

Bases essentielles pour sécuriser son site web | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer



LE NET EXPERT
AUDITS & EXPERTISES



EXPERTISES DE SYSTEMES DE
VOTES ELECTRONIQUES
LE NET EXPERT
fr



LE NET EXPERT
MISES EN CONFORMITE



LE NET EXPERT
FORMATIONS



LE NET EXPERT
ARNAQUES & PIRATAGES



Bases
essentielles
pour
sécuriser
son site web

Il faut savoir qu'internet peut se révéler vulnérable. La sécurité d'un site n'est pas à prendre à la légère, c'est quelque chose de très compliqué qui requiert des connaissances techniques approfondies afin de pouvoir identifier les vulnérabilités et mettre en place les mesures de protection nécessaires.

La sécurité d'un site web est un enjeu crucial et essentiel pour tout administrateur système soucieux de préserver et protéger son site. Les hackers sont toujours à la recherche de nouvelles failles, mais de multiples solutions de sécurité s'offrent à vous de plus simples et de plus pointues qui vous permettront de lutter contre les pirates et les hackers et protéger son site internet.

Voici quelques simples conseils sous forme d'une liste de bonnes pratiques qu'un professionnel doit appliquer à la rigueur pour se défendre des attaques automatiques et empêcher ceux qui visent votre site web d'y pénétrer :

1. Veiller sur la mise à jour de votre site web

Il faut d'abord veiller à mettre à jour correctement le serveur web qui héberge le site. Si vous faites appel à un hébergeur professionnel, c'est son travail. Par contre, si vous héberger votre site vous-même c'est à vous de faire les mises à jour nécessaires. Ensuite, le système de gestion du site doit également être à jour, ainsi que toutes les applications qui jouent un rôle dans l'administration du site.

Certains systèmes de gestion de contenu comme WordPress permettent d'effectuer facilement les mises à jour automatiquement. Comme ils offrent aussi une quantité très importante de plugins dont certains peuvent présenter des failles flagrantes. Je vous conseille alors de bien vous renseigner sur la qualité et l'efficacité d'un plugin avant de l'installer.

2. S'assurer du sauvegarde et de la protection

N'oubliez jamais d'effectuer une sauvegarde régulière pour votre site web et aussi que pour toutes les autres informations. Sa fréquence dépendra de la fréquence de la mise à jour du site, c'est-à-dire que vous devrez faire une sauvegarde de votre site à chaque fois que vous le mettez à jour. Vous vous rendrez compte de la grande valeur de cette sauvegarde le jour où votre site sera piraté malgré les précautions que vous avez prises.

Enfin, vous devez protéger l'accès au serveur web pour éviter les tentatives d'attaque du site. Par exemple, l'authentification http et l'une des pratiques sur laquelle vous pouvez compter pour protéger votre serveur web.

3. Protéger les données sensibles

Lorsque vous collectez des données personnels, mots de passe, données financières, il faut veiller sur leur sécurité mieux que tout le reste. Il s'agit non seulement d'une obligation vis-à-vis de vos utilisateurs mais aussi d'une contrainte légale.

Il est indispensable que vous chiffriez toutes les données stockées sur vos serveurs. Il faut aussi chiffrer la connexion (SSL) pour éviter que des données soient interceptées lors de la communication entre l'utilisateur et votre site.

Vous devez faire des mots de passe l'objet d'un soin tout particulier pour assurer plus de sécurité, pour cela ils doivent être cryptés avant d'être stockés.

Comme vous devez aussi « hacher » les mots de passe avec un algorithme approprié comme «bcrypt » ou « scrypt » qui sont difficiles à être attaqués, et évitez les usuels MD5 et SHA1 qui sont plus vulnérables.

4. Vérifier la sécurité de votre hébergeur

C'est une astuce de sécurité d'ordre plus général, il est très important que votre hébergeur vous propose des versions plus récentes de Apache, MySQL et PHP. Renseignez-vous auprès de votre hébergeur ou utiliser un fichier PHP pour obtenir ces informations cruciales.

5. Créer votre site web avec Wix

Vous pouvez choisir des outils qui vont sécuriser votre site à votre place.

Pour ceux qui veulent se simplifier la vie et choisir une solution aussi sécurisé que pratique, il existe Wix. Lire la suite...



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet..) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Bases essentielles pour sécuriser son site web | FunInformatique