MODUL PERTEMUAN ONLINE
STANDAR DAN KEBIJAKAN KEAMANAN SISTEM INFORMASI DAN TEKNOLOGI INFORMASI

A. PENDAHULUAN

Informasi saat ini sudah menjadi sebuah komoditi yang sangat penting. Bahkan ada yang mengatakan bahwa kita sudah berada di sebuah "information-based society".Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi, baik yang berupa organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintahan, maupun individual (pribadi). Survey Information Week (USA), 1271 system or network manager, hanya 22% yang menganggap keamanan sistem informasi sebagai komponen penting.Kesadaran akan masalah keamanan masih rendah.

1988. Keamanan sistem mail *sendmail dieksploitasi oleh Robert* Tapan Morris sehingga melumpuhkan sistem Internet. Kegiatan ini dapat diklasifikasikan sebagai "*denial of service attack".* Diperkirakan biaya yang digunakan untuk memperbaiki dan hal-hal lain yang hilang adalah sekitar $100 juta. Di tahun 1990 Morris dihukum (convicted) dan hanya didenda $10.000.

10 Maret 1997. Seorang hacker dari Massachusetts berhasil mematikan sistem telekomunikasi sebuah airport lokal (Worcester, Mass.) sehingga memutuskan komunikasi di control tower dan menghalau pesawat yang hendak mendarat.

Transisi dari single vendor ke multi-vendor sehingga lebih banyak yang harus dimengerti dan masalah interoperability antar vendor yang lebih sulit ditangani.Meningkatnya kemampuan pemakai di bidang komputer sehingga mulai banyak pemakai yang mencoba-coba bermain atau membongkar sistem yang digunakannya.Kesulitan dari penegak hukum untuk mengejar kemajuan dunia komputer dan telekomunikasi yang sangat cepat.

1999 Computer Security Institute (CSI) / FBI Computer Crime Survey menunjukkan beberapa statistik yang menarik, seperti misalnya ditunjukkan bahwa "disgruntled worker" merupakan potensi attack / abuse. Http://www.gocsi.com. Pada tahun 2000 beberapa situs web di Indonesia dijebol. Contoh terakhir: Bank BCA, Bank Lippo, Bank Bali.Cracker Indonesia ditangkap di Singapura

Pemanfaatan teknologi informasi dan komunikasi menyentuh hampir semua bidang mulai dari ekonomi, pendidikan, kesehatan hingga pertahanan dan keamanan. Teknologi informasi dan komunikasi sebagai salah satu unsur strategis dalam mendukung penyelenggaraan pertahanan dan keamanan sudah selayaknya mendapatkan perhatian lebih. Terlebih lagi dalam beberapa tahun terakhir, kejahatan yang melibatkan pembobolan atau pencurian informasi semakin gencar dan menyasar tidak hanya perorangan dan industri tetapi juga hinggake level pemerintahan dalam bentuk penyadapan oleh intelijen luar negeri terhadap sejumlah pejabat pemerintahan Indonesiasehinggakeamanan informasi sudah selayaknya mendapatkan prioritas khususnya dalam menunjang kebutuhan hankamnas.

Perangkat telekomunikasi yang digunakan untuk bertukar informasi harus dapat dijamin keamanannnya dan tidak ada celah kebocoran yang menyebabkan informasi dapat dicuri atau disadap. Oleh karena itu,dibutuhkan kebijakan bidang TIK yang terkait standarisasi keamanan perangkat telekomunikasi agar fungsi dan kegunaan perangkat telekomunikasi yang beredar di Indonesia dapat dipertanggungjawabkan dan terutama untuk menjamin keamanan informasi yang dipertukarkan melalui perangkat tersebut. Hal inidilakukan agar informasi yang dipertukarkan tetap terjamin validitas dan kerahasiaannya sehingga keakuratan informasi dapat dipertanggungjawabkan dan tidak menyesatkan pihak lain. Selain itu untuk menjamin keamanan tersebut perlu melibatkan sejumlah stakeholdersterkait baik pemerintah maupun industri (Wamala, 2011). Selain diperlukan kebijakan dan peran para stakeholders, hal lain yang juga perlu diperhatikan adalah keberadaan teknologi pengamanan yang memadai.

Dalam kaitannya dengan kebutuhan akan kebijakan tersebut, kajian ini dilakukan untuk memperolehgambaran awal yakni upaya penerapankeamanan perangkat telekomunikasi saat ini dan potensi serta kendala yang dihadapi dalam upaya penjaminan keamanan perangkat telekomunikasi baik untuk kebutuhan umum yakni masyarakat dan industri maupun kebutuhan khusus yakni militer, kepolisian, dan pejabat negara baik dari aspek teknologi, kelembagaan, maupun regulasiyang dirangkum ke dalam sejumlah pertanyaan penelitian yang dirumuskan berdasarkan perkembangan permasalahan pembobolan keamanan informasi yang diperoleh dari berbagai literatur baik buku maupun jurnal

Salah satu elemen utama yang menentukan reliabilitas pusat data pemerintahan serta sistem *government cybersecurity* yang diterapkannya, adalah kesesuaian sistem dengan standar regulasi keamanan siber yang

telah ditetapkan dan diakui secara global. Sistem yang telah memenuhi regulasi serta restriksi tersebut, dianggap mampu untuk menghalau segala macam ancaman serangan siber sekaligus melindungi keamanan data pemerintah. Suatu penyedia perlu memenuhi standard untuk menjamin keamanan penggunanya. Lalu, regulasi seperti apakah yang harus dipenuhi oleh sistem *government cybersecurity* dan bagaimana perannya dalam menjaga keamanan *government data center*?

B. TINJAUAN TEORI

1. Keamanan Sistem Informasi

G. J. Simons, keamanan informasi adalah bagaimana kita dapat mencegah penipuan (*cheating) atau, paling tidak, mendeteksi* adanya penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik

Keamanan informasi berarti melindungi informasi dan sistem informasi dari akses, penggunaan, pengungkapan, gangguan, modifikasi, teliti, inspeksi, rekaman atau kehancuran.

Informasi hal keamanan, keamanan komputer dan jaminan informasi yang sering digunakan secara bergantian. Bidang-bidang ini saling terkait sering dan berbagi tujuan bersama untuk melindungi kerahasiaan , integritas dan ketersediaan informasi, namun ada beberapa perbedaan yang halus antara mereka.

Perbedaan ini terletak terutama dalam pendekatan untuk subjek, metodologi yang digunakan, dan bidang konsentrasi. Keamanan informasi berkaitan dengan kerahasiaan, integritas dan ketersediaan data yang terlepas dari bentuk data dapat mengambil: formulir elektronik, cetak, atau lainnya. Keamanan komputer dapat fokus pada memastikan ketersediaan dan operasi yang benar dari sistem komputer tanpa memperhatikan informasi yang disimpan atau diproses oleh komputer. Kepastian informasi berfokus pada alasan untuk jaminan bahwa informasi dilindungi, dan dengan demikian penalaran tentang keamanan informasi.

Pemerintah , militer , perusahaan , lembaga keuangan , rumah sakit , dan swasta bisnis mengumpulkan banyak informasi rahasia tentang karyawan mereka, pelanggan, produk, penelitian, dan status keuangan. Sebagian besar informasi ini sekarang dikumpulkan, diproses dan disimpan pada elektronik komputer dan ditransmisikan di seluruh jaringan ke komputer lain. Jika informasi rahasia tentang pelanggan bisnis ‘atau keuangan atau produk jatuh baris baru ke tangan pesaing, seperti pelanggaran keamanan bisa menimbulkan konsekuensi negatif. Melindungi

informasi rahasia merupakan kebutuhan bisnis, dan dalam banyak kasus juga merupakan persyaratan etika dan hukum. Untuk individu, keamanan informasi memiliki dampak yang signifikan terhadap privasi , yang dipandang sangat berbeda di berbagai budaya .

Bidang keamanan informasi telah tumbuh dan berkembang secara signifikan dalam beberapa tahun terakhir. Ada banyak cara untuk mendapatkan masuk ke lapangan sebagai karier. Menawarkan banyak daerah untuk spesialisasi termasuk: mengamankan jaringan (s) dan sekutu infrastruktur , mengamankan aplikasi dan database , pengujian keamanan, sistem informasi audit , perencanaan kelangsungan bisnis dan digital forensik ilmu pengetahuan, dll. Jika kita berbicara tentang keamanan sistem informasi,selalu kata kunci yang dirujuk adalah pencegahan dari adanya virus,hacker,cracker dll. Padahal baerbicara masalah keamanan sistem informasi maka kita akan berbicara kepada kemungkinan adanya resikoyang muncul atas sistem tersebut.

2. Konsep Pertahanan Keamanan dalam Kepentingan Nasional

Robert Dorff (2004) menyatakan kepentingan suatu negara bangsa diperlihatkan dengan tingkah lakunya dalam membela, mengejar dan mempertahankan apa yang menjadi kepentingan dasarnya. Bagi banyak negara, kepentingan dasar suatu negara adalah menjaga wilayah,rakyat dan kedaulatannya. Semua unsur ini harus dipertahankan dan diperjuangkan agar tetap eksis dalam suatu negara. Mempertahankan kepentingan ini menjadi dasar dari tingkah laku suatu negara dalam berhubungan dengan negara lain dan aktor-aktor lain dalam sistem internasional, termasuk diantaranya melalui perang dan diplomasi (Dorff, 2004).

Menurut Alan Gyngell & Michael Wesley (2007), kepentingan nasional adalah suatu konsep permanen yang menjadi orientasi kebijakan luar negeri suatu negara. Dengan kata lain konsep kepentingan nasional selalu menjadi landasan bagi semua pengambilan keputusan luar negeri dan juga dalam menganalisa kebijakan luar negeri (Gyngell & Wesley, 2007: 23). Kepentingan nasional merupakan tujuan jangka panjang dari suatu negara yangmengikat semua elemen pemerintah dan bangsa untuk mencapainya.Dengan demikian, bidang keamanan nasional juga diperluas dari dunia nyata ke dunia maya sehingga muncul sebuah ancaman baru dalam sistem keamanan nasional yakni Cyber Wardan masing-masing negara bersaing untuk memenangkan Cyber War. Kekuatan untuk menghancurkan ancaman Cyber Wartelah mencapai tahap langsung dan serius pada sistem keamanan nasional. Dalam tatanan globalisasi semua

perangkat dapat mengakses informasi dimanapun sekaligus juga dapat diakses dari manapun.Kondisi ini memungkinkan penyalahgunaaninformasi yang dilewatkan melalui perangkat tersebut dengan menanamkan alat untuk mengambil maupun memodifikasi informasi untuk kepentingan tertentu.

3. Dasar Pemikiran dan Kebijakan TIK Nasional

Perkembangan teknologiinformasi dankomunikasidi dunia sudah sangat transparan dan memungkinkan setiapkejadiandan informasiyang ada di duniaini dapat diakses cepat dan mudahseolah meniadakan batas antar negara. Kondisi ini memungkinkan penyalahgunaaninformasi yang dilewatkan melalui perangkat tersebut dalam bentukmenyadapmaupun memodifikasi informasi untuk kepentingan tertentu. yang manahal tersebutmenjadi suatu ancamanterhadap keutuhan negara. Oleh karenanyaakan sangat berbahaya bagi suatu negara jika terus-menerus hanya menjadi pengguna dan menerima perangkat yang diproduksi dari luar (pihak asing) tanpa adanya jaminan standardisasikeamanan ataupun enkripsi yang dibuktikan dengan mengikuti peraturan nasional maupun internasional yang sudah ditetapkan oleh lembaga-lembaga berwenang.

4. Kebijakan Standarisasi Perangkat Umum

Standarisasi sebagai suatu unsur penunjang pembangunan mempunyai peran penting dalam usaha optimasi pendayagunaan sumber daya dan seluruh kegiatan pembangunan. Perangkat yang terstandardisasitermasuk juga perangkat pembinaan dan pengawasan sangat berperan dalam peningkatan perdagangan dalam negeri dan internasional, pengembangan industri nasional, serta perlindungan terhadap pemakai (operator maupun masyarakat)dimana tujuan akhir kegiatan standardisasiadalah terwujudnya jaminan mutu.

Sistem Standardisasi Nasional (SSN) merupakan dasar dan pedoman pelaksanaan setiap kegiatan standardisasi di Indonesia yang harus diacu oleh semua instansi teknis sesuai dengan Peraturan Pemerintah Nomor 15 Tahun 1991tentang Standardisasi Nasional Indonesia dan Keputusan Presiden Nomor 12 Tahun 1991 tentang Penyusunan, Penerapan dan Pengawasan Standardisasi Nasional Indonesia. Dalam rangka mewujudkan pelaksanaan Sistem Standardisasi Nasional, juga dilakukan pengembangan dan penerapan standardisasi di bidang telekomunikasi.Kegiatan standardisasi di bidang telekomunikasi sepenuhnya ditangani oleh instansi teknis, dalam hal ini adalah DirektoratJenderal Sumber Daya dan Perangkat Pos dan Informatika (SDPPI) yang dalam hal ini dilaksanakan oleh Direktorat Standardisasi

SDPPI.Subsistem-subsistem atau kegiatan-kegiatan yang saling terkait satu sama lain dalam Sistem Standardisasi Nasional terdiri dari perumusan standardisasi, penerapan standardisasi, pembinaan dan pengawasan standardisasi, kerjasama dan informasi standardisasi, metrologi dan akreditasi.

Tujuan dari kegiatan standardisasi pos dan telekomunikasi adalah:

a. Pengamanan terhadap jaringan pos dan telekomunikasi, yang merupakan aset nasional.
b. Menjamin interoperabilitas dan interkonektivitas berbagai perangkat dalam jaringan pos dan telekomunikasi.
c. Memberi kesempatan munculnya industri manufaktur nasional.
d. Memberi perlindungan terhadap para pengguna jasa (operator dan masyarakat) pos dan telekomunikasi.
e. Mengendalikan mutu perangkat.
f. Memberi kesempatan produk nasional bersaing di pasar global.

5. Kebijakan Standarisasi Perangkat Khusus

Penerapan standar keamanan perangkat khusus biasanya diterapkan secara nasional, dalam cakupan suatu negara saja.Pengembangan standar keamanan perangkat khususdi Indonesia dibantu oleh badan-badan intelijen negara yang bersangkutan, antara lain:

a. Badan Intelijen Negara (BIN),
b. Badan Intelijen Strategis (BAIS), dan
c. LembagaSandi Negara (Lemsaneg).

BIN dan Lemsaneg adalah Lembaga Pemerintah Nonkementerian (LPNK), yaitu lembaga negara di Indonesia yang dibentuk untuk melaksanakan tugas pemerintahan tertentu dari presiden, sedangkan BAIS berada di bawah komando Markas Besar Tentara Nasional Indonesia (Mabes TNI).Dari ketiga lembaga intelijen negara tersebut, yang memiliki fungsi yang berkaitan dengan keamanan sistem telekomunikasi militer adalah Lemsaneg.

Berdasarkan Peraturan Kepala Lembaga Sandi Negara Nomor OT.001/PERKA.122/2007 tentang Organisasi dan Tata Kerja Lembaga Sandi Negara, Lemsaneg mempunyai tugas melaksanakan tugas pemerintahdi bidang persandian sesuai dengan ketentuan peraturan perundang-undangan yang berlaku.Dalam melaksanakan tugas tersebut sesuai OT.001/PERKA.122/2007, Lembaga Sandi Negara menyelenggarakan fungsi:

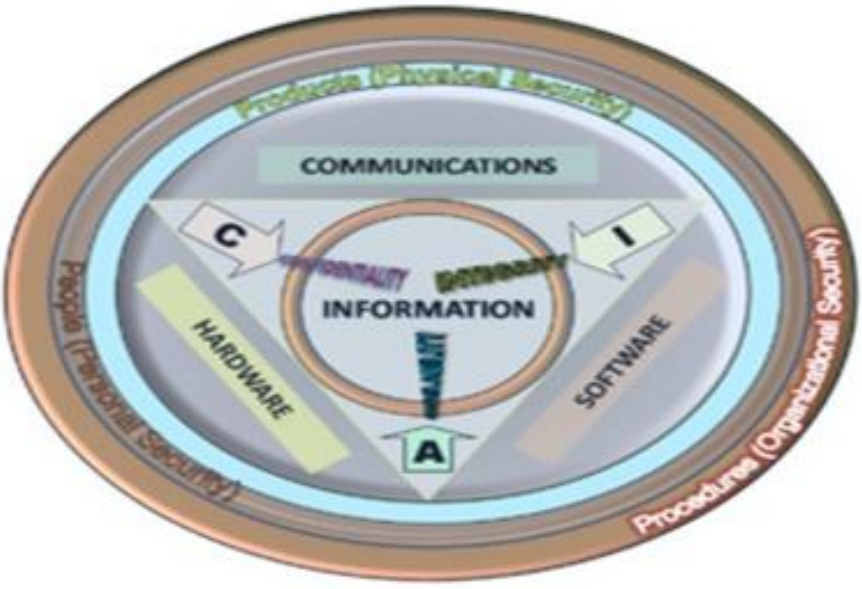
a. Pengkajiandan penyusunan kebijakan nasional di bidang persandian;

b. Koordinasi kegiatan fungsional dalam pelaksanaan tugas lemsaneg;
c. Fasilitas dan pembinaan terhadap kegiatan instansi pemerintah di bidang persandian;•Penyelenggaraan pembinaan pelayanan administrasi umum di bidang perencanaan umum, ketatausahan, organisasi dan tata laksana, kepegawaian, keuangan, kearsipan, hukum, persandian, perlengkapan dan rumah tangga.

6. Konsep Keamanan Teknologi Informasi dan Komunikasi Nasional

Konsep keamananyang ada dalam ranah TIK memiliki cakupan yang sangat luas. Keamanan melingkupi empat aspek, yaitu privacy/confidentiality, integrity,authentication, dan availability. Selain keempat hal di atas, masihada dua aspek lain yang juga sering dibahas, terutama dalam kaitannyadengan transasksi elektronik, yaitu access controldan non-repudiation(Garfinkel, 1995).

a. Privacy/ Confidentiality: Aspek terkait jaminan kerahasiaan isi dari informasi
b. Authentication: Aspek yang menyatakan bahwa informasi betul-betul asli, atau orang yang mengakses/memberikan informasi adalah betul-betul orang yang dimaksud
c. Integrity: Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi
d. Accesibility: Aspek iniberhubungan denganketersediaan informasi ketika dibutuhkan
e. Access control\: Aspek ini berhubungan dengan cara pengaturan akses kepadainformasi
f. Nonrepudiation: Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi



Gambar 1. Atribut Keamanan Informasi

Seringkali masalah keamanan bahkan tidak terlalu diperhatikan, terutama apabila penerapan tindakan-tindakan keamanan mengganggu performansi sistem. Tidak jarang tindakan-tindakan keamanan dikurangi atau bahkan ditiadakan(Dowd & McHenry, 1998).Berdasarkan celah keamanan, keamanan dapat diklasifikasikan menjadi empat(David J. Icove, 1997), yaitu :

a. Keamanan yang bersifat fisik (physical security).Keamanan fisik mencakup akses orang ke gedung, peralatan, dan media yang digunakan. Tidak menutup kemungkinan adalah kemudahan akses menuju berkas-berkas yang sudah dibuang yang mungkin memiliki informasi tentang keamanan, seperti catatan kata sandi (password) atau manual yang dibuang tanpa dihancurkan. Wiretappingatau hal-hal yang berhubungan dengan akses ke kabel atau komputer yang digunakan juga dapat dimasukkan ke alam kelas ini.Denial of servicejuga dapat dimasukkan ke dalam kelas ini. Denial of serviceadalah akibat yang ditimbulkan sehingga layanan yang seharusnya dapat diakses menjadi terhenti. Hal ini dapat terjadi misalnya dengan mematikan peralatan atau membanjiri saluran komunikasi dengan pesan-pesan yang bukan berasal dari peminta layanan, sehingga pemberi layanan menjadi sibuk.
b. Keamananyang berhubungan dengan orang (personel).Klasifikasi ini mencakup identifikasi orang yang mempunyai akses, misalnya karyawan suatu organisasi. Seringkali kelemahan keamanan bergantung kepada manusia. Teknik“social engineering” sering digunakan oleh kriminal, misalkan dengan berpura-pura sebagai orang yang berhak mengakses informasi namun lupa kata sandi (password) yang dimilikinya.
c. Keamanan dari data dan media serta teknik komunikasi (communications). Klasifikasi ini mencakup kelemahan-kelemahan yang terdapat di dalam perangkat lunak yang digunakan untuk mengelola data. Penyerang dapat memberikan virus atau trojan sehingga dapat mengumpulkan informasi (misalkan password) yang semestinya tidak berhak diakses.
d. Keamanan dalam operasi,termasuk prosedur yang digunakan untuk mengatur dan mengelola sistem keamanan, dan juga termasuk prosedur setelah serangan (post attack recovery).

Secara spesifik, serangan terhadap keamanan (security attack) di dalam sistem informasidapat dilihat dari fungsi peranan komputer atau jaringan computer sebagai penyedia informasi. Ada beberapa kemungkinan

serangan (attack) yang dapat terjadi(William Stallings, 1995)dan (Rahardjo, 1999), diantaranya:

- Interruption: Perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan kepada ketersediaan (availability) dari sistem. Contoh serangan adalah “denial of service attack”.
- Interception: Pihak yang tidak berwenang berhasil mengakses aset atau informasi. Contoh dari serangan ini adalah penyadapan (wiretapping).
- Modification: Pihak yang tidak berwenang tidak saja berhasil mengakses, akan tetapi dapat juga mengubah (tamper) aset. Contoh dari serangan ini antara lain adalah mengubah isi dari web site dengan pesan-pesan yang merugikan pemilik web site.
- Fabrication: Pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem. Contoh dari serangan jenis ini adalah memasukkan pesan-pesan palsu seperti e-mail palsu ke dalam jaringan komputer.

7. Penerapan Standar Keamanan TIK Nasional

a. Perangkat Umum

Salah satu dasar penerapan standar keamanan perangkat umum di Indonesia dapat dilihat dalam Peraturan Menteri Komunikasi dan Informatika Nomor 18 Tahun 2014 tentang Sertifikasi Alat dan Perangkat Telekomunikasi. Sertifikasi yang dimaksud adalah dokumen yang menjelaskan bahwa suatu perangkat telah melalui serangkaian proses pengujian. Adanya sertifikat ini memastikan bahwa perangkat bisa terhubung dan berkomunikasi dengan perangkat atau sistem yang sudah ada tanpa mengganggu dan terganggu oleh sistem komunikasi lainnya.Peraturan ini menjelaskan bahwa penerbit sertifikasi perangkat adalah Lembaga Sertifikasi, Direktorat Standarisasi Perangkat Pos dan Informatika. Untuk memperoleh sertifikat tersebut, perangkat yang diajukan harus melalui pengujian yang dilaksanakan oleh pelaksana pengujian (Balai Uji). Balai Uji yang telah ditetapkan adalah Balai Besar Pengujian Perangkat Telekomunikasi (BBPPT) Kementerian Komunikasi dan Informatika dan Innovation and Design Center(IDEC) PT. Telekomunikasi Indonesia.

b. Perangkat Khusus

Penerapan standard keamanan perangkat khusus memiliki standardyang tidak terbuka. Standardkeamanan untuk perangkat militer biasanya ditetapkan sendiri-sendiri secara khusus (proprietary) oleh pihak-pihak yang berkepentingan. Dengan adanya persyaratan keamanan telekomunikasi militer yang sangat ketat, standardmasing-masing pihak yang berkepentingan umumnya tidak diizinkan untuk diketahui pihak lain, sehingga dapat dikatakan standardkeamanan yang diberlakukan secara

internasional hamper tidak ada. Beberapa standard yang mungkin ada biasanya berupa standardkomunikasi umum antar pihak militer satu dengan pihak militer yang lainnya di mana tidak terdapat pertukaran informasi yang sangat rahasia pada komunikasi yang sedang berlangsung. Penerapan standardkeamanan perangkat militer biasanya diterapkan secara nasional, dalam cakupan suatu negara saja. Pengembangan standardkeamanan perangkat militer biasanya dibantu oleh badan-badan intelijen negara yang bersangkutan.Di Indonesia, peralatan-peralatan komunikasi militer yang digunakan oleh tiap angkatan (Angkatan Darat, Angkatan Laut, dan Angkatan Udara) dikatakan disertifikasi oleh Badan Penelitian dan Pengembangan masing-masing angkatan.Meskipun demikian,Lembaga Sandi Negara (Lemsaneg) memiliki rencana untuk mewajibkan penerapan standar keamanan perangkat. Saat ini Lemsaneg telah memiliki bagian Sub-direktorat Akreditasi dan Sertifikasi yang melakukan sertifikasi perangkat-perangkat dengan fitur-fitur kemanan. Lemsaneg memiliki rencana untuk mewajibkan sertifikasi perangkat khusus dengan mengusahakan undang-undang mengenai sertifikasi tersebut pada 2016 untuk mengatur persyaratan teknis perangkat-perangkat sandi.

C. LIMA STANDAR REGULASI YANG BERPERAN DALAM PENGAMANAN PUSAT DATA PEMERINTAHAN

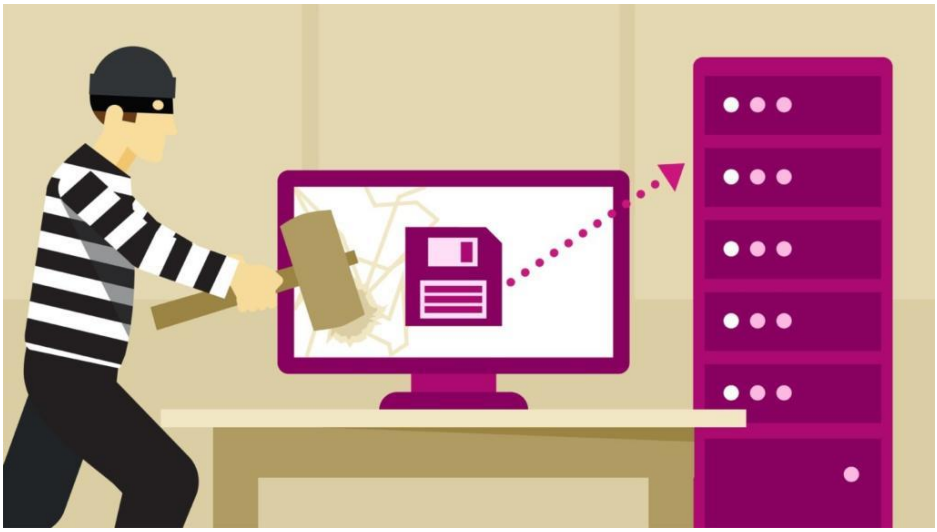
1. FIPS 140.2

Gambar 2. Fips 140.2

Federal Information Processing Standard yang lebih terkenal dengan istilah publikasi FIPS 140.2 adalah standar regulasi keamanan jaringan komputer pemerintahan yang dikembangkan oleh pemerintahan federal Amerika Serikat. Regulasi ini memfokuskan layanannya pada proses penyelidikan kode-kode rahasia atau kriptografi yang meliputi pengolahan data dan dokumen, enkripsi algoritma, serta sejumlah standar regulasi lain dalam teknologi informasi yang digunakan dalam ruang lingkup pemerintahan.

.

2. PII



Gambar 3. *Personally Identifiable Information*

Istilah PII merupakan singkatan dari *Personally Identifiable Information*. Standar regulasi PII bergerak untuk mendeteksi, membedakan, serta mencari jejak identitas individu maupun kelompok yang terhubung dengan sistem dalam pusat data utama.

Saat digunakan dalam pusat data pemerintahan yang telah menerapkan *government cybersecurity*, PII membantu pemerintah dan pihak-pihak terkait untuk menemukan identitas penyusup maupun peretas yang masuk ke dalam pusat data. Dengan begitu, keamanan dari pusat data pemerintahan akan tetap terjaga dari pihak luar yang tidak memiliki izin untuk mengolah atau melakukan transmisi data milik pemerintah.

3. HIPAA

Salah satu elemen utama dari pemerintahan adalah fasilitas kesehatan. Dalam hal ini, HIPAA (*Health Insurance Portability and Accountability*)

menjadi regulasi yang membawahi proses perekaman data serta aktivitas medis yang terjadi di fasilitas kesehatan suatu wilayah. Melalui HIPAA, seluruh informasi yang dibuat, diterima, dan disebarkan untuk kepentingan medis akan dijamin kerahasiaan serta perlindungannya.

Gambar 4. *Health Insurance Portability and Accountability*

Aturan Hukum dan Privasi HIPAA telah ada untuk melindungi data layanan kesehatan pribadi mulai tahun 1996. Seiring teknologi telah berubah dan informasi menjadi lebih mudah diakses, ada Juga telah direvisi karena perubahan lingkungan dan kemajuan teknologi selama bertahun-tahun. Semua peraturan ini telah disiapkan untuk membantu menjaga keamanan informasi pribadi.

Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan (HIPAA) dan Aturan Privasi HIPAA menetapkan standar untuk melindungi data pasien yang sensitif dengan menciptakan standar untuk pertukaran elektronik , Dan privasi dan keamanan informasi medis pasien oleh orang-orang di industri kesehatan. Sebagai bagian dari HIPAA, Aturan Penyederhanaan Administratif dirancang untuk melindungi kerahasiaan pasien, sambil membiarkan informasi medis diperlukan untuk dibagikan sambil menghormati hak pasien terhadap privasi. Sebagian besar penyedia layanan kesehatan, organisasi kesehatan, dan rencana kesehatan pemerintah Yang menggunakan, menyimpan, memelihara, atau mengirimkan informasi perawatan kesehatan pasien diminta untuk mematuhi peraturan privasi hukum HIPAA.

Tujuan utama HIPAA adalah untuk membantu individu mempertahankan cakupan asuransi kesehatan dengan: menyederhanakan prosedur administratif (Administrative Simplification Rules) dan mengendalikan biaya administrasi. Dengan begitu banyak informasi yang berpindah tangan antara penyedia layanan medis dan perusahaan asuransi kesehatan dan begitu banyak pihak lain di dunia layanan kesehatan, Undang-undang HIPAA tampaknya mempermudah penanganan dokumentasi dan informasi pasien yang sensitif di industri perawatan kesehatan, sementara Melindungi kerahasiaan informasi kesehatan pasien.

HIPAA bukan Hukum yang Melindungi Kerahasiaan Pasien dan Rekaman Kesehatan. HIPAA adalah undang-undang federal, ada banyak undang-undang individu lainnya yang bekerja untuk melindungi privasi pribadi Anda dan penanganan data yang terdapat dalam Catatan medismu Hukum dan peraturan ini bervariasi dari satu negara bagian ke negara bagian lainnya.

HIPAA adalah standar dasar dan setiap negara dapat menambahkannya dan memiliki standar tambahan mereka sendiri. Hukum HIPAA difokuskan untuk menyederhanakan sistem perawatan kesehatan dan memastikan keamanan bagi pasien. Judul IV adalah perlindungan yang menjamin perlindungan privasi untuk informasi medis Anda. Seiring dengan federal memastikan privasi Anda, hukum HIPAA dimaksudkan untuk menyebabkan berkurangnya aktivitas penipuan dan peningkatan sistem data. Bila dipatuhi sepenuhnya oleh semua yang diminta untuk mematuhi.

4 Aturan HIPAA untuk Kepatuhan oleh Penyedia Layanan Kesehatan

- HIPAA Privacy Rule – Melindungi jenis data yang dikomunikasikan
- HIPAA Aturan Keamanan – Melindungi database dan data untuk keamanan
- Aturan Penegakan HIPAA – Menunjukkan prosedur untuk penegakan dan prosedur untuk dengar pendapat dan hukuman.
- Peraturan Pemberitahuan Pelanggaran HIPAA – Memerlukan penyedia layanan kesehatan untuk memberitahukan Individu ketika telah terjadi pelanggaran informasi kesehatan yang dilindungi

HIPAA diterapkan pada Aturan Privasi, dan juga semua peraturan Penyederhanaan Administratif, berlaku untuk rencana kesehatan*, clearing house* perawatan kesehatan, dan penyedia layanan kesehatan yang mentransmisikan kesehatan Informasi dalam bentuk elektronik sehubungan dengan transaksi dimana Sekretaris HHS telah mengadopsi standar di bawah HIPAA (“entitas yang tercakup”).

Contoh aturan HIPAA yang tidak diterapkan pada orang atau perusahaan:

- perusahaan pengujian genetik langsung ke konsumen (DTC)
- aplikasi seluler yang digunakan Untuk tujuan kesehatan dan kebugaran
- praktisi pengobatan alternatif
- lembaga negara, seperti layanan perlindungan anak
- lembaga penegak hukum
- perusahaan asuransi jiwa
- sekolah
- atasan

Tujuan Aturan Keamanan HIPAA yaitu untuk memenuhi persyaratan kepatuhan oleh penyedia layanan kesehatan. Agar penyedia layanan mematuhi HIPAA, mereka harus memenuhi persyaratan yang ditetapkan oleh HIPAA Security Rule. Ini termasuk persyaratan dan pedoman seputar pengamanan administratif, fisik, dan teknis yang sesuai untuk memastikan kerahasiaan, integritas, dan keamanan informasi kesehatan yang dilindungi (PHI).

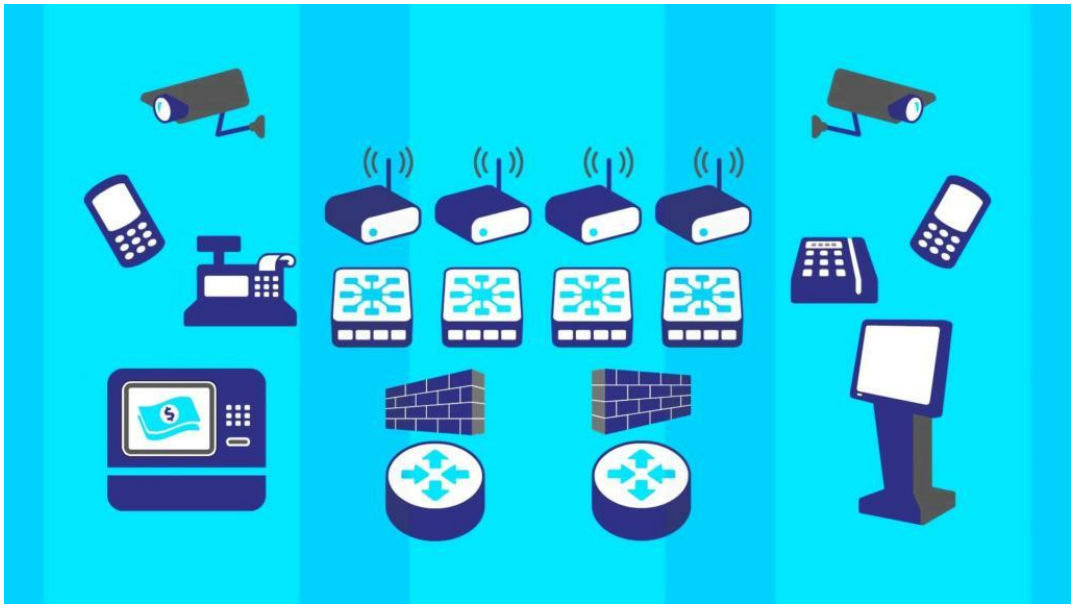
Beberapa penyedia layanan kesehatan telah mengambil langkah-langkah seperti mengendalikan akses ke kantor dengan file medis dengan sistem kartu kunci elektronik. Dan hanya mengizinkan karyawan membatasi akses terhadap jumlah minimum informasi yang dibutuhkan. Selain itu, penggunaan layanan khusus untuk membuat transaksi elektronik aman juga digunakan oleh banyak fasilitas medis dan penyedia asuransi. Jika Anda khawatir tentang apa yang dokter atau dokter anda lakukan untuk mematuhi undang-undang HIPAA, tanyakan kepada mereka langkah-langkah apa yang telah mereka lakukan untuk memastikan privasi Anda. Ingat bahwa jika mereka mematuhi HIPAA, mereka memiliki daftar panjang hal yang harus dilakukan untuk dianggap sesuai dengan HIPAA. Hukum privasi dan perlindungan data pasien yang sensitif diambil dengan sangat serius. Ada kemungkinan mereka mengikuti peraturan ini dengan sangat ketat karena undang-undang itu.

Jika asuransi kesehatan Anda berasal dari organisasi kesehatan kecil yang dikelola sendiri, mereka mungkin tidak harus mematuhi HIPAA Peraturan. Penting untuk diperiksa dengan mereka untuk melihat apakah mereka mematuhi, dan jika tidak, langkah apa yang mereka ambil sendiri untuk memastikan privasi Anda.

Pengecualian privasi HIPAA diberikan kepada penyedia layanan kesehatan dan orang lain yang diwajibkan untuk mengikuti HIPAA pengecualian di beberapa area di mana mereka tidak harus mengikuti

peraturan yang digariskan oleh Tindakan dan peraturan Anda harus memberi tahu diri Anda tentang tiga pengecualian privasi HIPAA yang paling umum sehingga Anda dapat mengetahui informasi atau data medis tentang Anda yang mungkin diungkapkan secara hukum dan tidak dilindungi oleh perlindungan HIPAA.

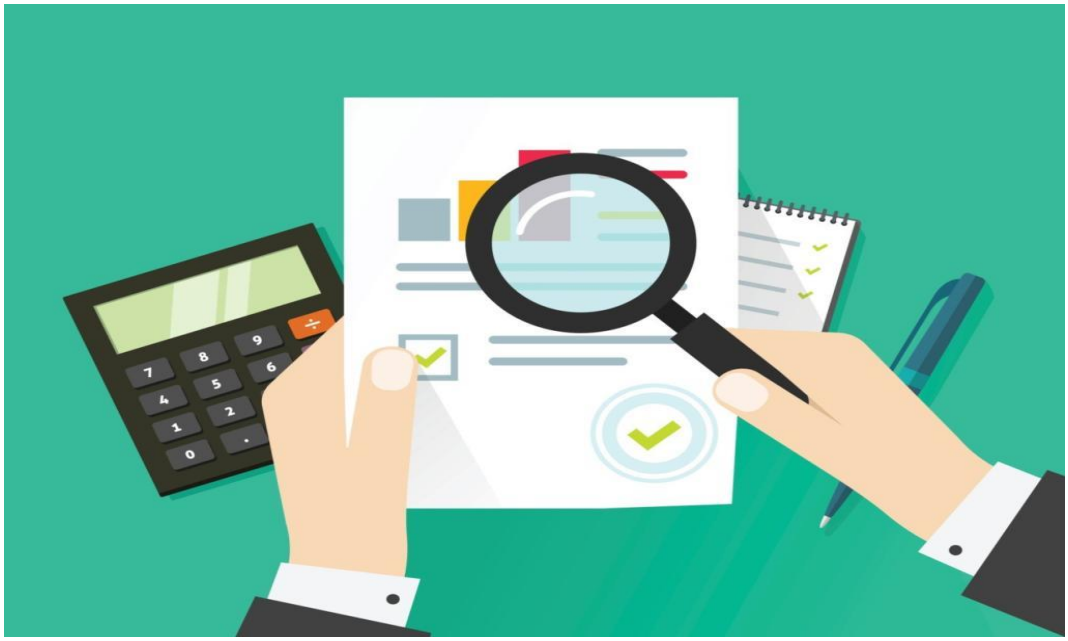
4. PCI DDS



Gambar5. *Payment Card Industry Data Security Standard*

Payment Card Industry Data Security Standard (PCI DDS) merupakan regulasi yang diberlakukan bagi institusi finansial atau perbankan, terutama institusi yang memiliki wewenang untuk menerbitkan kartu kredit. Praktik yang diterapkan PCI DDS difokuskan kepada pengembangan, pemeliharaan, serta pengawasan sistem pengamanan data pemegang kartu kredit. Hal ini bertujuan untuk mendeteksi dan mencegah kemungkinan insiden cyber threats yang terjadi.

5. FINRA



Gambar 6. *Financial Industry Regulatory Authority*

Tak jauh berbeda dari PCI DDS, FINRA atau *Financial Industry Regulatory Authority* juga bergerak dalam bidang organisasi finansial dari pemerintah. Program FINRA yang paling terkenal dinamakan '*sweep*', yakni program yang mengharuskan seluruh instansi finansial untuk memberikan respons terhadap surat pemeriksaan mengenai kesiapan instansi dalam menggalakkan upaya-upaya *cyber security*. Pemeriksaan ini dilakukan secara berkala untuk memastikan bahwa sistem pengamanan data instansi finansial tetap terjaga dan bekerja dengan seharusnya.

Itulah ulasan mengenai lima standar regulasi dari *government cybersecurity*. Memilih sistem pengamanan siber yang telah sesuai dan memenuhi seluruh regulasi tersebut, menjadi hal yang sangat krusial untuk keamanan data dan informasi sensitif dalam ruang lingkup instansi pemerintah.

DAFTAR PUSTAKA

1. David J. Icove. (1997). Collaring the cybercrook: an investigator's view. IEEE Spectrum, 31–36.
2. Dowd, P. W., & McHenry, J. T. (1998). Network Security: It's Time To Take It Seriously. IEEE Computer, September, 24–28.
3. Garfinkel, S. (1995). PGP: Pretty Good Privacy. O'Reilly & Associates,Inc.
4. J.M. Rodriguez Bejarano. (2012). Security in IP satellite networks: COMSEC and TRANSEC integration aspects. In Security in IP satellite networks: COMSEC and TRANSEC integration aspects. The Sixth Advanced Satellite Multimedia Systems Conference.
5. Juslin, J. (2003). Automatic backdoor analysis with a network intrusion detection system and an integrated service checker. Information Assurance Workshop.
6. Kiblat.mht. (2015). http://www.kiblat.net/2015/02/25/dan-inggris-retas-ponsel-seluruh-dunia-ini-10-hal-yang-perlu-anda-tahu/.
7. NargesArastouie, E. S. dan. (2011). Backdoor detection system using artificial neural network and genetic algorithm.
8. Paryati. (2008). Keamanan Sistem Informasi. Seminar Nasional Informatika 2008.
9. Rahardjo, B. (1999). Keamanan Sistem Informasi Berbasis Internet. Bandung: PT Insan Komunikasi / Infonesia.
10. Richardus, Eko, & Indrajit. (2011). MANAJEMEN KEAMANAN INFORMASI DAN INTERNET.
11. Schrittwieser, S., Fr¨uhwirt, P., Kieseberg, P., Leithner, M., Mulazzani, M., Huber, M., & Weippl, E. (2012). Guess Who's Texting You? Evaluating the Security of Smartphone Messaging Applications. SBA Research gGmbH
12. Stove, A. G. (2004). Low probability of intercept radar strategies. IEEE Proceedings on Radar, Sonar and Navigation, 151(5).
13. Wamala, F. (2011). ITU National Cyber Security Strategy Guide. ITU.
14. Wicaksono, N. (2007). AUREN: Sistem Pengamanan Smartphone dengan Penghapusan Informasi Berharga dan Pengiriman Informasi untuk pelacakan otomatis. Bandung.
15. William Stallings. (1995). Network and Internetwork Security. PrenticeHall.
16. Woods, S. S. dan C. (2012). Breakthrough silicon scanning discovers backdoor in military chip.