Principes de la sécurisation des connexions réseaux par authentification de l'utilisateur avec le protocole 802.1x

La sécurisation des accès au réseau de l'organisation répond à plusieurs cas d'usages :

- accès depuis Internet et en interne à
    - des utilisateurs à privilèges pour des tâches d'administration,
    - des utilisateurs de l'organisation pour accèder à des applications métiers,
    - des partenaires de l'organisation pour des services spécifiques.
      * accès en interne :
    - par le réseau filaire,
    - par le Wi-Fi.

L'organisation peut égaleemnt proposer un accès uniquement à Internet, depuis le réseau internet, généralement apr el Wi-Fi.

- otsçi regroupe concerne plusireur casd d'usaeue sujeiru périmètres répond à plusieurs objectifs :
- itr

Si les réseaux Wifi utilisés dans les entreprises voient désormais leurs accès relativement sécurisés (par du chiffrement WPA2 par exemple) et si les accès depuis l'Internet font l'objet de technologies sécuritaires bien établies (DMZ, pare-feux, UTM …), les prises murales sur lesquelles sont connectés les postes fixes des espaces de travail sont, dans la majorité des entreprises, “ouvertes à tous les vents” et toute personne circulant dans l'entreprise peut s'y connecter et s'introduire sur tout ou partie du réseau. L'objectif final visé par la mise en place du couple de technologies 802.1x / RADIUS va au delà de la simple sécurisation des accès par une authentification “forte” de la personne qui cherche à se connecter sur un port réseau. Cet objectif pourra aller jusqu'à la banalisation de toutes les prises réseau filaires de l'entreprise. Une prise réseau quelconque ne sera plus affectée à tel ou tel VLAN. C'est à partir de l'authentification de la personne qui cherche à se connecter au réseau que l'on va déduire le périmètre de sécurité dans lequel la placer : • Un refus pur et simple de connexion : aucun placement ; • Le placement dans un VLAN invité (“guest”) avec des prérogatives minimales, comme la simple obtention d'une adresse IP et d'un accès à Internet ; • Le placement dans un VLAN dédié, choisi en fonction notamment du service ou du groupe auquel appartient la personne ; • Le placement dans un VLAN à prérogatives importantes, comme un VLAN d'administration. Il existe des technologies de filtrage sur les adresses MAC : soit circonscrites à un commutateur (doté pour chacun de ses ports, d'une liste d'adresses MAC autorisées) ou même centralisées dans un serveur RADIUS. On sait maintenant que l'adresse MAC n'est plus un élément d'authentification fiable. Pour cette raison et pour le côté malaisé de la manipulation, et surtout de la récupération des adresses MAC (particulièrement quand il s'agit de postes appartenant à des personnes extérieures à l'entreprise), on laissera ces technologies de côté dans ce document.

Retour Authentification 802.1x

- Authentification réseau avec le protocole 802.1x

From:
/ - **Les cours du BTS SIO**

Permanent link:
/doku.php/reseau/802.1x/presentation?rev=1696688345

Last update: **2023/10/07 16:19**