

Exigences cybersécurité équipements

Les équipements déployés sur le parc de la DiRIF doivent respecter les exigences cybersécurité décrites ci-après.

Les équipements terrains ou de systèmes industriels de type **Panneaux à Message Variables, caméras, unité de mesure et de traitement, automates** sont concernés.

- Compléter (sans oublier de dater et signer) **la fiche engagement**, en annexe 2

L'équipe cybersécurité de la DiRIF peut être contactée par mail à l'adresse suivante:

contact-cybersecurite-dirif.dett@developpement-durable.gouv.fr

A - Connaître le Système d'Information

Etablir un inventaire des équipements déployés, et fournir pour chaque équipement:

- le type d'équipement, le constructeur de l'équipement et le modèle,
- le tatouage
- l'adresse IP
- la localisation d'installation physique (axe/sens/PR ou coordonnées GPS) et le secteur associé (Nord/Sud/Est/Ouest)
- la version applicative du firmware de l'équipement et la version applicative préconisée par le constructeur de l'équipement (ces versions doivent logiquement correspondre)
- la date de fin de support du firmware de l'équipement (si la fin de vie a été annoncée par le constructeur)

Inventorier les comptes utilisateurs et leur niveau de privilège

- Fournir la liste des comptes de services (comptes partagées): ex. root, admin, service, etc.
- Mettre en place des comptes nominatifs pour chaque compte d'administration
- Fournir la liste des comptes nominatifs des utilisateurs, en précisant leur rôle / leur profil

B - Authentifier et contrôler les accès

Changer les mots de passe par défaut / les mots de passe usine

- Respecter la politique de mots de passe, définie en annexe 3
- Stocker les mots de passe dans un conteneur Keepass2 ou KeepassXC (format "kdbx") et fournir la clé maître du Keepass à la DiRIF par une méthode sécurisée
- Les équipements d'un même type (ex: des stations RAD) et de même modèle peuvent partager un même mot de passe, Il est demandé que cette réutilisation de mots de passe

soit sectorisée (donc différente entre le Nord, le Sud, l'Est et l'Ouest).

- Le stockage des mots de passe sur l'équipement ne peut utiliser qu'un algorithme de chiffrement conforme au Règlement Général de Sécurité.
-

Remplacer les certificats par défaut sur l'équipement

- L'équipement doit permettre l'utilisation de certificats externes

C - Sécuriser les équipements

- Appliquer le principe du moindre privilège, c-à-d. que chaque intervenant sur l'équipement doit disposer d'un compte ayant uniquement les droits nécessaires à l'accomplissement de ses tâches
 - Paramétrer l'équipement de façon à ce qu'une temporisation soit effective après 3 échecs d'authentification successifs sur l'équipement
 - Fournir la matrice des flux entrants sur l'équipement, en renseignant l'annexe 6
 - Réduire les accès à Internet au strict minimum et renseigner la matrice des flux sortants sur Internet, dans la même annexe 6
 - N'activer que les protocoles ou services utiles au fonctionnement de l'équipement
-

Dans le cas où le système d'exploitation de l'équipement est basé sur Linux:

Durcir la configuration du système Linux

- au niveau du serveur SSH:
 - Désactiver la possibilité de se connecter en SSH avec le compte root
 - Désactiver la possibilité d'effectuer des redirections de flux

D - Sécuriser les applications web

Renforcer la protection du portail web (des équipements) contre les attaques

- Le portail web des équipements doit être exposé en HTTPS
- stocker les hashes de mots de passe avec un sel aléatoire

E - Sécuriser l'infrastructure réseau

Privilégier les installations filaires

- L'utilisation du Wi-Fi n'est possible que sous conditions, telles que précisés en Annexe 5
- Faire valider l'architecture réseau par l'équipe cybersécurité
- Une fois l'architecture réseau validée, faire paramétrer les équipements réseaux par le marché d'infogérance des réseaux de la DiRIF

F - Sécuriser l'administration

N'utiliser que des protocoles d'administration sécurisés

- **L'utilisation des protocoles suivants est proscrite:**

- telnet
 - HTTP
 - IMAP
 - SMTP
 - POP3
 - FTP
-

- **Seule l'utilisation des protocoles sécurisés est autorisée:**

- SSH v2
- HTTPS, avec TLS 1.3
- IMAPS
- SMTPS
- POP3S
- SFTP
- SNMP v3

Désactiver les services inutiles

G - Permettre la continuité d'activité et la maintenance

- **Mettre à jour les équipements avec la dernière version de firmware supportée par le constructeur**
- **Fournir les procédures** d'installation, de configuration/paramétrage et de sauvegarde/restauration des configurations des équipements
- Privilégier l'usage de produits qualifiés ou labellisés par l'ANSSI

H - Superviser et auditer

Journaliser les opérations suivantes:

- réussite et échec d'authentification
- ajout/suppression de compte ou de rôle/profil et affectation de droits
- démarrage/arrêt planifiée de l'équipement

- dysfonctionnements/défaillances/alarmes

Synchroniser les équipements sur une même source de temps (via le protocole NTP)