

Tugas UAS Keamanan Informasi



Nama:Muhammad Badar Annas

NIM:1310651217

JURUSAN TEKNIK INFORMATIKA  
FAKULTAS TEKNIK

## Soal 1

### Kontinuitas dan Masalah

#### Perencanaan pemulihan

#### PENGANTAR

Business Continuity dan Disaster Recovery Planning merupakan baris terakhir organisasi dari pertahanan: ketika semua kontrol lain telah gagal, BCP / DRP adalah kontrol akhir yang mungkin mencegah peristiwa drastis seperti cedera, hilangnya nyawa, atau kegagalan suatu organisasi. Sebagai profesional keamanan informasi, kita harus waspada dan melindungi organisasi kami dan staf dari peristiwa-peristiwa yang mengganggu.

#### BCP DAN DRP GAMBARAN DAN PROSES

Istilah dan konsep yang berhubungan dengan Business Continuity dan Disaster Recovery Perencanaan sering disalahpahami. Jelas pemahaman tentang apa yang dimaksud dengan baik. Business Continuity dan Disaster Recovery Planning, serta apa yang mereka memerlukan, sangat penting untuk CISSP® yang kandidat.

#### Perencanaan Kesiambungan Bisnis

Meskipun banyak organisasi hanya akan menggunakan frase Perencanaan Kesiambungan Bisnis. (BCP) atau Perencanaan Disaster Recovery bergantian, mereka adalah dua disiplin ilmu yang berbeda. Tujuan menyeluruh dari BCP adalah untuk memastikan bahwa bisnis akan terus beroperasi sebelum, sepanjang, dan setelah peristiwa bencana yang dialami. Fokus BCP adalah pada bisnis secara keseluruhan dan memastikan bahwa mereka yang kritis.

#### Perencanaan pemulihan bencana

Perencanaan pemulihan bencana (DRP) menyediakan rencana jangka pendek untuk mengatasi tertentu Mengurangi infeksi malware yang menunjukkan risiko menyebar ke

sistem lain adalah contoh dari gangguan berorientasi IT tertentu yang DRP yang akan alamat. DRP ini berfokus pada efisien berusaha untuk mengurangi dampak bencana dan tanggapan langsung dan pemulihan sistem TI penting dalam menghadapi signifikan peristiwa yang mengganggu.

#### Hubungan antara BCP dan DRP

adalah rencana menanggulangi, yang mencakup beberapa spesifik

#### Proses Pemulihan Bencana

Setelah membahas pentingnya Business Continuity dan Disaster Recovery Perencanaan dan contoh ancaman yang membenarkan gelar ini dari perencanaan, kita sekarang akan fokus pada langkah-langkah dasar yang terlibat dalam pemulihan dari bencana.

## Tim Aktifkan

Jika bencana dinyatakan, maka tim pemulihan harus diaktifkan. bergantung kepada lingkup bencana, komunikasi ini bisa membuktikan sangat sulit.

## Penyampaian

Salah satu aspek yang paling sulit dari pemulihan bencana adalah memastikan bahwa konsisten update status tepat waktu dikomunikasikan kembali ke tim pusat pengelolaan respon dan proses pemulihan.

## Analisis Dampak Perilaku Bisnis

Analisis Dampak Bisnis (BIA) adalah metode formal untuk menentukan bagaimana gangguan yang untuk sistem IT (s) dari sebuah organisasi akan berdampak persyaratan organisasi, proses, dan saling ketergantungan terhadap bisnis mission. analisis untuk mengidentifikasi dan memprioritaskan sistem TI kritis dan komponen.

## Strategi pemulihan

Sebuah situs berlebihan adalah duplikat produksi yang tepat dari sebuah sistem yang memiliki kemampuan untuk mulus mengoperasikan semua operasi yang diperlukan IT tanpa kehilangan layanan sampai akhir pengguna sistem. Sebuah situs berlebihan menerima backup data secara real time sehingga dalam terjadi bencana, para pengguna sistem tidak kehilangan data. Ini adalah bangunan dikonfigurasi persis seperti situs utama dan merupakan pilihan pemulihan yang paling mahal karena secara efektif lebih dari dua kali lipat biaya operasional TI

## Perjanjian Timbal Balik

Perjanjian timbal balik adalah kesepakatan dua arah antara dua organisasi di yang satu organisasi menjanjikan organisasi lain yang dapat bergerak dan berbagi ruang jika mengalami bencana.

## Rencana Terkait

Sebagaimana dibahas sebelumnya, Business Continuity Plan adalah rencana payung yang berisi rencana lain.

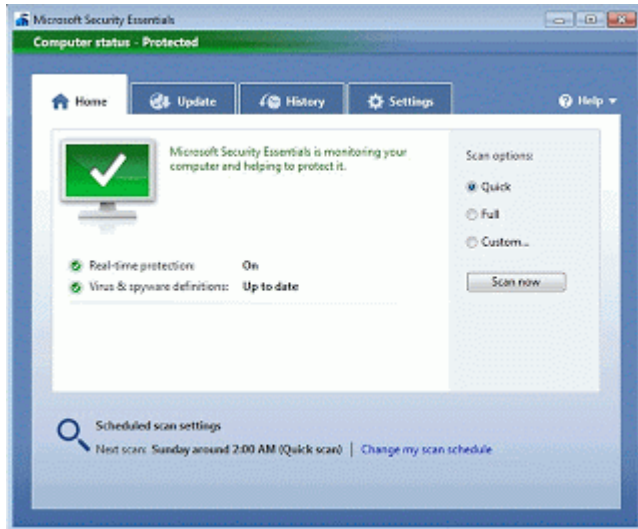
## DRP PENGUJIAN DAN PELATIHAN

Menyediakan prosedur untuk mempertahankan bisnis yang penting operasi sementara pulih dari gangguan yang signifikan. didasarkan pada dukungan untuk proses bisnis. Menyediakan prosedur untuk memulihkan operasi bisnis segera setelah bencana. Menyediakan prosedur dan kemampuan untuk mempertahankan organisasi penting, fungsi strategis pada Situs alternative. Berfokus pada informasi tanggapan keamanan untuk insiden sistem yang mempengaruhi dan / atau Jaringan.

## Soal 2

### Cara Menggunakan Microsoft Security Essentials

#### Tampilan Home

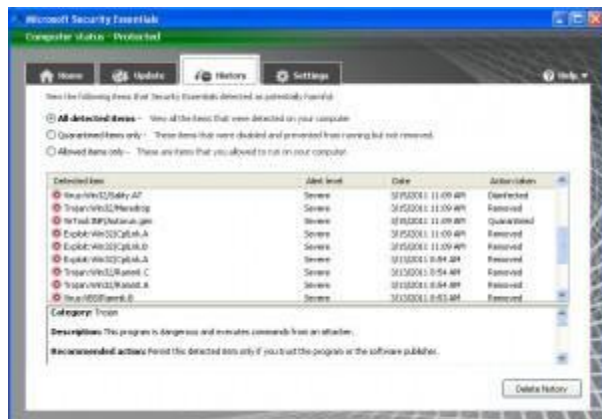


Tampilan “home” antivirus Microsoft security essentials. Berisi informasi real time protection terhadap keamanan laptop / pc anda. di bagian “Scan Option” terdapat 3 pilihan scan antivirus yaitu quick, full dan custom. Jika anda mencentang scan option “quick” maka antivirus tersebut akan menscan secara 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.

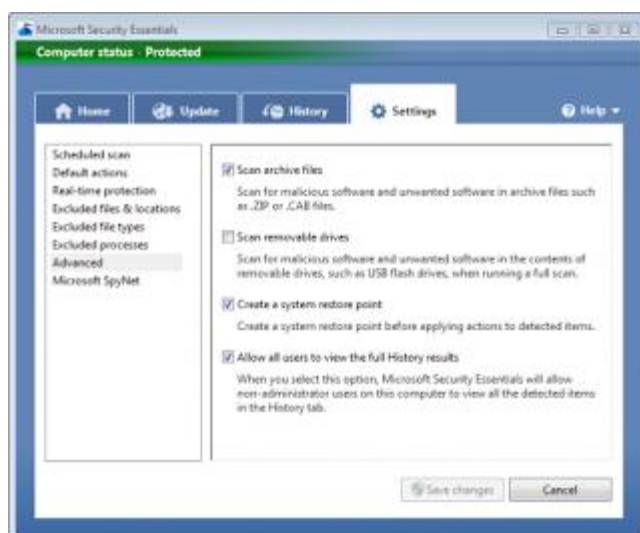
#### Tampilan tab Update



## Tampilan tab history



### 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. Saya lebih suka 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”

Pokoknya dijamin puas menggunakan antivirus Microsoft security essentials. Gratis, namun fitur dan tingkat securitynya tidak kalah jauh beda (malah lebih oke>>) dibanding antivirus gratis lainnya.

Segera upgrade dan update antivirus Microsoft security essentials anda karena virus, Trojan, worm, dan sebagainya makin hari makin ganas saja menyerang siapa saja. Baru-baru ini saja, saya terserang virus ganas sality (varian terbaru) dengan nama (win32/sality.AU). Untunglah setelah upgrade dan update, dan melakukan scanning secara full yang memakan waktu sekitar 7 jam untuk menscan kapasitas hardisk 160GB, kurang lebih 200an varian virus tersebut yang menjangkiti system pc saya terdisinfect (terobati), hanya dengan antivirus gratis yaitu antivirus Microsoft security essentials