Annexe 1 – Recommandations en matière de cybersécurité

La cybersécurité est plus qu'un mot à la mode : c'est quelque chose qui concerne chaque appareil connecté à Internet. La vidéosurveillance sur IP n'est pas à l'abri des cyberrisques, mais la mise en place de mesures élémentaires pour protéger et renforcer les réseaux et les appareils en réseau les rendra moins vulnérables à des attaques. Nous donnons, ci-après, des conseils et des recommandations pour créer un système de sécurité plus sûr.

Actions obligatoires à prendre pour la sécurité réseau d'équipements de base :

1. **Utiliser des mots de passe robustes**
   Veuillez vous référer aux recommandations suivantes pour définir les mots de passe :
   - La longueur du mot de passe doit être d'au moins 8 caractères.
   - Ils doivent être composés de deux types de caractères comprenant des lettres majuscules et minuscules, des chiffres et des symboles.
   - Ils ne doivent pas être composés du nom du compte dans l'ordre normal ou inversé.
   - Les caractères ne doivent pas se suivre, par ex. 123, abc, etc.
   - Les caractères ne doivent pas se répéter, par ex. 111, aaa, etc.
2. **Mettre à jour le micrologiciel et le logiciel client à temps**
   - Conformément à la procédure standard de l'industrie technologique, nous vous recommandons de maintenir à jour le micrologiciel de votre équipement (enregistreurs NVR et DVR, caméra IP, etc.) afin de garantir que votre système est doté des correctifs de sécurité les plus récents. Lorsque l'équipement est connecté au réseau public, il est recommandé d'activer la fonction de vérification automatique de la disponibilité de mises à jour afin d'obtenir rapidement les informations sur les mises à jour du micrologiciel fournies par le fabricant.
   - Nous vous conseillons de télécharger et d'utiliser la version du logiciel client la plus récente.

Recommandations à suivre pour améliorer la sécurité réseau de votre équipement :

1. **Protection matérielle**
   Nous vous suggérons de fournir une protection matérielle à vos équipements, en particulier les dispositifs de stockage. Par exemple, placez l'équipement dans une armoire ou une salle informatique spéciale, et appliquez des autorisations de contrôle d'accès et une gestion des clés sur mesure afin d'empêcher à tout personnel non autorisé d'entrer en contact physique avec les équipements pour éviter par ex. d'endommager le matériel, des connexions non autorisées à des équipements amovibles (disque flash USB, port série) etc.
2. **Modifier régulièrement votre mot de passe**
   Nous vous conseillons de modifier régulièrement vos mots de passe pour réduire les risques qu'ils soient devinés ou déchiffrés.
3. **Définir et mettre à jour les informations de réinitialisation des mots de passe à temps**
   L'équipement prend en charge la fonction de réinitialisation du mot de passe. Veuillez définir les informations relatives à la réinitialisation du mot de passe à temps, y compris l'adresse électronique de l'utilisateur final et les questions de protection du mot de passe. Si les informations changent, veuillez les modifier à temps. Lors de la configuration des questions de protection du mot de passe, il est conseillé de ne pas utiliser des questions (réponses) trop faciles à deviner.

4. **Activer le blocage de compte**
   La fonction de blocage de compte est activée par défaut. Nous vous recommandons de la laisser activée pour garantir la sécurité des comptes. Si un pirate tente de se connecter plusieurs fois avec un mot de passe incorrect, le compte concerné et l'adresse IP de la source seront bloqués.
5. **Modifier les ports par défaut des services HTTP et d'autres services**
   Nous vous conseillons de modifier les ports par défaut du service HTTP et des autres services en les choisissant dans la plage numérique allant de 1 024 à 65 535, ce qui permet de réduire le risque que des étrangers puissent deviner les ports utilisés.
6. **Activer HTTPS**
   Nous vous conseillons d'activer le protocole HTTPS. Vous accéderez ainsi au service Web au moyen d'un canal de communication sécurisé.
7. **Activer la liste blanche**
   Nous vous conseillons d'activer la fonction de liste blanche pour empêcher tout le monde, à l'exception des adresses IP spécifiées, d'accéder au système. Par conséquent, veillez à ajouter l'adresse IP de votre ordinateur et l'adresse de l'équipement qui l'accompagne à la liste blanche.
8. **Liaison d'adresse MAC**
   Nous vous recommandons de lier l'adresse IP et l'adresse MAC de la passerelle à l'équipement, réduisant ainsi le risque d'usurpation ARP.
9. **Assigner raisonnablement les comptes et les privilèges**
   En fonction des besoins d'activité et de gestion, ajoutez de manière raisonnable des utilisateurs et leur assigner un ensemble d'autorisations minimales.
10. **Désactiver les services inutiles et choisir les modes sécurisés**
    S'ils ne sont pas nécessaires et pour réduire les risques, désactivez certains services, tels que SNMP, SMTP, UPnP, etc.
    En cas de besoin, il est fortement recommandé d'utiliser les modes sécurisés, y compris mais sans limitation, les services suivants :
    - SNMP : choisissez SNMP v3 et configurez des mots de passe de chiffrement et d'authentification robustes.
    - SMTP : choisissez le protocole TLS pour accéder aux serveurs de messagerie.
    - FTP : choisissez le protocole SFTP et définissez des mots de passe robustes.
    - Point d'accès : choisissez le mode de chiffrement WPA2-PSK et définissez des mots de passe robustes.
11. **Chiffrement de la transmission audio et vidéo**
    Si vos contenus de données audio et vidéo sont très importants ou sensibles, nous vous recommandons d'utiliser la fonction de chiffrement de la transmission, afin de réduire les risques de vol des données audio et vidéo durant la transmission.
    Rappel : le chiffrement de la transmission entraînera une certaine baisse de l'efficacité de la transmission.
12. **Contrôle sécurisé**
    - Vérifier les utilisateurs connectés : nous vous conseillons de vérifier régulièrement les utilisateurs connectés afin de savoir si la connexion à l'appareil s'effectue sans autorisation.
    - Consulter le journal de l'équipement : en examinant les journaux, vous pouvez connaître les adresses IP utilisées pour la connexion à vos appareils et les principales opérations effectuées.

13. Journal réseau

Comme la capacité de stockage de l'équipement est limitée, le journal stocké sera limité. Si vous devez conserver le journal pour longtemps, il est recommandé d'activer la fonction de journal réseau afin de veiller à ce que les journaux essentiels soient synchronisés avec le serveur de journal réseau pour suivi.

14. Construire un environnement réseau sécurisé

Afin de garantir au mieux la sécurité des équipements et de réduire les cyberrisques potentiels, nous vous recommandons de :

- Désactiver la fonction de mappage de ports du routeur pour éviter les accès directs aux appareils Intranet à partir du réseau externe.
- Compartimenter et isoler le réseau en fonction des besoins réseau réels. Si la communication n'est pas nécessaire entre deux sous-réseaux, il est conseillé d'utiliser les technologies de réseau VLAN, GAP et d'autres pour compartimenter le réseau de sorte à obtenir une isolation réseau effective.
- Mettre en place le système d'authentification d'accès 802.1x pour réduire le risque d'accès non autorisés aux réseaux privés.