

TUGAS

KEAMANAN JARINGAN

“CYBER SECURITY ECOSYSTEM - GOVERNMENTS”



Nama : Mega Putri Rahmawati Darta

Kelas : D4 LJ IT B

NRP : 3122640038

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

TAHUN AJARAN 2022/2023

Governments atau pemerintahan merupakan salah satu instansi penting yang bertanggung jawab untuk melindungi warganya dan memastikan mereka aman saat berada di dunia nyata maupun dunia maya. Setiap pemerintahan suatu negara memiliki Computer Emergency Response Teams (CERTs) untuk koordinasi yang lebih baik lagi. Lembaga yang bertugas sebagai CERTs di Indonesia ialah BSSN (Badan Siber dan Sandi Negara). BSSN merupakan lembaga pemerintah yang berada di bawah dan bertanggung jawab kepada Presiden. Organisasi dan Tata Kerja BSSN kemudian diatur dalam Peraturan BSSN Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja BSSN. BSSN bukan merupakan lembaga baru namun merupakan transformasi peleburan lembaga keamanan informasi pemerintah yang telah ada sebelumnya, yaitu Lembaga Sandi Negara (Lemsaneg) dan Direktorat Keamanan Informasi, Direktorat Jenderal Aplikasi Informatika, Kementerian Komunikasi dan Informatika (KemenKominfo) sebagaimana diatur dalam Perpres Nomor 53 tahun 2017 tentang BSSN yang selanjutnya disempurnakan dengan Perpres Nomor 133 tahun 2017. Dengan dibentuknya BSSN, maka pelaksanaan seluruh tugas dan fungsi di bidang Persandian di Lemsaneg serta pelaksanaan seluruh tugas dan fungsi di bidang keamanan informasi, pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet, dan keamanan jaringan dan infrastruktur telekomunikasi yang ada di KemenKominfo dilaksanakan oleh BSSN. Dalam tujuan tujuan mengamankan data warga negara terdapat hal berikut yang dilakukan oleh pihak pemerintahan sebagai berikut :

1. Protect government information systems and critical infrastructures

Hal yang dilakukan oleh pemerintah yang pertama adalah melindungi sistem informasi pemerintah dan infrastruktur penting. Di Indonesia sudah diterapkan dengan adanya pembuatan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). UU ITE adalah undang-undang pertama di bidang Teknologi Informasi dan Transaksi Elektronik sebagai produk legislasi yang sangat dibutuhkan dan telah menjadi pionir yang meletakkan dasar pengaturan di bidang pemanfaatan Teknologi Informasi dan Transaksi Elektronik. UU ITE sendiri terbit pada 25 Maret 2008 dengan cakupan meliputi globalisasi, perkembangan teknologi informasi, dan keinginan untuk mencerdaskan kehidupan bangsa.

2. Increase the resilience and preparedness in dealing with cyber attacks

Selanjutnya hal kedua yang dilakukan oleh pemerintahan ialah meningkatkan ketahanan dan kesiapsiagaan dalam menghadapi serangan siber. Di Indonesia hal ini dibuktikan dengan dibuatnya Peraturan Presiden (PERPRES) Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital. Terdapat sosialisasi terhadap perpres tersebut yang dilakukan oleh BSSN sebagai bentuk tindaklanjut untuk mencegah kejadian-kejadian, hal-hal kebocoran data yang semakin meningkat sesuai dengan isu yang berkembang saat ini.

Terdapat sektor yang dianggap strategis yaitu jika terjadi gangguan, kerusakan, dan/atau kehancuran pada IIV dalam sektor dimaksud berdampak serius terhadap kepentingan umum, pelayanan public, pertahanan dan keamanan, atau perekonomian nasional.

1. Administrasi Pemerintahan
2. Energi dan Sumber Daya Mineral

3. Transportasi
4. Keuangan
5. Kesehatan
6. Teknologi Informasi dan Komunikasi
7. Pangan
8. Pertahanan

Berikut merupakan versi lengkap dari [Perpres No. 82 tahun 2022](#).

3. Define roles and responsibilities of various government agencies or ministries

Hal ketiga yang dilakukan adalah menetapkan peran dan tanggung jawab berbagai lembaga atau kementerian pemerintah. Di Indonesia sudah dilakukan penetapan peran dan tanggung jawab Lembaga pemerintahan dengan dibuatnya BSSN (Badan Siber dan Sandi Negara) pada 19 Mei 2017. BSSN ini merupakan gabungan dari :

- Direktorat Keamanan Informasi Kementerian Komunikasi dan Informatika
- IDSIRTII/CC (Indonesia Security Incident Response Team on Internet Infrastructure / Coordination Center) merupakan lembaga yang menanggulangi atau bertanggungjawab jika terjadi insiden. Contoh kasus insiden Indosat BGP tumbang 2014, handphone Pak Presiden SBY di sadap oleh Australia 2009.
- Lembaga Sandi Negara merupakan lembaga yang bertugas dalam hal enkripsi komunikasi. Contoh : adanya Cyber Sovereignty.

4. Riview or develop policies and relevant laws

Hal keempat yang harus dilakukan ialah meninjau atau mengembangkan kebijakan dan undang-undang yang relevan. Hal ini sudah diterapkan di Indonesia dengan adanya perubahan (amandemen) dari setiap undang-undang yang dianggap masih kurang sesuai ataupun sudah tidak relevan. Contohnya ialah adanya perubahan pada UU ITE dianggap memiliki sejumlah pasal karet dan kejanggalan, serta membatasi hak kebebasan berekspresi, mengeluarkan pendapat, dan menghambat kreativitas berinternet sehingga banyak masyarakat sipil mendesak Kementerian Koinfo, Kementerian Hukum dan HAM serta DPR untuk merevisi atau menghapus pasal-pasal yang dirasa kurang sesuai. Berikut merupakan [Salinan Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik](#).

5. Enhance security awareness among the citizens

Hal kelima yang dilakukan oleh pemerintahan ialah dengan meningkatkan kesadaran keamanan di kalangan warga. Hal ini sudah dilakukan contohnya saja dengan adanya sosialisasi mengenai Perpres No. 82 tahun 2022 yang diikuti oleh 150 peserta dari lintas kementerian/lembaga di antaranya Kementerian Koordinator Bidang Politik, Hukum dan Keamanan (Kemenko Polhukam), Kementerian Hukum dan Hak Asasi Manusia (Kemenkumhan), Kantor Staf Presiden (KSP), Badan Intelijen Negara (BIN), Kejaksaan Agung (Kejagung), hingga TNI dan POLRI. Sebenarnya tidak hanya di instansi negara aja tapi diperlukan juga sosialisasi di warga sipil biasa untuk menyadarkan mereka agar lebih berhati-hati dalam menyebarkan data pribadi.