Honeywell

Pratiques exemplaires générales en matière de sécurité

GUIDE TECHNIQUE DU SYSTÈME

APPLICATION

Honeywell déclare expressément que ses contrôleurs ne sont pas intrinsèquement protégés contre les cyberattaques. Ils sont exclusivement destinés à l'utilisation dans des réseaux privés. Toutefois, puisque les réseaux privés peuvent aussi être la cible de cyberattaques par des personnes bien équipées et compétentes en informatique, ils doivent être protégés. Afin d'atténuer les risques que constituent ces attaques, les clients doivent suivre les directives sur les pratiques exemplaires en matière de sécurité et d'installation pour tous les produits Honeywell fondés sur la PI.

Les directives suivantes décrivent les pratiques exemplaires générales en matière de sécurité pour les produits Honeywell fondés sur la PI. Les directives sont énumérées par ordre croissant d'atténuation du risque.

Les exigences précises pour chaque installation devraient être évaluées au cas par cas. Le niveau de sécurité des systèmes de la majorité des installations qui mettent en œuvre toutes les mesures d'atténuation énoncées dans ce document sera bien supérieur aux exigences requises. Généralement, la mise en œuvre des points 1 à 5 concernant les réseaux locaux est suffisante pour répondre aux exigences de la plupart des installations de réseaux de commandes d'automatisation.

RÉSEAUX LOCAUX INTÉGRANT DES CONTRÔLEURS WEBS

Assurez-vous que les systèmes fonctionnent selon une politique de mots de passe appropriée pour l'accès de l'utilisateur à tous les services. Cette directive comprend notamment les éléments suivants :

1. L'utilisation de mots de passe forts.
2. Un cycle de renouvellement de mot de passe recommandé.
3. Des identifiants et des mots de passe uniques pour chaque utilisateur.
4. Des règles de divulgation de mot de passe.
5. Si un accès à distance aux systèmes informatiques de contrôle du bâtiment est nécessaire, utilisez un réseau privé virtuel (RPV) pour diminuer les risques d'interception des données et éviter que les appareils de contrôles ne soient connectés directement à Internet.

Autres considérations

- Prévenez les accès non autorisés à l'équipement du réseau utilisé avec les systèmes fournis par les solutions WEBs. Comme pour tout système informatique, empêcher les accès physiques au réseau et à l'équipement réduit les risques d'une intervention non autorisée. S'assurer que les salles de serveur, les tableaux de connexions et l'équipement de TI sont dans des pièces verrouillées fait partie des pratiques exemplaires en matière de sécurité pour les installations de TI. L'équipement WEBs doit être installé à l'intérieur d'armoires de commande verrouillées, elles-mêmes situées dans des pièces fermées à clé.
- Une fois la mise en service terminée, assurez-vous que l'appareil est protégé par mot de passe et que les niveaux utilisateurs sont correctement attribués aux utilisateurs du site.
- Adoptez une politique de mise à jour adaptée à l'infrastructure du site dans le cadre de l'accord sur les niveaux de service. La politique devrait comprendre notamment une mise à jour à la version la plus récente des composants de systèmes suivants :
  - Micrologiciels des dispositifs comme les contrôleurs, les modules d'E/S, HMI, etc.
  - Logiciels de superviseur comme le logiciel WEBStation-AX.
  - Systèmes d'exploitation d'ordinateur et de serveurs.
  - Infrastructure réseau et systèmes d'accès à distance.
- Configurez des réseaux informatiques séparés : un réseau pour les systèmes de commandes d'automatisation et un réseau informatique d'entreprises pour le client. Vous pouvez y parvenir soit en configurant des réseaux locaux virtuels à l'intérieur de l'infrastructure de TI du client, soit en installant une infrastructure réseau isolée et dédiée aux systèmes de commandes d'automatisation.

31-00129F-01

- Une fois le système mis en ligne, limitez la fréquentation IP sur le réseau de commandes d'automatisation (au moyen de liste d'accès, par exemple) pour n'inclure que les types de protocoles nécessaires au bon fonctionnement, c'est-à-dire C-Bus, BACnet, etc. Pour obtenir plus de renseignements concernant le trafic de télécommunication requis pour assurer le fonctionnement des systèmes, consultez la documentation accompagnant le produit.
- Configurez l'infrastructure réseau de façon à restreindre l'accès aux serveurs Web lors d'une connexion aux contrôleurs WEB à l'aide d'un superviseur de système centralisé (p. ex., WEBStation-AX) et lorsque le système ne nécessite pas un accès direct au serveur Web des dispositifs.
- Les réseaux locaux virtuels dynamiques créés par allocation d'adresses MAC peuvent protéger le système d'une connexion d'un appareil non autorisé et réduire les risques associés à la surveillance des données sur le réseau par une personne.

Pour en savoir plus, consultez la section « Sécurité réseau » de la fiche technique spécifique au contrôleur.

Home and Building Technologies

Aux États-Unis :

Honeywell

715 Peachtree Street NE

Atlanta, GA 30308

customer.honeywell.com

31-00129F—01 M.S. 09-17
Imprimé aux États-Unis

Honeywell