TELETASK

trendsetter in domotics

INTERNET – SÉCURITÉ

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

Aucune sécurité logicielle n'offre une garantie à 100 %. Cependant, vous pouvez prendre certaines mesures de sécurité pour éviter que vos données ne tombent entre de mauvaises mains. TELETASK utilise donc toujours au moins le cryptage TLS (intégré à nos connexions TT Cloud) afin d'offrir un très haut niveau de sécurité.

CRYPTAGE TLS

Chez TELETASK, la sécurité complète consiste en une combinaison de différentes techniques. La sécurité de base avec une connexion sécurisée par TLS en plus permet d'éviter presque complètement les visites indésirables.

À quoi sert une connexion TLS cryptée ? TLS crypte non seulement les données, mais vérifie également chaque connexion pour garantir une sécurité élevée.

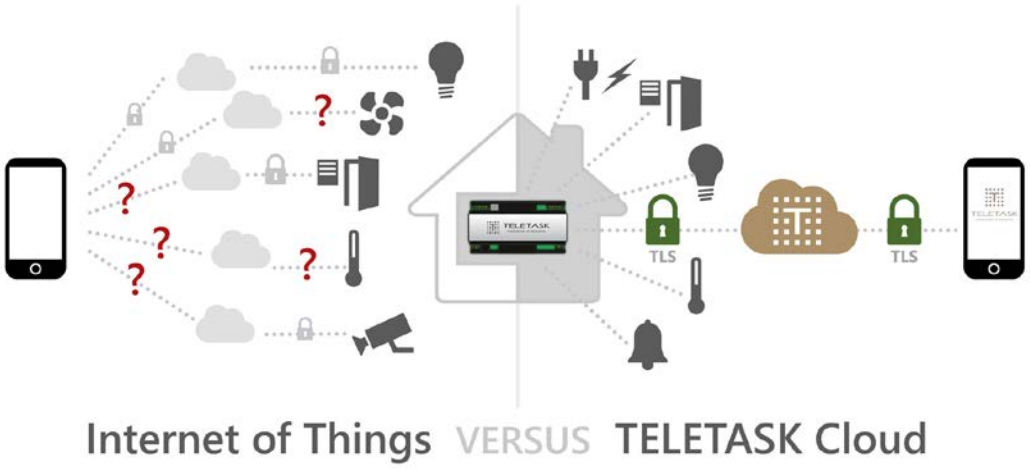
Les systèmes TELETASK utilisent un réseau de bus câblé en interne dans la maison. Une solution filaire est souvent non seulement plus robuste, mais aussi plus facile à sécuriser. De plus, il n'y a qu'une seule connexion logicielle à Internet, qui est toujours au moins cryptée avec TLS. C'est là que réside la différence avec un réseau IoT, où chaque capteur ou acteur individuel est connecté individuellement au cloud. Cela augmente considérablement le risque d'accès non désiré. C'est pourquoi TELETASK adopte une approche différente.

Votre connexion TELETASK fonctionne dans la maison via un bus filaire et un réseau de câblage Ethernet. Votre installateur peut également vous garantir une sécurité supplémentaire. A tout moment, à tout niveau.

En passant, n'oubliez pas que les gens peuvent entrer chez vous non seulement par voie électronique, mais aussi par la voie mécanique simple. Si vous souhaitez vous protéger contre les accès indésirables à votre habitation, vous devez également prévoir des portails, portes, fenêtres, toit et idem vitres et serrures de qualité. Jeter une pierre à travers une fenêtre est beaucoup plus facile pour un cambrioleur d'accéder à votre propriété que de pirater une connexion sécurisée par TLS.

TELETASK

trendsetter in domotics



CONNEXIONS TTCLOUD

Les connexions cloud (TTCloud) avec lesquelles TELETASK contrôle à distance les maisons et bâtiments intelligents, que ce soit ou non via une application sur votre smartphone, ordinateur de bureau ou tablette, sont toujours sécurisées avec au moins un cryptage TLS. De cette façon, vous êtes également protégé de manière optimale en dehors de votre réseau domestique. Par conséquent, aucune sécurité supplémentaire n'est requise pour les applications résidentielles et professionnelles.

Le TTCloud permet aux utilisateurs de se connecter à l'application TELETASK de n'importe où dans le monde pour surveiller et contrôler leurs applications domotiques. De plus, l'intégrateur système peut maintenir et mettre à jour toutes les applications TELETASK à distance via les « Services à distance » sécurisés.

CONFIGURATION LOCALE

Chez TELETASK, vous pouvez également choisir de ne communiquer que localement (dans la maison/le bâtiment). Votre échange n'est alors pas connecté au cloud et ne fonctionne donc que via votre réseau local. Vous gardez le contrôle à 100% sur les appareils et systèmes intégrés sans aucune connexion avec le monde extérieur.

Si vous travaillez avec une configuration locale, vous ne pouvez pas contrôler à distance votre installation de maison intelligente. C'est pourquoi presque tous les clients utilisent l'application smartphone standard entièrement sécurisée de TELETASK.

VPN

Grâce au cryptage TLS, il n'est plus nécessaire de travailler avec une connexion VPN. Si vous souhaitez toujours configurer votre propre connexion cloud, vous pouvez l'aborder de deux manières :

1. Vous pouvez simplement configurer votre routeur pour qu'il fonctionne avec la « redirection de port ». Cependant, cela ne fournit AUCUNE SÉCURITÉ ! TELETASK rejette donc complètement cette méthode.

2. Vous pouvez configurer le routeur pour qu'il fonctionne via un tunnel VPN : cela permet également un haut niveau de sécurité, tout comme avec TTcloud ci-dessus.

Donc si vous aimez toujours travailler avec une connexion VPN, TELETASK vous conseille vivement de choisir un VPN sécurisé et surtout de ne pas utiliser de «redirection de port». La responsabilité en incombe entièrement à l'intégrateur système qui établit ces connexions.

CONSEILS SUPPLÉMENTAIRES

1. Assurez-vous que l'unité centrale TELETASK et son accès LAN sont installés dans la zone protégée du système de sécurité de votre projet (security system protected area). L'intégrateur système doit s'assurer qu'il n'est pas possible de désactiver le système de sécurité à distance.

2. L'option de gestion à distance de votre routeur (côté WAN) doit être désactivée (la plupart des routeurs l'ont préprogrammée par défaut).

3. Lorsque vous utilisez le Wi-Fi, utilisez au moins WPA/PSK ou supérieur.

4. Lorsque vous quittez la maison ou le bâtiment, tous les routeurs Wi-Fi doivent être automatiquement désactivés. Cela peut être fait très facilement via le système TELETASK. Vous pouvez également arrêter automatiquement tous les routeurs Wi-Fi après une heure spécifiée ou pendant une période spécifiée (nuit) en coupant la prise de courant du routeur.

5. Ne fournissez pas de prises Ethernet accessibles au public, connectées au LAN sécurisé, dans les zones publiques.

6. Les prestataires de support technique externes peuvent avoir accès aux zones sécurisées (par exemple, le personnel de maintenance des ascenseurs...). Cependant, vérifiez-les afin qu'ils n'entrent pas dans votre réseau local sécurisé.

7. Utilisez toujours des mots de passe appropriés (minimum 8 caractères, minimum 1 lettre majuscule et 1 chiffre). Ne répétez pas vos mots de passe et utilisez de préférence un logiciel de gestion des mots de passe.

.

www.teletask.be