Kerahasiaan dan Keamanan

SSL

SSL atau Secure Socket Layer adalah cara sebuah situs web membuat koneksi secara aman dengan browser web pengguna. Setiap seseorang mengunjungi situs yang menggunakan teknologi SSL, tercipta sebuah saluran aman selama sesi browsing antara browser pengguna dan web server. SSL adalah standar industri untuk komunikasi web secara aman dan digunakan untuk melindungi jutaan transaksi online setiap hari. Web server harus memiliki sertifikat SSL sebelum dapat membuat koneksi SSL. Ketika seseorang mengaktifkan protokol SSL di server web mereka, mereka diminta untuk menjawab pertanyaan-pertanyaan seputar identitas mereka. Pertanyaan tersebut meminta informasi tentang situs dan perusahaan. Setelah permintaan sertifikat SSL selesai dilakukan, server web membuat dua kunci kriptografi, satu adalah kunci pribadi dan satunya lagi adalah Kunci Publik. SSL merupakan suatu teknologi keamanan standar global yang memungkinkan terjadinya komunikasi aman antara browser web dan server web. SSL digunakan oleh jutaan bisnis online dan individu untuk mengurangi risiko pencurian informasi yang bersifat sensitif, misalnya adalah nomor kartu kredit, nama pengguna, kata sandi dan surat elektronik dari pencurian atau perusakan oleh peretas dan pencuri identitas. Untuk menciptakan koneksi yang aman ini, dipasang suatu sertifikat SSL (sertifikat digital) pada server web untuk memberikan dua fungsi layanan, yaitu pengabsahan dan enkripsi.

SSL diperlukan untuk mengamankan situs dari ancaman keamanan. Ada juga alasan-alasan lain yang menjadi alasan perlunya menggunakan SSL. SSL merupakan pelindung ancaman pencurian data. Caranya dengan melakukan enkripsi data. Dengan begitu pihak-pihak yang tidak diinginkan tidak bisa membaca data yang dimiliki dan dikirimkan. SSL juga berfungsi untuk mengabsahkan pengguna. Artinya SSL memastikan bahwa pengguna mengirimkan informasi atau data ke server yang sesuai. Bukannya mengirim informasi ke hacker atau pihak-pihak tak bertanggung jawab. Ketika website sudah terpasang sertifikat SSL, browser menunjukkan notifikasi khusus. Di Internet Explorer notifikasi tersebut berwujud blok berwarna hijau di bagian address-bar. Sedangkan di Firefox dan Google Chrome notifikasi ditunjukkan dalam bentuk gambar gembok. Notifikasi ini berguna untuk meningkatkan reputasi dan kepercayaan pengunjung. Dengan adanya notifikasi, pengunjung situs tidak ragu untuk mengakses website. Algoritme mesin pencari atau search enginee juga lebih menyukai situs yang memiliki sertifikat SSL. Google bahkan memberikan imbauan kepada penggunanya untuk tidak mengunjungi situs yang tak punya sertifikat SSL. SSL juga meningkatkan peringkat website di mesin pencarian. Sebuah riset membuktikan bahwa kebanyakan situs dengan sertifikat SSL berada pada posisi yang lebih tinggi di mesin pencari.

Salah satu aspek paling penting sertifikat SSL adalah menemukan penyedia sertifikat yang baik. Sertifikat SSL dikeluarkan oleh Otorisasi Sertifikat (CA, singkatan dari Certivicate Authorization), pihak yang dipercaya untuk melakukan verifikasi identitas dan legitimasi setiap pihak yang meminta sertifikat. Peran CA adalah untuk menerima pengajuan sertifikat, verifikasi pengajuan, menerbitkan sertifikat dan memelihara informasi status sertifikat yang diterbitkan. SSL ada banyak jenisnya, ada yang berbayar dan ada juga SSL Gratis. Bagi yang menginginkan keamanan lebih bisa memilih SSL berbayar seperti RapidSSL, Comodo PositiveSSL, VeriSign Secure Site atau Geotrust. Contoh penyedia layanan sertifikat SSL gratis adalah DomaiNesia, yaitu melalui produk bernama Let’s Encrypt. Penyedia sertifikat SSL gratis juga banyak dijumpai di Internet. Jika tertarik untuk mencobanya, bisa mencari sendiri dengan bantuan mesin pencari seperti google, yahoo dan bing. Kata kunci untuk mencarinya juga bervariasi, contohnya adalah free ssl provider, free ssl certivicate atau free ssl saja. Contoh penyedia sertifikat SSL tersebut antara lain adalah ZeroSSL, SSL For Free dan Let's Encrypt. Masing-masing penyedia sertifikat tersebut memiliki situs online dengan alamat https://zerossl.com, www.sslforfree.com dan https://letsencrypt.org. Untuk penggunaan personal atau bisnis kelas menengah ke-bawah lebih baik menggunakan sertifikat versi gratis karena dapat mengurangi biaya operasional yang membebani pelaku bisnis.

SSL memungkinkan informasi sensitif dikirimkan dari server ke klien secara aman. Web server harus memiliki sertifikat SSL sebelum dapat membuat koneksi SSL. Setelah permintaan pembuatan sertifikat SSL selesai, server menciptakan dua kunci kriptografi, yaitu Public Key dan Private Key. Public key diberikan kepada browser bersamaan dengan sertifikat SSL untuk menciptakan sesi koneksi yang aman antara browser dan server. Publilc key digunakan oleh browser untuk mengenkripsi data yang yang dikirimkan dan diterima. Private Key digunakan server untuk melakukan dekripsi informasi dari browser. Private key sifatnya sangat rahasia dan tidak ada yang boleh tau, kunci inilah yang digunakan untuk membongkar enkripsi data dari dan ke server. Sertifikat SSL adalah sertifikat digital yang mengabsahkan identitas situs web dan mengenkripsi informasi yang dikirim ke server dengan menggunakan teknologi SSL. Sertifikat berfungsi sebagai identitas elektronik yang mendapatkan pengakuan dari pihak online saat berbisnis di Web. Jika pengguna Internet berusaha mengirimkan informasi ke server Web, browser pengguna tersebut akan mengakses sertifikat digital server kemudian melakukan koneksi secara aman.

HTTPS adalah singkatan dari hypertext transfer protocol secure. Https merupakan protokol komunikasi jaringan internet. HTTPS dapat diartikan sebagai bentuk protokol internet yang dapat dipercaya dan aman. HTTPS melindungi integritas serta kerahasiaan antara situs dan komputer pengguna. Dengan HTTPS data yang dikirimkan dari website ke pengunjung dijamin aman dan tidak dapat diketahui oleh pihak lain. Dengan menggunakan protokol HTTPS, orang lain juga sulit membajak isi data atau dokumen yang dikirim dari website ke pengunjung. Artinya hal-hal yang diperoleh pengunjung dari sebuah situs menjadi tidak dapat dibajak atau dicuri oleh orang lain. Ketika mempunyai akun bank digital, dan di dalam akun tersebut berisi banyak uang tabungan, maka agar dapat masuk ke akun tersebut harus menggunakan kata-sandi atau metode keamanan-keamanan lainnya. Dengan memberikan kata-sandi kepada orang lain, maka otomatis kemungkinan uang hilang menjadi lebih besar. Bisa saja tidak dapat mengakses akun bank digital tersebut karena kata-sandi akun diganti oleh orang lain. Oleh sebab itu, HTTPS sangat penting. Untuk menghindari pencurian kata-sandi dan data-data lainnya, maka sebuah website sebaiknya menggunakan protokol HTTPS. Dengan HTTPS semua data yang dikirimkan dari website diamankan melalui berbagai format sehingga tidak mungkin data-data dapat dicuri oleh pihak lain.

Sertifikat SSL membantu mengamankan sesi komunikasi dua komputer yang saling terhubung oleh jaringan internet. Pertukaran data seperti mengunjungi website, pengiriman dan penerimaan surat elektronik, membeli barang online, serta data-data penting perusahaan di-enkripsi agar tidak ada oknum tak bertanggung jawab yang berusaha menggunakan data-data tersebut secara ilegal. Jika memiliki website bisnis atau organisasi, maka Organization Validated SSL (OV SSL) adalah pilihan tepat. Untuk yang menjalankan bisnis online atau e-commerce SSL jenis Extended Validated SSL (EV SSL) adalah pilihan terbaik, karena EV SSL mempunyai tingkat keamanan paling tinggi. Bagi yang baru mengenal SSL dan ingin melakukan instalasi sendiri, diperlukan beberapa pertimbangan awal untuk melakukan keinginan tersebut. Diantaranya adalah pastikan dahulu akan menggunakan SSL gratis atau berbayar. Anda perlu mempertimbangkan hal tersebut berdasarkan kebutuhan dan anggaran. Beberapa SSL gratis memang sudah menyediakan fungsi-fungsi penting yang dibutuhkan website. Walaupun begitu, tetap saja fungsi-fungsi SSL secara lengkap ada pada SSL berbayar. Setelah memasang SSL melalui cPanel, Pengguna perlu mengarahkan website ke alamat baru, yang sebelumnya menggunakan HTTP menjadi HTTPS. Ini berlaku baik untuk SSL gratis maupun SSL berbayar. Anda bisa melakukannya menggunakan plug-in.

VPN

Virtual Private Network adalah teknologi transfer data yang memungkinkan penggunanya dapat terhubung ke jaringan publik dan menggunakannya sebagai penghubung dengan jaringan lokal. Dengan cara tersebut didapatkan

hak dan pengaturan yang sama seperti berada di dalam LAN. Salah satu masalah jaringan internet adalah tidak mempunyai dukungan yang baik terhadap keamanan. Sedangkan IP adalah kebutuhan dasar untuk melakukan pertukaran data antara beberapa LAN yang dipisahkan oleh jarak. VPN muncul untuk mengatasi persoalan tersebut. Virtual Private Network atau biasa disebut VPN adalah sebuah cara aman untuk mengakses LAN yang berada pada jarak tertentu, dengan menggunakan internet atau jaringan umum lainnya sebagai media untuk melakukan transmisi data. Salah satu fungsi vpn adalah mengamankan sesi komunikasi atau pertukaran data. Definisi VPN menurut IETF adalah sebuah emulasi WAN pribadi dengan menggunakan fasilitas shared-IP atau IP publik seperti Internet atau backbone IP private. VPN merupakan bentuk jaringan pribadi yang melalui jaringan publik, dengan menekankan keamanan data dan akses global melalui internet. Jalinan koneksi ini dibentuk melalui suatu tunnel (terowongan) virtual. VPN Menghubungkan komputer dengan jaringan publik secara pribadi, karena bersifat pribadi maka tidak semua orang bisa terhubung dan memiliki akses ke jaringan. Hal ini dilakukan untuk menjaga keamanan dalam pertukaran data atau informasi.

Penggunaan VPN dapat menghindari adanya penyusup saat melakukan transmisi data yang. VPN berfungsi menjaga kerahasiaan data, keutuhan data dan keabsahan sumber. Penggunaan VPN dapat menjaga kerahasiaan data dan informasi milik pengguna agar tidak digunakan orang lain. Jaringan yang bersifat publik bisa dibilang cukup berbahaya, dengan menggunakan VPN maka data tersebut bisa masuk dan keluar dengan aman. VPN juga berguna untuk menyelamatkan data dari oknum-oknum tidak bertanggung jawab. Program VPN memastikan proses transmisi data selesai dan diterima oleh penerima sesuai dengan permintaan pengguna tanpa adanya perubahan atau manipulasi data. Program pada VPN mampu melakukan verifikasi sumber pengiriman data yang diterima. VPN memastikan dan mengecek data yang masuk. Jika proses memeriksa keabsahan berhasil, maka informasi atau data dapat disetujui. Dalam hal ini VPN berguna untuk menganalisis sumber-sumber data yang tidak dipercaya sehingga dapat mencegah virus. Menggunakan server VPN pada jaringan komputer perusahaan untuk transmisi data yang bersifat rahasia dapat membantu mengatasi hal-hal tidak diinginkan, seperti pada kasus-kasus pencurian data yang marak terjadi.

Gurdeep Singh-Pall adalah seorang ahli perangkat lunak di perusahaan Microsoft, ia mengembangkan PPTP (Peer-to-Peer Tunneling Protocol) pada pertengahan tahun 1990. Meski banyak yang beranggapan PPTP adalah protokol vpn yang paling cepat, protokol ini pada dasarnya dirancang untuk akses dengan sambungan telepon (dial-up) dan memiliki tingkat enkripsi paling rendah. Gurdeep Singh Pall adalah salah satu wakil presiden perusahaan Microsoft dan merupakan bagian dari tim kepemimpinan senior Divisi Layanan Online. Gurdeep Singh Pall bergabung dengan Microsoft pada bulan Januari tahun 1990 sebagai insinyur desain perangkat lunak. Dia membuat banyak produk terobosan dalam masa jabatannya. Gurdeep Singh Pall adalah bagian dari tim pengembangan Windows NT. Ketika Microsoft memproduksi Windows XP pada tahun 2001 ia bekerja sebagai general manajer Windows Networking. Selama bekerja di Windows, ia memimpin desain dan implementasi teknologi inti jaringan seperti PPP, TCP/IP, UPnP, VPN, routing dan Wi-Fi. Gurdeep Singh Pall menulis protokol VPN pertama di industri sehingga menerima penghargaan Innovation of the Year dari PC Magazine pada tahun 1996. Ia juga menulis beberapa dokumen dan standar di bidang jaringan di badan standar IETF pada pertengahan tahun 1990.