

## Rédaction - Administration - Publicité

POLYMEDIA MEICHTRY SA  
Chemin de la Caroline 16  
CH-1213 Petit-Lancy - Genève  
Tél.: +41 (0)22 879 88 20  
Fax: +41 (0)22 879 88 25  
se@polymedia.ch - www.polymedia.ch  
UBS-Genève 240-439-025-00L  
IBAN: CH53 0024 0240 4390 2500 L  
SWIFT: UBSWCHZH12A  
CCP 12-1684-7

## Directeur général - Rédacteur responsable

Marcel Meichtry

## Rédaction et conseillers à la rédaction

Rédacteur en chef:  
Michel Giannoni, Ing. EPFL, Dr ès sc.  
m.giannoni@polymedia.ch

Rédacteur:  
Cedric Favre, ing. HES  
c.favre@polymedia.ch

Conseillers:  
Alain Henchoz, Dr es Sciences EPFL  
Olivier Lévy, Avocat

## Marketing et annonces Suisse romande:

Cedric Favre, ing. HES  
c.favre@polymedia.ch  
Tél.: +41 (0)22 879 88 20 - Fax: +41 (0)22 879 88 25

## Régie des annonces Suisse alémanique:

AXA Media  
Ludwig Binkert, Postfach 112, CH-4143 Dornach 2  
Tél.: +41 (0)61 703 14 35 - Fax: +41 (0)61 703 14 39  
binkert@axamedia.ch - www.axamedia.ch

## Administration, ventes

Marie-Christine Freund  
mc.freund@polymedia.ch

## Fabrication

Alex Loew  
a.loew@polymedia.ch

## Prix et parution

Le numéro:  
Suisse (TVA incluse) CHF 6.-  
Etranger CHF 14.-

Abonnements: 1 an 2 ans  
Suisse (TVA incluse) CHF 40.- CHF 70.-  
Etranger CHF 60.- CHF 100.-

Depuis le 1<sup>er</sup> janvier 1989, la revue **Sécurité Environnement** (4 fois/an) est couplé à **La Revue Polytechnique** (11 fois/an + numéros spéciaux). L'abonnement donne droit aux deux publications.

Les articles ne peuvent être reproduits ou traduits qu'avec l'autorisation écrite de la rédaction. Les auteurs des articles publiés ont seuls la responsabilité des théories et opinions qu'ils émettent.

Impression: SRO-Kundig SA, Genève

ISSN 0254-1262

## Sans fil mais pas sans soucis

Par Cedric Favre

Une récente étude sur la sécurisation des réseaux informatiques nous apprend que 20 % des réseaux sans fil d'entreprise ne sont pas protégés, ne serait-ce que par un protocole de cryptage. Et ceci dans trois principaux centres d'affaires que sont Paris, Londres et New York. Que le quidam qui achète son routeur *wireless* ne se soucie guère de la sécurité, on le comprend, mais une entreprise? Même si un fabricant de lacets n'a bien sûr pas le même intérêt qu'une grande banque pour les pirates modernes.

L'évolution des systèmes de sécurité pour les réseaux sans fil - et dans d'autres domaines également tels que les systèmes d'exploitation, les paiements électroniques, ... - fait invariablement évoluer les systèmes de piratage. C'est le principe du chat et de la souris (sans jeu de mot) ou du gendarme et du voleur. Nous avons affaire à: soit un jeu consistant à savoir qui réussira en premier à décrypter le protocole, soit un métier destiné à saisir des informations sensibles, à les exploiter ou à les revendre. Internet regorge d'outils permettant, même à l'amateur, de «craquer» le réseau de son voisin.

Alors pourquoi s'embêter à sécuriser son petit réseau en codant tous les paramètres avec des clés de chiffrement que l'on n'arrive pas à retenir, dans l'encyclopédie de tous nos mots de passe? Et avec des algorithmes toujours plus compliqués et, forcément, qui ralentissent de plus en plus nos transmissions. Pourquoi se masquer en cachant son identifiant, risquant de ne plus pouvoir s'y connecter avec un nouvel ordinateur? Tout cela fait partie des difficultés croissantes que l'on rencontre avec des appareils qui devraient, au contraire, nous faciliter la vie. Un minimum de sécurité est certes nécessaire pour empêcher des voisins malveillants d'utiliser votre sortie sur Internet - avec votre «signature» - pour naviguer dans des eaux troubles.

Quelques recommandations sont accessibles par le lien figurant sur notre site Internet. On y trouve, par exemple, que les adresses physiques des cartes réseaux doivent être enregistrées dans le routeur, que l'identité du serveur d'accès sans fil doit être nommé de façon vague afin qu'il ne puisse pas être reconnu, enfin qu'un audit régulier des réseaux *Wifi* devrait avoir lieu. Mais qui peut se le permettre? Les grandes entreprises avec leurs ingénieurs et spécialistes. Et pour les plus petites structures, ce sont les consultants qui peuvent venir en aide.

Pour les amateurs de sensations fortes, un nouveau type de fraude apparaît gentiment dans les villes: le *rogue hotspot* ou *hotspot* frauduleux. Comme un pot de miel, il est installé très temporairement, même simulé sur un ordinateur portable. Son but: subtiliser des informations confidentielles comme votre numéro de carte de crédit. Sa durée de vie est très courte pour éviter qu'il soit détecté.

Les réseaux sans fil ne riment pas encore avec «sécurité absolue».



## Sommaire

3/07 Septembre

### Articles

<b>SECURITE:</b>	
Des variateurs pour un entraînement sécurisé	..5
La protection contre les rayonnements électromagnétiques	.....6
Réseaux sans fil et sans filet	.....8

### ENVIRONNEMENT:

La culture d'entreprise sous les feux de la rampe	.....11
La pollution sonore	.....12
La valorisation des appareils électriques ou électroniques hors d'usage	.....14
Le Programme national de recherche sur l'utilité et les risques des plantes génétiquement modifiées	.....16

### Magazine

Des entreprises	.....4
-----------------	--------

Bibliographie	.....15
Technique	.....17
Le guide de la sécurité	.....18

### Informations générales

Conférence internationale sur le changement climatique et le tourisme	.....4
Le rôle des puits de carbone réévalué	.....10
Un appareil qui absorbe le gaz carbonique	.....13