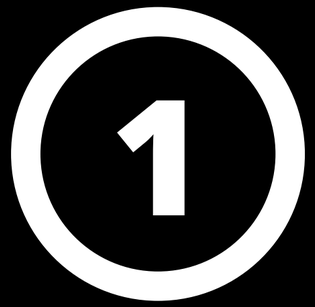

Mind-Data

La politique de sécurité de vos données



Authentification

La première étape vise à identifier la politique de l'organisme en matière de mot de passe, d'authentification et de vérrouillage de postes de travail. L'audit s'accompagne d'une démonstration de la vulnérabilité des mots de passe

- Identification de la politique de l'organisme en matière de mot de passe
- Identification de la politique en matière d'authentification et de vérrouillage des postes de travail

Habilitations

L'étape relative aux habilitations vise à déterminer la gouvernance des habilitations et la gestion des accès au sein de l'organisme, que ce soit au niveau de l'accès aux sessions, aux applications ou aux données réputées sensibles.

- Vérification des habilitations
- Gestion des accès au sein de l'organisme
- Vérification et gestion des accès aux sessions, aux applications ou aux données réputées sensibles

Incidents

L'audit vise à tester les infrastructures réseau et la réactivité des responsables de sécurité des systèmes d'information, au moyen de la réalisation de tests d'intrusion. L'évaluation porte notamment sur l'intégrité et la disponibilité des données en cas d'attaque informatique

- Audit des infrastructures réseau
- Évaluer la réactivité du responsable de sécurité informatique
- Évaluer l'intégrité et la disponibilités des données en cas d'attaque informatique

4

Poste de travail

L'audit vise à évaluer les pratiques individuelles en matière de vérrouillage ou d'accès aux postes de travail. En outre, cette étape de l'audit vise à apprécier l'actualité des systèmes d'exploitation au regard des dernières vulnérabilités et à assurer une mise à jour régulière du poste de travail

- Évaluer les pratiques individuelles en matière de verrouillage ou d'accès aux postes de travail
- Mise à jour des systèmes d'exploitation au regard des dernières vulnérabilités recensées

Mobile

L'audit vise à évaluer les vulnérabilités susceptibles d'affecter les terminaux mobiles de l'organisme et les risques induits de pénétration sur l'infrastructure générale

- Identification des vulnérabilités
- Identification des risques de pénétration sur l'infrastructure générale

Réseau

L'étape vise à conduire une analyse du réseau et des flux entrants et sortants afin d'apprécier la mise en place de protocoles d'échanges sécurisés. L'audit vise à mettre en place une politique d'usage du VPN et à sensibiliser sur les risques liés à la connexion au Wi-Fi public

- Apprécier la mise en place de protocoles d'échanges sécurisés
- Sensibilisation sur les risques liés à la connexion au Wi-Fi public

Serveurs

L'étape relative à apprécier l'actualité des serveurs et à procéder à leur mise à jour, à garantir l'accessibilité aux données et à mettre en place une politique d'accès aux outils et interfaces d'administrations. A l'issue de l'audit sur les serveurs, les usagers seront sensibilisés sur l'utilisation de l'HTTPS et les risques de récupération des mots de passe sur le Web.

- Audit de l'actualité des serveurs
- Mise en place d'une politique d'accès aux outils aux interfaces d'administrations
- Sensibilisation sur l'utilisation de l'HTTPS et sur les risques liés aux méthodes de récupération des mots de passe

8

Sauvegarde

L'audit en matière de sauvegarde vise à vérifier la régularité des sauvegardes données et à apprécier la politique de stockage des supports de sauvegarde. En outre, l'audit vise à prévoir les moyens de sécurité pour le transport des sauvegardes ainsi qu'à prévoir et tester régulièrement les plans de continuité d'activité qui peuvent être mis en place.

- Audit des procédures de sauvegarde des données
- Audit de la politique de stockage des supports de sauvegarde
- Réalisation de tests réguliers des plans de continuité d'activité au sein de l'organisme

Archivage

L'étape relative à l'archivage vise à apprécier les modalités d'accès aux données archivées et à mettre en place un mécanisme de destruction des archives obsolètes en conformité avec les mesures de sécurité technique élémentaires

- Audit des modalités d'accès aux données archivées
- Mise en place du mécanisme de destruction des archives obsolètes

Destruction des données

L'aspect relatif à la destruction des données vise à déterminer l'existence d'interventions de maintenance ou à mettre en place une politique permettant de retracer ces interventions. A l'issue de l'audit, une stratégie d'effacement des données sera mise en place afin d'être en conformité avec les principes liés à la protection des données personnelles.

- Mise en place de mécanismes de détection des interventions humaines
- Mise en place de dispositifs permettant de retracer les interventions
- Mise en place d'une stratégie d'effacement des données

11

Contrats de sous-traitance

L'étape relative aux contrats de sous-traitance vise à procéder à la révision de l'ensemble des contrats de sous-traitance afin d'apprécier la conformité de l'ensemble des clauses au droit lié à la protection des données personnelles et à prévoir les avenants permettant de mettre l'organisme et son client en conformité.

- Recensement et examen de l'ensemble des contrats des sous-traitance
- Elaboration des avenants permettant de rendre les dispositions contractuelles conformes au droit lié à la protection des données personnelles.
- Réalisation d'audits permettant de vérifier le respect des avenants aux contrats de sous-traitance

Echanges

L'étape relative aux échanges vise à déployer les logiciels permettant de procéder à des envois sécurisés en assurant le chiffrement, en amont, et la transmission par des canaux différents des données afin d'en conserver l'intégrité

- Mise en place de méthodes d'échanges sécurisés
- Examen et mise en place de canaux de transmission de données

Protection des locaux

L'étape relative à la protection des locaux vise à apprécier les principes en matière d'accès aux infrastructures de stockage des données et à vérifier les habilitations des personnels

- Examen des accès aux locaux
- Examen des habilitations des personnels

Développement

L'aspect de l'audit de sécurité relatif au développement vise à apprécier la conformité des développements informatiques envisagés et développés selon le principe de "privacy by design" au regard du droit lié à la protection des données personnelles puis à déployer des tests d'intrusion

- Audit du projet de développement de projet informatique
- Mise en conformité par défaut du développement informatique
- Réalisation de tests d'intrusion permettant de déceler les éventuelles failles susceptibles d'affecter le développement informatique

Chiffrement

L'étape relative au chiffrement vise à déployer des mécanismes de cryptage et de chiffrement des données de l'organisme lorsqu'elles sont traitées de manière active ou intermédiaire ou lorsqu'elles sont transmises à des tiers autorisés.

- Déploiement de méthodes de cryptage
- Déploiement de méthodes de chiffrement

Intégrité

L'étape relativeà l'intégrité vise à apprécier l'ensemble des mesures de sécurité technique ou opérationnelle permettant de préserver l'intégrité des données collectées, traitées ou stockées par l'organisme

- Déterminer les mesures de sécurité technique ou organisationnelle
- Déterminer les processus permettant de préserver l'intégrité des données

Signature

L'étape relative à la signature vise à assurer la traçabilité des modifications ou altérations apportées aux dossiers, fichiers ou données d'un organisme afin de déterminer les habilitations strictement nécessaires

- Déterminer les habilitations strictement nécessaires
- Déterminer la traçabilité des modifications ou altérations

CONTACT

Mind-Data