

Liste de contrôle

pour une infrastructure informatique sûre

- Authentification multi-facteurs pour les accès à distance
- Les systèmes d'exploitation et les programmes sont à jour
- Installation de mesures de protection techniques actuelles et conformes à l'état de la technique, telles que
 - Pare-feu
 - Scanneur de virus
 - Filtre anti-spam
 - Programmes de protection d'accès
 - Cryptage du réseau
 - Accès à distance authentifié (par ex. VPN)
 - Les correctifs de sécurité sont installés
- Formation des collaborateurs à l'utilisation des données et des e-mails
- Sauvegarde quotidienne des systèmes critiques
- Au moins une copie de sauvegarde est mise en miroir sur un serveur séparé et les sauvegardes sont régulièrement testées quant à leur capacité de restauration.
- Désigner un responsable informatique interne ou externe
- Mise en œuvre d'une gestion des autorisations avec des niveaux de pouvoir appropriés
- Mesures de sécurité physiques pour empêcher l'accès non autorisé aux systèmes informatiques (p. ex. salle de serveurs fermée à clé)
- Cryptage de données numériques considérées comme sensibles selon les lois/ordonnances applicables en matière de protection des données.
- Le réseau doit présenter une séparation claire entre l'environnement IT et l'environnement OT
- Mettre en place une déclaration de protection des données sur son site web conforme aux lois sur la protection des données, notamment lorsque le site traite des données personnelles via des cookies.
- Pour les transactions financières, lorsque le bénéficiaire est nouveau ou a changé, utiliser un moyen vérifier l'authenticité de l'ordre de transaction par une procédure sécurisée.
- Vérifier l'authenticité d'une commande de marchandises
- Consultez régulièrement [le site web du NCSC](#) pour vous tenir au courant des derniers e-mails d'hameçonnage.
- Utilisez-vous des mots de passe sûrs ?
- Éviter d'utiliser des réseaux WLAN publics non sécurisés (attaques de type „man-in-the-middle“)
- Existe-t-il un plan de reprise après sinistre et/ou un plan de continuité des activités ?