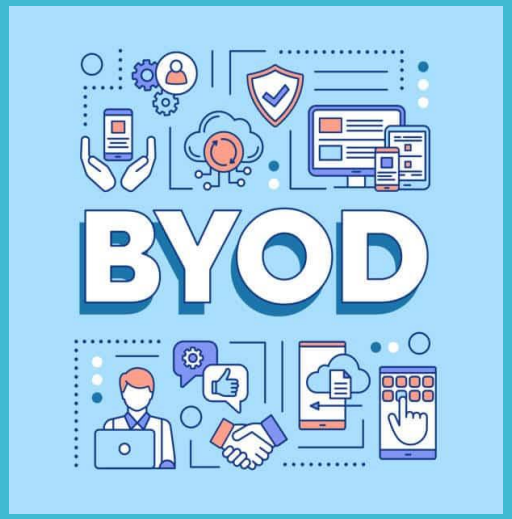
TP2 Bloc 3 :

Mise en place des bonnes pratiques BYOD

Maxence Hego
BTS SIO 1



Le BYOD est un acronyme pour Bring your own device ou amener votre matériel en français, il désigne la possibilité pour les salariés d'une entreprise d'**utiliser leur PC portable ou leur tablette** pour pouvoir travailler au sein de leur entreprise.

Cette pratique c'est énormément développé depuis la crise sanitaire de 2019 et le développement du télétravail.

Cependant si cette pratique comporte de nombreux avantage, elle comporte également des risques pour votre entreprise.

Nous verrons comment prévenir ou limiter ces risques.

Les outils essentiels :

Pour sécuriser votre poste informatique dans le cadre du BYOD, il est recommandé d'utiliser ces logiciels

VPN :
Vitual private Nework. Cet outil permet une connexion sécurisée et chiffrée pour accéder au réseau de l'entreprise.

Outils d'authentification à deux facteurs :
Garanti que seules les personnes autorisées accèdent à votre appareil. Ex : Microsoft Authentificator

Outil Patch management :
Permet de vérifier que toutes les mises à jour sont effectuées limitant ainsi les failles. Ex : Microsoft Endpoint Manager

Outils de chiffrements de données :
Permet de sécuriser les données sensibles de l'entreprise. Ex 7zip

Antivirus :
Nécessaire pour se protéger des malwares.

Pare Feu :
Permet de bloquer les connexions non autorisées

Système de visio-conférence certifié :
Pour garantir une utilisation conforme des données personnelles. Ex Tixéo

Gestionnaire de mots de passe : Pour conserver des mots de passe sécurisé. Ex KeePass/ZeniPass

Les logiciels interdit :

A l'inverse, certains logiciels ne doivent pas être présent sur votre outil de travail.

Les logiciels P2P ou peer-to-Peer : Ce sont des logiciels de partages des fichiers entre différents utilisateurs. Ils représentent un risque pour votre machine et les données de l'entreprise.

Logiciels de téléchargement illégal : Même raison

Stockage de données : Ne stocker pas vos données dans des Dropbox non validé par l'entreprise, risque de fuite.

Application de messagerie non sécurisées : Ex Telegram. Ne communiquez que sur les applications de messagerie fournit ou autorisé par l'entreprise.

Extension de navigateur non autorisé : Risque de Malware

De manière général, éviter de télécharger ou d'utiliser des applications non recommandées par votre entreprise.

Les outils de communication de l'entreprise :

Pour la communication au sein de l'entreprise veuillez favoriser les méthodes suivantes :

Outil de communication instané :
On retrouve comme application Slack ou encore Microsoft Teams

Application pour visio conférence :
Afin de communiquer avec vos collègues en distanciel vous pouvez utiliser l'un de ces logiciels : Zoom ou en alternative open source : Jitsi, BigBlueBottom

Outil de gestion de projet :
Afin de vous répartir les taches au sein d'une équipe, vous pouvez utiliser des logiciels comme Trello ou Asana. Wekan et Taiga sont des alternatives open source à ces deux logiciels.

Drive de stockage :
Permet de stocker les données dans un même espace accessible depuis plusieurs postes, que ce soit les vôtres ou ceux de vos collègues. Ex : OneDrive, GoogleDrive

VPN :
Permet de chiffrer les communications avec vos collègues

Mots de passe :

Afin de maintenir un accès sécurisé à vos appareils voici quelques règles pour les mots de passe

81 % des notifications de violations de données mondiales seraient liées à une problématique de mots de passe, voici quelques moyens pour vous protéger.

Mot de passe fort : Selon votre préférence, vous pouvez choisir parmi ces trois recommandations de la CNIL pour avoir un mot de passe sécurisé :

- 12 caractères avec majuscules, minuscules, chiffres et caractères spéciaux
- 14 caractères comprenant des majuscules, des minuscules et des chiffres
- Une phrase avec au minimum 7 mots.

Gestionnaire de mots de passe : Plutôt que modifier très légèrement le mot de passe que vous avez retenu, utiliser cet outil peut vous permettre de retenir plusieurs mdp fort. Ex ZeniPass

Authentification à deux facteurs : L'authentification à deux facteurs garanti une meilleure sécurité et est recommandé par la CNIL. Il s'agit le plus souvent d'un code à renseigner que vous avez reçu par mail ou SMS après avoir entré votre mot de passe. Ex : Microsoft Authentificator

Usage BYOD :

L'usage du BYOD a de nombreux avantages pour vous ou votre entreprise :

Pour Vous :

Le BYOD offre un **espace de travail plus confortable,** vous permettant de travailler sur des outils avec lesquelles **vous vous êtes familiarisé,** de plus le BYOD permet une certaine **flexibilité** dans votre organisation du travail vous permettant ainsi de trouver l'équilibre entre vie professionnelle et vie personnelle qui vous est idéal.

Pour l'entreprise :

Pour l'entreprise le BYOD permet de **réduire les coût** pour l'allocation du matériel, de plus on constate une **augmentation de la productivité** des salariés qui travaillent dans un environnement de travail qui leur est familier.

Usage BYOD :

Cependant l'usage du BYOD comporte de nombreux risques pour vous ou l'entreprise si vous n'adopter pas les bonnes pratiques

Un usage **non conforme** du BYOD peut entraîner **une fuite des données** de votre entreprise ou la contamination de votre poste puis du réseau de l'entreprise par **un malware.**

Quelques exemples :

Un ingénieur travaillant sur les plans des JO de Paris 2024 **s'est fait volé son PC** dans un train le 26 février. Cet incident a conduit à une perte d'image pour la mairie de Paris. Cet incident a pu se produire en raison d'une politique de BYOD. Article correspondant

En 2019 un salarié de Thales **s'est fait voler son ordinateur portable** contenant des données miliaires sensible. Article du figaro

En 2013 l'entreprise américaine Target a subi **une cyberattaque** rendu possible par l'ordinateur portable d'un salarié qui a été **infecté par un malware,** un tiers des données de la population américaine touché par cette attaque. Article correspondant

Il est donc nécessaire d'appliquer les recommandations listées précédemment.

THALES

Usage BYOD :

Pour aller plus loin et vous familiariser avec les enjeux du BYOD voici quelques ressources:

Site de la CNIL :

https://www.cnil.fr/fr/byod-quelles-sont-les-bonnes-pratiques
www.cnil.fr/fr/salaries-en-teletravail-quelles-sont-les-bonnes-pratiques-suivre

Guide utilisateur :

Si l'entreprise le souhaite elle peut également développer un guide d'utilisateur qui listes les bonnes pratiques BYOD ainsi qu'une fiche de référence qui donne un exemple de bon poste BYOD

Formation :

L'entreprise peut également organiser des formations, par vidéo ou par un intervenant, afin de former aux mieux les salariés.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS