TELETASK

trendsetter in domotics

INTERNET VEILIGHEID

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

Er bestaat geen software beveiliging die 100% garantie biedt. Het niveau van beveiliging is eerder een kwestie van tijd dan van veilig/niet veilig. TELETASK heeft beslist een VPN en TLS (TT Cloud) beveiliging aan te raden omdat dit een hoge beveiliging garandeert. De volledige beveiliging bestaat uit een combinatie van verschillende technieken. De basisbeveiliging met daarboven een TLS beveiligde verbinding maakt het perfect mogelijk om ongewenste bezoeken te vermijden. Men kan ook perfect werken met VPN-verbinding, maar dit is dankzij TLS niet nodig.

Wanneer uw TELETASK verbinding loopt via een standaard Ethernet bekabelingsnetwerk, dan kan uw installateur u van extra beveiliging voorzien. Op elk moment, op elk niveau.

Vergeet niet dat men uw woning niet enkel via elektronische weg maar ook via de simpele mechanische weg kan betreden. Indien u zich wenst te beschermen tegen ongewenste toegang tot uw woning dient u ook te voorzien in kwalitatieve poorten, deuren, ramen, dak en glas. Het gooien van een steen door een raam is voor een inbreker vaak veel makkelijker om toegang tot de eigendom te verkrijgen dan via het hacken van een VPN of TLS beveiligde verbinding.

TTCloud verbindingen (bv. voor de iSGUI app) maken gebruik van TLS beveiliging. Er is geen extra beveiliging nodig voor residentiële toepassingen.

Indien u VPN gebruikt; De router tussen uw TELETASK systeem en de WAN (internet) is het belangrijkste onderdeel om u te beschermen tegen ongewenste toegang tot en controle over uw TELETASK domotica systeem. De manier waarop u deze router configureert en gebruikt, bepaalt het niveau van beveiliging.

1. U kunt uw router configureren opdat hij zou werken met “port forwarding”: GEEN BEVEILIGING!

2. U kunt de router configureren opdat deze zou werken via een VPN tunnel: hiermee kan een hoge veiligheidsgraad worden bereikt. TELETASK raadt ten stelligste aan om een beveiligde VPN te gebruiken en dus zeker geen “port forwarding”.

TELETASK

trendsetter in domotics

Zolang er gewerkt wordt in een privaat netwerk (LAN) is er geen veiligheidsprobleem indien uw netwerkkabels zich in de beveiligde zones bevinden. Vanaf het ogenblik dat u een verbinding maakt met het internet via uw router, bent u echter niet langer in een fysisch beveiligde zone. VPN creëert daarom een veilige tunnel vanaf uw toestel (PC op afstand) naar uw router (thuisinstallatie) alsof uw mobiel toestel lokaal verbonden is met uw LAN. In een VPN verbinding zijn er verschillende mogelijke tunnelprotocols die hiervoor gebruikt kunnen worden: IPSEC, PPTP en L2TP.

Bij gebruik van de IPSEC of L2TP dient u een software/driver aan te kopen bij uw router verdeler en is er een meer complexe configuratie nodig dan bij een PPTP. Wij bevelen de IPSEC en L2TP protocollen aan, maar deze zijn niet zo eenvoudig in installatie. Indien u een PPTP gebruikt, is er een klantenlicentie ingesloten voor alle mobiele toestellen en PC's. Hier dient u het welgekende MS CHAP authenticiteitsmechanisme V2 te gebruiken (gebruik NIET de MS CHAP V1 of PAP).

EXTRA VOORDELEN

Dankzij het gebruik via de VPN beveiliging, heeft het volledige LAN van de klant een beveiligde toegang. Dit houdt ook de camera's, de netwerk hard disks en alle andere Ethernet uitrustingen in. VPN is een prijsgunstige oplossing voor een hoge beveiligingsgraad. Vandaag zijn goede VPN routers beschikbaar aan een lage prijs, daarnaast heeft TELETASK een volledig beschreven case over hoe men een VPN verbinding dient op te zetten. Vraag hiernaar bij uw lokale TELETASK verdeler.

EXTRA ADVIES

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.

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

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

Bij het verlaten van de woning of het gebouw dienen alle Wi-Fi routers 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).

Voorzie geen voor iedereen toegankelijke Ethernet contactdozen, verbonden met het beveiligde LAN, in publieke ruimtes.

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.

Gebruik een up-to-date en goed geconfigureerde firewall.

De VPN configuratie en set-up is een job voor een professionele ICT specialist die ervaren is op het gebied van alle beveiligingsproblemen.

Gebruik degelijke paswoorden (minimum 8 karakters lang, minimum 1 hoofdletter en 1 cijfer).