MICROSOFT WINDOWS : VULNERABILITY AND PATCH MANAGEMENT

Oleh : Felix Andreas Sutanto

Masalah keamanan selalu menjadi isu yang paling penting dalam pemilihan sistem operasi. Hal ini terbukti dengan suatu ungkapan yang sering kita dengar tentang Microsoft Windows. Windows adalah sistem operasi yang terkenal banyak masalah, banyak lubang yang bisa mengakibatkan kerawanan saat kita bekerja, oleh karena itu jangan memakai sitem operasi Windows. Meskipun demikian, harus diakui bahwa Windows telah menjadi teman bagi sebagian besar pemakai komputer di dunia. Windows telah menjadi favorit karena teknologinya sangat user friendly, plug and play dan banyak didukung oleh pengembang software lainnya. Hal inilah yang menyebabkan banyak orang selalu mengeksploitasi kelemahannya.

Microsoft sebagai pengembang software terbesar saat ini tentu saja sangat memperdulikan keamanan softwarenya. Ada beberapa Microsoft Management Tools untuk mengatasi vulnerability, namun banyak orang yang tidak mengetahui bagaimana cara mengimplementasikannya. Salah satunya adalah penerapan Patch Management untuk membuat komputer lebih aman. Cara ini adalah cara yang paling mudah untuk diterapkan, hanya saja beberapa pengguna komputer tidak menghiraukannya.

Mengamankan sistem adalah usaha untuk mencegah seseorang melakukan tindakan-tindakan yang tidak kita inginkan pada komputer, perangkat lunak, dan peralatan yang ada di dalamnya sehingga semuanya tetap dalam keadaan yang diinginkan. Membuat sistem aman, berarti membuat reputasi aman. Keamanan sistem akan diperoleh dengan memperbaiki kerapuhan sistem.

Kerapuhan Sistem (Vulnerability)

Kerapuhan sistem ditentukan dari seberapa jauh proteksi yang bisa diterapkan pada network, untuk menghadang seseorang dari luar sistem yang berusaha memperoleh akses illegal terhadap network tersebut. Selain itu juga kemungkinan adanya tindakan dari orang-orang dalam sistem yang memberikan akses kepada dunia luar yang bersifat merusak sistem jaringan.

Kerapuhan sistem bisa disebabkan karena adanya bug-bug (ketidaksesuaian algoritma pemrograman) yang tidak disadari oleh pemrogram sistem operasi. Hal inilah yang sering digunakan oleh hacker untuk membobol suatu sistem.

Untuk mengatasi eksploitasi yang tidak diinginkan, dikembangkanlah konsep Network Security Architecture yang terdiri dari 7 lapis tingkat sekuriti pada jaringan sebagai berikut :

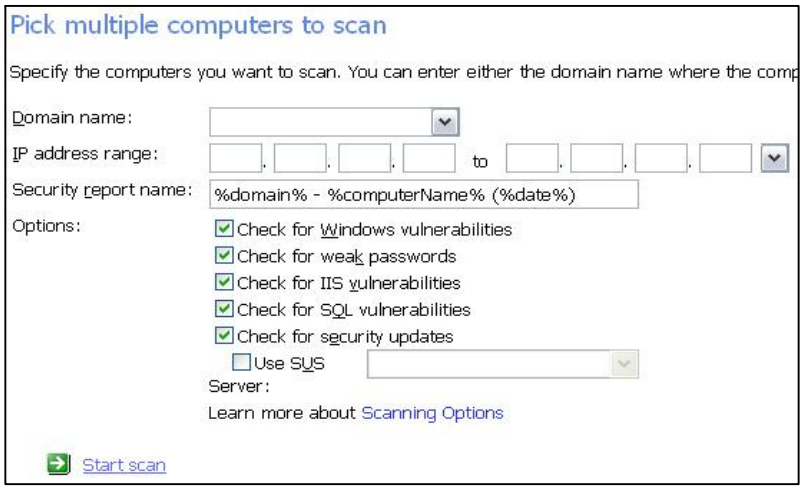
1. Kebijaksanaan : Mendefinisikan kebijakan-kebijakan organisasi dan cara mengimplementasikan

kebijaksanaan yang diambil terhadap prosedur-prosedur dasar dan peralatan yang digunakan.

2. Personil : Menentukan personil yang melakukan instalasi, konfigurasi, pengoperasian dan orang-orang yang mampu menjalankan akses-akses yang tersedia dalam sistem.
3. Local Area Network : Mendefinisikan peralatan-peralatan dan data-data yang harus mendapatkan proteksi
4. Batas Dalam Jaringan : Mendefinisikan lapisan sistem yang terkoneksi secara fisik. Memberikan batasan yang jelas antara jaringan lokal dengan jaringan luar.
5. Gateway : Mendefinisikan titik yang menjadi pintu utama untuk masuk dan keluar sistem. Sistem yang terkoneksi ke wide-area network seharusnya mengutamakan lapis ini.
6. Paket Filtering : Mendefinisikan platform yang berada di antara network interface gateway dengan network interface yang menjadi tempat penerapan metoda Firewall.
7. Batas Luar Jaringan : Mendefinisikan titik dimana sistem terhubung dengan wide-area network dan kita tidak memiliki kontrol langsung terhadap titik tersebut.

Untuk menganalisa adanya vulnerability dalam jaringan, Microsoft telah mengembangkan beberapa software, yaitu Microsoft System Management Server dan Microsoft Baseline Security Analyzer. Microsoft System Management Server seringkali digunakan untuk menganalisa kerapuhan hardware dan software. Selain itu juga digunakan untuk membangun fasilitas untuk pelayanan update software (Software Update Service).

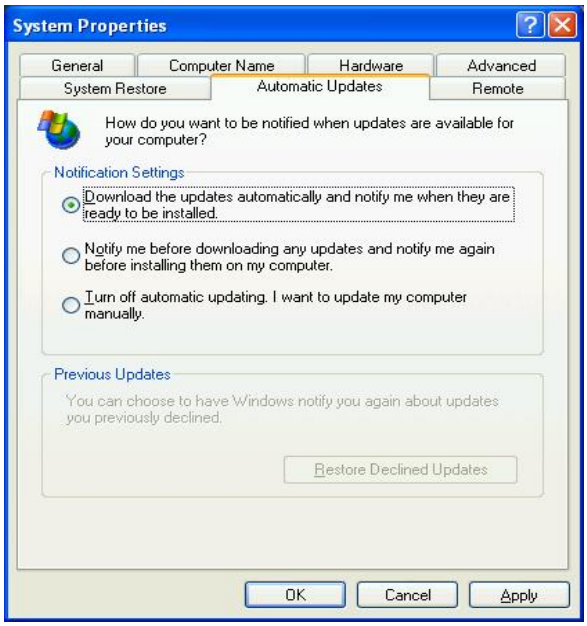
Sedangkan Microsoft Baseline Security Analyzer (MBSA) digunakan untuk menganalisa kerapuhan sistem operasi, IIS, SQL, Exchange, Security Updates dan Office Updates. MBSA sangat mudah digunakan untuk menganalisa suatu komputer, maupun sekelompok komputer dalam range IP address tertentu. Apabila ingin menganalisa vulnerability pada sistem operasi saja, cukup dengan memilih pada bagian Options. Hasil analisa akan menunjukkan kelemahan-kelemahan yang ada pada sistem serta cara yang dapat dilakukan untuk memperbaiki kerapuhan tersebut.



Gambar 1 : Tampilan MBSA

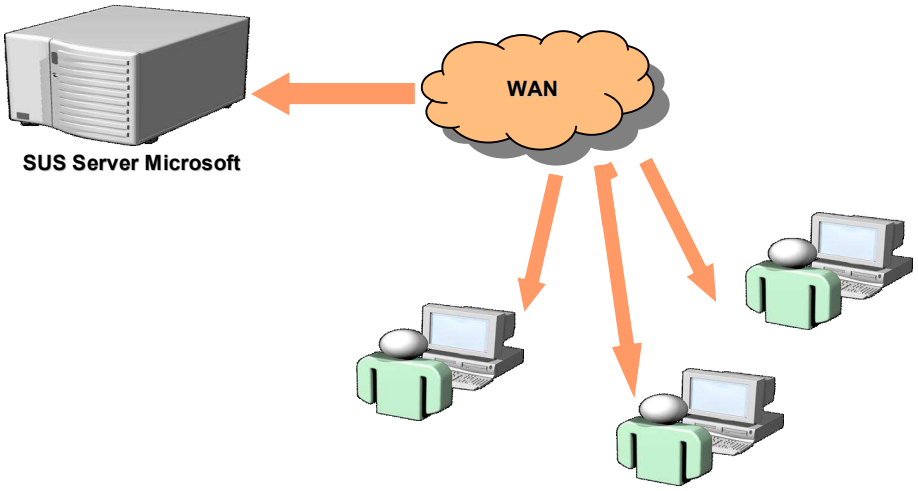
Patch Management

Microsoft menutup vulnerability melalui patch management. Implementasi termudah adalah melalui Automatic Updates untuk komputer client. Apabila komputer client memiliki akses ke internet, untuk memproteksi komputer tersebut dari serangan hacker dan worm, aktifkan Automatic Updates. Untuk mengaktifkan Automatic Updates cukup dengan membuka System Properties, kemudian buka pada bagian Automatic Updates. Pilih *Download the updates automatically and notify me when they are ready to be installed* pada bagian Notification Settings.



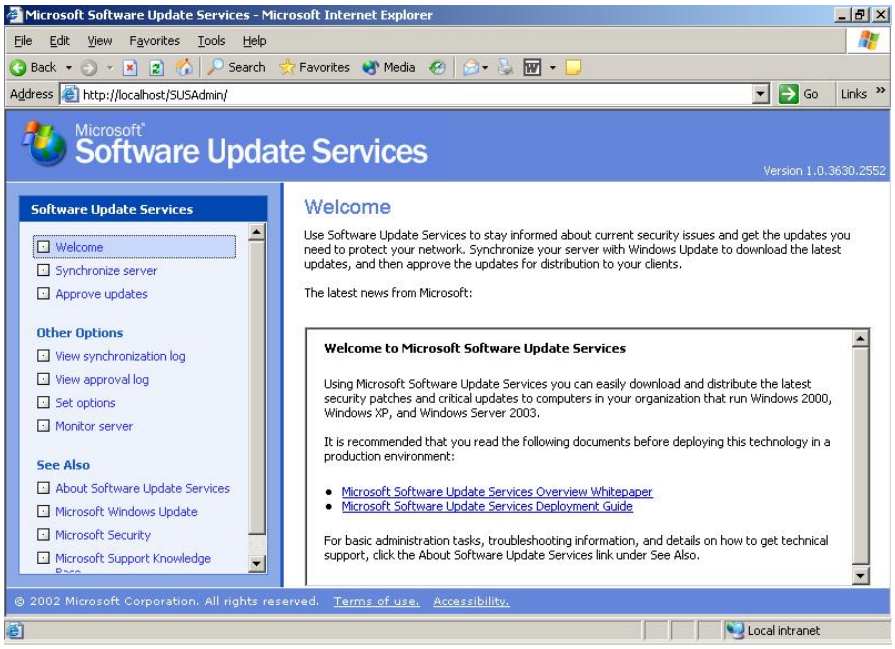
Gambar 2 : Automatic Updates pada Windows XP

Automatic Update akan menghubungkan komputer ke situs Microsoft dan melakukan download patch secara otomatis jika ada patch terbaru yang perlu diberikan dalam sistem.



Gambar 3 : Ilustrasi Automatic Updates

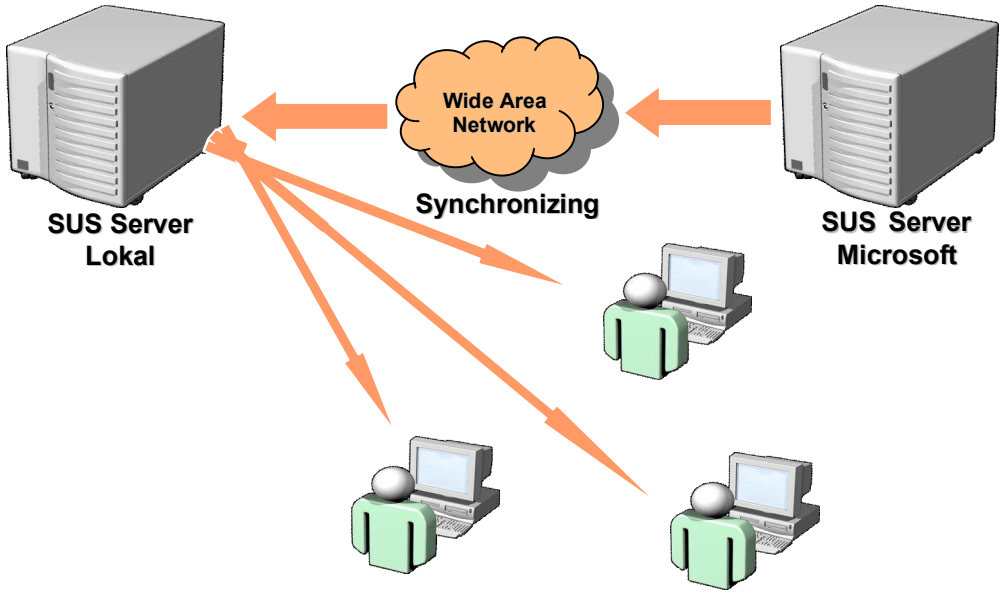
Apabila komputer client tidak terkoneksi ke internet, hal yang harus dilakukan adalah menginstalasi Software Update Service (SUS) pada server jaringan. Software Update Service sangat berguna untuk memperbaiki bug-bug yang ada dalam sistem, memperbarui komponen-komponen yang diperlukan untuk membuat sistem yang lebih baik. Kemampuan untuk mengirim pesan tentang hal yang dapat memicu vulnerability serta melakukan update secara otomatis membuat software ini berguna bagi orang yang tidak memperdulikan keamanan sekalipun. Software Update Service sudah terintegrasi dalam sistem opersi Windows 2000 SP3, Windows XP SP1 dan semua versi Windows 2003.



Gambar 4 : Software Update Services Console

Untuk menerapkan SUS, pada sistem operasi harus sudah terinstal Internet Information Service (IIS). SUS server secara otomatis juga menjadi web server bagi jaringan lokal. SUS server harus melakukan sinkronisasi dengan SUS Server Microsoft agar patch yang ada padanya adalah patch yang terbaru. Proses sinkronisasi dapat diatur jadwalnya sesuai dengan keinginan administrator jaringan, atau bisa pula dilakukan secara otomatis saat ada pembaharuan patch pada SUS server Microsoft.

Pada Software Update Service client tidak perlu melakukan koneksi langsung ke situs Microsoft. Yang perlu berhubungan langsung hanyalah komputer SUS server. Apabila ada patch terbaru dari SUS Server Microsoft, maka SUS Server Lokal akan melakukan sinkronisasi. Hasilnya akan didistribusikan kepada komputer client.



Gambar 5 : Ilustrasi Software Update Service

PUSTAKA :

Microsoft Corporation, Secure Architecture for Network and Data Infrastructure Accelerated Bootcamp, Microsoft Press, 2004

Bob Carver, Software and Patch Management, Microsoft TechNet TNT1-95