INFRASTRUCTURE SECURITY

WHAT'S INFRASTRUCTURE ??

- Infrastruktur = prasarana, yaitu segala sesuatu yg merupakan penunjang utama terselenggaranya suatu proses.
- Kebutuhan dasar pengorganisasian sistem sebagai layanan dan fasilitas yang diperlukan agar TI dapat berfungsi dengan baik

WHAT'S INFRASTRUCTURE ??

- Infrastruktur TI : sumber daya teknologi bersama yang menyediakan platform untuk aplikasi sistem informasi perusahaan yang terperinci.
- Terdiri dari fasilitas-fasilitas fisik, jasa-jasa, dan manajemen yang mendukung seluruh sumber daya komputasi dalam suatu organisasi.

WHAT'S INFRASTRUCTURE ??

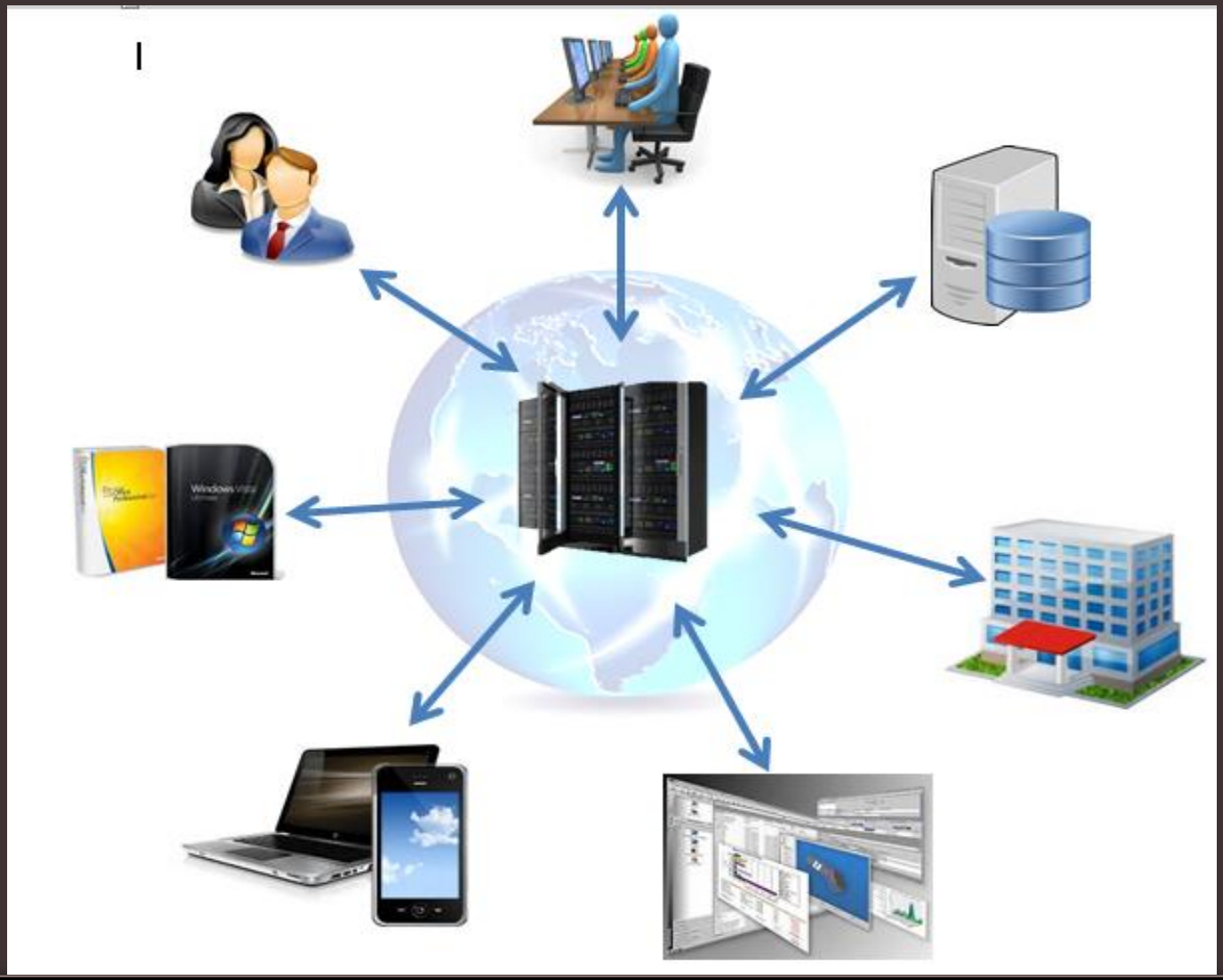
- Infrastruktur TI meliputi investasi peranti keras, peranti lunak, dan layanan seperti : konsultasi, pendidikan, dan pelatihan yang tersebar diseluruh unit bisnis dalam perusahaan.

WHAT'S INFRASTRUCTURE ??

Komponen Infrastruktur TI:

- Perangkat Keras Komputer
- Perangkat Lunak Komputer
- Manajemen dan Penyimpanan Data
- Jaringan/Telekomunikasi
- Internet
- Layanan dan Konsultasi Integrasi Sistem, dan
- Sistem Operasi

WHAT'S INFRASTRUCTURE ??



SERVER

- *Server* adalah sebuah *host* yang memiliki fungsi utama menyediakan layanan untuk *host* lain melalui jaringan.

SERVER

- Contoh:
  - *File Server* menyediakan layanan file sharing sehingga user dapat mengakses, memodifikasi, menyimpan & menghapus file
  - *Database Server* menyediakan layanan database untuk Web aplikasi pada server Web.
  - *Web Server* memberikan layanan konten Web untuk Web browser user

WHY LEARN SERVER SECURITY

- Server menyediakan berbagai macam layanan kepada user internal & eksternal
- Server menyimpan / memproses informasi sensitif bagi organisasi.
- Server sering menjadi sasaran penyerang karena nilai data dan layanannya.

KERENTANAN, ANCAMAN, DAN LINGKUNGAN SERVER

- Ancaman terhadap data dan sumber daya
  - bug di SO & software
  - kesalahan end user & admin.
- Faktor disengaja & tidak disengaja

KERENTANAN, ANCAMAN, DAN LINGKUNGAN SERVER

Bagaimana server harus diamankan ?

BENTUK ANCAMAN PADA SERVER

Ancaman keamanan untuk server:

- Malware, dapat mengeksploitasi bug software dalam server / SO untuk mendapatkan akses tidak sah ke server.
- Serangan Denial of Service (DoS) yang diarahkan ke server atau infrastruktur jaringan pendukungnya, untuk menghalangi user yang sah dalam memanfaatkan layanan.

BENTUK ANCAMAN PADA SERVER

Ancaman .....

- Perubahan informasi karena adanya user yg tidak sah bisa mengakses server
- Penyadapan akibat transmisi tidak terenkripsi.
- Entitas berbahaya bisa mendapatkan akses tidak sah ke sumber daya lain dalam jaringan melalui sebuah serangan pada server.

HOW TO SECURE SERVER

Kunci mempertahankan keamanan server:

- Merencanakan pembangunan server disertai dengan menangani aspek keamanannya sesuai dengan kegunaan, kinerja dan resiko

HOW TO SECURE SERVER

Kunci ……

- Menerapkan praktik manajemen keamanan & kontrol yang tepat
  - Kebijakan keamanan sistem informasi
  - Konfigurasi / kontrol dan manajemen perubahan
  - Penilaian risiko dan manajemen
  - Konfigurasi perangkat lunak standar
  - Kesadaran keamanan dan pelatihan
  - Perencanaan kelangsungan operasional dan perencanaan pemulihan bencana
  - Sertifikasi dan akreditasi.

HOW TO SECURE SERVER

Kunci ……

- Sistem operasi server dikonfigurasi sesuai persyaratan keamanan.
  - Patch dan upgrade SO
  - Menghapus / menonaktifkan layanan, aplikasi & protokol jaringan yang tidak perlu
  - Mengkonfigurasi otentikasi operasi sistem user
  - Mengkonfigurasi kontrol sumber daya
  - Menginstal dan mengkonfigurasi kontrol keamanan tambahan
  - Melakukan pengujian keamanan SO.

HOW TO SECURE SERVER

Kunci ……

- Aplikasi server dikonfigurasi sesuai persyaratan keamanan organisasi.
  - Patch dan upgrade server aplikasi
  - Menghapus / menonaktifkan layanan, aplikasi & konten sampel yang tidak perlu
  - Mengkonfigurasi otentikasi user dan akses kontrol
  - Mengkonfigurasi kontrol sumber daya server
  - Uji keamanan aplikasi dan server konten

HOW TO SECURE SERVER

Kunci ……

- Berkomitmen untuk menjaga proses yang sedang berlangsung untuk menjamin keamanan berikutnya.
  - Konfigurasi, melindungi & menganalisis file log secara berkelanjutan
  - Back up informasi penting
  - Membangun dan mengikuti prosedur
  - Pengujian & menerapkan patch secara tepat waktu
  - Pengujian keamanan secara berkala.

WORKSTATION

- Workstation adalah komputer yang memanfaatkan jaringan untuk berhubungan dengan komputer lain atau dengan server.
- Pemanfaatan jaringan bisa berupa sharing data, sharing printer dan sebagainya.

STANDAR KEAMANAN WORKSTATION

- Standar Keamanan Workstation Minimum
  - Keamanan Software / Update Software

    Keamanan dan update software dikonfigurasi secara otomatis, kecuali ada alasan yang dapat dibenarkan dan terdokumentasi.

    Pembaruan perangkat lunak diterapkan secara tepat waktu, dan tindakan untuk melindungi perangkat lunak yang rentan dilakukan sedini mungkin.

STANDAR KEAMANAN WORKSTATION

- Standar Keamanan .....
  - Host Berbasis Firewall

    Firewall dipasang untuk membatasi layanan apa saja yang diijinkan dan tidak.

    Mengaktifkan logging koneksi firewall untuk setiap aplikasi yang memungkinkan untuk diakses dari jarak jauh (database).

STANDAR KEAMANAN WORKSTATION

- Standar Keamanan .....
  - Anti virus dan anti malware

    Aplikasi anti-virus dikonfigurasi untuk :

    - Pembaruan signature setiap hari secara otomatis
    - Memberikan perlindungan real-time
    - Memblokir, mengkarantina dan mewaspadai eksekusi yang diduga file berbahaya / pengenalan sistem
    - Log aktivitas (fasilitas logging dipantau terpusat).

STANDAR KEAMANAN WORKSTATION

- Standar Keamanan .....
  - Inventarisasi Data

    Data yang diproduksi pada lingkungan komputasi lokal harus dipindai secara berkala.

    Setiap file yang tidak diperlukan harus dihapus dari sistem.
  - Password

    Persyaratan kompleksitas password.

    Password harus diubah secara berkala dan tidak boleh dibagi antara pengguna.

STANDAR KEAMANAN WORKSTATION

- Standar Keamanan .....
  - Transmisi Data

    Data yang dikirim melalui jaringan harus dilindungi dengan enkripsi.

  - Workstation *de-provisioning* atau *re-provisioning*

    Sebelum workstation dihapus dari layanan, semua data yang ada pada disk harus dihancurkan.

    Ketika workstation didistribusikan ke pengguna lain, akun user sebelumnya harus dihapus.

STANDAR KEAMANAN WORKSTATION

- Standar Keamanan .....
  - Keamanan Fisik

    Workstation Desktop harus berada dalam lingkungan yang aman, tidak dapat diakses oleh masyarakat umum.

    Workstation Laptop harus memiliki kunci kabel untuk mencegah pencurian.

    Mengaktifkan Screen Saver

STANDAR KEAMANAN WORKSTATION

- Standar Keamanan .....
  - *Backup*

    Workstation harus diback up secara teratur, dengan mekanisme yang diatur oleh perusahaan.