Rapport du D32

D32

Version 1 le 15 mai 2019

En vigueur JUIN 2017

I. Objectif D32

- Ce document définit les exigences techniques minimales auxquelles doivent répondre les systèmes de sécurité ou sureté raccordés à un réseau IP pour garantir un niveau de résistance aux attaques numériques dans des circonstances préalablement établies.

II. Méthodologie

- **Analyse des besoins et des risques numériques**
  (consiste à identifier les besoins à partir de l'analyse du contexte de l'installation)
  1. identifier les critères du risque numérique
  2. Formaliser le résultat de l'analyse des besoins et des risques
- **Conception**
  (consiste à proposer les solutions techniques aptes à répondre aux besoins préalablement identifiés pour l'installation du système)
  1. préconisations de fiabilité du système
  2. préconisations d'architecture du système

- **Réalisation de l'installation**
  (débute à la réception de la commande par l'installateur. Elle comporte la réalisation de l'installation, le contrôle et la mise en service, la formation, l'assistance des utilisateurs et la réception de l'installation)
  1. préconisation pour la confidentialité des données
  2. préconisation pour la disponibilité du système et de ses données
  3. préconisation pour l'intégrité des données
  4. préconisation pour la traçabilité

- **Maintenance**
  (correspond à toute la prériode d'activité de l'installation. Elle a pour objet de maintenir en bon état le système installé et de veiller à ce qu'elle rest adaptée aux besoins et aux risques , dans le respect des exigences du référentiel)

---

exploitation du système de sécurité

1. définir une politique fiable pour les mots de passe
2. maintenir à jour l'intégrité des équipements
3. octroyer aux utilisateurs les privilèges et les droits nécessaires à leur activité
4. définir une politique de sécurité pour le réseau
5. superviser le réseau, journaliser et définir une organisation de gestion d'incidents
6. sensibiliser les utilisateurs à la menace

---

maintenance du système de sécurité

1. maintenance préventive (entretien périodique)
2. fréquence des visiteurs de maintenance préventive
3. nature des opérations d'entretien périodique
4. suivi des visistes de maintenance

III. Tâches

1. les équipements informatiques, leur fonction, les risques potentiellement encourus
2. les accès réseaux, les équipements et les risques de malveillance encourus
3. le cloisonnement des réseaux et la maitrise des flux
4. la sécurité des postes de travail
5. la politique en matière d'authentification des utilisateurs
6. les précautions prises pour prévenir et détecter l'introduction de logiciels fraduleux (antivirus)
7. les éventuels moyens de détection des tentatives d'intrusion
8. la sécurisation des flux internet et messagerie
9. la politique de sécurité du système 'information, en particulier le plan de sauvegarde (moyens correctifs et préventifs mis en œuvre)

X. Annexes
CNPP: Centre national de prévention et protection