GUIDE

Dernière mise à jour : septembre 2018

Recommandations techniques ASERCOM relative à la cyber-sécurité des équipements connectés HVAC/R

Préface

De nombreux équipements HVAC/R tels que les compresseurs, ventilateurs ou contrôleurs sont désormais équipés de dispositifs connectés. Ceci comprend le Bluetooth, Wi-Fi ou connectivité LAN. Ce guide technique donne des recommandations sur la façon de les connecter de manière sécurisée à des smartphones, ordinateurs ou internet.
La structure de ce guide suit le cycle de vie d'une installation HVAC/R: il commence avec l'organisation et l'assemblage de l'architecture, se poursuit avec l'installation du système, sa maintenance durant son fonctionnement et se termine par les recommandations de sécurité informatique lors du démontage de l'installation.
Ce guide technique donne des recommandations "clé en main" pour des installations sur le terrain avec une sécurité renforcée Ces étapes vont aider à réduire la vulnérabilité des contrôleurs ou variateurs de vitesse installés ; cependant elles ne sont pas une alternative à un système de contrôle intégré. En particulier pour de grandes installations/entreprises il est fortement recommandé d'investiguer si un Système de Management de la sécurité de l'information (SMSI) est une étape nécessaire. Un bon point de départ pour cette investigation peut être une introduction aux Normes ISO 27001, UL2900 or IEC62443:
(voir:
https://www.iso.org/isoiec-27001-information-security.html ou https://fr.wikipedia.org/wiki/ISO/CEI_27001
https://en.wikipedia.org/wiki/Cyber_security_standards
Kobes, P.: Guideline Industrial Security ISO 62443 is easy; Berlin: VDE Verlag; 2017)

Il est également recommandé de vérifier régulièrement et suivre toute réglementation locale mise en place relative à la cyber-sécurité. La réglementation peut également évoluer dans le temps.

Image: pixabay

Remarque générale

Les Normes sur la cyber-sécurité, comme la CEI 62443, VDI/VDE 2182 et autres définissent trois rôles différents dans une installation connectée à internet.

a) Le fabriquant des appareils connectables tels que des contrôleurs, variateurs de fréquence ou capteurs (parfois dénommé “vendeur”)
b) L’intégrateur qui conçoit et installe le système sur le terrain en utilisant des équipements connectables (parfois dénommé contracteur)
c) Le propriétaire qui utilise l’équipement HVAC/R connecté

Une tâche très importante selon ces Normes est la communication : l’information sur la spécification, les besoins, cas d’usage, modifications et autres doivent être échangés entre ces trois intervenants. La Cyber-Security n’est pas un objectif statique, effectué une fois pour toute. Il est important de maintenir la communication et échange d’informations (par exemple avec transmission de mises à jour) pendant tout le cycle de vie du système sur le terrain. Cela signifie qu’il peut être raisonnable d’établir un cycle PDCA (cycle plan-do-check-act) pour le système durant sa durée de vie.
Dans les sections suivantes sont fournies des recommandations importantes. Néanmoins il est important de procéder à une analyse de risque individuelle pour déterminer si des mesures additionnelles ou plus complexes sont nécessaires pour protéger le système. Les étapes mentionnées dans ce guide technique couvrent la plupart des technologies et procédés. De plus il est aussi très important de faire un focus sur les personnes : les trois acteurs indiqués (fabriquant, intégrateur et propriétaire de l’équipement) doivent se former et sensibiliser régulièrement à la cyber-sécurité tous les employés impliqués.

Il se peut que certaines étapes proposées ne soient pas adaptées à toutes les installations. Il est important alors de sélectionner les étapes utiles et appropriées de ce guide technique.

Architecture / Planning

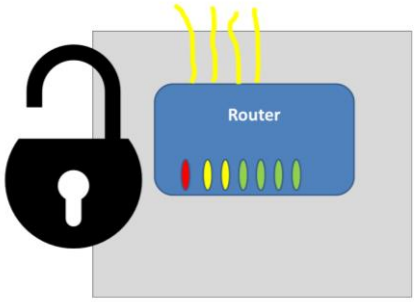
Créer une stratégie de défense en profondeur

Risque : Une mesure unique de protection d’un système HVAC/R system sur le terrain peut présenter des faiblesses et être vulnérable.
Solution: Au lieu de se reposer sur une contremesure unique pour prévenir des cyber-attaques, il est recommandé d’’utiliser plusieurs mesures complémentaires de protection. Si un hacker arrive à franchir la couche 1, il devra vaincre la deuxième protection, et ainsi de suite

Placer les composants connectés tel que routeurs dans une pièce ou local fermé

Risque: Si une personne non autorisée peut accéder physiquement à des composants connectés tel que routeur , pare-feu ou PLC , en particulier par l’intermédiaires de ports USB , elle peut aisément modifier le set-up et accéder à l’installation .

Solution: Placer les composants connectés tels que routeurs et pare-feu dans un emplacement ou pièce fermé à clé. S'assurer que seule une personne autorisée peut déverrouiller l'accès et que le verrouillage est systématique si aucune personne habilitée n'est sur les lieux.



Séparer les équipements connectés HVAC/R des autres éléments du réseau (bureau…) par segmentation (par exemple pare-feu): segmentation du réseau

Risque: Si l'équipement HVAC/R est sur la même branche de serveur que les équipements de bureau ou serveurs web une cyber-attaque sur un éléments peut facilement en contaminer d'autres .

Solution: Répartir l'installations en segments logiques avec des communications séparées (voir aussi https://en.wikipedia.org/wiki/Network_segmentation). Ceci peut être réalisé par exemple en implémentant des pare-feu entre deux branches.

Phase d'installation / mise en service

Changer les mots de passe par défaut pour le login (admin et utilisateur)

Risque: Des components tels que pare-feu ou routeur mais aussi des variateurs de fréquence contrôleurs ou ventilateurs EC avec une interface web, ont typiquement une interface de login . Il y a un login par défaut (nom et mot de passe de connexion) qui est décrit dans le manuel utilisateur. Si ces données par défaut ne sont pas changées un hacker peut facilement accéder au composant s'il trouve l'adresse IP du composant.

Solution: Les accès par défaut (identifiant et mot de passe) doivent être changés lors de l'installation.

Détruire les "comptes temporaires d'installation" après installation

Risque: Souvent les comptes d'accès temporaires (administrateur ou utilisateur) sont mis en place par le contracteur pendant l'installation. Ces comptes ont souvent des mots de passe très simples pour éviter des pertes de temps et de la complexité pendant l'installation.

Solution: Ces comptes temporaires utilisés lors de l'installation doivent être détruits lorsque l'installation est terminée ou protégé avec un mot de passe suffisamment sécurisé.

Utiliser des mots de passe contenant à la fois des lettres, nombres , caractères spéciaux et avec une longueur minimale de 8 caractères .

Image : pixabay

Risque: Avec un craqueur de mot de passe tel que *medusa* (partie de KALI Linux) il est facile d'essayer des milliers de mots de passe automatiquement .Ces outils utilisent typiquement des listes de mots de passe récupérés lors d'attaques antérieures chez des providers d'internet ou des sites marchands. . Ils contiennent des mots de passe fréquemment utilisés tels que *123456* ou *password*.
Solution: Utiliser des mots de passe davantage cryptés qui ne sont pas listés dans un dictionnaire ou se contentent de remplacer un par "i" par un "1" ou un "s" par un "5". Pour réduire le risque d'attaque la longueur minimale doit être de 8 caractères pour un mot de passe généré aléatoirement, et même davantage pour des mots de passe non aléatoires . Il est d'autre part fortement recommandé de ne pas utiliser le même mot de passe sur plusieurs installations.

Renforcer le système en fermant/ désactivant les ports, protocoles and adresse IP accessibles dans les composants connectés

Risque: Une adresse IP d'un ordinateur ou équipement électronique peut être comparée à une adresse de maison et un port (ex. 443) ou un protocole (ex. https) peut être comparé à la porte d'une maison. Les différentes applications web tels que emails, transferts de fichiers, ou sites internet ont des protocoles et ports individuels. Chacun port ouvert (rendu accessible) présente un risque d'intrusion.
Solution: Comme un équipement HVAC/R n'accède typiquement qu'à un serveur de maintenance et utilise une fonctionnalité limitée du web, les adresses IP accessibles et ports ouverts peuvent être réduits significativement. Il est recommandé de d'inactiver toutes les adresses IP sauf les quelques-unes qui sont réellement nécessaires et de fermer tous les ports qui ne sont pas utilisés. Un système de climatisation ne consulte pas de vidéos sur le site YouTube ni ne nécessite de communiquer avec Wikipédia par exemple .

Utilisez des transmissions de données cryptées (https, et non http , Bluetooth, VPN…)

Risque: Si des données sont transmises sans fil ou par l'intermédiaire d'un câble sans être cryptées , il a toujours le risque que quelqu'un écoute cette communication et par exemple accède au informations de login d'un composant électronique ou d'un système .

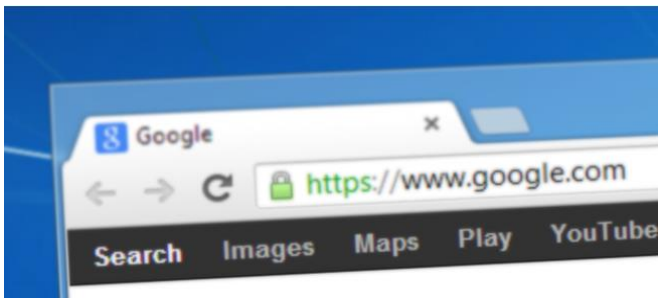


Image : pixabay

Solution: Un encryptage et authentification au niveau de l'état de l'art doit toujours être utilisés pour les transmissions de données et communications. Les technologies évoluant, il est important d'utiliser les meilleures technologies disponibles ce qui peut amener à changer de méthode d cryptage au bout d'un certain temps .

Maintenance pendant la durée de vie d'un système

Installez toutes les mises à jour disponibles pour les pare-feu, routeurs, smartphones/tablettes, PCs/Laptops… utilisés dans les installations HVAC/R

Risque: Des failles sécurité sont régulièrement identifiées. Les fabricants et distributeurs de logiciels et matériels éditent des pises à jours et patches pour leurs produits qui sont affectés. Si un composant non mis à jour est utilisé dans un circuit HVAC/R, le système est sensible aux cyber-attaques.

Solution: Il est nécessaire d'installer toutes les mises à jour et patchs publiés. Beaucoup de composants tels que des pare-feu ou routeurs ont l'option d'informer via email ou message texte dès qu'une mise à jour est disponible. Les équipes de maintenance peuvent alors réagir et installer les mises à jour. Au-delà des composants et logiciels utilisés sur les sites d'installations HVAC/R, il est également nécessaire de maintenir à jour tous les « outils » qui vont se connecter temporairement au système ,tels que smartphones, laptops ou PCs .

Desactivez le Bluetooth et Wifi si non utilisé ou non nécessaire

Image : pixabay

Risque: Il y a certains outils capables d'attaquer des connections Bluetooth. En champ libre une connexion Bluetooth peut être accessible sur une distance de 50 à 100m. En dehors d'une connexion par câble, une attaque Bluetooth peut s'opérer en dehors du périmètre d'un bâtiment fermé ou d'un espace clôturé .
Solution: Dans la plupart des cas une connexion Bluetooth n'est pas nécessaire 24h/24 / 7 Jours / semaine. Elle peut être éteinte la plupart du temps et active uniquement lorsqu'il y a besoin de transmettre des données. Ainsi une amélioration sensible de la cyber-sécurité est obtenue en désactivant toutes connexions sans fil quand non nécessaires.

Mettre à jour les comptes utilisateurs et administrateurs pendant la durée de vie du système.

Risque: Les employés du propriétaire de l'unité ou de l'entreprise de maintenance peuvent quitter leur Société et si leur compte n'est pas désactivé, ils peuvent toujours accéder à l'équipement connecté via internet
Solution: Mettre en place une procédure qui assure que les comptes des employés qui quittent une Société soient inactivés. Une situation similaire peut arriver si le propriétaire change de sous-traitant de maintenance. Si un dispositif de mot de passe dynamique est disponible sur le composant, il est recommandé d'utiliser ce dispositif de sécurité.

Démontage de l'installation.

Faire un Reset de tous les composants en paramétrage d'usine et effacer tous les mots de passe et données. Les mots de passe et données ne doivent pas être transmises à quiconque après désinstallation de l'équipement au cas où le même mot de passe soit utilisé sur plusieurs installations.

Risque: Si la fin de vie d'un équipement est atteinte, il sera désinstallé. Dans ce cas les données restent stockées dans les composants (tels que disques durs de PC, ou carte mémoire d'un contrôleur . Ces données peuvent être accessibles par une tierce partie lorsque le composant est démonté.
Solution: S'assurer que toutes les données sont effacées et que les réglages soient remis aux paramétrages usine par défaut avant de démonter les composants. Une attention particulière est à apporter sur les cartes mémoire embarquées (cartes SD) , lecteurs USB flash , mémoires cloud (situées sur internet, et non sur site) et les données contenues dans les smartphones or tablettes ou PCs.

GUIDE

Dernière mise à jour : septembre 2018

Revision Index

Revision	Change	Date
A	Initial issue	22.03.2018

Les présentes recommandations s'adressent aux fabricants/installateurs de systèmes de réfrigération à usage professionnel, industriel, commercial et domestique. Elles ont été formulées sur la base des informations considérées par *ASERCOM* comme représentant l'état actuel de la science et de la technique à l'heure de leur rédaction. Néanmoins, *ASERCOM* et ses sociétés membres déclinent toute responsabilité quant aux mesures (actes ou omissions) entreprises sur la base de ces recommandations.