Information pour les utilisateurs wireless: 10 conseils pour sécuriser votre connection

i

Pour vous aidez nous avons récapitulés les mesures à prendre pour avoir une connexion wireless sécurisé. Parfois les constructeurs d'équipements wireless ne fournissent pas les informations nécessaires pour sécuriser votre accès. De ce fait il est compréhensible que ce ne soit parfois pas clair, comment vous pouvez protéger votre réseau sans fil contre des intrusions. Dans l'article suivant, nous avons énuméré tous les points importants pour protéger votre réseau sans fil. Avec l'aide de cet article et du manuel d'instruction de votre produit, vous devriez pouvoir garantir une bonne sécurité. Pas toutes les mesures de sécurité mentionnées sont supportés par tous les équipements. Svp n'oubliez pas: En suivant cette directive vous protégez non seulement votre réseau sans fil, mais également toutes vos données et applications!

1

Activez le codage WEP (attention : vous devez l'activer sur l'access point aussi bien que sur toutes les cartes wireless). Employez toujours au minimum un codage sur 128-bits.Ne choisissez pas une suite de caractères simple comme clef mais une suite complexe par exemple A9FE10. Changez la clef WEP régulièrement.Cette mesure vous donne une meilleure sécurité et protège vos systèmes contre l'accès non désiré par des tiers.

2

Activez sur l'access point le control d'accès basé sur l'adresse MAC (adresse de la carte réseau) Entrez les adresses MAC des cartes réseaux que vous allez utilisez. Cette mesure évite que des tiers accède votre réseau.

3

Nommez votre SSID/ESSID d'une manière à ce qu'aucune corrélation de nom ne peut être faite entre le nom du réseau et celui du propriétaire. **Le propriétaire de l'access point ne peut pas être identifié par le nom du réseau.**

4

Cachez votre SSID. (AUCUNE diffusion du SSID). **Cacher le SSID rend votre réseau non public. Soyez prudent, en faisant ainsi pouvez également vous couper de votre propre access point.**

○ Mesure requise
● Mesure optionnel
[i] Information
[S] Support
[§] Information légale
[!] Important

5

Changer fréquemment votre username/password sur votre access point. Choisir un password compliqué, car les simple peuvent être deviné facilement.

6

Si vous n'utilisez pas votre connexion wireless pendant une longue période, éteignez votre access point. Ceci évite toute tentative d'intrusion durant cette période

7

Ne reliez pas votre access point à votre LAN interne si vous n'êtes pas suffisamment protégé contre des attaques de l'extérieur. Protégez vos share réseau avec un mot de passe, augmentez votre protection d'accès sur les postes de travail et les serveurs.

8

Protéger vos PC's et serveurs avec un software firewall. **Activer la protection d'accès sur tous vos systèmes**

9

Ne pas écrire le mot de passe, et ne pas utiliser 2 fois le même. Ceci réduit la probabilité d'une intrusion.

10

Vérifier votre fichier de log, pour détecter d'éventuelles attaques.

S

Vous pouvez avoir du support pour vos différents problèmes sur le forum de discussion indépendant suivant :

www.wireless-forum.ch

W)))) F
Wireless-Forum

§

Prenez garde aux réseaux wireless non protégés. Vous pourriez avoir des problèmes juridiques si quelqu'un utilise illicitement votre access point

!

D'après la statistique établie par: www.wireless-bern.ch approx. **60%** des access point **ne sont pas encryptés.**
Remarque : La plupart des fonctions de sécurité mentionnées ci-dessus sont inactive lorsque vous achetez votre produit sans fil.