NIST SP 800-44v2: PEDOMAN PANDUAN SISTEM KEAMANAN PUBLIK WEB SERVER

Oleh :
Azhari S. Barkah
Dosen STMIK Amikom Purwokerto

Abstrak

World Wide Web (WWW) adalah salah satu cara yang paling penting bagi suatu organisasi untuk mempublikasikan informasi, berinteraksi dengan pengguna internet, dan membangun kehadiran e-commerce atau e-government. Akan tetapi, jika sebuah organisasi tidak tepat dalam mengkonfigurasi dan mengoperasikan situs Web umum, mungkin akan rentan terhadap berbagai ancaman keamanan. Web server merupakan tempat atau wadah di mana informasi tersebut disimpan dan dipublikasikan untuk dapat diakses oleh pengguna internet. Oleh karena itu, diperlukan sebuah sistem keamanan publik web server, sesuai dengan tujuannya yaitu mengamankan dan melindungi kerahasiaan, integritas dan ketersediaan informasi tersebut.

Kata kunci: keamanan publik web server, keamanan sistem informasi, world wide web, internet

PENDAHULUAN

Keamanan data elektronik menjadi hal yang sangat penting adanya. Keamanan data elektronik tersebut tidak hanya untuk perusahaan-perusahaan yang bergerak dibidang IT saja, akan tetapi untuk industri lain seperti: perusahaan yang bergerak di bidang jasa, perdagangan, organisasi non profit, institusi pendidikan, instansi pemerintah, media pemberitaan, dan sebagainya, serta perseorangan atau individu.

Web server merupakan tempat atau wadah untuk menyimpan dan mempublikasikan segala informasi yang ditampilkan dalam dokumen WWW yang dapat diakses oleh pengguna internet melalui Web browser. Informasi yang tersedia dalam WWW adalah informasi yang bersifat umum hingga informasi yang bersifat penting dan rahasia. Informasi tersebut dapat diakses secara langsung dan atau melalui proses otentikasi terlebih dahulu.

Informasi atau data adalah aset yang sangat berharga yang harus dikelola dan dipelihara sehingga informasi tersebut dapat dipergunakan sebagaimana

fungsinya. Web server adalah aset yang dipergunakan untuk mengelola, menyimpan dan memelihara informasi atau data tersebut. Agar web server dapat menjalankan fungsinya diperlukan sebuah standar sistem keamanan publik Web server, dimana sistem keamanan publik Web server tersebut dijadikan sebagai pedoman dalam membangun sistem informasi berbasis internet.

Dalam hal ini National Institute of Standards and Technology (NIST) telah mengembangkan dokumen ini sebagai kelanjutan dari tanggung jawab hukum di bawah manajemen keamanan informasi federal Act (FISMA) tahun 2002. Dokumen tersebut dituangkan dalam Guidelines on Securing Public Web Servers National Institute of Standards and Technology Special Publication 800-44 Version 2. Natl. Inst. Stand. Technol. Spec. Publ. 800-44 Ver. 2, 142 pages (sep. 2007).

PEMBAHASAN

Apa itu sistem keamanan publik Web server

Sistem keamanan publik Web server adalah suatu sistem yang dibangun untuk mengatur, mengelola dan menjaga agar Web server dapat melakukan fungsinya sebagai wadah untuk menyimpan, mengelola dan memelihara serta mempublikasiksan informasi. Sistem keamanan Web server harus memenuhi aspek-aspek utama dalam keamanan sistem informasi. Aspek-aspek tersebut diantarannya adalah:

a. Confidentiality (kerahasiaan) aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat di akses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.
b. Integrity (integritas) aspek yang menjamin bahwa data tidak berubah tanpa ada ijin pihak yang berwenang (authorized), menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integritas ini.
c. Availability (ketersediaan) aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait.

Mengapa diperlukan sistem keamanan publik Web server

World Wide Web (WWW) adalah suatu sistem pertukaran informasi melalui internet. Pada tingkat paling dasar, Web dapat dibagi menjadi dua komponen utama: Web server, merupakan aplikasi yang membuat informasi tersedia malui internet (sebagai wadah untuk mempublikasikan informasi), dan Web browser, digunakan untuk mengakses dan menampilkan informasi yang tersimpan di Web server.

Peran penting web server tersebut sering menjadi target penyerangan di dalam sebuah jaringan yang dimiliki sebuah organisasi. Akibatnya, dukungan untuk mengamankan Web server dan infrastruktur jaringan yang dimilik harus lebih diperhatikan oleh mereka. Berikut ini, beberapa contoh ancaman keamanan khususnya untuk Web server:

a. Entitas berbahaya yang mungkin mengekploitasi bug dalam perangkat lunak Web server, yang mendasari sistem operasi, atau konten aktif untuk mendapatkan akses tidak sah ke Web server. Contoh dari akses yang tidak sah termasuk mendapatkan akses ke file atau folder yang tidak seharusnya dapat diakses oleh publik dan mampu menjalankan perintah dan atau menginstal perangkat lunak pada Web server.
b. Serangan DoS (*denial of service*) yang diarahkan ke Web server atau ke infrastruktur jaringan pendukung. Menolak dan menghalangi pengguna yang sebenarnya untuk menggunakan layanan tersebut.
c. Informasi yang penting di dalam Web server mungkin dibaca atau di modifikasi tanpa ijin.
d. Informasi sensitif yang dikirim tanpa enkripsi dari Web server ke Web browser sangat rentan untuk disadap.
e. Informasi Web server dapat diubah untuk tujuan yang berbahaya. Deface situs Web adalah ancaman ini yang sering dilaporkan.
f. Server dapat digunakan sebagai titik distribusi alat untuk menyerang, pornografi, atau menyalin material secara ilegal.

Web server juga memungkinkan menghadapi serangan tidak langsung untuk memperoleh informasi dari pengguna mereka. Dalam serangan ini, pengguna akan

dikelabui atau secara otomatis diarahkan untuk mengunjungi situs Web berbahaya yang tampak sah. Hal ini akan mengakibatkan pengguna secara tidak sadar memberikan informasi kepada pihak yang tidak bertanggung jawab, sebagai contoh dalam kasus ini adalah kasus yang dialami oleh pengguna internet banking.

Untuk menghadapi dan mengatisipasi semua kerentanan keamanan dan isu keamanan baik secara fisik maupun logik dibutuhkan sebuah sistem keamanan publik Web server yang dapat digunakan sebagai acuan atau pedoman dalam mengamankan seluruh informasi yang dimiki dan telah disimpan dan dipublikasikan melalui Web server.

Apa itu NIST SP 800-44 ver2?

a. NIST SP 800-44 ver2 merupakan suatu struktur dan rekomendasi pedoman yang dikembangkan oleh National Institute of Standards and Technology yang disiapkan untuk digunakan oleh lembaga federal.
b. Dokumen tersebut juga dapat digunakan oleh organisasi non pemerintah secara sukarela dan tidak tunduk pada hak cipta.
c. Suatu proses sistem keamanan publik Web server yang menyeluruh yang dapat di implementasikan bagi organisasi pemerintahan ataupun non pemerintahan dan kalangan industri di berbagai bidang.
d. Proses perencanaan, pengelolaan, pemeliharaan, evaluasi, implementasi dan pengaturan keamanan publik Web server yang singkat dan mudah.
e. NIST SP 800-44 ver2 merupakan proses yang seimbang antara fisik dan logik keamanan publik Web server baik secara teknik dan prosedural.

Apa isi dari NIST SP 800-44 ver2?

Isi dari NIST SP 800-44 ver2, meliputi 7 bahasan utama dalam membangun sistem keamanan Web server. 7 bahasan utama tersebut, antara lain:

a. Perencanaan dan pengelolaan Web server.
b. Mengamankan sistem operasi Web server.
c. Mengamankan Web server.
d. Mengamankan konten Web.
e. Menggunakan otentikasi dan teknologi enkripsi.

f. Menerapkan keamanan infrastruktur jaringan.
g. Administrasi Web server.

Perencanaan dan pengelolaan Web server

Aspek yang paling penting dari penyelenggaraan keamanan Web server adalah perencanaan yang hati-hati terlebih dahulu untuk instalasi, konfigurasi, dan persiapan. Perencanaan yang hati-hati akan memastikan bahwa Web server seaman mungkin dan sesuai dengan kebijakan organisasi yang relevan. Banyak permasalahan keamanan Web server yang terjadi karena tidak ada perencanaan atau kontrol manajemen. Pentingnya kontrol manajemen tidak dapat dilebih-lebihkan. Di banyak organisasi, struktur dukungan TI sangat terfragmentasi. Fragmentasi ini menyebabkan inkonsistensi, dan inkonsistensi ini dapat menyebabkan kerentanan terhadap keamanan dan isu lainnya.

Beberapa aspek yang harus diperhatikan dalam perencanaan dan pengelolaan Web server antara lain:

a. Pemenuhan sumber daya manusia (SDM) dalam bidang sistem keamanan dan administrasi Web server.
b. Perencanaan Web server yang harus memenuhi berbagai aspek, seperti biaya yang ditimbulkan dan infrastruktur.
c. Pemilihan platform Web server yang tepat.

Mengamankan sistem operasi Web server

Melindungi Web server dari serangan membutuhkan hardening OS (sistem operasi) yang mendasarinya, aplikasi Web server, dan jaringan untuk mencegah entitas berbahaya dari serangan langsung ke Web server. Langkah pertama dalam mengamankan Web server, adalah dengan hardening OS (sistem operasi) yang mendasarinya.

Aspek utama dalam mengamankan sistem operasi web server ini diantaranya meliputi:

a. Instalasi dan konfigurasi sistem operasi.
b. Pengujian keamanan sistem operasi tersebut.

Mengamankan Web server, setelah OS terinstall dan aman, dapat dimulai melakukan instalasi perangkat lunak Web server. Sebelum memulai proses ini, membaca dokumentasi Web server dengan hati-hati dan memahami berbagai pilihan yang tersedia selama proses instalasi. Juga, pastikan untuk mengunjungi official perangkat lunak Web server atau mengunjungi situs database kerentanan keamanan Web. Dalam proses awal instalasi perangkat lunak tersebut memulai dengan langkah dasar untuk memenuhi perangkat lunak tersebut dapat berjalan dengan baik di didalam sistem operasi.

Dalam mengamankan Web server beberapa aspek yang harus diperhatikan diantaranya adalah:

a. Melakukan instalasi perangkat lunak Web server secara aman.
b. Mengkonfigurasi akses kontrol Web server.

Mengamankan konten Web

Konten Web merupakan bagian dari isi informasi yang ditampilkan di halaman Web browser. Konten Web tersebut merupakan bagian yang penting untuk diamankan. Kerentanan keamanan Web server dapat melalui konten Web. Untuk mengamankan konten Web tersebut beberapa aspek utama yang harus diperhatikan diantaranya:

a. Bagaimana cara mengatasi serangan langsung pada konten.
b. Mengamankan konten aktif dengan teknologi generasi konten.

Menggunakan otentikasi dan teknologi enkripsi

Penggunaan otentikasi dan teknologi enkripsi sangat diperlukan sekali, hal ini diterapkan untuk melakukan pengamanan pengiriman dan penerimaan data informasi yang termasuk dalam kategori informasi penting dan rahasia. Aspek-aspek dalam menggunakan otentikasi dan teknologi enkripsi diantaranya:

a. Menentukan persyaratan otentikasi dan enkripsi.
b. Dasar-dasar otentikasi.
c. Teknologi SSL/TLS.
d. Mengatasi serangan yang hebat.

Menerapkan keamanan infrastruktur jaringan

Keamanan Web server tidak hanya meliputi aspek logik saja, tetapi juga meliputi aspek fisik, di mana, aspek fisik ini memiliki peran yang sangat penting. Aspek fisik ini meliputi kondisi fisik infrastruktur jaringan, penempatan Web server, serta menjauhkan dari masalah pencurian data, atau bahkan pencurian infrastruktur yang digunakan untuk Web server tersebut.

Beberapa hal utama yang harus diperhatikan diantaranya:

a. Komposisi dan struktur jaringan.
b. Elemen konfigurasi jaringan.

Administrasi Web server

Administrasi Web server ini terkait dengan pengelolaan dan pemeliharaan serta pengaturan baik konfigurasi perangkat lunak Web server atau isi konten Web tersebut. Di dalam administrasi Web server ini dilakukan oleh seorang Administrator yang telah ditunjuk oleh manajemen organisasi.

NIST SP 800-44 ver2 tidak meliputi aspek:

a. Mengamankan jenis server jaringan.
b. Firewall dan router yang digunakan untuk melindungi Web server.
c. Pertimbangan keamanan Web yang terkait dengan perangkat lunak klien (web browser).
d. Pertimbangan khusus untuk lalu lintas situs Web yang tinggi dengan beberapa host.
e. Mengamankan server back-end yang dapat mendukung Web server seperti database server, file server dan sebagainya.
f. Service lain dari HTTP dan HTTPS.
g. SOAP style Web service.
h. Proteksi hak kekayaan intelektual.

KESIMPULAN

Keuntungan utama dari NIST SP 800-44 ver2 berhubungan dengan kepercayaan publik. Sama seperti halnya standar keamanan informasi seperti iso 17799 atau standar keamanan informasi yang lain yang mencerminkan jaminan kualitas. Beberapa point keuntungan yang lain:

a. Memberikan kemudahan dalam penelusuran dan penanganan masalah keamanan Web server.
b. Dengan perencanaan yang matang akan dapat menekan biaya investasi sehingga akan mengurangi beban biaya manajemen.
c. Menjamin ketersediaan dan layanan informasi yang tepat guna.

Keamanan sistem informasi memiliki peran yang sangat penting dan tidak boleh diabaikan sedikit pun, di mana, informasi merupakan aset yang sangat berharga yang harus terus dijaga dan dipelihara agar informasi tersebut tidak dapat dipergunakan oleh pihak-pihak yang tidak bertanggung jawab.

a. Ketika memilih sistem informasi berbasis internet harus direncanakan secara matang dan dikelola secara berkesinambungan agar kelangsungan sistem informasi tersebut dapat dipergunakan sebagai mana fungsinya.
b. Pembangunan dan pengelolaan publik Web server harus mengacu pada pedoman sistem keamanan publik Web server untuk mendapatkan hasil yang maksimal sehingga jaminan akan kelangsungan informasi terus berkesinambungan.
c. Sistem keamanan publik Web server tidak hanya terkait dalam permasalah-permasalahan teknis saja, tetapi juga permasalah-permasalah non teknis yang logis dari sudut pandang bisnis. Oleh karena itu, dalam melindungi aset informasi tersebut harus menjadi tanggung jawab penuh dan bagian dari bisnis.
d. Pekerjaan keamanan merupakan pekerjaan yang terus menerus berkesinambungan, oleh karena itu, organisasi harus memberikan perhatian khusus serta selalu memperbaharui sistem keamanan yang telah diterapkan, di mana teknik-teknik penyerangan di dalam dunia maya begitu pesat perkembangannya.

DAFTAR PUSTAKA

NIST (National Institute of Standards and Technology), *Guideline on Securing Public Web Server*, http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf 05 Februari 2008

Melwin Syafrizal, S.Kom, ISO 17799: *Standar Sistem Manajemen Keamanan Informasi*, http://www.scribd.com/doc/28247411/Jurnal-Ttg-ISO-17799 19 November 2008