Lettre Cyber 67

Juillet / août 2022

Une bonne hygiène informatique, c'est quoi ???

La sécurité informatique n'est plus une option. Cette sécurité doit se rapprocher des préoccupations économiques, stratégiques ou de la e-réputation. Voici, en 10 points, des mesures d'hygiène à respecter.

1/ Sensibiliser et former : Ces formations doivent porter sur la législation en vigueur, les risques et menaces, le maintien de la sécurité, l'authentification et le contrôle d'accès, le paramétrage, le cloisonnement et la journalisation.

2/ Identifier et cartographier vos systèmes : Identifier la totalité de vos outils numériques, créer un inventaire des comptes privilégiés et les maintenir à jour, organiser les arrivées et les départs ou les changements de fonction, limiter les connexions réseaux.

3/ Authentifier et contrôler les accès : Distinguer et identifier les accès au système, distinguer les rôles (Utilisateur / Administrateur), gérer l'attribution des droits, vérifier et gérer les mots de passe, protéger les mots de passe stockés sur le système, penser à changer les éléments d'authentification par défaut.

4/ Sécuriser les postes : Mettre en place un niveau de sécurité minimal sur le parc, se protéger des menaces relatives aux supports amovibles (station blanche), activer et configurer le pare-feu local des postes de travail, chiffrer les données sensibles transmises.

5/ Sécuriser le réseau : Segmenter le réseau avec cloisonnement, vérifier la sécurité des réseaux Wi-Fi et la séparation des usages, utiliser des protocoles réseaux sécurisés, mettre en place une passerelle d'accès sécurisé à internet, cloisonner les services visibles depuis internet, protéger la messagerie professionnelle, contrôler et protéger l'accès aux salles serveurs.

6/ Sécuriser l'administration : Utiliser un réseau dédié et cloisonné pour l'administration du système, limiter au maximum les droits d'administration.

7/ Gérer le nomadisme : Prendre des mesures de sécurisation physiques des terminaux nomades, chiffrer les données sensibles, sécuriser la connexion des postes nomades, adopter des politiques de sécurité.

8/ Se maintenir à jour : Définir une politique de mise à jour des composants, anticiper les fins de maintenance des logiciels et des systèmes d'exploitation.

9/ Superviser, auditer, réagir : Mettre en place une journalisation, mettre en place une politique de sauvegarde, procéder à des contrôles, désigner un référent SI, définir une procédure de gestion des incidents.

10/ Pour aller plus loin : Mener une analyse de risque, privilégier l'usage de produits et services certifiés, élaborer un plan de gestion de crise, de continuité d'activités et de reprise d'activités.

Recevoir cette lettre info par mail, envoyez-nous votre demande :
arnaud.schweitzer@gendarmerie.interieur.gouv.fr ou mathieu.knobloch@gendarmerie.interieur.gouv.fr

EXEMPLE SIMPLIFIÉ D'UNE CARTOGRAPHIE RÉSEAU