Keamanan Jaringan

(Esai 2)

Oleh:

Aldo Faiz Winarno (3122640039)

D4 LJ IT B

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

TAHUN 2023

Cyber

Awal mula adanya cyber pada tahun 2005, ditandai dengan adanya Convergence of ICT, yaitu penggabungan teknologi yang berbeda, seperti telepon, komputer, televisi, dan internet, menjadi satu platform. Convergence of ICT membawa berbagai manfaat, seperti peningkatan efisiensi, keterjangkauan, dan kemudahan penggunaan teknologi.

Terdapat 4 bagian dalam menghubungkan satu teknologi dengan teknologi lainnya, yaitu:

- Apps
- Transport
- Internet
- Net. Access

Dulu, ke-empat bagian tersebut saling berpisah, dimana Apps dan Transport merupakan Apps dan Security, kemudian Internet merupakan Infrastuktur dan Net. Access merupakan media komunikasi. Namun saat ini ke-embat bagian tersebut telah menjadi satu dan saling membutuhkan satu dengan lainnya.

Bisnis/Perusahaan

Saat ini, dunia IT tidak lepas dengan yang namanya bisnis atau perusahaan. Setiap perusahaan bisnis pasti menggunakan IT didalamnya. Dulu, IT hanya merupakan bagian support yang membantu bisnis itu berjalan. Namun saat ini, IT telah menjadi bagian dari Business Support yang mendukung core-business tersebut berjalan. Apabila IT tidak diimplementasikan dalam bisnis tersebut maka memungkinkan core-business tersebut tidak akan dapat berjalan atau masih mengimplementasikan cara tradisional. Oleh karna itu, IT sangat penting dalam sebuah perusahaan yang menjalankan bisnis saat ini.

Pemerintah

Pemerintah merupakan stakeholder yang sangat penting. Pemerintah berkewajiban untuk melindungi warganya dan memastikan mereka aman dan terlindungi di dunia maya. Untuk mencapai tujuan itu, beberapa pemerintah telah mengembangkan Strategi Keamanan Nasional yang menguraikan rencana mereka untuk:

- Melindungi sistem informasi dan infrastruktur yang penting
- Meningkatkan ketangguhan dan kesiapsiagaan dalam menghadapi serangan siber
- Menetapkan peran dan tanggung jawab berbagai lembaga atau kementerian pemerintah
- Meninjau atau mengembangkan kebijakan dan undang-undang yang relevan
- Meningkatkan kesadaran keamanan di antara warga

Pemerintah telah memiliki satu badan untuk bertugas untuk membantu menjalankan beberapa rencana tersebut. Badan tersebut adalah BSSN (Badan Siber dan Sandi Negara).

BSSN

BSSN (Badan Siber dan Sandi Negara) adalah sebuah lembaga pemerintah Indonesia yang bertanggung jawab dalam bidang keamanan siber dan sandi negara. Tugas utama BSSN adalah melindungi sistem informasi negara dan mencegah serangan siber yang berpotensi merugikan kepentingan negara dan masyarakat Indonesia. BSSN bertindak sebagai pusat koordinasi untuk memperkuat sistem keamanan siber nasional dan memberikan nasihat teknis terkait keamanan siber kepada pemerintah, swasta, dan masyarakat umum.

BSSN mengambil dari 3 lembaga terkait keamanan siber dan sandi negara sebelumnya, yaitu Lembaga Sandi Negara (LSN), Direktorat Siber dan Sandi Negara (DSSN) yang berada di bawah Kementerian Komunikasi dan Informatika (Kominfo) dan IDSIRTI. Namun, dengan semakin kompleksnya ancaman keamanan siber dan perlunya koordinasi yang lebih baik antara berbagai lembaga terkait, pemerintah Indonesia memutuskan untuk membentuk Badan Siber dan Sandi Negara.

BSSN bertanggung jawab langsung kepada Presiden dan memiliki tugas untuk mengoordinasikan seluruh kegiatan keamanan siber dan sandi negara di Indonesia. BSSN juga berperan dalam memberikan nasihat teknis terkait keamanan siber dan sandi negara kepada pemerintah, swasta, dan masyarakat umum.

Sejak didirikan, BSSN telah melakukan berbagai upaya untuk meningkatkan keamanan siber dan sandi negara di Indonesia. Beberapa kegiatan yang dilakukan antara lain menyusun kebijakan dan strategi keamanan siber nasional, mengembangkan sistem pengamanan informasi dan teknologi siber nasional, serta memberikan pelatihan dan sertifikasi untuk tenaga ahli keamanan siber.

Perpres No.82 Tahun 2022

Perpres ini berisi sektor - sektor vital yang ada di Indonesia. Beberapa sector tersebut yaitu:

- administrasi pemerintahan;
- energi dan sumber daya mineral;
- transportasi;
- keuangan;
- kesehatan;
- teknologi informasi dan komunikasi;
- pangan;
- pertahanan;

Kebijakan ini dimaksudkan untuk mendorong penggunaan teknologi informasi dalam pengadaan barang dan jasa pemerintah, yang diharapkan dapat meningkatkan transparansi, akuntabilitas, dan efektivitas pengadaan.

UU ITE

UU ITE merupakan undang-undang yang pertama kali diterbitkan pada tahun 2008. UU ITE bertujuan untuk mengatur transaksi elektronik dan perlindungan informasi di Indonesia.

Sejak pertama kali diterbitkan, UU ITE telah mengalami beberapa kali perubahan dan penyesuaian. Perubahan tersebut bertujuan untuk menyesuaikan UU ITE dengan perkembangan teknologi dan tuntutan masyarakat serta untuk menghilangkan ketidakpastian hukum yang terjadi dalam praktik penerapannya.Pada tahun 2016, UU ITE mengalami perubahan yang cukup signifikan.

Network Operator

Operator jaringan memperoleh alamat IP dan nomor AS dari Registri Internet Regional (seperti APNIC). Mereka menyediakan infrastruktur penting yang memungkinkan pengguna untuk terhubung ke Internet dengan merutekan paket dan mengumumkan rute ke jaringan lain.

Selebihnya tentang operator jaringan:

- Kepentingan utama: memastikan ketersediaan tinggi dan stabilitas jaringan untuk pelanggan mereka.
- Umumnya, mereka memiliki kebijakan untuk mencegah penggunanya melakukan penyalahgunaan jaringan. Mereka juga menyediakan titik kontak melalui database whois untuk melaporkan penyalahgunaan atau insiden keamanan.
- Di beberapa negara, mereka bekerja sama dengan CERT Nasional dalam menangani insiden keamanan.