



Trusted Application®

by  BeeWare



# Les 7 mythes de la sécurité Web

## Ce qu'il faut impérativement savoir pour prendre les bonnes décisions

Avec les virus, les spams et autres malwares, la sécurité informatique apparaît comme un monde complexe et une affaire de spécialistes. Les entreprises investissent dans la protection de leurs réseaux à l'aide de firewalls et de détecteurs d'intrusions. Les utilisateurs protègent leur poste de travail à l'aide d'antivirus. Mais qu'en est-il de la sécurité d'un site Web, de l'application mise en ligne et de la responsabilité de ses dirigeants ?



### 1 Mon application est 100 % fiable et sécurisée

**FAUX**

**L'application sans bug n'existe pas.**

Une faille de sécurité n'est rien d'autre qu'un bug qui, en outre, est souvent considéré d'importance secondaire par les développeurs dont le métier et l'objectif premier ne sont pas la sécurité mais la rapidité et le résultat fonctionnel. Une situation encore aggravée par la fréquence d'évolution des applications Web et les délais de mise en ligne qui laissent peu de temps pour réaliser des tests de sécurité.

### 2 Mon hébergeur sécurise mon application

**FAUX**

**Il sécurise l'infrastructure réseau et système.**

Un hébergeur sécurise son architecture à l'aide de firewalls et de détecteurs d'intrusions qui fonctionnent au niveau du réseau et dont le but consiste à protéger l'infrastructure d'hébergement.

Mais ces défenses s'avèrent inutiles lorsqu'il s'agit d'éviter qu'un utilisateur mal intentionné détourne à son profit un formulaire ou un script dont le code serait insuffisamment sécurisé.

# Les 7 mythes de la Sécurité Web

Ce qu'il faut impérativement savoir pour prendre les bonnes décisions

## INFO & CONTACT

09 74 76 74 02 (coût d'un appel local)

✉ info@prowebserenity.com

www.prowebserenity.com

### Sans paiement en ligne, un site ne court aucun risque

#### FAUX

**Les cybercriminels ciblent toutes sortes de bases de données.**

Même si les cartes de crédit sont une cible convoitée des pirates, les données de paiement en ligne ne représentent qu'un faible pourcentage des vols réalisés.

La très grande majorité des données recherchées réside dans des bases de données commerciales ou marketing : listes d'invités, de clients, de commandes, résultats financiers ... autant de données qui s'achètent et circulent sur les réseaux du banditisme moderne.

### La technologie SSL sécurise les Applications

#### FAUX

**SSL protège le paiement, mais ni vos applications ni vos données.**

La technologie SSL a été développée pour sécuriser l'authentification et la confidentialité des flux de données. Elle établit un canal chiffré entre le serveur et le navigateur du poste client mais n'inspecte pas les données véhiculées.

Les pirates ont même une préférence pour les sites en SSL ou HTTPS puisque leurs attaques, cryptées, deviennent invisibles des sondes de détection d'intrusion. SSL protège la communication mais pas les données qui restent stockées en clair sur les serveurs.

### Mon assurance Responsabilité civile couvre mon activité Web

#### FAUX

**Une activité Web nécessite une assurance « du fait du site ».**

L'assurance Responsabilité civile d'une entreprise couvre son activité traditionnelle. Dans le cas de la création ou de l'extension d'une activité via un site Web, une assurance responsabilité civile complémentaire dite « du fait du site » doit être souscrite.

### Mon site Web n'intéresse pas les pirates

#### FAUX

**Même un site vitrine, vide de contenu, peut servir de piège.**

Ce n'est pas parce qu'un site ne contient pas de données de valeur qu'il ne sera pas la cible d'attaques. En effet, à travers les sites Web, les cybercriminels visent souvent les internautes et les codes d'accès stockés sur leurs postes. Leur technique consiste à déposer des « pièges » logiciels sur des sites anodins qui vont ensuite infester les machines des visiteurs. Le dommage pour le site ne se situe pas au niveau des données, mais de sa réputation qui est immédiatement ternie.

### La sécurité est coûteuse et complexe à installer

#### FAUX

**Le tarif Pro Web Serenity commence à quelques dizaines d'euros par mois.**

Il n'y a pas obligation à acheter et à installer des équipements pour se sécuriser. Bee Ware propose des solutions économiques, basées sur le filtrage de votre trafic, disponibles sous forme d'abonnement et sans investissement préalable.



Bee Ware SA  
210, Avenue Frederic Joliot  
13852 Aix-en-Provence Cedex  
France

Tél : + 33 (0)4 88 19 60 10  
Fax : + 33 (0)4 42 38 28 62  
www.bee-ware.net

Bee Ware est éditeur de solutions de protection des applications Web depuis 2001. L'offre de Bee Ware est aujourd'hui constituée d'une suite complète dédiée à la protection des sites et applications Web. i-Watch, Analyse des applications basée sur le monitoring du trafic, i-Sentry, Firewall Web et XML, et i-Trust solution de Web SSO, répondent ainsi à l'ensemble de la problématique : Performance, Sécurité et Authentification. Conception / réalisation : indexel - Photo ©2009 JupiterImages