adw network
Vos réseaux sans fil en toute sécurité

WiFi'BYOD : service d'intégration sécurisée des équipements personnels des collaborateurs

La nouvelle tendance du BYOD « Bring Your Own Devices »

Au sein de votre établissement, de nombreux collaborateurs utilisent de plus en plus leurs équipements personnels pour travailler (ordinateurs portables, tablettes, smartphones, …). Pour les responsables informatiques et responsables de la sécurité comment gérer cette problématique ?

Les impacts et les risques du BYOD

- **Accès aux données confidentielles de votre structure**

Un visiteur quel qu'il soit peut accéder à l'ensemble de vos informations interne si votre réseau WiFi est mal protégé. Vos données sont accessibles par n'importe qui.

- **Fuite des données professionnelles**

Vos collaborateurs vont utiliser leurs terminaux pour consulter, transférer et stocker des données souvent stratégiques voir confidentielles à l'entreprise. Un terminal non maitrisé facilitera la fuite de vos données pour les Hackers informatiques.

- **Propagation de virus au sein de l'entreprise**

En utilisant leurs propres matériels, vos employés devront se connecter au réseaux interne de l'entreprise. Un matériel non protégé peut engendrer la propagation de virus et causer de nombreux dégâts.

- **Saturation des connexions WiFi**

Un grand nombre de terminaux connectés augmentera conséquemment le nombre de connexion au réseau WiFi de votre structure. Il est important de redimensionner vos installations pour une meilleure connectivité.

- **La non-conformité de la loi**

Chaque structure proposant un accès Internet doit être conforme à la loi relative à la lutte contre le terrorisme c'est-à-dire de répondre aux exigences légales de sécurité et de traçabilité en conservant l'ensemble des données de connexion.

Tél 04 78 58 39 53 contact@adw-network.com www.adw-network.com

adw network
Vos réseaux sans fil en toute sécurité

WiFi'BYOD : service d'intégration sécurisée des équipements personnels des collaborateurs

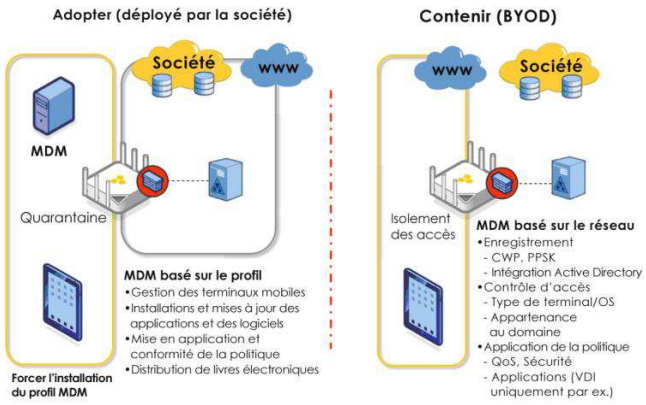
WIFI'BYOD est une prestation d'assistance technique d'aide à la mise en place d'une stratégie de sécurisation des accès wifi pour les équipements personnels de vos collaborateurs.

Notre solution en 2 points s'articule autour de 2 points essentiels :

♦ La connexion des utilisateurs au réseau

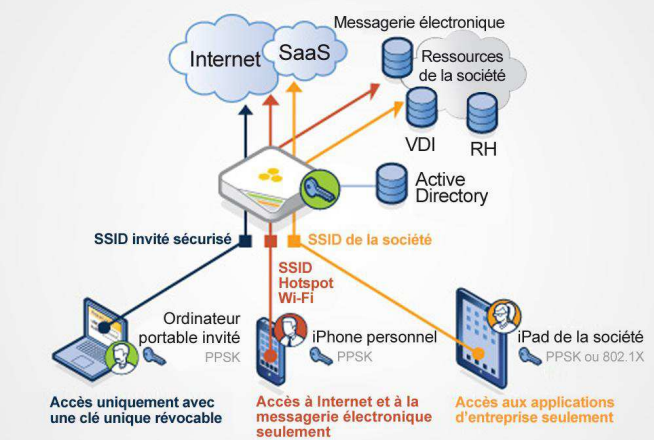
Il existe 2 politiques pour les DSI :

- Soit une solution s'appuyant sur des logiciels dits MDM (Mobile Device Management) pour intégrer les équipements personnels des employés au sein de l'entreprise. Ces logiciels en mode agent s'assurent que les terminaux connectés disposent des bons logiciels, droits d'accès et paramètres de sécurité avant de les autoriser à se connecter au réseau.
- Soit une solution qui repose sur les périphériques réseau (WiFi et LAN) pour gérer les connexions des terminaux. Il n'y a pas d'agent à installer sur le terminal client. C'est particulièrement à ce niveau que nous apportons notre expertise radio pour proposer et mettre en place la sécurisation des accès WiFi.



♦ Authentification et accès

- Autoriser la connexion des équipements personnels des employés nécessite des solutions d'authentification et de gestion des accès. A moins d'installer sur ces équipements des certificats (802.1x) qui peuvent devenir très complexes à gérer, d'autres solutions de type « hotspot » WiFi permettent de gérer simplement ces connexions.
- Une solution s'appuyant sur des couples login/password, l'association avec une Mac adresse et la reconnaissance du profil d'utilisateur (serveur radius et /ou annuaire LDAP) permet d'authentifier les utilisateurs, la traçabilité et de limiter leurs accès aux ressources internes en fonction de leurs profils.



Notre service WIFI'BYOD vous accompagne dans la mise en place d'outils et d'applications pour intégrer en toute sécurité les terminaux personnels des employés au sein de votre architecture réseau

Cette prestation se décompose en trois étapes :

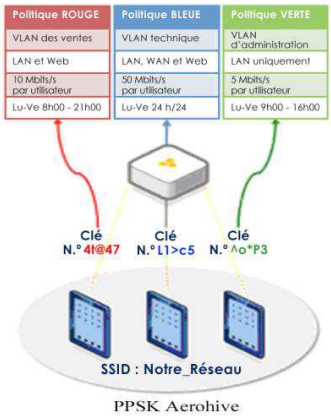
1/ Audit complet de votre infrastructure WiFi et Lan (nombre de jours en fonction de la complexité de votre réseau).

2/ Recommandations et préconisations pour la mise en place d'une stratégie BYOD.

3/ Assistance technique pour la mise en place d'une passerelle de sécurisation des accès WiFi ou la configuration des équipements WiFi déjà installés si cela est possible.

[3 schémas : source AEROHIVE]

Exemple de PSK type



PPSK Aerohive

Tél 04 78 58 39 53 contact@adw-network.com www.adw-network.com