KEAMANAN JARINGAN
(SUMMARY MODUL DAN PERBEDAAN APACHE WEB SERVER NGINX IIS)

Fifin Nur Rahmawati
Dosen : Dr. Ferry Astika Saputra ST, M.Sc
3122640040
D4 LJ-Teknik Informatika

PROGRAM STUDI TEKNIK INFORMATIKA
DEEPARTEMEN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK ELEKTRONIKA NEGERI SURABAYA
2023/2024

Perbedaan Apache, Nginx, IIS

- **Apache HTTP Server** adalah perangkat lunak web server sumber terbuka dan gratis yang digunakan untuk melayani permintaan dari klien untuk mengakses halaman web atau file lainnya

- **NGINX** adalah perangkat lunak web server sumber terbuka yang dapat digunakan untuk memproses permintaan HTTP, TCP, dan UDP.
  NGINX dapat dikonfigurasi dengan file konfigurasi teks sederhana atau melalui antarmuka pengguna yang disediakan oleh pihak ketiga. NGINX juga dapat digunakan sebagai server proxy, load balancer, dan cache, sehingga membuatnya sangat fleksibel dan dapat dikustomisasi sesuai kebutuhan pengguna.
  Selain itu, NGINX juga dilengkapi dengan fitur-fitur keamanan seperti proteksi terhadap serangan DDoS dan serangan XSS (Cross-Site Scripting).

- **Microsoft IIS** adalah server web bawaan dari sistem operasi Windows Server. IIS dapat digunakan untukmenjalankan aplikasi web yang dibangun dengan teknologi Microsoft seperti ASP.NET.

Perbedaan	**Apache**	**Nginx**	**IIS**
Penanganan Traffic	Menggunakan MPM untuk pemrosesan traffic. Ada 3 MPM dengan tingkatan efisiensi yang berbeda, diantaranya mpm_prefork, mpm_worker dan mpm_event	Menggunakan algoritma bersifat asinkrot, event-driven dan non blocking untuk pemrosesan traffic	NginX lebih unggul dari Apache dari segi ***penanganan*** website dengan ***traffic*** yang tinggi.
Pemrosesan Konten Dinamis	Memiliki modul untuk memproses konten dinamis, konfigurasinya mudah	Bergantung pada software tambahan untuk memproses konten dinamis. Harus menghubungkan dengan NGINX terlebih dahulu	Seperti pada IIS 6.0, situs berisi semua konten, baik statis maupun dinamis, yang terkait dengan situs tersebut. Namun, setiap situs harus berisi setidaknya satu aplikasi, yang diberi nama aplikasi root
Akses Konfigurasi tingkat direktori	Menggunkan file htaccess, memungkinkan kostumisasi server tanpa mengubah konfigurasu utama	Tidak menawarkan akses konfigurasi di tingkat direktori	menggunakan jalur di dalam file Metabase untuk menentukan ***tingkat konfigurasi*** (layanan, ***direktori*** virtual, ***direktori*** fisik).
Cara mencari File yang diminta Request	Mencari file yang diminta request melalui document tree	Meminta request dengan mengurai URL	Fungsi pertama dari IIS adalah memproses permintaan data yang masuk dari klien ke server. Setelah itu IIS akan mengirimkan data dari server ke klien

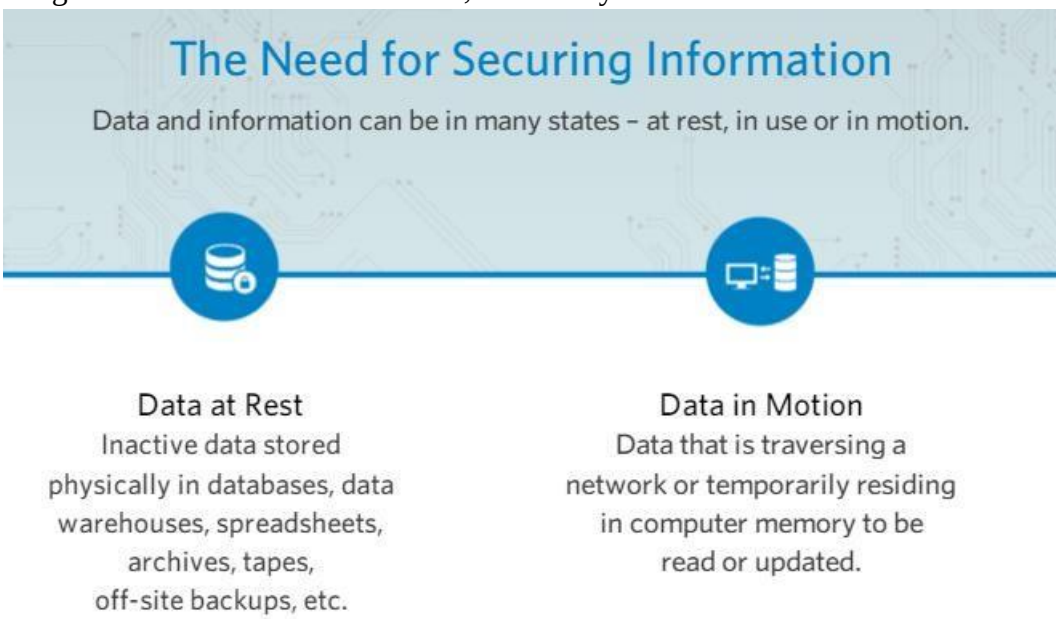
			sesuai apa yang diminta.
Kemampuan Caching	Menggunakan modul mod_cache atau Varnish	Melalukan caching menggunakan FastCGI dan mampu menangani lebih banyak request daripada Vanish milik apache	Untuk lebih meningkatkan performa untuk aplikasi dinamis, cache output ***IIS*** memberi administrator ***kemampuan*** untuk menyimpan konten dinamis
Keamanan	Rentan terhadap serangan DDoS dan serangan web lainnya	Cukup aman terhadap serangan web, namun tetap rentan terhadap serangan DDoS	Cukup aman terhadap serangan web dan DDoS, namun memerlukan konfigurasi yang tepat

Summary Modul 1

A. System Interdependencies

Jaringan yang dapat digunakan untuk bekerja sama dengan penggunaan protocol bagaimana system tersebut dan jaringan .

Pengamanan sebuah data informasi , diantaranya :



- Data istirahat, → data yang sedang tidak aktif dan disimpan pada database,
- Data bergerak→ data yang tertjnggal pada memori computer untu dibaca dan melakukan pemaharuan .

Tujuan utama keamanan informasi adalah menjaga kerahasiaan, integritas, dan ketersediaan(CIA) aset dan sistem informasi.

Kerahasiaan

Informasi tidak tersedia atau dipublikasikan kepada individu, entitas, atau proses yangtidak berwenang. Contohnya adalah : Nama pengguna dan kata sandi (atau kredensial pengguna) untuk mengakses email web hanya boleh diketahui oleh pengguna. Isi komunikasi email hanya boleh tersedia bagi penerima yang dituju.

Integritas

Menjaga keakuratan dan kelengkapan aset.
Contohnya adalah : Email yang diterima atau dikirim tidak diubah dari bentuk aslinya.

Ketersediaan

Dapat diakses dan digunakan sesuai permintaan oleh entitas yang berwenang tanpapenundaan.
Contohnya adalah : Karena komunikasi email sangat penting bagi perusahaan, layanan email ini harus tersedia setiap saat.

Ancaman, Kerentanan, dan Risiko

Ancaman adalah penyebab potensial dari dampak yang tidak diinginkan pada sistem atau organisasi. Ada beberapa kategori ancaman seperti ancaman alam, ancaman manusia dan ancaman lingkungan potensi untuk memberikan dampak yang tidak diinginkan pada sebuah system organisasi, ancaman dapat terjadi disebabkan olehancaman alami, ancaman lingkungan, dan ancaman dari manusia

Kerentanan adalah kelemahan dalam prosedur dalam keamanan sistem, desain, implementasi, atau kontrol inteltal yang dapat dilakukan (dipicu secara tidak sengaja atau dieksploitasi secara sengaja) dan mengakibatkan pelanggaran keamanan atau pelanggaran kebijakan keamanan sistem.

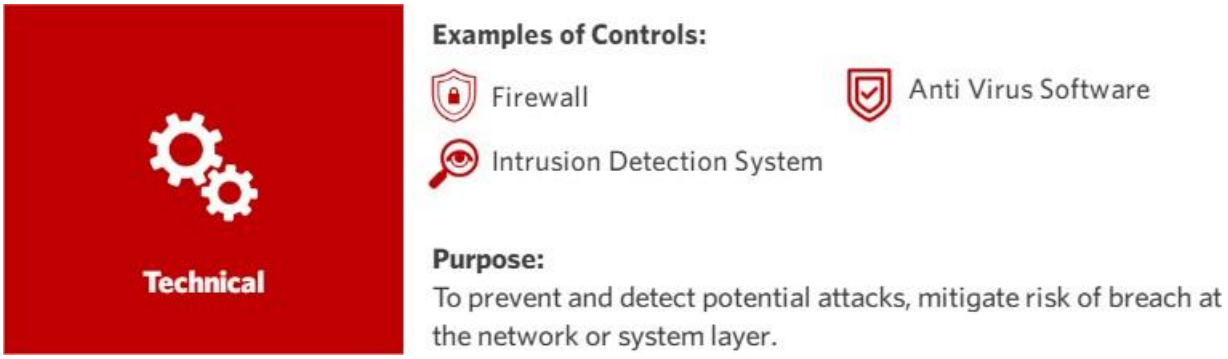
Risiko adalah kemungkinan sumber ancaman tertentu menjalankan potensi kerentanan, dan dampak yang dihasilkan dari peristiwa buruk tersebut pada organisasi.

Security Controls

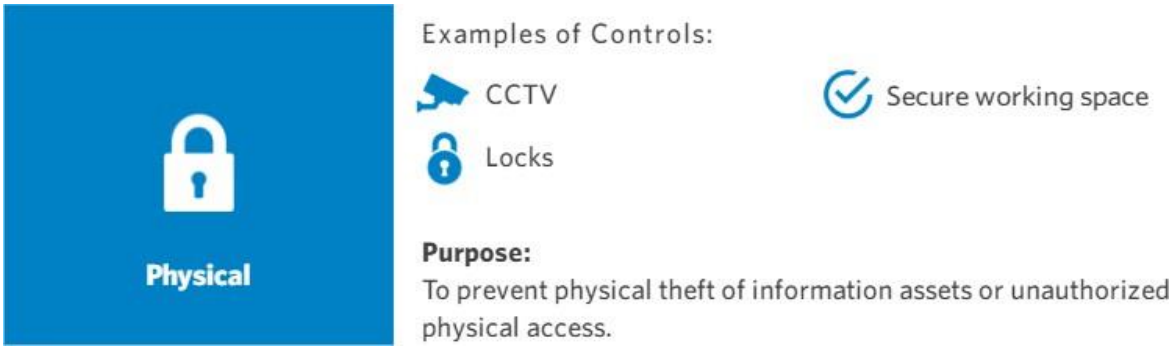
Security Controls adalah tindakan pencegahan yang dilakukan organisasi untuk melindungiaset informasi. Security Controls juga dapat mengurangi risiko.Beberapa kategori Security Controls diantaranya adalah Policy and Procedures, Technical, dan Physical. Kontrol security dibagu menjadi 3 diantaranya, peraturan dan prosedur, technical, danphysical

Policy and Procedures → membuat semua orang sadar akan pentingnya keamanan, menentukan roles sertatanggung jawab, dan ruang lingkup masalah.

Technical → mencegah dan mendeteksi potensi serangan, mengurangi risiko pelanggaranpada layer network atau system.

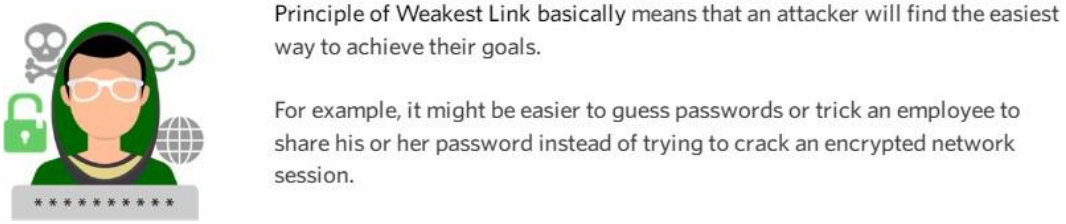


Physical → mencegah pencurian fisik aset informasi atau akses fisik yang tidak sah

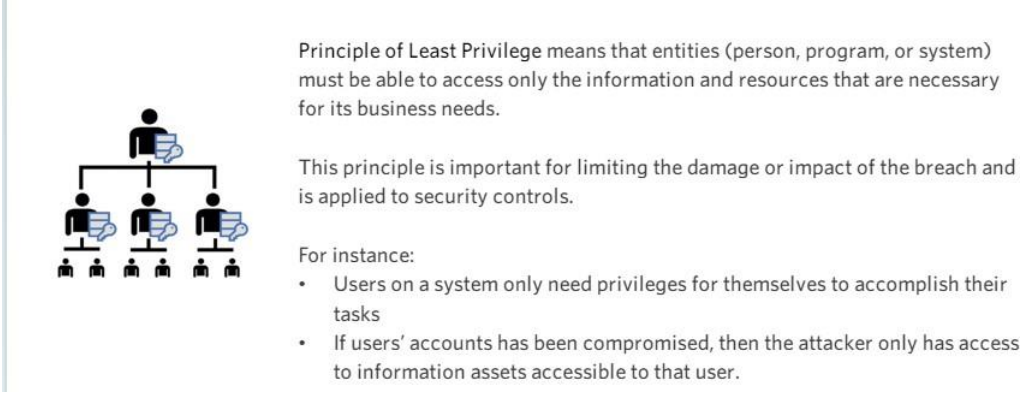


Prinsip Keamanan

Dua prinsip keamanan yang sangat bergunayaitu Principle of Weakest Link dan Principle of Least Privilege.



Principle of Weakest Link
Principle of Weakest Link pada dasarnya berarti bahwa penyerang akan menemukancara termudah untuk mencapai tujuan mereka.
Misalnya, mungkin lebih mudah untuk menebak kata sandi atau mengelabui karyawan untuk membagikan kata sandinya daripada mencoba memecahkan jaringanyang terenkripsi.



Principle of Least Privilege
Prinsip of Least Privilege pada dasarnya berarti bahwa entitas (orang, program, atausistem) harus dapat mengakses hanya informasi dan sumber daya yang diperlukan untuk kebutuhan bisnisnya. Prinsip ini penting untuk

membatasi kerusakan atau dampak pelanggaran dan diterapkan pada Security Controls.

Misalnya, pengguna pada suatu sistem hanya membutuhkan hak istimewa bagi diri mereka sendiri untuk menyelesaikan tugas-tugas mereka. Jika akun pengguna telah disusupi, penyerang hanya memiliki akses ke aset informasi yang dapat diakses olehpengguna tersebut.