeschakeld te worden (de meeste routers hebben dit standaard zo voorgeprogrammeerd).

3. Wanneer u Wi-Fi gebruikt, gebruik hier dan minimaal WPA/PSK of hoger.

4. Bij het verlaten van de woning of het gebouw, dienen alle Wi-Fi routers best automatisch uitgeschakeld te worden. Dit kan heel eenvoudig gebeuren via het TELETASK systeem. U kunt eveneens alle Wi-Fi routers automatisch afsluiten na een bepaald tijdstip of voor een bepaalde periode (nacht) door het stopcontact van de router uit te schakelen.

5. Voorzie geen publiek toegankelijke Ethernet contactdozen, verbonden met het beveiligde LAN, in publieke ruimtes.

6. Externe technische supportverleners mogen toegang hebben tot de beveiligde zones (bijvoorbeeld onderhoudspersoneel voor de lift...). Controleer deze echter zodat ze niet in uw beveiligde LAN binnentreden.

7. Gebruik altijd degelijke paswoorden (minimum 8 karakters lang, minimum 1 hoofdletter en 1 cijfer). Herhaal uw paswoorden niet en gebruik bij voorkeur software om paswoorden te beheren.

www.teletask.be