Tips Mengamankan Website

Oleh Adi Sumaryadi

Website merupakan salah satu media untuk menyampaikan informasi yang penting ke pengguna internet diseluruh dunia, informasi ini tentunya akan terganggu bahkan menjadi menjadi hal yang tidak diinginkan ketika websitenya dihack oleh orang yang tidak bertanggungjawab. Untuk mengurangi resiko jebolnya website milik kita ada beberapa tips sederhana yang bisa anda gunakan

Website merupakan salah satu media untuk menyampaikan informasi yang penting ke pengguna internet diseluruh dunia, informasi ini tentunya akan terganggu bahkan menjadi menjadi hal yang tidak diinginkan ketika websitenya dihack oleh orang yang tidak bertanggungjawab. Untuk mengurangi resiko jebolnya website milik kita ada beberapa tips sederhana yang bisa anda gunakan :

1. Amankan semua informasi yang berhubungan dengan account hosting anda jika website anda dihosting disebuah provider, mulai dari informasi password hingga account filemanager. Biasakan anda untuk selalu logout setelah menggunakan control panel apalagi ketika menggunakannya bukan dikomputer milik kita pribadi.

2. Gunakan uploader yang benar-benar aman jika anda akan mengupload file-file web anda ke server, lebih baik menggunakan SCP atau SecureCopy dari pada menggunakan FTP biasanya, jika anda terpaksa menggunakan FTP, gunakan FTP dalam mode secure atau SFTP supaya data anda terenkripsi saat pengiriman, bagaimanapun cracker selalu memanfaatkan celah yang memungkinkan untuk menguasai sebuah website.

3. Proteksi semua folder dan matikan semua direktori listing yang ada di dokumen root website anda, proteksi bisa menggunakan setting dari webserver atau setidaknya anda menyimpan file index.html yang menutup direktori dari pengunjung yang iseng.

4. Jika anda membuat website menggunakan CMS opensource seperti Joomla, Wordpress, Drupal, AuraCMS dan sebagainya, pastikan anda terus mengupdate dengan versi terakhir dan terus melakukan patching atau penambalan kebocoran system jika dikeluarkan release oleh pengembang opensource tersebut, oleh karena itu jangan malas untuk selalu berkunjung ke situs resmi opensource anda untuk informasi patching.

5. Kurangi tingkat kesalahan saat pemograman dilakukan buat anda yang membangun website dengan sourcecode sendiri, lebih baik kita mematikan pesan error untuk menghindari pengunjung melihat kelemahan system yang kita miliki.

6. Penyerangan website biasanya dilakukan melalui dua sisi yaitu sisi server dan sisi aplikasi, untuk sisi aplikasi pastikan semuanya aman dengan semaksimal mungkin melakukan validasi pada form-form yang ada diwebsite anda hal ini membantu anda untuk mengurangi resiko SQL Injection dan penanaman backdoor atau aplikasi tersembunyi yang memungkinkan craker bisa masuk berulang-ulang. Pemasangan captcha atau kode keamanan berupa kata-kata acak yang ditampilkan dalam format image pada form-form tertentu juga akan sangat membantu anda mengurangi serangan dari mesin-mesin spam internet.

7. Sedangkan dari sisi server jika anda hosting berarti anda mempercayakan keamanan server pada provider hosting anda, oleh karena itu sebaiknya anda memilih provider hosting yang terpercaya. Jika anda mempunya server sendiri alahkah lebih baiknya jika anda menggunakan skema dmilitary zone untuk lebih mengamankan server anda dimana aplikasi,database dan firewall bekerja dengan maksimal, yang terakhir, jangan lupa untuk selalu mengupdate apllikasi yang terpasang di server anda.

Kata Kunci :