Forum: The Blender Clan 'tchat

Topic: Avenir du blender clan

Subject: Re: Avenir du blender clan

PostÃ© par: Bibi09

Contribution le : 15/6/2021 7:59:49

Les problèmes de sécurité ont lieu à différents niveaux : 1. l'hébergeur et 2. l'administrateur du site. Ca dépend donc, dans un premier temps, de la solution d'hébergement.

En terme d'hébergement, on peut parler de la sécurité du serveur lui-même (règles pour Apache, règles de parefeu, protection contre les DDoS, etc). Donc si c'est un site auto-hébergé, là oui il faut se prendre le chou sur la mise en place de règles de sécurité et un expert en la matière est requis. Pour un site hébergé par un professionnel, ce genre de chose devrait déjà être grandement pris en charge. Pour rappel, un professionnel a des obligations en terme de qualité de service.

Un autre point de sécurité, et c'est majoritairement le cas des attaques que tu décris Redstar, c'est au niveau de la base de données puisqu'elles contiennent les données personnelles.
Si on développe notre propre site/forum, il est évident qu'il faut maîtriser le sujet des connexions à la base de données : chiffrement des informations, qualité du chiffrement, stockage des identifiants pour se connecter à la base de données, etc.
Si on passe par une plateforme clé en main de type WordPress ou Drupal, il faut lui faire confiance. Cependant, des failles de sécurité/backdoors sont régulièrement détectées et il faut donc se tenir au courant des mises à jour de ces plateformes pour les corriger. C'est à l'administrateur du site d'opérer ces mises à jour, souvent automatisées ou, pour les cas plus complexes devant être réalisés manuellement, bien documentées.
Quand tu parles d'administrations piratées, comme malheureusement les hôpitaux, cela est souvent dû à un manque de mises à jour de leurs logiciels. Du coup, les pirates peuvent aisément exploiter des failles découvertes des années auparavant. Un exemple ici, même si c'est pas directement lié à du piratage. L'article précise toutefois les problèmes de sécurité liés à cette obsolescence.
https://www.lemonde.fr/pixels/article/2015/11/11/une-panne-informatique-a-l-aeroport-d-orly-liee-a-windows-3-1_4807479_4408996.html

Il y a aussi les droits sur les fichiers hébergés, en particulier ceux qui servent à faire tourner le site (par exemple des scripts .php ou .py). Là, la personne en charge du site y applique sa responsabilité. Cependant, si on suit rigoureusement les recommandations des plateformes installées on ne devrait pas trop s'en soucier. Par exemple en suivant l'installateur d'un WordPress, à la façon dont on installe un programme sous Windows, celui-ci donne des indications sur les droits d'accès à des fichiers ou dossiers sensibles à son bon fonctionnement.

Enfin, gérer les certificats de sécurité pour chiffrer les communications et éviter qu'un pirate ne capte par exemple les identifiants et mots de passe des utilisateurs. On comprendra aisément que l'intérêt principal, c'est de voler ceux d'un administrateur qui a tous les droits sur le site en question.

Sans certificat comme sur le BC actuel, les données sont envoyées en clair. Une attaque de type "man in the middle" servirait donc à connaître les identifiants et mots de passe de chacun d'entre nous. Notez qu'apparemment, le BC ne souffre pas de ces lacunes puisque le site fonctionne toujours bien.
Avec un certificat, les identifiants et mots de passe sont chiffrés et donc il est plus difficile d'usurper l'identité de quelqu'un.

Pour écrire ce message, j'ai fait appel à mes souvenirs en sécurité. Je suis pas du tout un pirate et encore moins un Anonymous !