

Appareils connectés, porte d'entrée de la domotique

# Connectivité 4.0

**Futurologues et chefs d'entreprises sont unanimes: la mise en réseau croissante d'appareils compatibles internet va révolutionner notre art et manière de vivre et de travailler dans les temps futurs. Mais ce trend comporte également des risques. La menace de cyberattaques sur les infrastructures critiques telles que la distribution d'électricité et d'eau, préoccupe depuis des années les organismes de sécurité. Ces derniers temps, les messages concernant les failles de sécurité et les attaques sur les systèmes de commandes et sur d'autres appareils connectés se multiplient.**

Ce que les experts comme John Matherly, fondateur de Shodan, dévoilent sur l'état de sécurité des systèmes connectés, fait frémir. Shodan est un navigateur de recherche destiné à l'Internet des objets. Le portail se rend automatiquement sur chaque routeur internet et vérifie si les ports sont ouverts ou s'ils sont redirigés. Si un appareil répond, Shodan vérifie immédiatement les protocoles possibles et les mots de passe standards. Ainsi, le portail trouve une multitude d'appareils accessibles librement sur internet et met les résultats à disposition de tout intéressé.

En juillet 2016, un rapport publié par Kaspersky montrait que dans le monde, environ 188 000 systèmes de commande industriels étaient accessibles directement via internet. Il ne faut pas être expert pour se représenter le potentiel de dégâts. Cela s'étend d'agressions sur de simples commandes, jusqu'à des attaques sur des infrastructures de grande ampleur, expérience subie par une ville finlandaise en novembre dernier. Le réseau de chauffage urbain avait en effet été paralysé par des pirates informatiques durant plusieurs jours.

## Accès à distance et sécurité

Le transfert de port (port forwarding), de nos jours souvent utilisé, représente un grand risque à ne pas sous-estimer. Afin de protéger l'infrastructure technique de manière optimale, il faut un concept de sécurité global. La société HOOC SA propose un système innovant et facile à utiliser, permettant d'assurer la sécurité de l'accès à distance aux commandes et réseaux. Il est constitué de passerelles HOOC, d'une infrastructure de Cloud HOOC et d'un logiciel client HOOC. Il s'agit ainsi d'une «solution tout en un» innovante.

- *Sécurité au niveau du transport des données:* une passerelle HOOC installée dans un réseau à distance se connecte automatiquement au Cloud HOOC. L'établissement de la communication s'effectue ainsi toujours de l'intérieur vers l'extérieur. La connexion est sécurisée par un cryptage AES et est authentifiée par des attestations. Aucune connexion venant de l'extérieur, ni transfert de port ne sont nécessaires pour son fonctionnement.
- *Sécurité au niveau de l'authentification:* pour authentifier l'utilisateur, HOOC utilise la combinaison d'une adresse mail et d'un mot de passe sûr. Chaque personne dispose explicitement d'une adresse mail et doit s'identifier en conséquence pour se connecter. Avant d'accorder l'accès, ce principe permet une identification réciproque des parties engagées.
- *Gestion simple et transparence:* le portail de gestion intégré dans le Cloud HOOC permet un management simple et intuitif de l'ensemble de la solution ainsi que les autorisations d'accès aux réseaux à distance. Il ne faut pas de connaissance informatique approfondie.



Une passerelle HOOC installée dans le réseau se connecte automatiquement au Cloud HOOC.

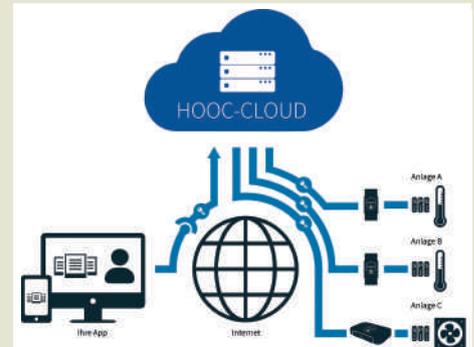
die. Tous les accès sont enregistrés en permanence. On peut ainsi vérifier à tout moment quel utilisateur a eu accès à un réseau et pendant combien de temps.

- *Technologie de base pour services de niveau supérieur*: des connexions sûres sont à la base de la technologie HOOC et assoient simultanément les conditions fondamentales pour la mise en réseau des appareils connectés. Le Cloud HOOC propose toute une gamme de fonctionnalités et de caractéristiques pour applications haut de gamme, de hiérarchie supérieure. ■

HOOC SA  
3930 Visp  
Tél. 027 948 46 00  
info@hooc.ch  
www.hooc.ch

### Des solutions pour accès à distance fiable et sans danger

HOOC développe, exploite et entretient des plateformes logicielles et des composants matériels pour un accès aux installations et aux données à distance en toute sécurité. L'objectif est de pouvoir relier les données à disposition sur la plateforme logicielle avec de nouveaux services à valeur ajoutée. HOOC offre à ses clients son expertise en matière d'interconnexion d'installations et de données. Grâce à des interfaces standardisées, il est également possible d'intégrer



dans la plateforme de communication des applications spécifiques aux clients.

L'entreprise suisse traditionnelle est fortement ancrée dans la branche CVC et dans l'industrie de l'automatisation du bâtiment. Elle s'investit pour la qualité et la fiabilité. Les solutions se caractérisent par leur facilité de manipulation sur site. Elles sont particulièrement adaptées aux besoins des installateurs, des opérateurs et des prestataires de maintenance.

## Sécurité totale.

Les produits électriques élaborés sont garants de la réalisation technique, de la facilité et du confort d'utilisation. Le signe de sécurité (S) de l'Inspection fédérale des installations à courant fort ESTI est synonyme de la sécurité électrique. Le (S) témoigne le respect des prescriptions légales, lequel est garanti par des tests et par la surveillance du marché.

**Vous trouverez des infos sur [www.esti.admin.ch](http://www.esti.admin.ch)**



Les produits portant ce label font preuve de sécurité.

