Senarai Lima Prinsip Keamanan Sistem Pemerintahan Berbasis Elektronik

Ditulis oleh Happy Chandraleka, S.T.
Pranata Komputer pada
Pusat Kebijakan Sistem Ketahanan Kesehatan dan Sumber Daya Kesehatan
Ditulis di Jakarta, 07 Dzulhijjah 1445 H/ 14 Juni 2024 M

Ada lima prinsip keamanan informasi dalam Sistem Pemerintahan Berbasis Elektronik (SPBE) yaitu:

1. Kerahasiaan
2. Keutuhan
3. Ketersediaan
4. Keaslian
5. Kenirsangkalan

Lima prinsip ini termaktub dalam pasal 40 Peraturan Presiden Republik Indonesia nomor 95 tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik yang ditetapkan pada 2 Oktober 2018.

Lima prinsip ini pula yang menjadi standar teknis keamanan data dan informasi sebagaimana tertuang dalam Peraturan Badan Siber dan Sandi Negara nomor 4 tahun 2021 pada pasal 19. Peraturan ini diketok pada 19 Mei 2021.

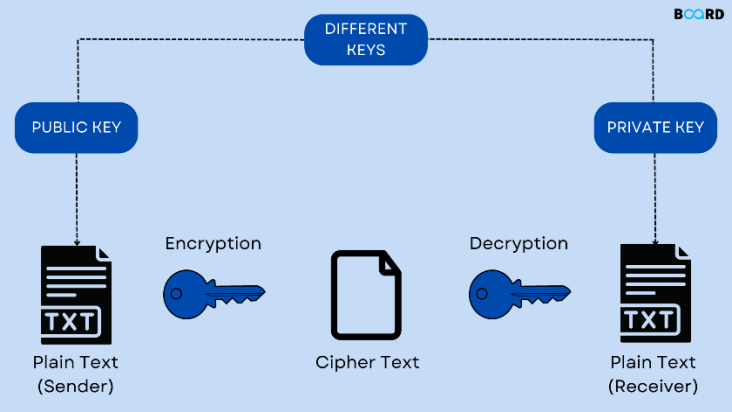
Lima prinsip tersebut harus tercakup dalam semua sumber daya terkait dengan data dan informasi, infrastruktur SPBE, dan aplikasi SPBE.

Kerahasiaan (Confidentiality)

Aspek kerahasiaan maksudnya data dan informasi tersebut hanya tersedia atau bisa diakses hanya untuk orang-orang yang diberi hak saja. Aspek kerahasiaan dilakukan dengan cara membuat klasifikasi informasi maksudnya membuat filter bahwa informasi tersebut ada yang bersifat umum, terbatas, atau rahasia. Ini cara yang pertama.

Cara yang kedua, aspek kerahasiaan dapat dicapai dengan cara penerapan pembatasan akses terhadap data dan informasi sesuai dengan kewenangan dan kebijakan yang telah digariskan.

Cara yang ketiga, dilakukan dengan penerapan sistem kriptografi. Kriptografi adalah suatu teknik untuk mengacak informasi (enkripsi) sehingga informasi tersebut tidak tersedia dalam bentuk *plain text*. Sehingga siapa pun yang berhasil mendapatkan informasi teracak itu harus mengembalikan (dekripsi) pesan yang teracak ke bentuk semula.



(https://www.boardinfinity.com/blog/cryptography-explanation-and-types/)

Keutuhan (Integrity)

Aspek keutuhan maksudnya data atau informasi tersebut utuh dan tidak berubah. Kalau pun bisa diubah hanya oleh orang-orang yang diberi kewenangan. Aspek keutuhan dilakukan dengan menerapkan pendeteksian modifikasi.

Selain itu aspek keutuhan dapat dilakukan dengan menerapkan tanda tangan elektronik tersertifikasi. Saat ini Balai Sertifikasi Elektronik (BsrE) merupakan penyelenggara tanda tangan elektronik di Indonesia.

Ketersediaan (Availability)

Aspek ketersediaan ini maksudnya adalah bahwa data atau informasi tersebut harus dapat diakses kapan saja dan di mana saja. Bila tidak dapat diakses berarti telah terjadi gangguan pada sistem penyedia data dan informasi tersebut.

Aspek ketersediaan dapat dicapai dengan menerapkan sistem pencadangan (backup) secara berkala. Membuat perencanaan untuk menjamin data dan informasi dapat selalu diakses.

Selain itu perlu dilakukan pula sistem pemulihan (recovery) yang handal sebagai antisipasi bila terjadi insiden.

Keaslian (Authentication)

Aspek keaslian maksudnya sistem mengenali bahwa sistem sedang berhadapan dengan orang yang memiliki kewenangan untuk mengakses. Aspek ini dapat dicapai dengan melakukan verifikasi dan validasi.

Verifikasi maksudnya adalah sistem berhadapan dengan pemilik akun yang sah. Misalnya dengan mengirimkan kode verifikasi ke nomor handphone atau alamat email yang dimasukkan pengguna.

Validasi maksudnya data dan informasi yang diberikan sah dan akurat. Misalnya seorang pengguna memasukkan kata sandi atau PIN saat melakukan transaksi elektronik.

Teknologi untuk mengimplementasikan aspek ini adalah dengan tanda tangan elektronik, enkripsi, Two-Factor Authentication (2FA) atau Multi-Factor Authentication (MFA), sertifikat digital, dan otoritas berbasis peran.

(https://www.zoho.com/blog/directory/why-is-mfa-important-for-your-business.html)

Kenirsangkalan (Nonrepudiation)

Aspek kenirsangkalan maksudnya adalah menjamin informasi tersebut tidak dapat disangkal oleh pihak pengirim atau penerima. Aspek ini dapat diterapkan dengan implementasi tanda tangan elektronik tersertifikasi atau sertifikat elektronik.