TELETASK

trendsetter in domotics

INTERNET SAFETY

HOW SAFE IS IT TO CONTROL YOUR HOUSE/ BUILDING OVER THE INTERNET?

There is no such software protection as a 100% protection. The level of protection is more a question of time than of safe/not safe. TELETASK decided to recommend the use of VPN and TLS (TTCloud) protection because this is a proven state-of-the-art protection. The total protection is a combination of different techniques. The basic TELETASK protection with on top VPN tunnelling or a TLS protected connection makes it a perfect team to avoid unwanted entries.

As your TELETASK connection runs over worldwide standard Ethernet cabling, your system integrator can provide extra propriety security if you like. Any time, any level.

Don't forget that entering your house or building is not only possible via electronic way, but also by simple mechanical way. If you want to protect against unwanted access you should also use proper gates, doors, windows, roof, glass. Throwing a stone through a window may be much easier for a burglar than hacking a VPN or TLS protected connection.

TTCloud connections (f.i. for iSGUI control) use TLS security and don't need extra security actions for standard residential applications.

If you use VPN: The router between your TELETASK system and the WAN (internet) is the most important part in protecting you against unwanted access and control of your TELETASK Home Automation system. The way you configure and use this router is defining the security level.

1. You can configure your router to work with port forwarding: NO SECURITY !

2. You can configure to work with VPN tunnelling: high security level can be realized. TELETASK strongly recommends to use Secure VPN and not to use port forwarding.

As long as we are working in a private network (LAN) there is no security problem if your network cables are inside the secured zone. From the moment on that you connect through your router to the internet you are no longer inside a physically secure zone. VPN creates a secure tunnel from your remote device to your router, like your device is connected directly to your LAN

In VPN there are several possible tunnelling protocols which can be

TELETASK

trendsetter in domotics

used: IPSEC, PPTP and L2TP.

When using IPSEC or L2TP, you will need to purchase software/drivers from the router supplier and there is a more complex configuration needed then for PPTP. We do recommend IPSEC and L2TP protocols but they are not easy to handle.

If you use PPTP, the client license is included with all mobile devices and PC's. The well reputed MS CHAP authentication mechanisms V2 must be used (don't use MS CHAP V1 or PAP).

EXTRA ADVANTAGES

Due to the VPN protection approach, the whole LAN of the customer has secured access. This includes camera's, network hard disks and all other Ethernet equipment.

VPN is a price effective solution for a high level of protection. Good VPN routers today are available at low cost. TELETASK has full case document on how to setup a VPN connection. Ask for it at your local TELETASK distributor.

EXTRA ADVICE

Make sure that the TELETASK central unit and its LAN access is installed in the secure zone of you project (security system protected area).

The System Integrator should not make it possible to disarm the security system from remote site.

The 'remote management' feature of your router (WAN-side) should be disabled (most routers have this setting of by default).

If you use Wi-Fi, use at least WEP protection. TELETASK advises to use WPA/PSK.

When leaving the house or building, automatically switch off all Wi-Fi routers (can be done easily with your TELETASK system). You can also switch off the Wi-Fi routers automatically after a certain time of the day (night).

Do not provide Ethernet wall sockets, which are connected to the protected LAN, in public rooms.

External technical support persons may have access to the secured zones (for example maintenance people of the elevator company...). Keep track of them to avoid that they can access the secured LAN.

Use an up-to-date and well configured firewall.

VPN configuration and setup is a job for a professional ICT specialist who is aware of all security issues.

Use always a proper password (minimum 8 characters long, min. 1 capital and 1 digit).