

Cybersécurité

Vie privée et Confidentialité de ses données sous Windows 10 ?

Microsoft collecte des données sous Windows 10 par plusieurs biais :

- **Le service de télémétrie** (connu sous les nom de Diagnostic Tracking Service ou de Universal Telemetry Client).
- **L'assistant personnel** Cortana et le composant Windows Desktop Search.
- Les **paramètres de personnalisation** de l'expérience utilisateur.
- **Les applications universelles de Microsoft** également appelées Windows Apps, Packaged Apps.
- L'utilisation de **comptes d'ouverture de session**.
- Le service de stockage dans le nuage **OneDrive**.

Les données recueillies par Microsoft peuvent être stockées et traitées aux États-Unis ou dans tout autre pays dans lequel Microsoft, ses filiales ou prestataires de service sont implantés.

<i>Le service de télémétrie</i>
• Des données sensibles et personnelles sont inévitablement collectées • Envoie d'information • Des informations du système d'exploitation et l'identifiant de l'appareil • Données de configuration matérielle • Logiciels, pilotes et micrologiciels installés • Données de performance • Le type d'appareil • Adapter le niveau de télémétrie au besoin de confidentialité (configuration un niveau de télémétrie le plus réduit possible au regard du besoin en confidentialité) • Activer le niveau de télémétrie de base/sécurité/télémétrie • Désactiver l'envoi de rapports par MSRT et Windows Defender

<i>L'assistant personnel</i>
• Envoyer des courriels ou des messages ; • Faire des recherches sur Internet ; • Exécuter des applications ; • Transmettre des rappels en fonction de l'heure, des rendez-vous et de la géolocalisation de l'utilisateur. • Désactiver l'agent personnel Cortana • Restreindre l'utilisation de Windows Desktop Search

<i>Paramètres de personnalisation</i>
• Des données de saisies clavier ou manuscrites • Des données de saisies clavier ou manuscrites • Les carnets d'adresses et de contacts

Durcir les paramètres de personnalisation de l'expérience utilisateur Désactiver la géolocalisation
--

<i>Les applications universelles</i>

Désactiver l'identifiant unique de publicité Maîtriser les applications universelles Restreindre les applications universelles et leurs accès Bloquer ou désinstaller les applications universelles
--

<i>Services dans le nuage</i>

Désactiver OneDrive

Cybersécurité : EDF stage deuxième année

Règles de cybersécurité

JOURNALISATION

- | |
|---|
| <p>Selon les besoins de sécurité du système, il est recommandé :</p> <ul style="list-style-type: none">• de privilégier les solutions de journalisation centralisées,• de s'assurer du bon horodatage des équipements pour que l'exploitation des journaux soit efficace,• de définir une durée de rétention minimum et maximum des journaux. |
|---|

CONNAÎTRE LE SYSTÈME D'INFORMATION; MAÎTRISER LES COMPTES ET ACCÈS

Pour chaque système, il est nécessaire de définir différents types d'accès (utilisateur, administrateur, exploitant...) et les conditions d'attribution des comptes. Les droits avancés ne sont donnés que si nécessaires et uniquement sur les fonctions nécessaires.

Les accès administrateurs se font en respectant les règles.
--

PRINCIPE DU MOINDRE PRIVILÈGE

Seuls les administrateurs chargés de l'administration des postes/équipements doivent disposer de ces droits lors de leurs interventions.

RÉSEAUX D'ADMINISTRATION DÉDIÉ

- | |
|---|
| <p>Selon les besoins de sécurité du système, il est recommandé :</p> <ul style="list-style-type: none">• de privilégier en premier lieu un cloisonnement physique des réseaux dès que cela est possible, cette solution pouvant représenter des coûts et un temps de déploiement importants ;• au minimum, de mettre en œuvre un cloisonnement logique par VLAN. |
|---|

SÉCURISER ET CLOISONNER LES SYSTÈMES D'INFORMATION

Cloisonnement et confinement : Afin d'avoir une segmentation efficace et simple à implémenter, il est nécessaire de l'intégrer dès la conception. Une segmentation du réseau doit être réalisée afin d'éviter une compromission des hôtes et particulièrement des machines sensibles. Un cloisonnement pourra se faire via des sous réseaux IP dédiés, des infrastructures dédiés ou des pare-feu. Ces éléments de cloisonnement devront être identifiés et supervisés. Ils pourront, dans le cadre d'une crise cyber sécurité, être utilisés afin de confiner un réseau ou un système.

- Une séparation des domaines de production (Nucléaire, Hydraulique,...) est nécessaire.
- Des protocoles sécurisés (http / https; ftp / sftp; telnet / ssh) doivent être autant que possible utilisés, que ce soit sur des réseaux publics ou sur des réseaux internes.
 - Les flux doivent être filtrés et restreints aux seuls flux nécessaires.
 - La méthode de chiffrement doit être robuste (AES).
- La méthode d'authentification doit être centralisée et de préférence doit utiliser des certificats client.
- L'administration du point d'accès doit se faire de manière sécurisée (réseau dédié et cloisonné, mise en œuvre d'un guide gestion des comptes,...)

Accès au réseau Internet : L'accès au réseau Internet se fait au travers des infrastructures proposées par la DSIT.

SUPERVISER ET AUDITER LES SYSTÈMES D'INFORMATION

Afin de disposer de journaux pertinents, il est nécessaire de déterminer, dès la phase de conception, les composants critiques du système d'information. Pour chacun de ces composants, il convient d'analyser la configuration des éléments journalisés (format, taille maximale des fichiers, ...). Une étude contextuelle du système d'information doit être effectuée afin d'identifier les scénarios d'attaques éventuels. Quelques exemples d'événements à journaliser sont les paquets bloqués (pare-feu), les échecs et succès d'authentification (systèmes et applications), les erreurs de protocoles (services).

La réalisation d'audits réguliers des systèmes d'information est essentielle car elle permet d'évaluer concrètement l'efficacité des mesures mises en œuvre et leur maintien dans le temps. Les systèmes à auditer peuvent, par exemple, être identifiés en fonction de la sensibilité. Plusieurs méthodes d'audit peuvent être mises en œuvre en fonction des attentes.

AUTRES RÈGLES

- Dépollution de son support amovible (clé USB avant toutes utilisations)
- Ne pas brancher quelconque appareil sur son poste (Téléphone portables, tablettes, ...)
 - Ne jamais laisser son poste allumé si l'on s'absente
 - Signaler si un mail ou un support est suspect
 - Gérer ses mots de passe
 - Recommandation KeePass
 - Déclarer une perte ou un vol
 - Usage pro-perso bien distinct
- Régulièrement exercice de test de phishing via boîte mail ou appel
- Beaucoup d'exercices de test de cyber pour préparer les usagers aux éventuels piratages ou risques.