TELETASK

trendsetter in domotics

INTERNET – SÉCURITÉ

EST-IL VRAIMENT FIABLE DE GÉRER VOTRE MAISON/PROJET VIA INTERNET?

Aucune sécurité pour software ne peut vous garantir une protection à 100%. Le niveau de protection est plutôt une question de temps que de sûre/pas sûre. TELETASK vous conseille une protection VPN ou TLS (TTCloud) qui vous garantit une haute sécurité. La protection complète consiste en une combinaison de différentes techniques. Avec la protection de base TELETASK avec surtout un tunnel VPN ou une connexion TLS protégée, il est parfaitement possible d'éviter des visiteurs indésirables.

Si votre connexion TELETASK s'effectue par un réseau de câbles standard Ethernet, votre installateur peut vous procurer une protection propriétaire supplémentaire. A chaque instant, à chaque niveau.

N'oubliez pas que l'on peut s'introduire dans votre maison par voie électronique mais aussi par simple voie mécanique. Si vous désirez à vous protéger contre des intrus, il est nécessaire d'équiper votre maison de portails, portes, fenêtres, toits et vitres de bonne qualité. Pour un voleur il est souvent plus facile de s'introduire dans une maison en brisant une vitre par une pierre que de pirater une connexion VPN ou TLS.

Les connexions TT Cloud (p. ex. pour le contrôle iSGUI) utilisent la protection TLS et n'ont pas besojn d'autres actions de sécurité quand il s'agit d'applications résidentielles standards.

Si vous utilisez VPN: Le routeur entre votre système TELETASK et le WAN (internet) est la section la plus importante à sécuriser contre l'accès indésiré et le contrôle de votre système domotique TELETASK. La façon par laquelle vous configurez et employez ce router détermine le niveau de protection.

1. Vous pouvez configurer votre router pour fonctionner avec "port forwarding": AUCUNE PROTECTION !

2. Vous pouvez aussi configurer votre router pour fonctionner par l'intermédiaire d'un tunnel VPN: de cette façon vous pouvez atteindre un degré élevé de protection. TELETASK vous conseille vivement d'employer une connexion VPN

TELETASK

trendsetter in domotics

et pas la fonction “port forwarding”.

Si vous travaillez dans un réseau privé (LAN) il n’y a aucun problème de sécurité si vos câbles de réseau se situent dans une zone protégée. Dès l’instant qu’un router opère sur internet il ne se trouve plus longtemps dans une zone de protection physique. C’est pourquoi VPN crée un tunnel sûr à partir de votre appareil (PC à distance) vers votre router (installation au domicile) comme si votre appareil était directement connecté avec votre LAN.

Avec une connexion VPN plusieurs protocoles tunnels sont possibles: IPSEC, PPTP et L2TP.

Pour employer IPSEC ou L2TP vous devrez vous procurer un software/driver chez votre distributeur de router, une configuration plus complexe que pour un PPTP, s’avère nécessaire. Nous vous conseillons les protocoles IPSEC et L2TP, cependant ils ne sont pas si faciles à l’usage.

Si vous employez un PPTP, une licence client y est inclue pour tous les appareils et PC mobiles. Ici il y a lieu d’employer le MS CHAP, mécanisme d’authenticité V2 (n’employez pas le MS CHAP V1 ou PAP).

AVANTAGES SUPPLÉMENTAIRES

Grâce à l’emploi d’une protection VPN, le LAN du client a un accès complètement sécurisé. Ceci implique aussi les caméras, les hard discs de réseau et tout autre équipement d’Ethernet. VPN est une solution peu coûteuse pour un degré de protection aussi élevé. Actuellement de bon routers VPN sont disponibles à un prix avantageux. TELETASK dispose en plus d’une description totale comment procéder pour installer une connexion VPN. Demandez plus d’informations à votre distributeur local TELETASK.

CONSEIL SUPPLÉMENTAIRE

Assurez-vous que l’unité centrale TELETASK et son accès LAN sont installés dans la zone sécurisée de votre projet (security system protected area).

L’intégrateur de système doit faire de sorte qu’il est impossible de déconnecter le système de protection à distance.

La possibilité “remote management” de votre router (côté WAN) doit être déconnectée (la plupart des routeurs l’ont d’avance préprogrammé automatiquement).

Lorsque vous employez Wi-Fi, employez au moins la protection WEP. TELETASK conseille l’emploi de WPA/PSK.

Lorsque vous quittez la maison ou le bâtiment tous les Wi-Fi routers doivent automatiquement être déconnectés (aisé moyennant le système TELETASK). Vous pouvez également clôturer tous les routers Wi-Fi après un temps bien déterminé du jour (nuit). Ne prévoyez pas de prises de contact Ethernet, raccordées au LAN sécurisé, dans des espaces publics.

Les assistants techniques peuvent avoir accès aux zones sécurisées (par exemple le personnel d’entretien de l’ascenseur...). Contrôlez–les afin d’éviter qu’ils pénètrent dans le LAN sécurisé.

Faites usage d’un bon firewall actualisé et bien configuré.

La configuration VPN et le setup est un travail de spécialiste ICT professionnel, ayant beaucoup d’expérience dans le domaine d’une pareille protection.

Employez toujours un mot de passe adéquat (8 caractères au minimum, une majuscule et un chiffre).

ISO 9001
BUREAU VERITAS
Certification
Nº BE008171-1