Keamanan Jaringan

Oleh:

Aldo Faiz Winarno (3122640039)

D4 LJ IT B

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

TAHUN 2023

Rangkuman Modul 1

Tujuan Utama Keamanan Informasi
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 yang tidak berwenang.
- Integritas
  Menjaga keakuratan dan kelengkapan aset.
- Ketersediaan
  Dapat diakses dan digunakan sesuai permintaan oleh entitas yang berwenang tanpa penundaan.

Contoh Konteks dari Tujuan Utama Keamanan

- Kerahasiaan
  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
  Email yang diterima atau dikirim tidak diubah dari bentuk aslinya.
- Ketersediaan
  Karena komunikasi email sangat penting bagi perusahaan, layanan email ini harus tersedia setiap saat.

Ancaman, Kerentanan, dan Risiko

- Ancaman
  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.
- Kerentanan
  Kerentanan adalah cacat atau kelemahan dalam prosedur 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
  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 melindungi aset informasi. Security Controls juga dapat mengurangi risiko.

Beberapa kategori Security Controls diantaranya adalah Policy and Procedures, Technical, dan Physical.

Fungsi Security Controls

- Policy and Procedures
  Untuk membuat semua orang sadar akan pentingnya keamanan, menentukan roles serta tanggung jawab, dan ruang lingkup masalah.
- Technical
  Untuk mencegah dan mendeteksi potensi serangan, mengurangi risiko pelanggaran pada layer network atau system.
- Physical
  Untuk mencegah pencurian fisik aset informasi atau akses fisik yang tidak sah.

Prinsip Keamanan

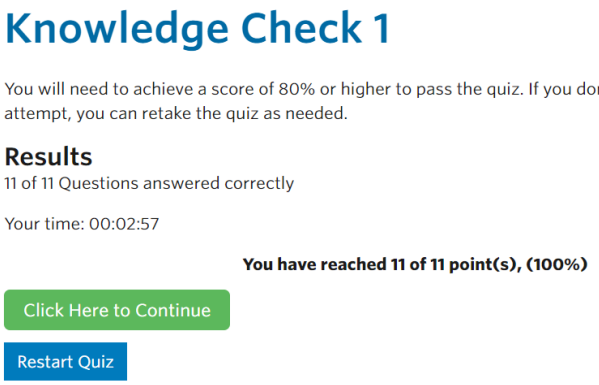
Seperti yang dapat kita lihat, ada berbagai jenis Security Controls yang harus diterapkan berdasarkan penilaian risiko. Dalam hal ini, ada dua prinsip keamanan yang sangat berguna yaitu Principle of Weakest Link dan Principle of Least Privilege.

- Principle of Weakest Link
  Principle of Weakest Link pada dasarnya berarti bahwa penyerang akan menemukan cara termudah untuk mencapai tujuan mereka.

  Misalnya, mungkin lebih mudah untuk menebak kata sandi atau mengelabui karyawan untuk membagikan kata sandinya daripada mencoba memecahkan jaringan yang terenkripsi.

- Principle of Least Privilege
  Prinsip of Least Privilege pada dasarnya berarti bahwa entitas (orang, program, atau sistem) 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 oleh pengguna tersebut.



Web Server

Apache HTTP Server
adalah salah satu server web yang paling populer dan paling banyak digunakan di seluruh dunia. Apache dapat berjalan pada sistem operasi berbasis Unix dan Windows, serta memiliki banyak fitur dan opsi konfigurasi yang fleksibel.

Nginx
adalah server web ringan dan cepat yang digunakan oleh banyak situs web besar di seluruh dunia. Nginx dapat digunakan sebagai server web utama atau sebagai server reverse proxy.

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

Perbandingan

	Apache HTTP Server	Nginx	Microsoft IIS
Popularitas	Sangat populer, digunakan pada sekitar 40% situs web di seluruh dunia	Sangat populer, digunakan pada sekitar 20% situs web di seluruh dunia	Digunakan pada sekitar 8% situs web di seluruh dunia
Arsitektur	Arsitektur modular	Arsitektur event-driven dan asinkronus	Arsitektur monolitik
Performa	Cukup cepat, namun dapat menjadi lambat jika ada banyak permintaan sekaligus	Sangat cepat dan efisien dalam menangani banyak permintaan secara bersamaan	Cukup cepat, namun kurang efisien dibandingkan dengan Apache dan Nginx
Konfigurasi	Memiliki opsi konfigurasi yang sangat fleksibel	Konfigurasi relatif mudah dengan beberapa opsi tambahan yang tersedia	Memiliki opsi konfigurasi yang cukup rumit dan membutuhkan keahlian khusus
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
Dukungan	Dukungan komunitas yang besar dan banyak sumber daya online	Dukungan komunitas yang besar dan banyak sumber daya online	Dukungan resmi dari Microsoft dan banyak sumber daya online
Platform	Bisa dijalankan di berbagai sistem operasi, termasuk Unix, Linux, dan Windows	Bisa dijalankan di berbagai sistem operasi, termasuk Unix, Linux, dan Windows	Hanya bisa dijalankan pada sistem operasi Windows