Tips Mengamankan Website Toko Online dari Serangan Hacker

Oleh: Didik Edhi W

Pernahkah anda berpikir website anda akan di hack? Apakah akibatnya jika website anda mengalami hal tersebut? Antisipasi apakah yang harus anda lakukan untuk mencegah hacker masuk? Kebiasaan buruk apa saja yang harus anda hindari?

A. Latar Belakang

Saat ini memiliki website menjadi kebanggaan semua orang yang memiliki usaha. Website merupakan sarana branding profil seseorang maupun perusahaan yang efektif karena bisa secara langsung diakses oleh semua orang tanpa ada batasan ruang dan waktu. Selain untuk branding, website bisa digunakan juga untuk kampanye, mencari teman/relasi, dll.

Semakin banyak masyarakat Indonesia yang mengerti manfaat website dan internet sehingga jumlah pemakai internet dari tahun ke tahun terus bertambah seiring waktu dan lebih-lebih didukung biaya internet yang murah dan akses yang semakin mudah. Masyarakat mulai mengalihkan strategi promosi dari yang semula konvensional, sekarang menggunakan internet dan website. Website menjadi suatu kebutuhan wajib bagi mereka yang memiliki bisnis. Jika anda perhatikan dunia online di Indonesia, pertambahan website baru per harinya cukup besar. Dunia usaha semakin semarak dengan tumbuhnya usaha pembuatan website dan toko online. Termasuk saya ikut terjun didalamnya. Ada yang menggunakan sistem sewa dan ada yang beli putus.

Saya ingin sedikit mengulas saja khusus untuk para pemula yang ingin terjun ke bisnis online. Mungkin anda perlu tahu, perbedaan antara keduanya yaitu sistem sewa tidak memungkinkan anda memiliki kontrol penuh atas website sedangkan pada sistem beli putus anda berhak atas kontrol penuh website yakni **Control Panel Hosting** dan **Control Panel Super Administrator**. Kalau anda menggunakan sistem sewa jika terjadi error web maka anda tidak dipusingkan untuk menangani error sendiri karena tanggung jawab ada pada perusahaan pembuatnya. Sebaliknya, pada system beli putus, tanggung jawab error sepenuhnya ada di tangan anda. Anda memegang kendali sepenuhnya atas Cpanel Hosting dan Control panel Super Administrator.

Semua keputusan bagaimana cara memiliki website ada di tangan anda dengan pertimbangan utama apakah anda siap jika sewaktu-waktu terjadi error atau terkena serangan hacker. Paling tidak minimal anda harus tahu bahasa pemrograman jika anda ingin memiliki website dengan system beli putus.

B. Ancaman Hacker tidak bisa di tebak atau di ramalkan?

Jika anda seorang pengelola website atau web developer, tentunya anda sadar akan ancaman Hacker yang sewaktu-waktu bisa merusak web atau toko online anda. Saya berharap masalah hack ini tidak menimpa anda. Berdasarkan pengalaman, rasanya pusing kalo website error karena hacker. Lebih susah mengatasinya daripada error yang lainnya.

Pada kesempatan ini saya ingin berbagi pengalaman selama menjalankan beberapa bisnis online dengan website terutama masalah sekuriti website. Beberapa kali saya mengalami serangan hacker dari tingkat rendah sampai tingkat tinggi. Dan hal ini terjadi ketika website saya berada di posisi pertama halaman Google. Lambat laun ranking merosot jauh dan bahkan ada yang terjun bebas dari beberapa mesin pencarian besar dunia.

Oiya, Jika anda awam dengan istilah hack, saya akan sedikit memberikan gambaran singkat tentang hack. Hacked diartikan sebagai suatu tindakan yang dilakukan untuk merusak system dalam website. Proses hacked masuk melalui lubang keamanan pada web yang terbuka. Tingkatan hack berdasarkan dampak kerusakannya bisa dibedakan dari tingkat rendah hingga tingkat tinggi. Akibatnya bisa menyebabkan website mengalami loading yang sangat berat, website tidak bisa diakses, tampilan berubah, url di arahkan ke web lain, system web tidak berjalan normal. Dan orang yang melakukan tindakan tersebut dikenal sebagai **HACKER**.

Bagi saya tindakan hacker yang berusaha merusak website adalah sangat meresahkan saya yang notabene adalah *pebisnis online*. Pernah kejadian Dunia serasa hilang, pengunjung dan order menurun drastis. Penghasilan online jadi merosot . Memang saya akui kalau pada saat itu saya sangat awam dengan sekuriti web dan menganggapnya kurang penting. Setiap web dan toko online yang saya buat tidak semuanya dipersenjatai **Sistem Sekuriti Handal**. Saya terlalu yakin bahwa CMS (*Content Management System*) yang saya gunakan sudah aman dari serangan dari luar. Saya baru sadar bahwa CMS seperti Joomla, Wordpress, Drupal, dll bersifat *Open Source*.

Artinya siapa saja boleh mengembangkannya sehingga dari waktu ke waktu CMS tersebut akan terus berkembang memperbaiki dirinya. Dari sinilah sebenarnya masalah muncul. Sistem sekuriti adalah salah satu bahan pengembangan CMS dibagikan secara terbuka kepada siapa saja yang ingin memperbaikinya. Oleh karena itu, celah-celah keamanan CMS yang open source biasanya lebih mudah dikenali oleh para Hacker daripada yang CMS tidak open source.

Berkali-kali website saya mengalami kerusakan dan jadi bulan-bulanan hacker. Alhamdulillah setiap kerusakan masih bisa saya tangani meski terkadang harus berhari-hari memelototi error yang ada. Bermacam-macam error sudah berhasil saya atasi. Makanya dengan keyakinan penuh saya membuka layanan perbaikan website yang rusak untuk membantu anda mengatasi kerusakan website/toko online separah apapun. Insyaallah dengan pertolongan Allah SWT, BISA..!

"Belajar dari pengalaman tersebut, perlahan dan pasti saya mulai bisa mengenali tanda-tanda, kunci permasalahan dan solusi untuk website yang rusak karena diserang Hacker."

Saya ingin mengatakan bahwa masih banyak masyarakat yang awam dan kurang kepedulian terhadap sekuriti website. Ketika mereka sudah memiliki website dan bisa nangkring di halaman pertama Search Engine Google biasanya akan terlena dengan jumlah pengunjung dan order yang terus mengalir. Padahal sebagian besar website yang ada dihalaman pertama pencarian merupakan sasaran utama para Hacker yang berniat merusak atau hanya menguji sistem sekuriti website anda

"**Tak ada Gading yang tak retak**". Pepatah ini juga berlaku dalam dunia online. Tidak ada website yang sempurna, setiap web pasti memiliki lubang keamanan sendiri-sendiri. Saya harap anda harus bisa menanamkan sikap kehati-hatian jika anda adalah salah satu pengguna CMS yang bersifat Open source seperti Joomla, Wordpress, Magento, Drupal dll. Sikap hati-hati dan waspada harus dibangun sejak awal

membangun website guna mengantisipasi serangan hacker yang bakal sewaktu-waktu menyerang website anda.

C. Dampak Kerusakan Website yang terkena Serangan Hacker

Adapun kerugian jika suatu website mendapatkan serangan Hacker yang menyebabkan website rusak? **Pertama** adalah tampilan website pada umumnya menjadi rusak atau mengalami loading data yang sangat berat. Jika waktu loading sangat lama atau tampilan rusak maka pengunjung tidak akan betah berlama-lama melihat halaman website dan bersegera untuk meninggalkannya. **Kedua,** website yang terkena hacked jika dibiarkan rusak berlama-lama maka akan menurunkan posisi ranking di Search Engine dan fatalnya hilang dari daftar index Search Engine. Kejadian tidak terindexnya web di search engine pernah juga menimpa website saya. Pada saat itu web mengalami serangan tingkat tinggi dan beberapa teman programmer tidak bisa membantu menyelesaikannya. **Ketiga,** ada kemungkinan website sudah terinjeksi virus, malware, dan sejenisnya bisa merugikan dan membahayakan pengguna lain jika mereka mengakses halaman website tersebut. Penularannya seperti virus jika komputer pengguna tidak memiliki sekuriti yang handal. **Keempat,** pengiriman email spam oleh script injeksi yang disisipkan oleh hacker secara otomatis menyebabkan website anda bisa di banned oleh Search Engine karena dianggap melakukan spamming. **Kelima**, website anda akan disuspend oleh pihak Hosting karena menyebabkan overload server. Seperti anda ketahui jika suatu server mengalami overload maka semua website yang di hosting pada server tersebut juga akan mengalami gangguan. Biasanya setiap perusahaan Hosting memiliki rekaman jejak setiap website yang dicurigai membebani server. **Keenam**, hal terparah yaitu website akan mati dengan sendirinya karena ditinggal pengunjung, disuspend hosting, dan di depak dari Search Engine. Ngeri juga kalau poin 6 terjadi yaa...Web mati berarti penghasilan online juga berhenti.

D. Kebiasaan Hacker yang harus anda ketahui

Berdasarkan pengalaman, ada **5 Kebiasaan Hacker** yang bisa dikenali ketika merusak website diantaranya

1. Hacker Biasanya menyerang bagian kulit website saja misalkan merubah file **index.html** atau **index.php** yang merupakan file utama dan pertama ketika website dibuka. Yang terjadi adalah tampilan halaman depan berubah.
2. Hacker merubah isi file **.htaccess** website anda.
3. Hacker biasanya menyisipkan atau menginjeksi script yang bila pemilik menjalankan websitenya bisa menyebabkan script beranak pinak menyerang semua file atau menyebabkan loading website menjadi sangat berat.
4. Hacker kadang melakukan **Redirect Domain** ke domain tertentu sehingga jika pengguna mengetikkan nama domain kita di browser maka akan menuju ke alamat web lain.
5. Hacker terkadang juga bisa **menambah dan merubah nama file** website. Masalah ini disebabkan karena bobolnya akun CPanel Hosting anda. Sebagai pemilik website anda sebaiknya hafal dan mengetahui folder dan file penyusun web anda. Jadi adanya file asing yang tidak biasa bisa dikenali dengan mudah.
6. Hacker terkadang **menyisipkan script email otomatis**. Yang terjadi adalah jika pemakai membuka website maka akan terjadi pengiriman email otomatis ke semua email yang sudah disetting oleh para Hacker.

Jika anda mengalami tanda-tanda tersebut sebaiknya anda segera melakukan cek dan analisis file yang ada dan membersihkan file web dari malware dan sejenisnya. Berdasarkan pengalaman saya ada **10 Tindakan Pencegahan** yang bisa dilakukan untuk meminimalisasi serangan hacker.

1. Mensetting Permission file dan folder website anda secara benar. Lakukan setting permission untuk **folder 755** dan **file 644**. Khusus **untuk file config** anda bisa **setting permission ke 444**.

2. Penyamaran Link URL login administrator website. Misalkan, Jika anda pengguna CMS opensource seperti Joomla atau Wordpress maka link default admin sangat mudah diketahui. Anda bisa menggunakan plugin atau modul yang berfungsi untuk menyamarkan link URL admin.
3. Setiap CMS selalu menyertakan link footer berupa cms yang digunakan misalkan: *Powered by Joomla,Wordpress dll.* Agar tidak memberi jalan hacker maka anda harus menghilangkannya demi alasan keamanan.
4. Memasang Firewall untuk website yang mencegah script asing menginjeksi file dalam website. Gunakan plugin dan modul sekuriti pada setiap web CMS.
5. Selalu update versi CMS yang anda gunakan. Sebaiknya selalu gunakan versi CMS yang terbaru. Biasanya versi terbaru dibuat untuk menutup menghilangkan bug-bug di versi sebelumnya.
6. Anda sebaiknya melakukan perubahan akun control panel hosting dan administrator secara berkala dan menggunakan password yang bersifat Alphanumeric atau gabungan huruf dan angka.
7. Jangan membuat akun yang mudah ditebak misalkan menggunakan nama, tanggal lahir.
8. Jangan memberikan akses user untuk melakukan upload file ke website anda melalui form. Hal ini sangatlah beresiko sekali. Hacker biasa melakukan SQL Injection melalui form yang ada di website. Terkadang File yang dikirim bisa membuka celah keamanan server anda. Jika anda mengijinkan user mengupload gambar maka sebaiknya batasi tipe file (*Extention*) gambar yang digunakan.
9. Gunakan SSL (Security Socket language) untuk mengakses URL website. SSL merupakan protocol yang digunakan untuk pengamanan online dengan cara mengenkripsi semua data yang diinputkan melalui form website.
10. Di internet banyak sekali software sekuriti yang bersifat gratis atau berbayar. Lindungi komputer (PC) anda dengan software sekuriti yang handal kalau perlu yang berbayar. Karena biasanya yang berbayar lebih memberikan perlindungan yang baik dan bisa dipertanggungjawabkan.

11. Lakukanlah Backup Database dan File secara berkala sehingga jika sewaktu-waktu website rusak karena di hack bisa di restore ulang database dan filenya.

E. Kebiasaan Buruk yang harus dihindari

Kerusakan website toko online sudah sering terjadi dan penyebab utamanya adalah lemahnya system sekuriti website dan faktor kelalaian manusia yang terkadang ceroboh terhadap serangan virus, malware, atau Trojan. Saya menyarankan hindari tindakan/kebiasaan kurang baik dibawah ini jika website anda tidak mau disusupi hacker:

1. Tidak memasang software sekuriti anti virus, anti malware, dan anti Trojan pada komputer yang sering digunakan untuk online.
2. Kebiasaaan mendownload produk/software sembarangan. Banyak masyarakat kita suka sesuatu produk/software yang dibagikan secara gratis. Dan tanpa disadari sebenarnya dari sanalah serangan itu dimulai.
3. Kebiasaan menggunakan akun website dan cpanel hosting secara sembarangan misalkan akses melalui warnet.
4. Kebiasaan membuka email asing yang melampirkan attachment biasanya berisi iming-iming hadiah atau berita yang membuat kita panik.
5. Kebiasaan Malas untuk melakukan update CMS, plugin, modul dan software sekuriti yang digunakan ke versi yang terbaru.

F. Penutup

Kita semua tahu dan sadar bahwa kita tidak bisa menghentikan serangan Hacker, serangan itu bisa terjadi kapan pun dan di mana pun. Tapi paling tidak anda bisa melakukan pencegahan jangan sampai website atau toko online anda memberikan celah bagi mereka Hacker untuk masuk ataupun Anda bisa meminimalisasi kerusakan dengan mengetahui gejala dan tanda-tanda yang ditimbulkannya.

Dengan beberapa tips dari pengalaman saya di atas saya berharap mulai saat ini sadari pentingnya sekuriti web. Jika anda ingin membuat website atau toko online jangan lupa selalu tanyakan tentang **Sekuriti Web** yang akan anda dapatkan. Sebagus apapun website tanpa sekuriti adalah kurang baik untuk kelangsungan bisnis jangka panjang.

Jika anda mengalami kerusakan web dan tidak bisa mengatasinya, dengan senang hati saya akan membantu anda.

Semoga Bermanfaat……!

G. Biografi Penulis:

Didik Edhi Wibowo
CEO kursuswebpro.com
Facebook: http://www.facebook.com/kursuswebpro

Office:
Mutiara Darussalam A3/11
Jl Pitara Raya Depok
Telp: 021-99235798 – HP: 08175011058
Email: kursuswebpro@gmail.com

Layanan:
Kursus website – Kursus toko online – Error handling – Desain Web & SEO

Owner dari bisnis online:
www.tokomainananak.com
www.rumahobatherbal.com
www.tokoplusafiliasi.com
www.mitrafastpay.com
www.jasawebsitepro.com