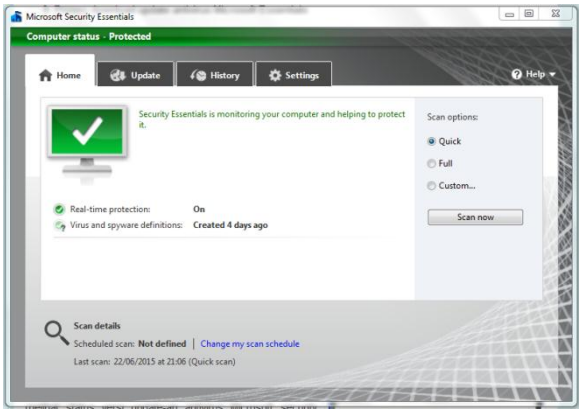
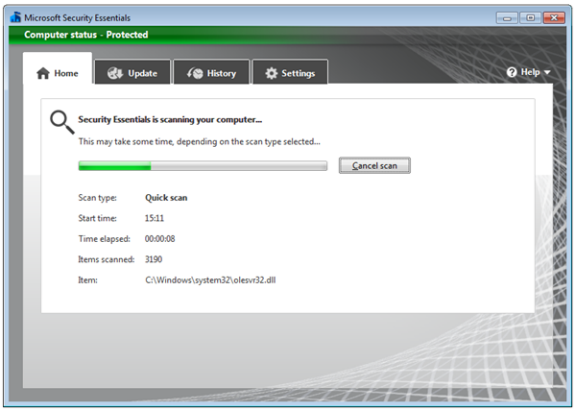
ALIF RAHMAN 1310651204

Microsoft Security Essentials

Tampilan Home & Scan

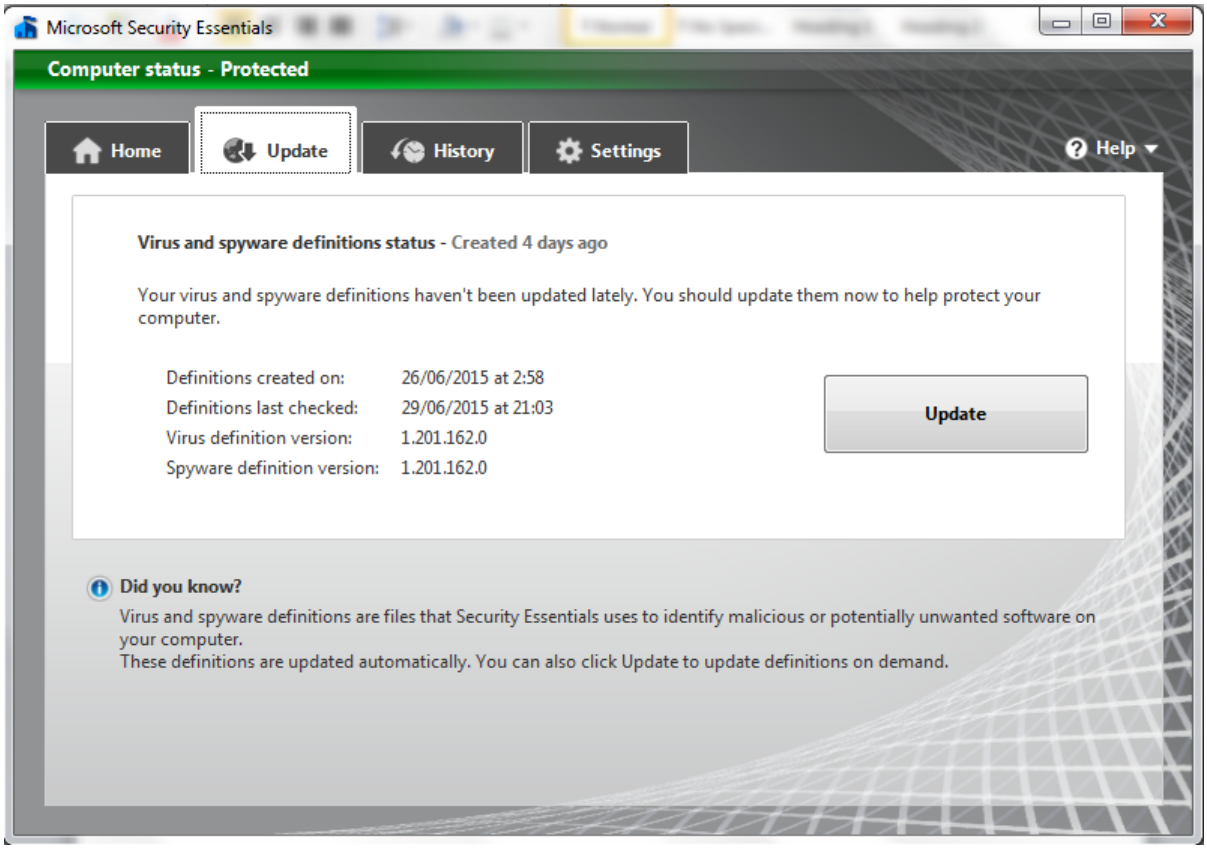




Tampilan “home & Scan” antivirus Microsoft security essentials. Berisi informasi real time protection terhadap keamanan laptop / pc anda. di bagian “Scan Option” terdapat 3 pilihan scan antivirus yaitu quick, full dan custom. Jika anda mencentang scan option “quick” maka antivirus tersebut akan menscan secara cepat hanya menscan drive C saja. Untuk pilihan scan option “full” maka seluruh drive anda akan terscan secara menyeluruh, menghabiskan banyak waktu jika menggunakan pilihan ini, tapi hasil scan lebih terasa maksimal. Pengalaman untuk hardisk sekapasitas 160 GB dengan isi hampir 95 % memakan waktu hingga kurang lebih 7 jam. Jika anda memilih scan option “custom” maka anda bebas memilih drive apa yang ingin anda scan.

ALIF RAHMAN 1310651204

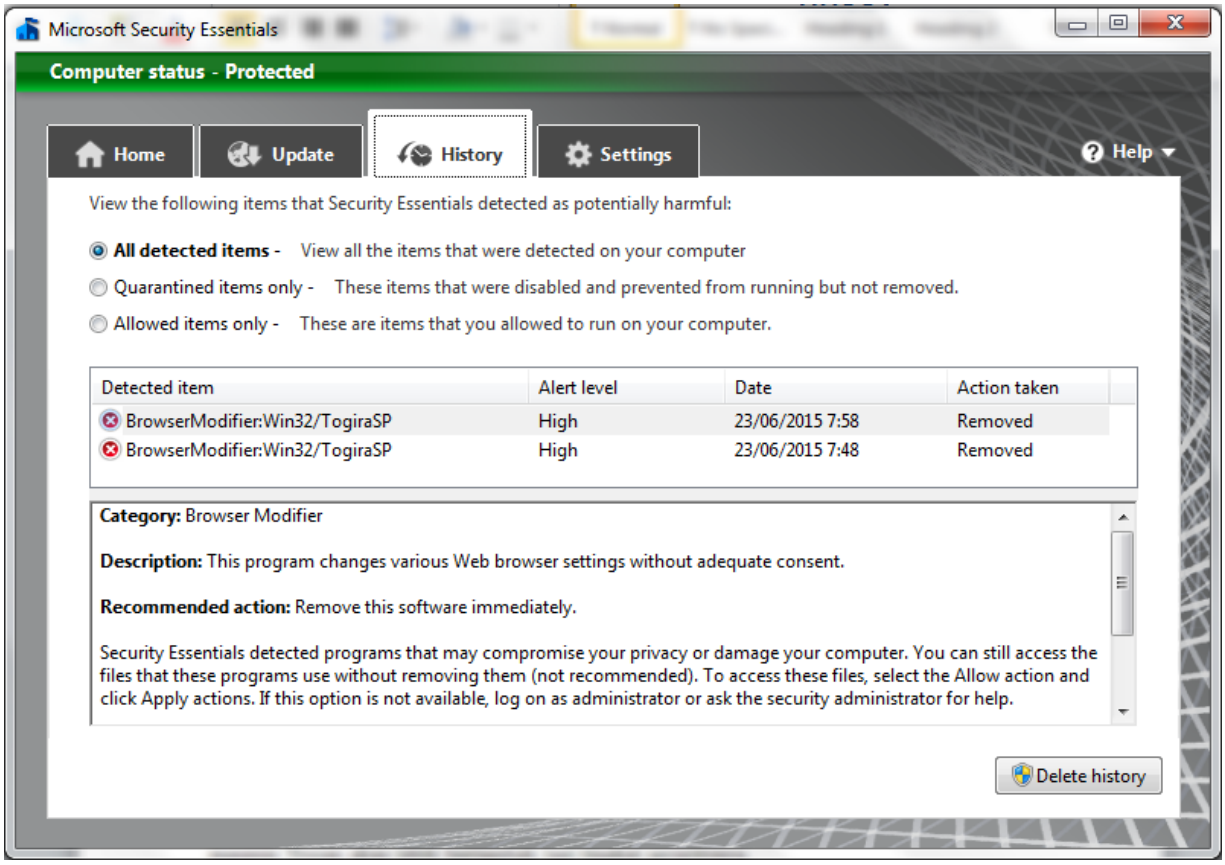
Tampilan tab Update



Tampilan tab “UPDATE” antivirus Microsoft security essentials. Berisi informasi virus dan spyware defenitions. Disini anda bisa melihat status versi update-an antivirus Microsoft security essentials anda. Biasanya jika melewati waktu update lebih dari 7 hari maka panel dari antivirus tersebut akan berwarna kuning dan meminta update. Tapi saya sarankan lebih sering update maka lebih baik. Untuk meng-update antivirus ini diperlukan koneksi internet langsung. Fasilitas update secara manual tidak disediakan. Tapi jangan khawatir jika koneksi internet yang anda gunakan stabil, maka proses update akan berjalan dengan lancar tanpa hambatan.

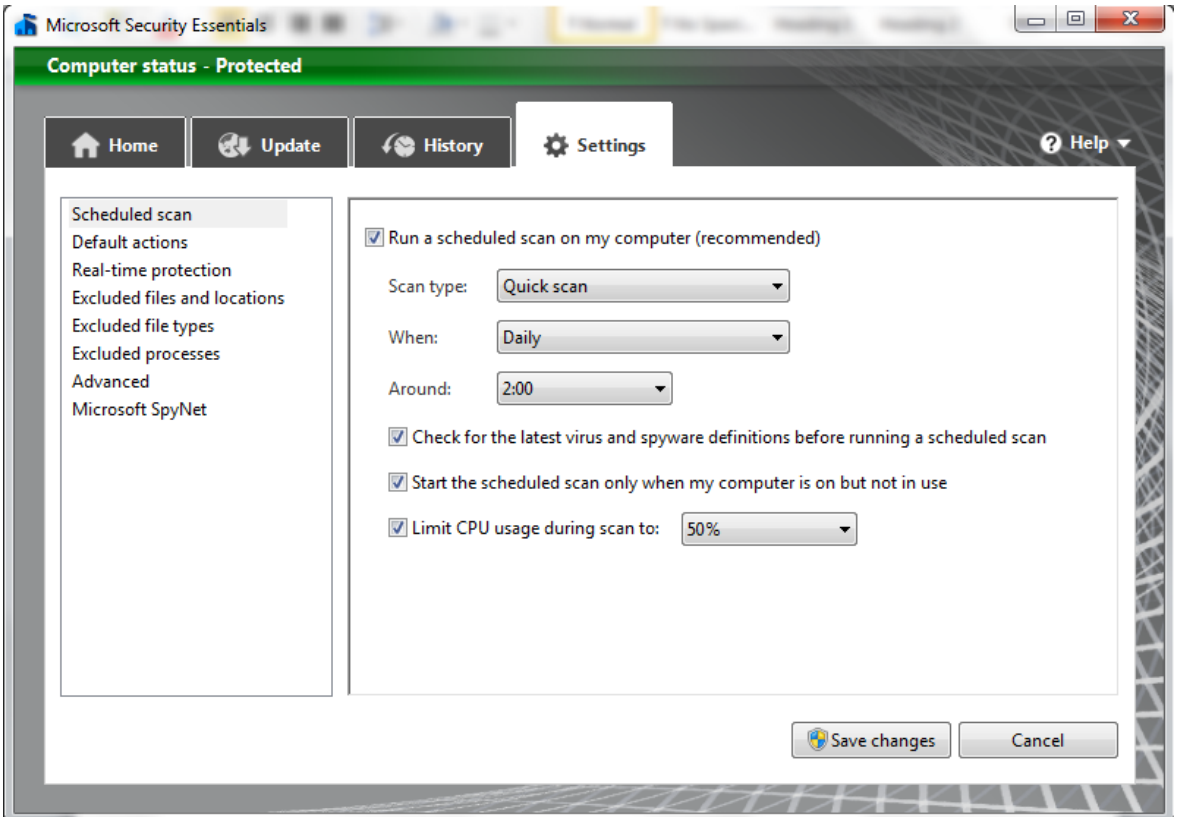
ALIF RAHMAN 1310651204

Tampilan tab history



Tamplian tab “HISTORY” antivirus Microsoft security essentials. Disini anda akan melihat beberapa detected item yang berhasil dibersihkan atau di quarantine oleh antivirus ini beserta informasi jenis virus, Trojan dsb hingga informasi system yang terinfeksi. Jika anda ingin mensubmit informasi tersebut, silahkan klik menu “help” di bagian kanan atas panel antivirus Microsoft security essentials kemudian klik “submit malicious software sample” yang nantinya dalam update-an Microsoft security essentials berikutnya database varian virus maupun Trojan akan lebih bertambah lagi tingkat securitynya.

Tampilan tab Settings



Tampilan tab “Settings” antivirus Microsoft security essentials. Lakukan pengaturan setting antivirus disini. Anda bebas mengatur konfigurasinya menurut keinginan anda masing-masing. Namun saya akan menitikberatkan pada bagian “Scheduled scan” dan “Microsoft SpyNet”.

- Pada bagian “Scheduled scan” khususnya “limit CPU usage during scan to” agar kiranya diset ke 50% (optional). Semakin tinggi angka yang anda set pada bagian ini maka semakin cepat pula proses scan virus berlangsung tapi memakan resource yang terlampau banyak. Jika program yang anda buka banyak maka akan mengakibatkan kondisi pc / laptop anda menjadi hang. Sebaliknya jika terlalu rendah, maka proses scan virus akan berjalan dengan sangat lambat. Untuk itu saya selalu menset ke 50%, tapi kembali lagi kepada anda, semua tergantung pada spesifikasi laptop / pc bawaan.
- Pada bagian “Microsoft SpyNet” terdapat tiga pilihan yaitu I do not want join Spynet, Basic membership, dan advanced membership. dengan pilihan yang ketiga. Adapun penjelasan mengenai hal ini bisa anda lihat sendiri di bagian “Microsoft Spynet”

Jangan lupa agar selalu menyimpan semua konfigurasi setting antivirus Microsoft security essentials anda dengan mengklik “Save Changes”

ALIF RAHMAN 1310651204

ACCESS CONTROL

Salah satu bagian mendasar dalam Information System Security adalah Access Control. Menurut definisi dari CISSP (Certified Information System Security Profesional) Study Guide, Access Control didefinisikan sebagai suatu proses untuk mengatur / mengontrol siapa saja yang berhak mengakses suatu resource-rosource tertentu yang terdapat di dalam sebuah sistem.

Di dalam proses ini akan diidentifikasi siapa yang sedang melakukan request untuk mengases suatu resource tertentu dan apakah orang tersebut memiliki hak akses (authorized) untuk mengakses resource tersebut. Access control memproteksi data terhadap unauthorize access atau akses yang dilakukan oleh orang yang memang tidak memiliki hak akses terhadap reource tersebut. Akses di sini bisa berupa melihat data (view) ataupun melakukan perubahan terhadapt suatu data (modify). Dengan demikian Access Control mendukung terwujudnya

1. Confidentiality Memastikan data hanya bisa dilihat oleh orang yang memiliki hak akses untuk melihat data tersebut atau dikenal dengan istilah No Unauthorized Read
2. Integrity Memastikan data hanya bisa ditulisi dan diubah oleh orang yang memiliki hak akses untuk melakukan penulisan ataupun pengubahan terhadap data tersebut atau dikenal dengan istilah No Unauthorized Write

Ketika membahas tentang Access Control, kita akan menemui dua entitas utama yang terlibat, yaitu :

1. Subject of the Access Control Yang menjadi subject di sini adalah entitas yang mengajukan request / permintaan untuk melakukan akses ke data.
2. Object of the Access Control Yang menjadi object di sini adalah entitas yang mengandung atau mengatur data. Atau dengan kata lain object adalah resource yang tersedia di dalam suatu sistem

Least Privilege, Dalam menyusun dan membuat perencanaan Access Control, salah satu prinsip yang harus dipegang adalah Least Privilege. Yang dimaksud dengan Least Privilege di sini adalah hanya memberikan hak akses yang memang dibutuhkan oleh subject yang bersangkutan untuk melakukan tugas-tugas yang memang menjadi bagian dari tanggung jawabnya. Yang perlu dicatat di sini adalah jangan pernah memberikan akses penuh (Full Access) terhadap semua resource yang tersedia di dalam sistem kepada subject. Berikan hak akses sesuai dengan yang dibutuhkannya. Tujuan utama dari prinsip ini adalah meminimalisir terjadinya Authorization Creep atau suatu kejadian yang tidak disengaja di mana suatu subject diberi hak akses yang seharusnya tidak dia miliki. Kondisi ini tentunya memiliki potensi untuk memunculkan threat / ancaman terhadap sistem yang kita miliki. Access Control sendiri dapat dibagi menjadi 3, yaitu Physical Access Control, Administrative Access Control, dan Logical Access Control.

Physical Access Control, Physical Access Control ditujukan untuk membatasi akses secara fisik ke perangkat hardware yang membangun suatu sistem Physical Access Control terbagi menjadi tiga bentuk, yaitu

1. Perimiter Security

   Perimiter Security bertujuan untuk membatasi akses masuk ke area atau lokasi di mana perangkat hardware berada. Contoh nyata dari penerapan Perimiter Security adalah penggunaan pagar dan tembok, penerapan limited access room di mana hanya beberapa orang saja yang diijinkan memasuki suatu ruangan tertentu. Pembatasan masuk ruangan bisa dilakukan menggunakan kunci ruangan ataupun perangkat autentikasi semisal card reader dan perangkat biometric seperti finger print scanner.

2. Cable Protection

   Proteksi kabel dapat dilakukan melalui beberapa cara, yaitu shielding untuk meningkatkan ketahanan terhadap EMI (Electro Magnetic Interference), memilih jenis kabel yang tahan terhadap EMI seperti fiber optic, dan juga penggunaan conduit untuk memproteksi kabel dari gangguan kerusakan secara fisik seperti misalnya gigitan tikus. Penggunaan cable shielding dimaksudkan untuk memproteksi data yang dilewatkan melalui suatu kabel dari gangguan EMI (protected the data). Sedangkan penggunaan conduit dimaksudkan untuk

memproteksi kabel itu sendiri secara fisik dari serangan yang mungkin mengakibatkan kerusakan secara fisik (protected the cable).

3. Pembagian Area Kerja

Pembagian area kerja secara fisik di antara karyawan ditujukan untuk meminimalisir terjadinya shoulder surfing. Yang dimaksud dengan istilah shoulder surfing adalah di mana seorang karyawan dapat melihat dan mengamati aktifitas yang dilakukan oleh karyawan lainnya dengan mengintip lewat balik bahu. Memang terdengar konyol, tetapi beberapa aksi pencurian password juga dilakukan dengan mekanisme seperti ini. Selain itu, dengan membagi area kerja secara fisik dapat menghidarkan seorang karyawan untuk mengetahui dan mempelajari keseluruhan proses yang sifatnya sensitif. Seorang karyawan hanya mengetahui sebagian saja dari proses sensitif tersebut yaitu proses yang memang menjadi bagian dari area kerja dan tanggung jawabnya.

Administrative Access Control, Administrative Access Control akan berisi sekumpulan peraturan dan strategi untuk membatasi akses terhadap suatu resource tertentu dalam upaya pengaman terhadap sistem. Selain itu, Administrative Access Control juga berbicara mengenai mekanisme monitoring / pengawasan dan pendeteksian terhadap pelanggaran akses terhadap suatu resource. Ada 4 point utama yang terkandung dalam Administrative Access Control, yaitu:

1. Policies and Procedure

Di sini berbicara mengenai penyusunan aturan / kebijakan dan prosedur yang jelas berkaitan dengan akses terhadap resource-resource yang terdapat di dalam sistem. Dalam point ini peranan dan dukungan dari pimpinan dalam tataran eksekutif sangatlah penting sehingga kebijakan dan juga prosedur yang sudah disusun memiliki kekuatan (dan terkadang memang perlu agak dipaksakan) untuk bisa diimplementasikan dan diikuti oleh semua karyawan yan terlibat di dalam sistem. Tanpa adanya dukungan dari pimpinan maka kebijakan dan prosedur yang sudah disusun menjadi powerless atau tak memiliki kekuatan apa-apa.

2. Hiring Pratices

Di sini berbicara mengenai mekanisme perekrutan karyawan baru. Dalam proses perekrutan, salah satu point yang perlu diperhatikan adalah tanggapan dan pendapat dari si calon karyawan tersebut berkenaan dengan kebijakan dan prosedur

yang sudah disusun. Rekrutlah karyawan yang memang sejalan dan sependapat dengan kebijakan dan prosedur yang berlaku di perusahaan.

3. Security Awareness Training

   Selain merekrut karyawan yang sependapat dengan kebijakan dan prosedur yang berlaku, perllu juga dilakukan pelatihan / training berkaitan dengan security awareness. Di sini setiap karyawan akan dijelaskan dan disadarkan betapa pentingnya aspek keamanan terhadap sistem. Diharapkan setelah mengikuti pelatihan ini setiap karyawan dapat mengikuti dan menjalankan setiap kebijakan dan prosedur yang berkaitan dengan keamanan sistem dengan penuh tanggung jawab karena telah menyadari betapa pentingnya aspek keamanan sistem yang terkandung di dalamnya.

4. Monitoring

   Point terakhir adalah monitoring atau pengawasan terhadap kebijakan dan prosedur yang berlaku. Di sini akan dilakukan pemantauan apakah setiap prosedur sudah dilakukan dengan baik atau adakah pelanggaran-pelanggaran yang terjadi terhadap kebijakan dan prosedur yang berlaku. Tujuan utama dari point ini adalah memastikan setiap kebijakan dan prosedur yang berlaku berjalan dengan baik.

Logical Access Control, Logical Access Control akan berbicara mengenai hal-hal teknis yag diberlakukan untuk melakukan pengaturan / pengendalian akses terhadap resource-resource yang ada di dalam suatu sistem. Ada 3 point utama yang terkandung dalam Logical Access Control, yaitu:

1. Object Access Restriction

   Point ini dimaksudkan untuk mengijinkan akses kepada authorized user. Hal ini bisa dilakukan dengan menggunakan Role Based Access Control di mana akan didefinisikan akses apa saja yang diijinkan kepada seorang atau sekumpulan karyawan berkaitan dengan jabatan dan wewenang yang dimilikinya.

2. Encryption

   Melakukan penyandian data sehinga data hanya bisa dibaca oleh orang-orang yang memang memiliki hak akses.

3. Network Architecture / Segregation

   Melakukan segmentasi pada infrastruktur jaringan komputer yang ada. Hal ini ditujukan untuk menghindari adanya aksi pencurian data yang dilakukan melalui infratruktur jaringan yang ada.