Privasi dan Keamanan Informasi

Akademi Esensi TIK untuk Pimpinan Pemerintahan

UNITED NATIONS ESCAP / APCICT

Akademi Esensi TIK untuk Pimpinan Pemerintahan

Privasi dan Keamanan Informasi

APCICT ASIAN AND PACIFIC TRAINING CENTRE FOR INFORMATION AND COMMUNICATION TECHNOLOGY FOR DEVELOPMENT

Akademi Esensi TIK untuk Pimpinan Pemerintahan

Privasi dan Keamanan Informasi

Korespondensi mengenai laporan ini harus ditujukan ke alamat surel: apcict@un.org

Dicetak di Republik Korea
ST/ESCAP/2934

Desain sampul: Mr. Ho-Din Ligay

Kontak:

Asian and Pacific Training Centre for Information and Communication Technology for Development (APCICT/ESCAP)
5th Floor G-Tower, 175 Art Center Daero
Yeonsu-gu, Incheon, Republic of Korea
Tel +82 32 458 6650

Email: apcict@un.org

TENTANG SERI MODUL

Pada era informasi dewasa ini, kemudahan akses informasi telah mengubah cara kita hidup, bekerja dan bermain. Ekonomi digital *(digital economy)*, juga dikenal sebagai ekonomi pengetahuan, ekonomi jaringan atau ekonomi baru, ditandai dengan adanya pergeseran dari produksi barang ke sebuah pembentukan ide. Hal tersebut menunjukkan semakin pentingnya peran Teknologi Informasi dan Komunikasi (TIK) dalam tatanan ekonomi secara khusus dan masyarakat secara umum.

Akibatnya, pemerintah di seluruh dunia semakin fokus pada pemanfaatan TIK untuk Pembangunan yang dikenal dengan istilah *ICTs for development* (ICTD). Bagi pemerintah tersebut, TIK untuk Pembangunan atau ICTD bukan hanya sekadar pengembangan industri TIK atau sektor ekonomi, melainkan juga mencakup pemanfaatan TIK dalam rangka mendorong pertumbuhan ekonomi, serta pembangunan sosial dan politik.

Namun, salah satu kendala yang dihadapi pemerintah dalam penyusunan kebijakan TIK adalah ketidakakraban para penyusun kebijakan terhadap teknologi yang akan digunakan dan juga terus berkembang serta kompetensi untuk pemanfaatan TIK dalam rangka pembangunan nasional. Karena seseorang tidak mungkin mengatur hal yang tidak dimengerti olehnya, banyak dari mereka yang akhirnya menghindari penyusunan kebijakan di bidang TIK. Akan tetapi, menyerahkan penyusunan kebijakan TIK kepada para teknolog juga keliru karena seringkali mereka kurang mawas terhadap impilkasi kebijakan dan sosial dari teknologi yang mereka kembangkan dan gunakan.

Seri modul *Akademi Esensi Teknologi Informasi dan Komunikasi untuk Pimpinan Pemerintahan* telah dikembangkan oleh Asian and Pacific Training Centre for Information and Communication Technology for Development (APCICT) untuk:

1. Penyusun kebijakan, baik di tingkat pemerintahan pusat maupun daerah yang bertanggung jawab terhadap penyusunan kebijakan TIK;
2. Aparatur pemerintah yang bertanggung jawab terhadap pengembangan dan implementasi apilkasi-aplikasi berbasis TIK; serta
3. Manajer di sektor publik yang ingin memanfaatkan perangkat TIK untuk manajemen proyek.

Seri modul ini dibuat untuk meningkatkan pengetahuan terhadap isu-isu pokok terkait ICTD, baik dari perspektif kebijakan maupun teknologi. Tujuannya bukan untuk penyusunan manual TIK teknis, tetapi lebih kepada memberikan pemahaman yang baik mengenai kemampuan teknologi digital saat ini dan kemana arah teknologi serta implikasinya terhadap penyusunan kebijakan. Topik-topik yang dibahas dalam modul ini telah diidentifikasi melalui analisis kebutuhan pelatihan dan survei terhadap materi-materi pelatihan di seluruh dunia.

Modul-modul yang ada telah dirancang sedemikian rupa agar dapat digunakan untuk pembelajaran mandiri oleh para pembaca atau juga sebagai rujukan untuk program pelatihan. Modul-modul tersebut berdiri sendiri dan saling berkaitan satu sama lain, serta telah diusahakan agar setiap modul terhubung dengan tema dan pembahasan pada modul-modul lainnya. Tujuan jangka panjangnya adalah agar modul-modul tersebut dapat digunakan dalam pelatihan bersertifikasi.

Setiap modul diawali dengan tujuan modul dan target pembelajaran yang ingin dicapai sehingga pembaca dapat menilai progres mereka. Isi modul terdiri dari bagian-bagian yang

termasuk di dalamnya studi kasus dan berbagai latihan untuk memperdalam pemahaman terhadap konsep utama. Latihan-latihan tersebut dapat dikerjakan secara individu maupun berkelompok. Gambar dan tabel disajikan untuk mengilustrasikan aspek-aspek tertentu dari pembahasan. Referensi dan bahan daring juga disertakan agar pembaca mendapatkan pengetahuan tambahan mengenai materi yang diberikan.

Pemanfaatan ICTD sangatlah beragam sehingga terkadang studi kasus dan berbagai contoh, baik dalam satu modul maupun antar modul mungkin terlihat saling kontradiktif. Hal ini memang diharapkan. Inilah gairah dan tantangan dari disiplin ilmu baru yang saat ini terus berkembang dan sangat menjanjikan sehingga semua negara mulai menggali kemampuan TIK sebagai alat pembangunan.

Sebagai bentuk dukungan bagi seri modul versi cetak ini, telah tersedia sebuah media pembelajaran jarak jauh—Akademi Virtual APCICT (http://e-learning.unapcict.org)—dengan konsep ruang kelas virtual yang memuat presentasi pengajar dalam bentuk video dan modul presentasi dalam format PowerPoint.

UCAPAN TERIMA KASIH

Modul Akademi Esensi TIK untuk Pimpinan Pemerintahan: Privasi dan Keamanan Informasi ini disiapkan oleh Freddy Tan, di bawah bimbingan Kiyoung Ko, Direktur Asian and Pacific Training Centre for Information and Communication Technology for Development (APCICT). Adapun penyelarasan modul dilakukan oleh Robert De Jesus.

Modul ini juga mendapat komentar substantif dari para peserta acara *Consultative Meeting on Capacity Building for Digital Development*, yang diselenggarakan pada 27-28 November 2019, di Incheon. Masukan dan tinjauan tambahan juga diberikan oleh International Telecommunications Union (ITU) dan Information and Communications Technology and Disaster Risk Reduction Division (IDD)-ESCAP.

Desain sampul dibuat oleh Ho-Din Ligay, sementara tata letak oleh Angielika Bartolome dan Gyubin Hwang. Sze-shing Poon dan Sara Bennouna melakukan koreksi naskah. Joo-Eun Chung dan Ho-Din Ligay memberi dukungan administratif dan bantuan lain yang diperlukan untuk penerbitan modul ini.

Alih Bahasa untuk modul ini dilakukan oleh Yudho Giri Sucahyo, Yova Ruldeviyani, dan Muhammad Sidratul Muntaha Al Mutawakkil Alallah.

TUJUAN MODUL

Modul ini bertujuan untuk:

1. Menjelaskan konsep privasi dan keamanan informasi, serta konsep terkait lainnya;

2. Menjelaskan ancaman terhadap keamanan informasi dan cara mengatasinya;

3. Membahas kebutuhan untuk pembentukan dan implementasi kebijakan mengenai keamanan informasi, termasuk siklus hidup keamanan informasi; serta

4. Memberikan gambaran umum mengenai standar keamanan informasi dan perlindungan privasi yang digunakan oleh berbagai negara dan organisasi keamanan informasi internasional.

HASIL PEMBELAJARAN

Setelah mempelajari modul ini, pembaca diharapkan dapat:

1. Menjelaskan privasi dan keamanan informasi, serta konsep terkait lainnya;

2. Mengenali ancaman terhadap keamanan informasi;

3. Menilai kebijakan keamanan informasi yang ada saat ini menurut standar internasional keamanan informasi dan perlindungan privasi; serta

4. Merumuskan atau membuat rekomendasi mengenai kebijakan keamanan informasi yang sesuai konteks.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR KOTAK

DAFTAR STUDI KASUS

1. Kebutuhan Keamanan Informasi

Bab ini bertujuan untuk:

- Menjelaskan konsep informasi dan keamanan informasi; serta
- Menjelaskan berbagai standar yang diterapkan pada aktivitas keamanan informasi

Kehidupan manusia saat ini sangatlah bergantung pada teknologi informasi dan komunikasi (TIK). Hal ini menjadikan setiap individu, organisasi dan negara sangat rentan mengalami serangan terhadap sistem informasi, seperti gangguan siber *(cyber-intrusions)*, terorisme siber *(cyber-terrorism)*, kejahatan siber *(cyber-crime)*, dan sejenisnya. Hanya sedikit dari individu dan organisasi yang siap menghadapi serangan-serangan tersebut. Pemerintah memiliki peranan penting dalam memastikan keamanan informasi dengan memperluas infrastruktur informasi-komunikasi dan membangun sistem agar terlindung dari ancaman keamanan informasi.

Modul ini fokus kepada keamanan informasi yang merupakan bagian dari keamanan siber *(cyber security)*. Isu-isu mengenai kebebasan berekspresi secara daring, hak asasi daring, kekerasan terhadap perempuan dan anak perempuan (VAWG) secara daring, pelecehan secara digital *(digital abuse)* dan kekerasan seksual secara daring, ujaran kebencian secara daring, perundungan siber *(cyberbullying)*, dan langkah perlindungan anak secara daring (COP) dikecualikan dalam modul ini, dan kesemuanya dapat membentuk modul terpisah lainnya mengenai kesadaran keamanan internet/daring.

1.1. Konsep Dasar dalam Keamanan Informasi

Apakah yang dimaksud informasi?

Pada umumnya, informasi didefinisikan sebagai hasil dari aktivitas mental, yaitu sebuah produk tanwujud *(intangible)* atau abstrak yang disebarkan melalui media. Dalam ranah TIK, informasi merupakan hasil dari pengolahan, manipulasi, dan pengorganisasian data yang merupakan sekumpulan fakta.

Dalam ranah keamanan informasi, informasi didefinisikan sebagai sebuah “aset”, yaitu sesuatu yang bernilai (berharga) dan karenanya harus dilindungi. Definisi informasi dan keamanan informasi dalam ISO/IEC 27001:2005 akan digunakan di sepanjang pembahasan modul ini.

Nilai yang diberikan pada informasi saat ini mencerminkan pergeseran dari masyarakat agraris menuju masyarakat industri dan pada akhirnya menjadi masyarakat yang berorientasi informasi. Dalam masyarakat agraris, tanah merupakan aset terpenting dan negara dengan produksi biji-bijian terbesar memiliki keunggulan kompetitif. Dalam masyarakat industri, kekuatan modal, seperti memiliki cadangan minyak, merupakan faktor utama dalam hal daya saing. Dalam masyarakat yang berorientasi pada pengetahuan dan informasi, informasi merupakan aset terpenting. Sedangkan kemampuan untuk mengumpulkan, menganalisis, dan menggunakan informasi merupakan keunggulan kompetitif bagi negara mana pun.

Karena perspektif telah bergeser dari nilai aset bersih menjadi nilai aset informasi, maka disepakati bahwa informasi memang perlu dilindungi. Informasi itu sendiri lebih berharga daripada media yang menyimpan informasi. Tabel 1 di bawah ini menunjukkan perbandingan aset informasi dengan aset nyata *(tangible)*.

Sebagaimana yang terlihat pada Tabel 1, aset informasi sangat berbeda dengan aset nyata. Dengan demikian, aset informasi rentan terhadap berbagai jenis risiko (bahaya).

Tabel 1. Perbandingan Aset Informasi dan Aset Nyata

Karakteristik	Aset informasi	Aset nyata
Bentuk – pemeliharaan	Tidak memiliki bentuk fisik dan bersifat fleksibel	Memiliki bentuk fisik
Nilai – Berubah	Nilainya menjadi lebih tinggi saat digabungkan dan diproses	Nilai total merupakan jumlah dari setiap nilai
Berbagi	Reproduksi aset informasi tak terbatas dan orang-orang dapat berbagi nilai aset tersebut	Reproduksi tidak mungkin; dengan adanya reproduksi, nilai aset berkurang
Media – ketergantungan	Membutuhkan media untuk membawanya	Dapat dibawa secara bebas (karena bentuk fisiknya)

Risiko terhadap Aset Informasi

Seiring dengan meningkatnya nilai aset informasi, keinginan untuk mendapatkan akses terhadap informasi dan mengendalikannya juga menjadi meningkat. Berbagai kelompok terbentuk dalam rangka memanfaatkan aset informasi untuk berbagai tujuan, dan beberapa di antaranya mengerahkan segala upaya untuk memperoleh aset informasi dengan cara apa pun. Upaya yang dimaksud dalam kelompok terakhir adalah akses tidak sah (peretasan), penggunaan tidak sah (pembajakan), penghancuran sistem informasi melalui virus komputer, dan sejenisnya. Berbagai risiko yang menyertai informatisasi ini akan dibahas pada Bab 2 modul ini.

Berbagai aspek negatif dari lingkungan berorientasi informasi adalah sebagai berikut:

Meningkatnya perilaku tidak etis yang muncul dari anonimitas – TIK dapat dimanfaatkan untuk menjaga anonimitas sehingga memudahkan individu tertentu untuk terlibat dalam tindak kejahatan atau perilaku tidak etis, termasuk memperoleh informasi secara ilegal.

Konflik atas kepemilikan dan kendali informasi – Kerumitan yang disebabkan oleh kepemilikan dan kendali informasi telah meningkat seiring meluasnya informatisasi. Misalnya, saat pemerintah berupaya membangun basis data informasi pribadi di bawah payung *e-government*, beberapa sektor menyatakan kekhawatirannya atas kemungkinan terjadinya pelanggaran privasi saat penyingkapan informasi pribadi kepada pihak lain.

Kesenjangan informasi dan kesejahteraan antar kelas dan negara – Ukuran pemegang aset informasi dapat menjadi barometer kesejahteraan dalam masyarakat yang berorientasi pada pengetahuan/informasi. Negara maju memiliki kapasitas untuk menghasilkan lebih banyak informasi dan mendapatkan keuntungan dari penjualan produk informasi. Sebaliknya, negara-negara miskin informasi membutuhkan investasi besar hanya untuk dapat mengakses informasi.

Meningkatnya keterbukaan informasi akibat jaringan yang handal – Masyarakat yang berorientasi pada pengetahuan/informasi adalah masyarakat jaringan. Seluruh dunia terhubung seperti jaringan tunggal yang berarti kelemahan di satu bagian jaringan dapat berdampak buruk pada bagian jaringan yang lain.

Apakah yang dimaksud dengan keamanan informasi?

Keamanan informasi didefinisikan sebagai penjagaan kerahasiaan, keutuhan, dan ketersediaan informasi.[1] Keamanan informasi biasanya juga melibatkan pencegahan atau setidaknya mengurangi kemungkinan akses, penggunaan, pengungkapan, gangguan, penghapusan/penghancuran, kecurangan, modifikasi, inspeksi, pencatatan atau devaluasi yang tidak sah/tidak tepat, meskipun mungkin juga menyangkut pengurangan dampak buruk dari berbagai insiden. Informasi dapat berbentuk apa pun, misalnya elektronik atau fisik, nyata (misalnya dokumen) atau abstrak (misalnya pengetahuan).

Fokus utama keamanan informasi adalah perlindungan kerahasiaan, keutuhan, dan ketersediaan data (juga dikenal sebagai 3 aspek CIA atau *CIA Triad*) yang seimbang, di samping juga mempertahankan fokus pada implementasi kebijakan yang efisien, tanpa mengganggu produktivitas organisasi.

Sebaliknya, keamanan siber tidak hanya mencakup keamanan informasi, melainkan juga keamanan infrastruktur digital, seperti sistem *Supervisory Control and Data Acquisition* (SCADA) dan sistem *Internet-of-Things* (IoT), yang melebihi perlindungan informasi berharga.

4R Keamanan Informasi

4R Keamanan Informasi adalah informasi yang tepat *(Right Information)*, orang yang tepat *(Right People)*, waktu yang tepat *(Right Time)* dan bentuk yang tepat *(Right Form)*. Pengaturan 4R merupakan cara paling efisien untuk menjaga dan mengontrol nilai informasi.

[1] International Organization for Standardization. (2018). *Information technology — Security techniques — Information security management systems — Overview and vocabulary* (ISO/IEC Standard No. 27000). Diakses dari https://www.iso.org/standard/73906.html

Gambar 1. 4R Keamanan Informasi

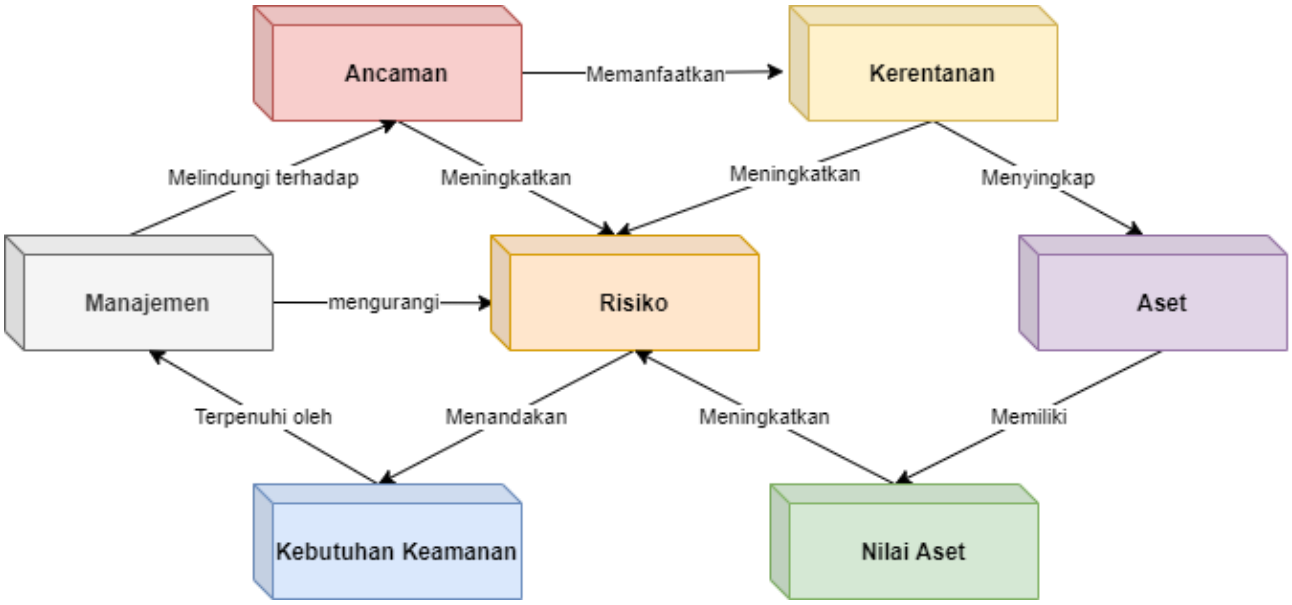
Informasi yang tepat *(Right Information)* mengacu pada akurasi dan kelengkapan informasi yang menjamin keutuhan atau integritas informasi.

Orang yang tepat *(Right People)* berarti informasi hanya tersedia bagi individu-individu yang berwenang, yang menjamin kerahasiaan.

Waktu yang tepat *(Right Time)* mengacu pada aksesibilitas informasi dan kegunaannya atas permintaan pihak berwenang. Hal ini menjamin ketersediaan (informasi).

Bentuk yang tepat *(Right Form)* mengacu pada penyediaan informasi dalam format yang tepat.

Untuk menjaga keamanan informasi, 4R harus diterapkan dengan sebaik mungkin. Artinya, kerahasiaan, keutuhan, dan ketersediaan harus diperhatikan saat menangani informasi.



Gambar 2. Hubungan antara Aset informasi dan Risiko

Keamanan informasi juga membutuhkan pemahaman yang jelas mengenai nilai aset informasi, ancaman serta kerentanannya terhadap ancaman tersebut. Hal ini dikenal sebagai manajemen risiko. Gambar 2 di atas menunjukkan hubungan antara aset informasi dan risiko.

Risiko ditentukan oleh nilai aset, ancaman, dan kerentanan. Rumusnya adalah sebagai berikut:
Risiko = ∫ (Nilai Aset, Ancaman, Kerentanan)

Risiko berbanding lurus dengan nilai aset, ancaman dan kerentanan. Dengan demikian, risiko dapat ditingkatkan atau dikurangi dengan memanipulasi besar nilai aset, ancaman dan kerentanan. Hal ini dapat dilakukan melalui manajemen risiko.

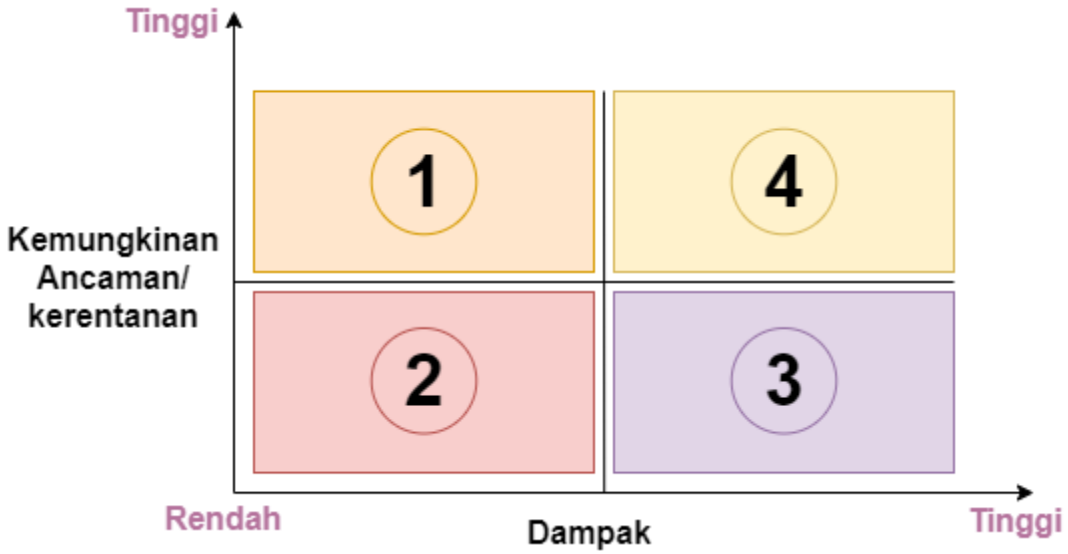
Adapun metode manajemen risiko adalah sebagai berikut:

Pengurangan risiko (mitigasi risiko) – Hal ini dilakukan saat kemungkinan adanya ancaman/kerentanan terhadap ancaman tinggi, tetapi efeknya rendah. Hal ini memerlukan pemahaman mengenai apa saja ancaman dan kerentanan yang ada, mengubah atau menguranginya, dan menerapkan langkah penanggulangan. Namun pengurangan risiko tidak mengubah nilai risiko menjadi “0”.

Penerimaan risiko – Hal ini dilakukan saat kemungkinan adanya ancaman/kerentanan terhadap ancaman rendah dan kemungkinan dampaknya kecil atau masih bisa diterima.

Pemindahan risiko – Jika risiko terlalu tinggi atau organisasi tidak dapat menyiapkan kontrol yang diperlukan, risiko dapat dipindahkan ke luar organisasi. Contohnya adalah mengambil polis asuransi.

Penghindaran risiko – Jika ancaman dan kerentanan sangat mungkin terjadi dan dampaknya juga sangat tinggi, yang terbaik adalah menghindari risiko dengan mengalihdayakan (*outsourcing*) perangkat pemrosesan data dan juga staf.



Gambar 3. Metode Manajemen Risiko

Gambar 3 di atas merupakan representasi grafis dari keempat metode manajemen risiko. Pada gambar tersebut, kuadran 1 adalah pengurangan risiko, kuadran 2 adalah penerimaan risiko, kuadran 3 adalah pemindahan risiko dan kuadran 4 adalah penghindaran risiko.

Pertimbangan utama dalam memilih metode manajemen risiko yang tepat adalah efektivitas biaya. Analisis efektivitas biaya harus dilakukan sebelum rencana pengurangan, penerimaan, pemindahan, atau penghindaran resiko ditetapkan.

1.2. Standar Aktivitas Keamanan Informasi

Aktivitas keamanan informasi tidak dapat dilakukan secara efektif tanpa pengerahan rencana administratif, fisik dan teknis terpadu.

Banyak organisasi telah merekomendasikan standar aktivitas keamanan informasi. Contohnya antara lain Organisasi Internasional untuk Standardisasi dan Komisi Elektroteknik Internasional (ISO/IEC), (ITU-U), kebutuhan keamanan informasi dan evaluasi poin-poin pada *Certified Information Systems Auditor* (CISA) milik Information Systems Audit and Control Association (ISACA), serta *Certified Information Systems Security Professional* (CISSP) milik Konsorsium Sertifikasi Keamanan Sistem Informasi Internasional atau (ISC)[2]. Standar-standar tersebut merekomendasikan aktivitas keamanan informasi terpadu, seperti perumusan kebijakan keamanan informasi, pembangunan dan pengoperasian organisasi keamanan informasi, manajemen sumber daya manusia, manajemen keamanan fisik, manajemen keamanan teknis, audit keamanan, dan manajemen kontinuitas bisnis.

Dalam Tabel 2 berikut tercantum berbagai standar terkait domain keamanan informasi.

Tabel 2. Domain Keamanan Informasi serta Standar dan Sertifikasi Terkait

Domain Keamanan	ISO/IEC 27001	CISA	CISSP
	Kebijakan keamanan informasi	Manajemen dan Tata Kelola IT	Arsitektur dan Rekayasa Keamanan
	Organisasi Keamanan Informasi		
	Manajemen Aset	Perlindungan Aset Informasi	Manajemen Keamanan dan Risiko
	Keamanan Sumber Daya Manusia		
	Manajemen Insiden Keamanan Informasi		

[2] (ISC)². (2020). *Cybersecurity Certification: CISSP - Certified Information Systems Security Professional*: (ISC). Diakses dari http://www.isc2.org/cissp

Administratif	Aspek Keamanan Informasi pada Manajemen Kontinutias bisnis		
	Hubungan Pemasok Kepatuhan	Proses Audit Sistem Informasi	Penilaian dan Pengujian Keamanan
Fisik	Keamanan Fisik dan Lingkungan		Keamanan Aset
Teknis	Kriptografi Keamanan Komunikasi Keamanan Operasi	Operasi dan Ketahanan Bisnis Sistem Informasi	Operasi Keamanan Keamanan Komunikasi dan Jaringan
	Kontrol Akses		Manajemen Identitas dan Akses
	Akuisisi, Pengembangan, dan Pemeliharaan Sistem	Akuisisi, Pengembangan, dan Implementasi Sistem Informasi	Keamanan Pengembangan Perangkat Lunak

ISO/IEC27001 fokus kepada keamanan administratif. Secara khusus, ia menekankan dokumentasi dan audit operasi sebagai perilaku administratif dan ketaatan pada kebijakan/pedoman dan hukum. Diperlukan konfirmasi dan langkah penanggulangan berkelanjutan oleh administrator. Jadi, ISO/IEC27001 mencoba mengatasi titik lemah sistem keamanan, peralatan, dan sejenisnya dengan cara administratif

Sebaliknya, tidak disebutkan keamanan sumber daya manusia atau fisik dalam CISA, yang fokus kepada kegiatan audit dan kontrol terhadap sistem informasi. Oleh karena itu, peran auditor dan kinerja proses audit menjadi sangat penting.

Fokus utama CISSP[3] terletak pada keamanan teknis. CISSP menekankan pengembangan perangkat lunak, manajemen akses dan identitas, keamanan komunikasi dan jaringan, serta keamanan operasi.

[3] Ibid

Latihan:

1. Kaji atau nilailah tingkat kesadaran keamanan informasi setiap orang di organisasi Anda!

2. Langkah-langkah keamanan informasi apakah yang diterapkan organisasi Anda? Klasifikasikan langkah-langkah tersebut dalam empat metode keamanan informasi!

3. Identifikasi contoh langkah keamanan informasi pada domain administratif, fisik, dan teknis di organisasi Anda atau di organisasi lain di negara atau yurisdiksi Anda!

Peserta pelatihan dapat melakukan latihan ini dalam kelompok kecil. Jika peserta berasal dari negara yang berbeda, kelompok kecil bisa dibentuk berdasarkan negara.

Uji Kompetensi:

1. Apa perbedaan informasi dengan aset-aset lainnya?

2. Mengapa keamanan informasi menjadi perhatian para pembuat kebijakan?

3. Bagaimanakah cara untuk memastikan keamanan informasi? Sebutkan perbedaan berbagai metode penanganan keamanan informasi!

4. Sebutkan perbedaan ketiga domain keamanan informasi (administratif, fisik, dan teknis)!

2. Tren dan Arah Keamanan Informasi

Bab ini bertujuan untuk:

- Memberikan gambaran umum mengenai ancaman terhadap keamanan informasi; dan
- Menjelaskan langkah penanggulangan terhadap ancaman tersebut

2.1. Jenis-Jenis Ancaman Siber

Ancaman Eksternal

Ancaman eksternal adalah serangan oleh non pegawai dan umumnya dilakukan secara jarak jauh dari luar kantor organisasi. Contoh ancaman eksternal seperti peretasan, penolakan layanan atau serangan *Denial-of-Service* (DoS), dan *malware*.

Ancaman Internal

Ancaman internal adalah serangan oleh pegawai atau kontraktor yang memiliki akses fisik terhadap sistem, jaringan, dan aplikasi sebuah organisasi. Serangan tersebut biasanya dilakukan oleh karyawan/kontraktor yang tidak senang terhadap organisasinya. Tanpa disadari, serangan internal juga dapat difasilitasi oleh karyawan/kontraktor yang menggunakan rekayasa sosial dan memanfaatkan karyawan yang kurang sadar terhadap keamanan.

2.2. Jenis-Jenis Ancaman Eksternal

Peretasan *(Hacking)*

Peretasan merupakan tindakan mendapatkan akses terhadap komputer atau jaringan komputer dalam rangka mendapatkan atau mengubah informasi di dalamnya tanpa izin yang sah.

Peretasan dapat diklasifikasikan sebagai peretasan hiburan, kriminal, atau politik, tergantung pada tujuan serangannya. Peretasan hiburan *(recreational hacking)* adalah modifikasi program dan data tanpa izin hanya demi memuaskan rasa penasaran peretas semata. Peretasan kriminal *(criminal hacking)* digunakan dalam penipuan atau pengintaian. Sedangkan peretasan politik *(political hacking)* merusak situs web untuk menyiarkan pesan politik yang tidak sah.

Belakangan ini, peretasan [4] semakin menyangkut terorisme siber *(cyber terrorism)* dan peperangan siber *(cyberwarfare)*, yang menjadi ancaman besar bagi keamanan nasional. Tren baru lainnya menunjukkan kelompok peretasan yang menyasar situs-situs penting yang memuat kepentingan nasional dan menyimpan informasi yang sangat sensitif.

[4] Cross, D. (10 Januari 2017). *World's Most Recent & Biggest Hacking Incidents*. Web Hosting Media. https://webhostingmedia.net/recent-biggest-hacking-incidents.

Kotak 1. Contoh Peretasan Hiburan dan Kriminal

Bank JPMorgan Chase Diretas

Lebih dari 80 juta rekening pengguna bocor kepada peretas pada tahun 2014.

Sekelompok peretas Rusia menyerang salah satu bank terbesar di Amerika Serikat. Mereka berhasil membobol 76 juta rekening pribadi dan 7 juta rekening usaha kecil. Mereka menerobos 90 komputer server JPMorgan Chase dan dapat melihat semua informasi pribadi pemilik rekening.

Para peretas mencuri informasi dasar, seperti nama, nomor telepon, alamat surel, dan alamat rumah.

Denial-of-Service (DoS) dan DoS terdistribusi (DDoS)

Serangan penolakan layanan atau *Denial-of-Service* (DoS) menghasilkan aksi pada komputer atau perangkat jaringan yang mengakibatkan proses, sumber daya, atau aktivitas lain berjuang keras dan gagal merespons dengan baik. Sementara serangan penolakan layanan terdistribusi atau *Distributed Denial-of-Service* (DDoS) terjadi saat beberapa perangkat terkena serangan DoS dari berbagai lokasi yang tersebar.

Lalu lintas serangan tertentu atau pemanfaatan kerentanan yang menyebabkan target menjadi tidak responsif umumnya sama, baik untuk serangan DoS maupun DDoS. Berbagai sumber yang terlibat dalam serangan DDoS sering kali membuat serangan lebih sulit ditangkal dan umumnya lebih berhasil melawan target yang lebih besar dan merespons lebih cepat.[5]

Studi Kasus 1: Situs Web global terkena serangan DDoS

Surel Spam

Spam merupakan pesan elektronik komersial massal yang tidak diharapkan yang dikirim melalui layanan komunikasi informasi seperti surel. Spam adalah media yang murah dan efektif untuk iklan. Belakangan, spam digunakan untuk menyebarkan kode berbahaya atau merampas informasi pribadi. Terkadang, jenis spam ini dikirim dari PC zombie yang dalam kebanyakan kasus telah terinfeksi oleh kode berbahaya *(malicious codes)*.

Pada Oktober 2016, penjahat siber *(cybercriminal)* melancarkan serangan DDoS dan mengganggu sejumlah situs web, di antaranya: Twitter, Netflix, PayPal, Pinterest, dan PlayStation Network.

Serangan itu mengejutkan karena pada satu waktu ukurannya mencapai 1 Tbps. Kelompok di balik serangan tersebut melakukan hal ini dengan menggabungkan dua puluh ribu perangkat IoT, mengubahnya menjadi botnet dan sebenarnya membanjiri lalu lintas penyedia hosting DNS Dyn.

Diambil (dengan modifikasi) dari: https://www.welivesecurity.com/2016/12/30/biggest-security-incidents-2016/.

[5] SecureAuth. (14 Juli 2017). Diakses dari secureauth_ciam_infographic_170714.pdf. Irvine.

Studi Kasus 2: Sumber Surel Spam Terbesar Dunia Ditutup

Botnet Rustock, sebuah jaringan komputer internasional yang terinfeksi virus, selama bertahun-tahun menghasilkan miliaran surel per hari, mempromosikan apotek daring tanpa izin hingga pil impotensi dengan harga murah.

Pada Maret 2011, sesuai perintah pengadilan, Microsoft dengan didukung Marshal AS menyita server yang diperkirakan mengendalikan hampir satu juta PC Windows secara diam-diam.

Server-server tersebut disewa dari perusahaan *hosting* internet komersial di seluruh Mid-West AS yang tampaknya tidak menyadari keterlibatannya dalam Rustock. Server Komando dan Kendali (C&C) ini akan memberikan instruksi untuk menginfeksi *Home PC* dan *Business PC* di seluruh dunia.

Diambil (dengan modifikasi) dari: https://www.telegraph.co.uk/technology/news/8391532/Worlds-biggest-source-of-spam-email-shut-down.html.

Pengelabuan *(Phishing)*

Pengelabuan atau *phishing* merupakan penggunaan surel atau pesan untuk mendapatkan informasi sensitif seperti nama pengguna, kata sandi, dan detail kartu kredit dengan menggunakan entitas yang tepercaya. Hal ini biasanya dilakukan melalui *spoofing* surel atau pesan instan, dan sering kali mengarahkan pengguna agar memasukkan informasi pribadi di situs web palsu yang tampilan dan nuansanya mirip dengan situs resmi.

Studi Kasus 3: Penipuan Siber Terbesar di Kerajaan Serikat (UK)

Unit Aksi Penipuan Kepolisian Metropolitan UK memperkirakan penipuan senilai 59 juta pound sterling berhasil dicegah di UK setelah tiga pria dinyatakan bersalah melakukan penipuan *phishing* yang canggih untuk mengakses rekening nasabah bank di 14 negara.

Sekitar 2.600 halaman *phishing* yang meniru situs web perbankan dianalisis oleh Met Police Central e-Crime Unit (PCeU), Serious Organized Crime Agency (SOCA), dan Dinas Rahasia AS (US Secret Service).

Orang-orang di balik penipuan tersebut ditelusuri hingga ke UK, tempat mereka tinggal di hotel-hotel mewah di London sembari terus menipu para korban.

Petugas kemudian menemukan server yang berisi rincian 30.000 pelanggan bank dengan 12.500 di antaranya berada di UK dan 70 juta alamat surel pelanggan yang akan menjadi sasaran penipuan *phishing* berikutnya.

Para pelaku ditahan sejak 2016 selama 20 tahun. Petugas penyidik DI Jason Tunn mengatakan pada saat itu bahwa kasus tersebut adalah "kasus terbesar yang pernah ditangani PCeU hingga saat ini dan mungkin akan menjadi kasus *phishing* siber terbesar di UK sejauh ini".

Kasus tersebut adalah penipuan siber terbesar di UK. Pada puncaknya, penipuan itu berhasil meraup hingga 2 juta pound sterling dalam seminggu.

Diambil (dengan modifikasi) dari: UK's biggest ever cyber scammers stole £113m by calling victims pretending to be from their BANK: Fraudsters used bin bags full of cash for shopping sprees, bought supercars and a Lahore mansion. Diakses dari https://www.dailymail.co.uk/news/article-3792417/Fraud-ring-boss-gang-stole-113million-UK-firms.html

Penjejalan Kredensial *(Credential Stuffing)*

Penjejalan kredensial merupakan jenis serangan siber dengan pencurian kredensial akun yang biasanya terdiri dari daftar nama pengguna dan/atau alamat surel serta kata sandi yang sesuai (sering kali berasal dari pelanggaran data di server pihak ketiga) yang digunakan untuk mendapatkan akses tidak sah terhadap berbagai akun pengguna melalui permintaan *login* otomatis berskala besar ke sebuah aplikasi web. Serangan penjejalan kredensial dapat terjadi karena banyak pengguna menggunakan kembali kombinasi nama pengguna/sandi yang sama di berbagai situs sebagaimana laporan sebuah survei bahwa 81 persen pengguna telah menggunakan kembali sandi mereka di dua situs atau lebih dan 25 persen pengguna menggunakan sandi yang sama hampir di sebagian besar akun mereka.[6]

Studi Kasus 4: Akun State Farm AS Terkena Serangan Penjejalan Kredensial

Pada Agustus 2019, perusahaan asuransi Amerika Serikat, State Farm, mengirimkan pemberitahuan melalui surel kepada para pengguna yang kredensial *login*-nya telah bocor atau diketahui penyerang saat serangan penjejalan kredensial.

Penyerang mengumpulkan nama pengguna dan kata sandi yang bocor akibat pelanggaran data organisasi lain serta menggunakan kredensial tersebut untuk mencoba mendapatkan akses terhadap akun di State Farm. State Farm juga telah mengatur ulang kata sandi akun yang kredensial *login*-nya telah bocor.

Diambil (dengan modifikasi) dari: *State Farm Accounts Compromised in Credential Stuffing Attack*. Diakses dari https://www.bleepingcomputer.com/news/security/state-farm-accounts-compromised-in-credential-stuffing-attack/-113million-UK-firms.html

Kode Berbahaya *(Malicious code)*

Kode berbahaya mengacu pada program-program yang dapat menyebabkan kerusakan pada sistem saat dijalankan. Virus, *worm*, dan *trojan horse* merupakan jenis kode berbahaya.

Virus komputer adalah program komputer atau kode pemrograman yang merusak sistem dan data komputer dengan cara mereplikasi dirinya sendiri dan dengan menyalin ke program lain, sektor boot komputer, atau dokumen.

Worm adalah virus yang bereplikasi yang tidak mengubah file selain yang berada di memori aktif, menggunakan bagian sistem operasi yang otomatis dan biasanya tidak terlihat oleh pengguna. Replikasinya yang tidak terkendali menghabiskan sumber daya sistem, memperlambat atau menghentikan tugas lainnya. Umumnya, *worm* baru terdeteksi hanya saat hal tersebut terjadi.

Trojan horse adalah program yang seolah berguna dan/atau tidak berbahaya tetapi sebenarnya bersifat jahat seperti memuat program tersembunyi atau skrip perintah yang membuat sistem rentan terhadap gangguan.

[6] Ibid.

Studi Kasus 5: Republik Islam Iran: *Worm* Stuxnet Menandai Era Baru Perang Siber

Worm Stuxnet ditemukan pada berbagai komputer di Republik Islam Iran pada bulan Juni 2010 oleh sebuah perusahaan keamanan Belarusia. *Worm* tersebut telah menginfeksi lebih dari 100.000 sistem komputer di seluruh dunia, kebanyakan di Iran.

Los Angeles Times melaporkan bahwa: "*Stuxnet* disebut sebagai senjata siber paling canggih yang pernah dilancarkan, karena sifat berbahayanya yang diyakini secara diam-diam menargetkan peralatan tertentu yang digunakan dalam program nuklir Iran."

Kode yang ditargetkan dirancang untuk menyerang sistem *Siemens Simatic WinCC SCADA*. Sistem Siemens digunakan di berbagai fasilitas untuk mengelola jaringan pipa, pembangkit nuklir, dan berbagai peralatan utilitas dan manufaktur. Meskipun *worm stuxnet* mempengaruhi banyak sistem, banyak yang berspekulasi bahwa *worm* tersebut dibuat secara khusus untuk menargetkan fasilitas nuklir Iran. Pencipta *worm* tersebut masih belum diketahui.

Diambil (dengan modifikasi) dari: Ken Dilanian, *"Iran's nuclear program and a new era of cyber war"*, *Los Angeles Times*, 17 Januari 2011, diakses dari http://articles.latimes.com/2011/jan/17/world/la-fg-iran-cyber-war-20110117;

Kim Zetter, *"Iran: Computer Malware Sabotaged UraniumCentrifuges"*, Wired, 29 November 2010, diakses dari http://www.wired.com/threatlevel/2010/11/stuxnet-sabotage-centrifuges/; dan Wikipedia, *"Stuxnet"*, diakses dari http://en.wikipedia.org/wiki/Stuxnet.

Ransomware adalah program yang seolah berguna dan/atau tidak berbahaya, tetapi sebenarnya sangat bersifat jahat seperti mengancam mempublikasikan data korban atau terus menerus memblokir akses terhadap data korban hingga korban membayar uang tebusan.

Studi Kasus 6: Serangan Siber *WannaCry* Merugikan NHS Sebesar 92 juta Pounds Akibat 19.000 Janji Dibatalkan

Peretasan bernama *WannaCry*, yang mematikan ratusan ribu komputer di seluruh dunia dengan pesan permintaan tebusan dari peretas, mencapai sepertiga dari layanan rumah sakit (*hospital trust)* dan 8 persen praktik umum *(general practice)*. Sekitar 1 persen dari seluruh pelayanan National Health Service (NHS atau NHS trust) terganggu selama seminggu.

Peretasan tersebut menyebabkan lebih dari 19.000 janji dibatalkan, menyebabkan kerugikan bagi NHS sebesar 20 juta pound sterling antara 12-19 Mei dan 72 juta pound sterling saat pembersihan dan peningkatan sistem TI yang dilakukan setelahnya.

Serangan siber menyebabkan 200.000 komputer mengunci pengguna dengan tulisan pesan eror berwarna merah yang menuntut mata uang Bitcoin. Serangan itu dituduhkan pada peretas elit Korea Utara setelah penyelidikan selama setahun.

Diambil (dengan modifikasi) dari: The Telegraph; WannaCry cyber-attack cost the NHS £92m as 19,000 appointments cancelled, diakses dari https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled

Ancaman Persisten Tingkat Lanjut

Ancaman persisten tingkat lanjut atau *advanced persistent threat* (APT) merupakan serangan jaringan, yaitu saat orang yang tidak berwenang mendapatkan akses ke jaringan dan tetap di sana tanpa terdeteksi dalam jangka waktu yang lama. Maksud dari serangan APT lebih kepada pencurian data dibandingkan menyebabkan kerusakan pada jaringan atau organisasi.[7] APT menyerang sasaran organisasi di berbagai sektor yang memiliki informasi bernilai tinggi, seperti pertahanan nasional, manufaktur, dan industri keuangan.

Penyerang APT sering kali menggunakan *spear fishing*, sejenis manipulasi psikologis, untuk mendapatkan akses ke jaringan melalui cara yang sah. Setelah akses tercapai, penyerang membuat pintu belakang *(back door)*.

Langkah selanjutnya adalah mengumpulkan kredensial pengguna yang valid (khususnya kredensial administratif) dan melintasi jaringan secara lateral, serta memasang lebih banyak pintu belakang. Pintu belakang tersebut memungkinkan penyerang untuk menginstal utilitas palsu dan membuat “infrastruktur hantu” untuk mendistribusikan *malware* yang tetap tersembunyi di depan mata.

[7] Rosencrance, L. (27 Agustus 2020). *What is advanced persistent threat?* SearchSecurity. Diakses dari https://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT.
.

Studi Kasus 7: RSA Terkena Serangan APT

Pada bulan Maret 2011, RSA, divisi keamanan EMC, mengumumkan bahwa mereka telah menjadi sasaran sebuah serangan dan informasi terkait produk autentikasi dua faktor SecurID RSA telah dicuri oleh penyerang.

Investigasi menyatakan bahwa serangan tersebut masuk dalam kategori APT. Serangan APT menjadi tantangan signifikan bagi seluruh perusahaan besar. Untuk mengidentifikasi APT, organisasi perlu menerapkan teknologi yang tidak hanya sekadar mengidentifikasi semua potensi ancaman melalui analisis perilaku, melainkan juga dapat menguji semua hal mencurigakan di lingkungan virtual.

Autentikasi dua faktor merupakan metode yang lebih disukai untuk memberikan keamanan yang lebih kuat daripada sekadar menggunakan nama pengguna dan kata sandi saja. Salah satu metode paling umum dari autentikasi dua faktor adalah dengan menggunakan *key fob* atau token yang menyediakan kode acak yang harus dimasukkan pengguna selain nama pengguna dan kata sandi untuk mengautentikasi dan mendapatkan akses ke situs atau aplikasi.

RSA adalah penyedia solusi autentikasi dua faktor terkemuka, dan kunci serta tokennya ada di mana-mana. Dengan jutaan pelanggan mengandalkan RSA untuk memberikan keamanan tambahan dan melindungi akun mereka dari akses yang tidak sah, hal ini menjadi masalah karena peretas jahat saat ini mungkin memiliki kunci untuk menembus perlindungan tersebut.

RSA meyakinkan kliennya bahwa informasi yang diekstrak tidak akan membuat pelanggan SecurID RSA berhasil diserang langsung. Namun, informasi ini berpotensi dimanfaatkan untuk mengurangi efektivitas implementasi autentikasi dua faktor saat ini sebagai bagian dari serangan yang lebih luas. Lockheed-Martin, klien RSA, menjadi korban peretasan berikutnya, dan tampaknya peretasan tersebut dilakukan oleh orang yang sama (lihat studi kasus di atas).

Diambil (dengan modifikasi) dari: Tony Bradley, *"RSA SecurID Hack Shows Danger of APTs"*, *PCWorld*, 19 Maret 2011, diakses dari http://www.pcworld.com/businesscenter/article/222555/rsa_securid_hack_shows_danger_of_apts.html; dan Warwick Ashford, *"RSA hit by advanced persistent threat attacks"*, *Computer Weekly*, 18 Maret 2011, diakses dari http://www.computerweekly.com/Articles/2011/03/18/245974/RSA-hit-by-advanced-persistent-threat-attacks.htm.

2.3. Jenis-Jenis Serangan Internal

Pegawai/Kontraktor Yang Jahat

Serangan internal merupakan salah satu ancaman terbesar yang dihadapi oleh data dan sistem kita. Pegawai yang jahat–terutama anggota tim TI yang memiliki pengetahuan dan akses ke jaringan, pusat data (*data center)*, dan akun admin–dapat menyebabkan kerusakan serius pada jaringan, sistem, dan data organisasi.

Kurangnya Kesadaran Keamanan Pegawai

Pelatihan untuk menumbuhkan kesadaran keamanan bagi pegawai dapat membantu memberantas perilaku berisiko yang berpotensi menyebabkan pelanggaran siber *(cyber breaches)*. Program pelatihan dapat mengatasi berbagai ancaman yang dihadapi oleh

organisasi, khususnya serangan seperti surel *phishing*, *ransomware*, dan penipuan rekayasa sosial melalui telepon, pesan teks, atau saluran media sosial.

Rekayasa Sosial

Istilah “rekayasa sosial” mengacu pada serangkaian teknik yang digunakan untuk memanfaatkan orang agar membocorkan informasi rahasia. Meskipun mirip dengan tipu muslihat atau penipuan, istilah ini biasanya berlaku untuk tipu daya dalam rangka pengumpulan informasi atau akses sistem komputer. Dalam kebanyakan kasus, penyerang tidak pernah bertemu langsung dengan para korban.

2.4. Tren dalam Ancaman Keamanan Informasi[8]

Salah satu aktivitas penting dalam menjaga keamanan informasi adalah analisis tren ancaman keamanan. Hal ini mengacu kepada pencarian pola dalam ancaman keamanan dari waktu ke waktu untuk mengidentifikasi berbagai cara saat pola tersebut berubah dan berkembang, membelok ke arah yang baru, atau bergeser. Proses pengumpulan dan pengkorelasian informasi yang berulang-ulang serta penyempurnaan profil kejadian dilakukan untuk mengantisipasi kemungkinan adanya ancaman dan menyiapkan penanganan yang tepat terhadap ancaman tersebut.

Organisasi yang melakukan analisis tren ancaman keamanan informasi dan berbagi laporan tren ancaman keamanan antara lain:

- FireEye (https://www.fireeye.com/current-threats/threat-intelligence- reports.html)
- IBM (https://www.ibm.com/security/data-breach/threat-intelligence /)
- Microsoft (www.microsoft.com/en-us/security/operations/security- intelligence-report)
- Symantec (https://www.symantec.com/security-center/threat-report)
- Verizon (https://enterprise.verizon.com/resources/reports/dbir/)

Tren ancaman keamanan informasi yang telah dilaporkan akan dijelaskan sebagai berikut.

Automasi Alat Serangan[9]

Saat ini, para penyusup *(intruders)* menggunakan alat otomatis yang dapat mengumpulkan informasi tentang ribuan *host* internet dengan cepat dan mudah. Jaringan dapat dipindai dari lokasi yang jauh dan *host* yang memiliki kelemahan tertentu dapat diidentifikasi menggunakan alat otomatis tersebut. Para penyusup membuat katalog informasi untuk nantinya digunakan, dibagikan, atau diperdagangkan dengan penyusup lain, atau langsung menyerang. Beberapa

[8] Shimeall, T. J., & Williams, P. (2002). Models of information security trend analysis. *Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Defense and Law Enforcement*. Diakses dari https://doi.org/10.1117/12.479291

.

[9] Carnegie Mellon University. *Software Engineering Institute*. The CERT Division. Diakses dari https://www.sei.cmu.edu/about/divisions/cert/index.cfm.

.

alat atau *tools* (seperti Cain & Abel) mengotomatiskan serangkaian serangan kecil terhadap sasaran keseluruhan. Misalnya, penyusup dapat menggunakan penyadap paket *(packet sniffer)* untuk mendapatkan kata sandi *router* atau *firewall*, *login* ke *firewall* untuk menonaktifkan filter, dan selanjutnya menggunakan layanan berkas jaringan *(network file service)* untuk membaca data di server.

Alat Serangan Yang Sulit Terdeteksi

Beberapa alat serangan menggunakan pola serangan baru yang tidak terdeteksi oleh alat deteksi yang ada. Misalnya, teknik anti-forensik digunakan untuk menutupi atau menyembunyikan sifat alat serangan. Alat polimorfik berubah bentuk setiap kali digunakan. Alat-alat ini menggunakan protokol umum seperti *hypertext transfer protocol* (HTTP), sehingga sulit untuk membedakannya dengan lalu lintas jaringan yang sah.[10] *Worm Messenger* MSN merupakan contoh yang bagus untuk hal ini. *Worm* pada klien *Instant-Messaging* (IM) *Messenger MSN* mengirimkan berkas yang dirancang untuk menginfeksi sistem ke berbagai kontak dari daftar kontak yang telah terinfeksi. Sebelumnya, ia akan memberikan peringatan terlebih dahulu bahwa mereka akan menerima sebuah berkas. Yang mengkhawatirkan dari hal ini adalah perilaku pengguna IM yang asli telah ditirunya.[11]

Deteksi Kerentanan Lebih Cepat

Setiap tahun, kerentanan yang baru ditemukan dalam produk perangkat lunak yang dilaporkan pada Pusat Koordinasi Tim Tanggap Darurat Komputer (CERT/CC) lebih dari dua kali lipat jumlahnya, sehingga menyulitkan administrator untuk terus mengikuti pembaruan tambalan (*patch)*. Penyusup mengetahui hal tersebut dan memanfaatkannya.[12] Beberapa penyusup melancarkan serangan *zero-day* (atau *zero hour*), yaitu ancaman komputer yang memanfaatkan kerentanan aplikasi komputer yang tidak memiliki tambalan atau perlindungan karena belum diketahui oleh administrator. [13]

Meningkatnya Ancaman Asimetris dan Konvergensi Metode Serangan

Ancaman asimetris adalah kondisi saat penyerang lebih unggul daripada pelindung. Jumlah ancaman asimetris meningkat dengan otomatisasi penyebaran ancaman dan kecanggihan alat serangan.

---

[10] Ramasubramanian, S., Ansari, S., & Purcell, F. (2005). Governing Internet Use: Spam, Cybercrime and e-Commerce. In D. Butt (Ed.), *Internet governance: Asia-Pacific Perspectives* (pp. 89–104). essay, APDIP. Diakses dari https://www.unapcict.org/sites/default/files/2019-01/Internet%20Governance%20-%20Asia-Pacific%20perspectives.pdf.

[11] Kotadia, M. (5 April 2005). *E-mail worm graduates to IM* ZDNet. https://www.zdnet.com/article/e-mail-worm-graduates-to-im/.

[12] Ramasubramanian, S., Ansari, S., & Purcell, F. (2005). Governing Internet Use: Spam, Cybercrime and e-Commerce. In D. Butt (Ed.), *Internet governance: Asia-Pacific Perspectives* (pp. 89–104). essay, APDIP. Diakses dari https://www.unapcict.org/sites/default/files/2019-01/Internet%20Governance%20-%20Asia-Pacific%20perspectives.pdf.

[13] Wikimedia Foundation. (31 Desember 2020). *Zero-day (computing)*. Wikipedia. Diakses dari https://en.wikipedia.org/wiki/Zero-day_(computing).

Konvergensi metode serangan mengacu pada gabungan berbagai metode serangan yang dilakukan penyerang untuk membuat jaringan global yang mendukung aktivitas jahat terkoordinasi. Misalnya, Zbot, dikenal sebagai Zeus, adalah paket *malware* yang tersedia untuk diperjualbelikan di forum *underground*. Paket ini berisi *builder* yang dapat menghasilkan bot yang dapat dieksekusi dan juga berkas-berkas server web (PHP, gambar, *template* SQL) untuk digunakan sebagai server komando dan kendali *(command and control server)*. Meskipun Zbot merupakan *back door* umum yang dapat membuat pengguna jarak jauh dan tidak sah memiliki kendali penuh, fungsi utama Zbot adalah memperoleh keuntungan finansial — mencuri kredensial daring seperti FTP, surel, perbankan elektronik *(online banking)*, dan kata sandi daring lainnya.[14]

Meningkatnya Ancaman Serangan Infrastruktur

Serangan infrastruktur merupakan serangan yang secara luas memengaruhi komponen utama internet. Serangan tersebut menjadi perhatian karena besarnya jumlah organisasi dan pengguna di internet serta meningkatnya jumlah data pribadi di internet untuk menjalankan bisnis sehari-hari. Serangan infrastruktur mengakibatkan bocornya informasi sensitif, penyebaran informasi yang keliru, dan pengalihan sumber daya dari tugas lain yang signifikan.

Peretasan merupakan contoh serangan infrastruktur. Istilah "peretasan" mengacu pada tindakan mendapatkan akses terhadap komputer atau jaringan komputer untuk mendapatkan atau mengubah informasi tanpa izin resmi.

Peretasan dapat dikelompokkan sebagai peretasan hiburan, kriminal, atau politik, tergantung pada tujuan serangan. Peretasan hiburan merupakan modifikasi program dan data tanpa izin hanya untuk memuaskan rasa penasaran peretas semata. Peretasan kriminal digunakan dalam penipuan atau pengintaian. Sedangkan peretasan politik membahayakan situs web dengan menyiarkan pesan politik yang tidak sah.[15]

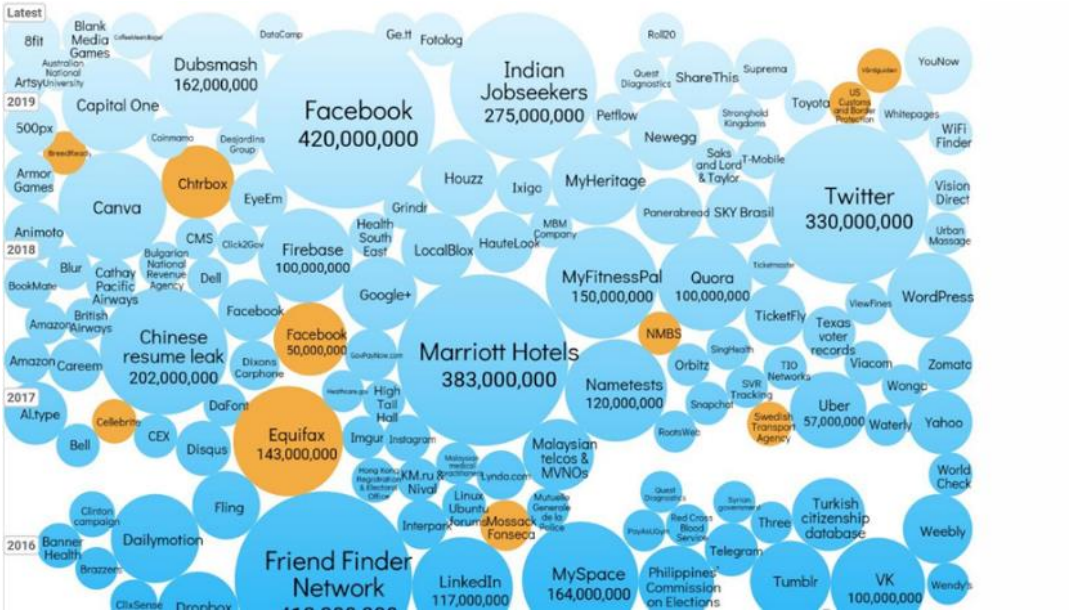
Belakangan ini, peretasan semakin berhubungan dengan teror siber *(cyberterror)*, politik siber *(cyberpolitics)*, dan peperangan siber *(cyberwarfare)*, yang menjadi ancaman besar bagi keamanan nasional.

Tren baru lainnya menunjukkan berbagai kelompok peretasan yang menyasar situs utama yang memuat kepentingan nasional dan menyimpan informasi yang sangat sensitif.

[14] Korolov, M. (27 Juni 2019). *Apa itu botnet? Saat pasukan perangkat IoT yang terinfeksi menyerang*. CSO Online. Diakses dari https://www.csoonline.com/article/3240364/what-is-a-botnet.html.

[15] Denning, D. E., Arquilla, J., & Ronfeldt, D. (2001). Aktivisme, Hacktivisme, dan Terorisme Siber: Internet Sebagai Alat Untuk Mempengaruhi Kebijakan Luar Negeri. Dalam *Network dan Netwar. Masa Depan Teror, Kejahatan, dan Militansi* (hlm. 239–288). essay, RAND Corporation.

Gambar 4 menunjukkan tren volume pelanggaran data *(data breach)*.



Gambar 4. Statistik Pelanggaran Data *(Data Breach)*

Sumber: *Information is Beautiful*.

Studi Kasus 8: Melawan Peretasan – Studi Kasus Nasional

Kejaksaan Agung Republik Indonesia (RI) secara kelembagaan memperkuat dan merevitalisasi lembaga dengan menyiapkan, merancang, dan merumuskan Satgas Kejahatan Siber yang beranggotakan para jaksa yang secara khusus memiliki pengetahuan, kemampuan, keterampilan dan keahlian dalam menangani kasus-kasus kejahatan siber.

Satgas tersebut terdiri dari tiga (3) unit khusus, yaitu:

- Pertama, Unit Kejahatan Terkait Komputer, bertugas menangani tindak kejahatan yang memanfaatkan fasilitas komputer atau teknologi informasi sebagai alat untuk melakukan kejahatan tersebut;
- Kedua, Unit Kejahatan Terhadap Komputer, bertugas menangani kejahatan yang ditujukan pada komputer dan teknologi informasi; serta
- Ketiga, Unit Sekretariat dan Kerja Sama, memberikan dukungan dalam penanganan perkara dan kerja sama, baik secara nasional maupun internasional.

Teknis: Alat dan teknik untuk mengidentifikasi serta mengumpulkan informasi terkait *botnet* aktif.

- Praktik terbaik *(best practice)* privasi dan keamanan informasi untuk mengurangi aktivitas *botnet*
- Praktik terbaik *registrar* dan *registry* untuk mengurangi aktivitas *botnet*
- Pengembangan kapasitas untuk *e-commerce* dan penyedia transaksi daring

Sosial: Inisiatif pendidikan berbasis luas *(broad-based education)* tentang keselamatan dan keamanan Internet

- Pemfasilitasan akses TIK yang aman bagi pengguna.

Toolkit PTF ITU SPAM adalah paket komprehensif untuk membantu perencana kebijakan, pembuat peraturan, dan perusahaan dalam menyesuaikan kebijakan dan memulihkan keyakinan melalui surel. Perangkat ini juga merekomendasikan berbagi informasi antar negara untuk mencegah masalah internasional.

Perubahan Tujuan Serangan

Dahulu, serangan komputer dan jaringan dilakukan karena rasa ingin tahu atau demi kepuasan diri. Sekarang, umumnya demi uang, fitnah dan pengrusakan. Selain itu, jenis-jenis serangan tersebut hanya mewakili sebagian kecil dari spektrum luas kejahatan siber.

Kejahatan siber merupakan pengrusakan, gangguan, atau distorsi data digital atau arus informasi yang disengaja untuk alasan politik, ekonomi, agama, atau ideologis. Kejahatan paling umum di antaranya seperti peretasan, DoS, kode berbahaya (malicious code), dan rekayasa sosial. Belakangan ini, kejahatan siber telah menjadi bagian dari terorisme siber dan peperangan siber yang berdampak buruk terhadap keamanan nasional.

Apa saja yang diperoleh oleh pelaku kejahatan siber tersaji pada Tabel 3 berikut ini.

Tabel 3. Hasil dari Kejahatan Siber di Tahun 2017

Butir	**Kisaran harga (dalam USD)**
Kredensial *login* lembaga publik non-keuangan	1
Kartu Debit atau Kartu Kredit	5-110
SIM, akun loyalitas *(loyalty account)*	20
Info *login* layanan pembayaran daring, seperti Paypal	20-200
Ijazah/Akte	100-400
Rekam medis	1-1,000

Paspor	1,000-2,000

Sumber: Experian Stack, B. (6 Desember 2017). *Here's How Much Your Personal Information Is Selling for on the Dark Web*. Experian. Diakses dari https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

2.5 Peningkatan Keamanan

Mengingat tren ancaman keamanan dan teknologi serangan, pertahanan yang kuat memerlukan strategi fleksibel yang dapat beradaptasi terhadap lingkungan yang berubah, prosedur dan kebijakan yang terdefinisi dengan baik, penggunaan teknologi keamanan yang tepat, dan kewaspadaan yang terus menerus.

Hal ini sangat membantu untuk memulai program peningkatan keamanan dengan menentukan status keamanan saat ini. Sejalan pula dengan program keamanan adalah prosedur dan kebijakan yang terdokumentasi, serta teknologi yang mendukung implementasinya.

Keamanan administratif

Keamanan administratif terdiri dari strategi, kebijakan, dan pedoman keamanan informasi.

Strategi keamanan informasi menentukan arah seluruh aktivitas keamanan informasi.

Kebijakan keamanan informasi merupakan rencana tingkat tinggi yang terdokumentasi untuk keamanan informasi seluruh organisasi. Ia memuat kerangka kerja untuk membuat keputusan khusus, seperti rencana keamanan administratif dan fisik.

Karena kebijakan keamanan informasi harus memiliki sudut pandang jangka panjang, kebijakan tersebut harus menghindari konten khusus teknologi dan mencakup pengembangan perencanaan kontinuitas bisnis (BCP) yang efektif.

Pedoman keamanan informasi harus ditetapkan sesuai dengan strategi dan kebijakan keamanan informasi. Pedoman tersebut harus menetapkan peraturan untuk setiap bidang yang berhubungan dengan keamanan informasi. Karena pedoman tersebut harus komprehensif dan berskala nasional, maka pedoman tersebut harus dikembangkan dan disampaikan oleh pemerintah agar ditaati oleh organisasi.

Standar keamanan informasi harus khusus dan spesifik sehingga dapat diterapkan pada semua bidang keamanan informasi. Setiap negara sebaiknya mengembangkan standar setelah menganalisis standar keamanan administratif, fisik, dan teknis yang banyak digunakan di seluruh dunia. Standar harus sesuai dengan lingkungan TIK yang berlaku.

Strategi, kebijakan, dan pedoman keamanan informasi suatu negara harus sesuai dengan hukum terkait. Ruang lingkupnya harus berada dalam batas-batas hukum nasional dan internasional.

Proses dan Operasi Keamanan Informasi

Saat strategi, kebijakan, dan pedoman keamanan informasi telah ditetapkan, prosedur dan proses pengoperasian keamanan informasi juga perlu ditentukan. Karena masyarakat adalah orang-orang yang melakukan serangan terhadap informasi atau membocorkan informasi internal, maka manajemen sumber daya manusia merupakan faktor terpenting dalam pengoperasian keamanan informasi. Oleh karena itu, diperlukan hal-hal berikut:

1. Program pendidikan dan pelatihan keamanan informasi - Terdapat banyak metode untuk meningkatkan tingkat keamanan informasi suatu organisasi, tetapi pendidikan dan pelatihan merupakan aktivitas mendasar. Anggota organisasi harus menghargai kebutuhan keamanan informasi dan memperoleh keterampilan yang dibutuhkan melalui pendidikan dan pelatihan. Namun, penting untuk mengembangkan berbagai program demi memaksimalkan keikutsertaan anggota karena program pendidikan dan pelatihan keamanan informasi standar mungkin kurang efektif.

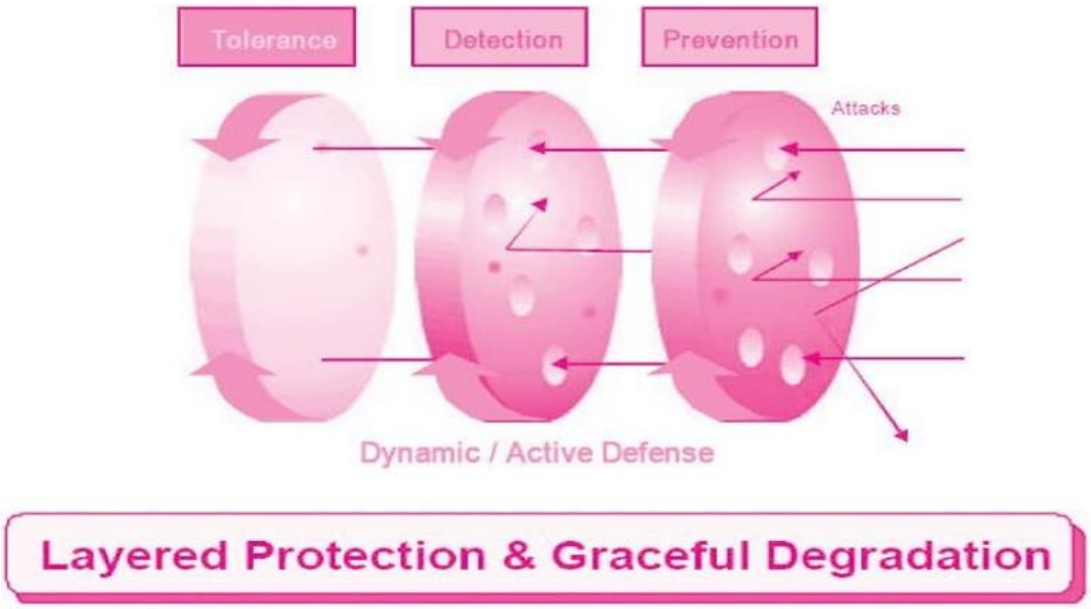
2. Memperkuat promosi melalui berbagai acara - Keikutsertaan pegawai penting dalam keberhasilan penerapan strategi, kebijakan, dan pedoman keamanan informasi. Keamanan informasi harus dipromosikan kepada para pegawai melalui berbagai aktivitas sehari-hari.

3. Mengamankan dukungan - Meskipun mungkin tingkat kesadaran keamanan informasi pegawai ada yang tinggi dan mereka memiliki kemauan kuat untuk menjaga keamanan informasi, tetap saja sulit untuk memastikan keamanan informasi tanpa adanya dukungan dari pihak tertinggi di organisasi. Dukungan dari *Chief Executive Officer* (CEO) dan *Chief Information Officer* (CIO) harus diperoleh.

Keamanan Teknologi

Berbagai teknologi dikembangkan demi membantu organisasi mengamankan sistem informasinya dari para penyusup. Teknologi tersebut membantu melindungi sistem dan informasi dari serangan, mendeteksi aktivitas yang tidak biasa atau mencurigakan, dan menangani peristiwa yang memengaruhi keamanan.

Sistem keamanan saat ini telah dirancang dan dikembangkan berdasarkan model *Defense-In-Depth* (DID) yang mengarah pada manajemen terpadu dari teknologi yang terlibat. Model ini berbeda dengan pertahanan perimeter *(perimeter defense)* yang hanya memiliki satu lapis pertahanan terhadap semua ancaman. Model DID terdiri dari pencegahan, deteksi dan toleransi, dengan kondisi ancaman terus berkurang di setiap fase (lihat Gambar 5).



Gambar 5. Model *Defense-In-Depth* (DID)

Sumber: Defense Science Board Task Force, *Protecting the Homeland: Defensive Information Operations 2000 Summer Study Volume II* (Washington, D.C., 2001), hlm. 5, diakses dari http://www.carlisle.army.mil/DIME/documents /dio.pdf.

Teknologi Pencegahan

Teknologi pencegahan atau *(prevention technology)* melindungi dari adanya penyusup dan ancaman di tingkat sistem atau penyimpanan. Teknologi tersebut meliputi:

1. Kriptografi - Juga disebut sebagai enkripsi, kriptografi merupakan proses menerjemahkan informasi dari bentuk aslinya (disebut teks terang atau *plaintext*) ke dalam bentuk kode yang tidak dapat dipahami (disebut teks tersandi atau *ciphertext*). Deskripsi mengacu pada proses mengambil *ciphertext* dan menerjemahkannya kembali menjadi *plaintext*. Kriptografi digunakan untuk melindungi berbagai aplikasi. Informasi lebih lanjut mengenai kriptografi dan teknologi terkait (IPSec, SSH, SSL, VPN, OTP, dll.) tersedia di halaman web berikut:

   - IETF RFC (http://www.ietf.org/rfc.html)
   - Pertanyaan Umum mengenai Kriptografi Saat Ini di RSA Laboratories (http://www.rsa.com/rsalabs/node.asp?id=2152)

2. *One-time password* (OTP) – Sesuai dengan namanya, OTP hanya dapat digunakan satu kali. Kata sandi statis dapat lebih mudah diakses dengan cara kehilangan kata sandi *(password loss)*, *sniffing* kata sandi, peretasan kata sandi *brute-force*, dan sejenisnya. Risiko ini dapat dimitigasi dengan terus-menerus mengubah kata sandi, sebagaimana yang dilakukan OTP. Oleh karena itu, OTP digunakan untuk mengamankan transaksi keuangan elektronik seperti perbankan daring.

3. *Firewall* - *Firewall* mengatur aliran lalu lintas antara jaringan komputer dengan tingkat

kepercayaan berbeda seperti antara internet, yang merupakan zona tanpa kepercayaan, dan jaringan internal, yang merupakan zona dengan tingkat kepercayaan yang lebih tinggi. Zona dengan tingkat kepercayaan menengah, terletak di antara internet dan jaringan internal tepercaya, sering disebut sebagai jaringan perimeter *(perimeter network)* atau zona demiliterisasi.

4. Alat analisis kerentanan - Karena peningkatan jumlah metode serangan dan kerentanan pada aplikasi yang umum digunakan, kerentanan sistem perlu dinilai secara berkala. Dalam keamanan komputer, kerentanan merupakan kelemahan yang memberikan celah bagi penyerang untuk menganggu atau merusak sebuah sistem. Kerentanan dapat disebabkan oleh sandi yang lemah, kekutu *(software bugs)*, virus komputer, injeksi kode skrip, injeksi SQL, atau *malware*. Alat analisis kerentanan dapat mendeteksi kerentanan yang ada. Alat tersebut bisa dengan mudah didapat secara daring dan juga terdapat beberapa perusahaan yang menyediakan layanan analitik. Namun, yang tersedia secara gratis untuk komunitas internet dapat disalahgunakan oleh penyusup. Untuk informasi lebih lanjut, kunjungi:

   - Riset Kerentanan Secunia (https://www.flexera.com/products/operations/software-vulnerability-research/secunia-research/advisories.html)
   - Arsip Kerentanan SecurityFocus (http://www.securityfocus.com/bid)
   - 100 *Tools* Keamanan Jaringan Teratas (http://sectools.org)

   Alat penganalisis kerentanan jaringan yang menganalisis kerentanan sumber daya jaringan seperti *router*, *firewall*, dan server.

   Alat analisis kerentanan server yang menganalisis berbagai kerentanan seperti sandi lemah, konfigurasi lemah, dan kesalahan izin file *(file permission error)* dalam sistem internal. Alat analisis kerentanan server memberikan hasil yang relatif lebih akurat daripada alat analisis kerentanan jaringan karena alat ini menganalisis lebih banyak kerentanan dalam sistem internal.

   Alat analisis kerentanan web menganalisis kerentanan aplikasi Web seperti XSS dan injeksi SQL melalui web. Untuk informasi lebih lanjut, kunjungi Proyek Keamanan Aplikasi Web Terbuka pada alamat https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.

5. Alat Celah Udara *(Air Gap Tool)* - *air gap, air wall,* atau *air gapping* merupakan langkah keamanan jaringan yang digunakan pada satu atau komputer atau lebih untuk memastikan bahwa jaringan komputer yang aman terisolasi secara fisik dari jaringan yang tidak aman, seperti internet publik atau jaringan area lokal (LAN) yang tidak aman. Selama bertahun-tahun, anjuran yang berlaku dari sebagian besar pakar keamanan siber adalah melakukan pendekatan keamanan dengan strategi pertahanan mendalam (perlindungan berlapis) daripada dengan strategi celah udara *(air gap)*.

6. Isolasi peramban *(browser isolation)* - Isolasi peramban merupakan model keamanan siber yang bertujuan untuk mengisolasi secara fisik aktivitas meramban pengguna internet (dan risiko siber terkait) dari jaringan dan infrastruktur lokal. Teknologi isolasi peramban mengambil pendekatan model ini dengan berbagai cara, tetapi semuanya berusaha

mencapai tujuan yang sama, yaitu isolasi peramban web dan aktivitas meramban pengguna yang efektif sebagai metode untuk mengamankan peramban web dari pemanfaatan keamanan berbasis peramban, serta ancaman *web-borne* seperti *ransomware* dan *malware* lainnya.

Teknologi Pendeteksian

Teknologi pendeteksian digunakan untuk mendeteksi dan melacak keadaan abnormal dan gangguan dalam jaringan atau sistem penting. Teknologi pendeteksian meliputi:

1. Antivirus – Perangkat lunak antivirus merupakan program komputer untuk mengidentifikasi, menghalangi, atau menghilangkan kode berbahaya, seperti *worm*, serangan *phishing*, *rootkit*, *trojan horse*, dan *malware* lainnya.[16]

2. Sistem deteksi gangguan (penyusupan) atau *intrusion detection system* (IDS) – IDS mengumpulkan dan menganalisis informasi dari berbagai area di dalam komputer atau jaringan untuk mengidentifikasi kemungkinan adanya pelanggaran keamanan. Fungsi deteksi gangguan meliputi analisis pola aktivitas abnormal dan kemampuan untuk mengenali pola serangan.

3. Sistem pencegahan gangguan atau *intrusion prevention system* (IPS) – Pencegahan intrusi berupaya mengidentifikasi potensi ancaman dan menanggulanginya sebelum digunakan dalam serangan. IPS memantau lalu lintas jaringan dan mengambil tindakan langsung terhadap potensi ancaman sesuai dengan seperangkat aturan yang ditetapkan oleh administrator jaringan. Misalnya, IPS mungkin memblokir lalu lintas alamat IP yang mencurigakan.[17]

4. Sistem *sandbox malware* – *Sandbox malware* merupakan sistem keamanan yang memisahkan eksekusi berbagai program, biasanya dalam rangka untuk mengurangi penyebaran *malware*. Ia sering digunakan untuk menjalankan program atau kode yang belum teruji atau tidak tepercaya–mungkin dari pihak ketiga yang belum terverifikasi atau tidak tepercaya, pemasok, pengguna atau situs web–dalam sebuah *sandbox* tanpa membahayakan mesin *host* atau sistem operasi. *Sandbox* umumnya mengendalikan program dengan ketat, dan membatasi akses program terhadap *disk*, memori, dan jaringan.

5. Analisis lalu lintas jaringan atau *network traffic analysis* (NTA) – Analisis lalu lintas jaringan merupakan aktivitas pertahanan siber yang aktif. NTA merupakan “proses pencarian secara iteratif dan proaktif melalui jaringan untuk mendeteksi dan mengisolasi ancaman tingkat lanjut yang berhasil berpaling dari solusi keamanan yang ada”[18]. Hal ini berbeda

---

[16] Wikimedia Foundation. (1 Februari 2021). *Antivirus software*. Diakses dari Wikipedia. http://en.wikipedia.org/wiki/Antivirus_software.

[17] Gillis, A. S. (12 Februari 2020). *What is an Intrusion Prevention System (IPS)?* SearchSecurity. Diakses dari https://searchsecurity.techtarget.com/definition/intrusion-prevention.

[18] Egede, I. (31 Juli 2018). Threat Hunting for File Hashes as an IOC. Infosec Resources. https://resources.infosecinstitute.com/topic/threat-hunting-for-file-hashes-as-an-ioc.

dengan langkah manajemen ancaman tradisional, seperti *firewall*, sistem pencegahan intrusi (IDS) dan sistem *sandbox malware*, biasanya memerlukan penyelidikan data berbasis bukti setelah muncul peringatan terkait potensi ancaman.

Teknologi Integrasi

Teknologi integrasi mengintegrasikan berbagai fungsi penting untuk keamanan informasi aset inti *(core assets)*, seperti memprediksi, mendeteksi, dan melacak gangguan. Teknologi integrasi antara lain:

1. Manajemen keamanan perusahaan atau *enterprise security management* (ESM) – Sistem ESM mengelola, mengontrol, dan mengoperasikan solusi keamanan informasi seperti IDS dan IPS berdasarkan kebijakan yang konsisten. ESM digunakan sebagai strategi untuk mengatasi kelemahan berbagai solusi lainnya dengan memanfaatkan keunggulan masing-masing solusi keamanan informasi dan memaksimalkan efisiensi keamanan informasi di bawah kebijakan yang konsisten.

   ESM yang dapat mengelola teknologi keamanan secara sintetis baru muncul belakangan ini karena kurangnya sumber daya manusia yang dapat mengoperasikan teknologi keamanan, meningkatnya serangan mutakhir seperti konvergensi metode serangan, dan munculnya alat serangan yang sulit terdeteksi. Dengan ESM, efisiensi manajemen meningkat dan langkah penanggulangan aktif terbentuk.

2. Manajemen risiko perusahaan atau *enterprise risk management* (ERM) – ERM merupakan sistem yang dapat memprediksi seluruh risiko yang berhubungan dengan organisasi, termasuk area di luar keamanan informasi, dan secara otomatis mengonfigurasi langkah pencegahan. Penggunaan ERM untuk melindungi informasi memerlukan penetapan tujuan manajemen risiko dan desain pengembangan sistem yang tepat. Sebagian besar organisasi membangun dan mengoptimalkan ERM mereka melalui lembaga konsultasi keamanan informasi profesional daripada melakukannya sendiri.

Pertanyaan:

1. Ancaman keamanan informasi apakah yang rentan bagi organisasi Anda? Mengapa?

2. Solusi teknologi keamanan informasi apakah yang tersedia di organisasi Anda?

3. Apakah organisasi Anda memiliki kebijakan, strategi, dan pedoman keamanan informasi? Jika ya, seberapa memadai hal tersebut mengingat ancaman yang rentan terhadap organisasi Anda? Jika tidak, kebijakan, strategi, dan pedoman keamanan informasi apakah yang akan Anda rekomendasikan untuk organisasi Anda?

Uji Kompetensi:

1. Mengapa penting melakukan analisis tren ancaman keamanan informasi?

2. Mengapa manajemen sumber daya manusia merupakan faktor terpenting dalam operasi keamanan informasi? Apa aktivitas utama dalam manajemen sumber daya manusia untuk keamanan informasi?

3. Jelaskan model keamanan teknologi *Defense-In-Depth* (DID). Bagaimana cara kerjanya?

3. Aktivitas Keamanan Informasi

Bab ini bertujuan untuk:

- Memberikan contoh aktivitas keamanan informasi dari berbagai negara untuk dijadikan pedoman dalam penyusunan kebijakan keamanan informasi; dan
- Menyoroti kerja sama internasional dalam menerapkan kebijakan keamanan informasi

3.1. Pengembangan Strategi Keamanan Informasi Nasional

Strategi Keamanan Informasi

Kebutuhan Strategi Keamanan Informasi Nasional (NISS) ditentukan oleh kompleksitas jaringan komputer yang saling terhubung saat ini. Instansi pemerintah harus bertanggung jawab atas keamanan sistem Teknologi Informasi dan Komunikasi (TIK) miliknya. Faktanya, lembaga nasional juga semakin bergantung pada sistem TIK pihak ketiga yang dioperasikan oleh entitas komersial yang mungkin berada di luar batas negara mereka.

Meskipun sebagian besar negara menyadari pentingnya penyelarasan keamanan informasi yang lebih baik, masih banyak yang berjuang menerjemahkan kesadaran ini ke dalam rencana aksi konkret.

Menyatakan visi dalam pengembangan NISS telah menjadi hal lumrah. Beberapa tujuan umumnya antara lain:

- Lingkungan Infrastruktur TIK Nasional yang Aman, Andal dan Tangguh
- Petugas Keamanan Siber yang Sangat Terampil
- Program Pelatihan dan Kesadaran Keamanan Siber Nasional
- Pemberlakuan Peraturan Perundang-Undangan Nasional untuk Menangani Kejahatan Siber
- Kerja Sama Keamanan Nasional dan Internasional

Dalam strategi NISS yang lebih maju, juga terdapat beberapa tujuan sebagai berikut:

- Program Analisis dan Penanganan Ancaman Siber Nasional
- Program Kepatuhan dan Pelacakan Keamanan Siber Nasional
- Program Penelitian, Inovasi, dan Kewirausahaan Keamanan Siber Nasional

Dalam pengembangan NISS, mengadopsi standar atau kode praktik internasional juga menjadi hal lumrah.

Contoh standar teknis seperti ISO 27001 dan UN/EDIFACT (United Nations/Electronic Data Interchange for Administration, Commerce and Transport).

Contoh Kode Etik seperti Majelis Eropa (Council of Europe) dan Organisasi Kerja Sama dan Pembangunan Ekonomi (OECD).

Contoh Praktik dan Kebutuhan Industri seperti Forum Keamanan Eropa (ESF), Institut Standar dan Teknologi Nasional (NIST), serta Departemen Perdagangan dan Industri (DTI) Kerajaan Serikat.

3.2. Contoh Strategi Keamanan Informasi Nasional

Strategi Keamanan Informasi Amerika Serikat

Pasca serangan teroris pada 11 September 2001 (9/11), Pemerintah Amerika Serikat membentuk Kementerian Keamanan Dalam Negeri untuk memperkuat keamanan nasional, bukan hanya terhadap ancaman fisik, melainkan juga terhadap ancaman siber.

Strategi keamanan informasi Amerika Serikat antara lain: Strategi Nasional untuk Keamanan Dalam Negeri, Strategi Nasional untuk Keamanan Fisik Infrastruktur dan Aset Kritis, serta Strategi Nasional untuk Pengamanan Ruang Siber (Dunia Maya).

Strategi Nasional untuk Pengamanan Ruang Siber[19] memiliki visi keamanan ruang siber serta perlindungan infrastruktur dan aset kritis (sangat penting). Strategi tersebut menetapkan tujuan dan aktivitas khusus untuk mencegah serangan siber terhadap infrastruktur dan aset kritis. Lima prioritas nasional yang yang ditetapkan dalam Strategi Nasional untuk Pengamanan Ruang Siber adalah:

- Sistem Penanganan Keamanan Ruang Siber Nasional
- Program Pengurangan Kerentanan dan Ancaman Keamanan Ruang Siber Nasional
- Program Pelatihan dan Kesadaran Keamanan Ruang Siber Nasional
- Mengamankan Ruang Siber Pemerintah
- Keamanan Nasional dan Kerja Sama Keamanan Ruang Siber Internasional

Strategi Siber Nasional[20] terbaru dirilis pada September 2018. Empat pilar utama yang ditetapkan adalah:

- Melindungi Rakyat Amerika, Tanah Air, dan Cara Hidup Rakyat Amerika
  - Mengamankan Jaringan dan Informasi Federal
  - Mengamankan Infrastruktur Kritis
  - Memerangi Kejahatan Siber dan Meningkatkan Pelaporan Kejadian
- Mendorong Kesejahteraan Rakyat Amerika
  - Memupuk Ekonomi Digital yang Hidup dan Tangguh

[19] The White House. (2003). (rep.). *The National Strategy to Secure Cyberspace*. Diakses dari https://www.hsdl.org/?view&did=1040

[20] The White House. (2018). (rep.). *National Cyber Strategy of the United States of America*. Diakses dari https://www.defense.gov/Explore/News/Article/Article/1641969/white-house-releases-first-national-cyber-strategy-in-15-years/

    - Membina dan Melindungi Kecerdasan Amerika Serikat
    - Mengembangkan Tenaga Kerja Keamanan Siber yang Unggul
- Menjaga Kedamaian melalui kekuatan atau kemampuan
    - Meningkatkan Stabilitas Siber melalui Norma Tindakan Negara yang Bertanggung Jawab
    - Menerapkan dan Mencegah Tindakan yang Tidak Diperbolehkan di Ruang Siber
- Meningkatkan Pengaruh Amerika
    - Mendorong Internet yang Terbuka, Dapat Dioperasikan, Andal, dan Aman
    - Membangun Kapasitas Siber Internasional

Memperketat Undang-Undang Keamanan Informasi

Undang-Undang Peningkatan Keamanan Siber 2014 (CSEA)[21] pertama kali diberlakukan pada tahun 2002 dan direvisi terakhir kali pada tahun 2014. Undang-undang (UU) ini berisi bab kedua dari Undang-Undang Keamanan Dalam Negeri. UU tersebut mengatur amandemen pedoman hukuman untuk hal-hal seperti kejahatan komputer tertentu, pengecualian penyingkapan darurat, pengecualian iktikad baik, larangan iklan internet ilegal dan perlindungan privasi. RUU tersebut juga menyediakan "kemitraan sukarela publik-swasta berkelanjutan untuk meningkatkan keamanan siber, dan untuk memperkuat penelitian dan pengembangan keamanan siber, pengembangan dan pendidikan tenaga kerja, kesadaran dan kesiapsiagaan publik, serta untuk tujuan lainnya."

Strategi Keamanan Informasi Kerajaan Serikat (UK)

Pemerintah Kerajaan Serikat merilis Strategi Keamanan Siber Nasional 2016-2021[22]. Visi tahun 2021 berbunyi bahwa Kerajaan Serikat aman dan kuat terhadap ancaman siber, serta sejahtera dan yakin dalam dunia digital.

Demi mewujudkan visi tersebut, ditetapkan tujuan sebagai berikut:
- Melindungi *(Defend)*
    - Kami memiliki sarana untuk melindungi Kerajaan Serikat dari ancaman siber yang berkembang, untuk menangani kejadian secara efektif dan untuk memastikan jaringan, data, dan sistem Kerajaan Serikat terlindungi dan tangguh.
- Menangkal *(Deter)*
    - Kerajaan Serikat dapat menjadi sasaran yang sulit bagi seluruh bentuk agresi di ruang siber. Kami mendeteksi, memahami, menyelidiki, dan menghancurkan tindakan agresif terhadap kami, serta mengejar dan mengamankan pelaku. Kami memiliki sarana untuk mengambil tindakan ofensif di ruang siber.

[21] U.S. Government Printing Office. (2014). *An Act to Provide for an Ongoing, Voluntary Public-Private Partnership to Improve Cybersecurity, and to Strengthen Cybersecurity Research and Development, Workforce Development and Education, and Public Awareness and Preparedness, and for Other Purposes*.

[22] HM Government. (2016). (rep.). *National Cyber Security Strategy 2016-2021*. Diakses dari https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

- Mengembangkan *(Develop)*
  - Kami memiliki industri keamanan siber yang inovatif dan berkembang, didukung oleh penelitian dan pengembangan ilmiah terkemuka di dunia. Kami memiliki saluran bakat mandiri yang menyediakan berbagai keahlian untuk memenuhi kebutuhan nasional kami di seluruh sektor publik dan swasta. Analisis dan keahlian mutakhir milik kami dapat membuat Kerajaan Serikat menemui dan mengatasi ancaman serta tantangan di masa mendatang.

Strategi Keamanan Informasi Uni Eropa

Saat ini, negara-negara di Uni Eropa memiliki Strategi Keamanan Siber Nasional atau *National Cybersecurity Strategy* (NCSS) sebagai fitur kebijakan utama. Strategi tersebut membantu mereka mengatasi risiko yang berpotensi merusak hasil manfaat ekonomi dan sosial dari ruang siber.

Dalam kertas kebijakan Komunikasi *(Communication)* tertanggal Mei 2006[23], Komisi Eropa menjelaskan strategi Uni Eropa untuk keamanan informasi saat ini yang terdiri dari sejumlah langkah yang saling bergantung dan melibatkan banyak pemangku kepentingan. Langkah-langkah tersebut di antaranya adalah pembentukan Kerangka Peraturan untuk Komunikasi Elektronik pada tahun 2002, penjelasan inisiatif i2010 untuk pembentukan Masyarakat Informasi Eropa, dan pembentukan Badan Keamanan Informasi dan Jaringan Eropa (ENISA) pada tahun 2004. Menurut kertas kebijakan tersebut, langkah-langkah ini mencerminkan pendekatan tiga cabang untuk masalah keamanan dalam Masyarakat Informasi yang meliputi langkah jaringan dan keamanan informasi (NIS) tertentu, kerangka peraturan untuk komunikasi elektronik (mencakup masalah privasi dan keamanan data), serta perang melawan kejahatan siber.

Dalam kertas Komunikasi tertanggal Desember 2006, Komisi Eropa merilis Program Eropa untuk Perlindungan Infrastruktur Kritis (EPCIP) untuk memitigasi kerentanan infrastruktur kritis (sangat penting). [24] Program ini merupakan sekumpulan langkah yang bertujuan untuk meningkatkan perlindungan infrastruktur kritis di Eropa, di seluruh Negara Uni Eropa dan di seluruh sektor kegiatan ekonomi yang relevan. Inisiatif Uni Eropa mengenai Perlindungan Infrastruktur Informasi Penting (CIIP) bertujuan untuk memperkuat keamanan dan ketahanan infrastruktur Teknologi Informasi dan Komunikasi (TIK) yang vital.

Kertas kebijakan Komunikasi mencatat berbagai serangan terhadap sistem informasi, penyebaran perangkat seluler yang meningkat, munculnya *ambient intelligence*, dan peningkatan tingkat kesadaran pengguna sebagai masalah keamanan utama yang ingin

[23] Commission of the European Communities, A strategy for a Secure Information Society – "Dialogue, partnership and empowerment" (2006). Brussels, Belgium. Diakses dari https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0251&qid=1612332935197&from=EN.

[24] Commission of the European Communities, A European Programme for Critical Infrastructure Protection (2006). Brussels, Belgium. Diakses dari https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF.

ditangani oleh Komisi Eropa melalui dialog, kemitraan, dan pemberdayaan. Strategi ini dijelaskan dalam kertas Komunikasi tersebut (lihat Kotak 2).

Kotak 2. Dialog Para Pemangku Kepentingan Komisi Eropa

Komisi Eropa mengusulkan serangkaian langkah yang dirancang untuk membangun dialog para pemangku kepentingan yang inklusif dan terbuka:

- Latihan penolokukuran *(benchmarking)* kebijakan nasional terkait jaringan dan keamanan informasi, untuk membantu mengidentifikasi praktik yang paling efektif sehingga dapat diterapkan secara lebih luas di seluruh Uni Eropa. Secara khusus, latihan ini akan memperkenalkan praktik terbaik untuk meningkatkan kesadaran usaha kecil dan menengah (UKM) dan masyarakat tentang risiko dan tantangan terkait keamanan jaringan dan informasi; serta
- Diskusi terstruktur para pemangku kepentingan mengenai cara terbaik untuk memanfaatkan instrumen peraturan yang ada. Diskusi ini akan diadakan dalam bentuk konferensi dan seminar.

Kemitraan

Penyusunan kebijakan yang efektif membutuhkan pemahaman yang jelas mengenai sifat tantangan yang akan ditangani, serta data ekonomi dan statistik yang andal dan mutakhir. Oleh karena itu, Komisi Eropa akan meminta Badan Keamanan Informasi dan Jaringan Eropa (ENISA) untuk:

- Membangun kemitraan kerja sama dengan negara-negara anggota dan para pemangku kepentingan untuk mengembangkan kerangka kerja yang tepat dalam rangka mengumpulkan data; serta
- Menguji kelayakan sistem peringatan dan berbagi informasi Eropa untuk mempermudah penanganan efektif terhadap ancaman. Sistem ini termasuk portal multibahasa Eropa yang berfungsi untuk menyediakan informasi sesuai ancaman, risiko, dan peringatan.

Secara paralel, Komisi Eropa akan mengundang negara-negara anggota, pihak swasta dan komunitas penelitian untuk membentuk kemitraan guna memastikan ketersediaan data terkait industri keamanan TIK.

Pada Maret 2009, Komisi Eropa memakai kertas kebijakan Komunikasi mengenai Perlindungan Infrastruktur Informasi Penting (CIIP) - "Melindungi Eropa dari serangan dan gangguan siber skala besar: meningkatkan kesiapan, keamanan, dan ketahanan".[25] CIIP menetapkan sebuah rencana (Rencana Aksi CIIP) untuk memperkuat keamanan dan

[25] Commission of the European Communities, *Critical Information Infrastructure Protection: "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"* (2009). Brussels, Belgium. Diakses dari https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52009DC0149&qid=1612333230526&from=EN.

ketahanan infrastruktur TIK yang vital. Tujuannya untuk merangsang dan mendukung pengembangan kemampuan kesiapsiagaan, keamanan, dan ketahanan tingkat tinggi, baik di tingkat nasional maupun Eropa. Pendekatan ini secara luas didukung oleh Dewan Eropa pada tahun 2009.[26] Rencana aksi CIIP dibangun berdasarkan lima pilar: (1) kesiapsiagaan dan pencegahan; (2) deteksi dan penanganan; (3) mitigasi dan pemulihan; (4) kerja sama internasional; serta (5) kriteria infrastruktur kritis Eropa di bidang TIK. Rencana aksi CIIP menentukan hal-hal yang harus dilakukan di bawah setiap pilar tersebut oleh Komisi Eropa, Negara-negara anggota dan/atau industri, dengan dukungan ENISA.

Agenda Digital Eropa (DAE)[27] diadopsi pada Mei 2010, dan Kesimpulan Dewan *(Council Conclusions)*[28] yang berkaitan menyoroti pemahaman bersama bahwa kepercayaan dan keamanan merupakan prasyarat mendasar untuk penggunaan TIK yang luas dan oleh karenanya dibutuhkan pula untuk mencapai tujuan dimensi pertumbuhan cerdas Strategi Eropa 2020.[29] DAE menekankan perlunya seluruh pemangku kepentingan untuk bekerja sama dalam upaya holistik untuk memastikan keamanan dan ketahanan infrastruktur TIK. Untuk mencapai hal ini, DAE menekankan pentingnya untuk fokus pada pencegahan, kesiapsiagaan dan kesadaran, serta mengembangkan mekanisme yang efektif dan terkoordinasi untuk menangani bentuk serangan dan kejahatan siber baru yang semakin canggih. Pendekatan ini menjamin bahwa baik dimensi preventif dan reaktif dari tantangan tersebut benar-benar diperhitungkan.

Langkah-langkah yang telah diambil sebagaimana dalam Agenda Digital adalah sebagai berikut:

- Komisi Eropa menyetujui proposal *pengarahan serangan terhadap sistem informasi*[30] pada September 2010. Proposal ini bertujuan untuk memperkuat perang melawan kejahatan siber dengan memperkirakan sistem hukum pidana negara anggota dan meningkatkan kerja sama antara otoritas peradilan dan otoritas penting lainnya. Proposal tersebut juga menjelaskan ketentuan untuk menangani bentuk serangan siber baru, khususnya botnet.

[26] Council of the European Union, *Council Resolution of 18 December 2009 on a collaborative European approach to Network and Information Security* (2009). Belgium, Brussels. Diakses dari https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:321:0001:0004:EN:PDF.

[27] European Commission, *A Digital Agenda for Europe* (2010). Brussels, Belgium. Diakses dari https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0245&qid=1612333676302&from=EN.

[28] Council of the European Union, *Council Conclusions on the Digital Agenda for Europe* (2010). Brussels, Belgium. Diakses dari https://data.consilium.europa.eu/doc/document/ST-10130-2010-INIT/en/pdf.

[29] European Council, *Conclusions of the European Council* (25/26 Maret 2010) (2010). Brussels, Belgium. Diakses dari https://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/en/ec/113591.pdf.

[30] European Commission, *Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision* (2010). Brussels, Belgium. Diakses dari https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010PC0517&qid=1612334410667&from=EN.

- Selain itu, Komisi Eropa pada saat yang sama mengajukan proposal[31] untuk mandat baru memperkuat dan memodernisasi ENISA dalam rangka meningkatkan penjagaan dan keamanan jaringan. Memperkuat dan memodernisasi ENISA akan membantu Uni Eropa, negara anggota, dan para pemangku kepentingan swasta mengembangkan kemampuan dan kesiapan mereka untuk mencegah, mendeteksi, dan menangani tantangan keamanan siber.

Konvensi Dewan Eropa tentang Kejahatan Siber

Pada tahun 2001, Uni Eropa mengumumkan Konvensi Dewan Eropa tentang Kejahatan Siber (CECC) yang "menetapkan pedoman bagi semua pemerintahan yang ingin mengembangkan undang-undang terhadap kejahatan siber" dan "menyediakan kerangka kerja sama internasional di bidang ini." 39 negara Eropa menandatangani perjanjian tersebut, termasuk Kanada, Jepang, Afrika Selatan, dan Amerika Serikat. Hal ini membuat CECC, yang mulai berlaku pada Juli 2004, menjadi "satu-satunya perjanjian internasional yang mengikat terkait persoalan tersebut dan telah diberlakukan hingga saat ini." [32]

Badan Keamanan Jaringan dan Informasi Eropa (ENISA)

ENISA didirikan oleh Parlemen Eropa dan Dewan Uni Eropa pada 10 Maret 2004 "untuk membantu meningkatkan keamanan jaringan dan informasi dalam Komunitas (Uni Eropa) dan untuk mendorong lahirnya budaya jaringan dan keamanan informasi untuk kepentingan masyarakat, konsumen, bisnis dan organisasi sektor publik." [33]

Visi *Permanent Stakeholder Group* (PSG) untuk ENISA [34] yang tercetus pada Mei 2006 menjadikan ENISA sebagai pusat keamanan jaringan dan informasi yang unggul, sebuah forum bagi pemangku kepentingan NIS, dan pendorong kesadaran keamanan informasi untuk semua warga Uni Eropa. Untuk tujuan tersebut, aksi jangka panjang ENISA berikut ini ditetapkan dalam Visi PSG (lihat Gambar 6):

---

[31] European Commission, *Proposal for A Regulation Of The European Parliament And Of The Council Concerning The European Network And Information Security Agency* (ENISA) (2010). Brussels, Belgium. Diakses dari https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010PC0521&qid=1612334562226&from=EN.

[32] *Council of Europe action against Cybercrime*. Council of Europe. Diakses dari https://www.coe.int/en/web/portal/coe-action-against-cybercrime.

[33] European Commission, *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration* (2010). Brussels, Belgium. Diakses dari https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010PC0520&qid=1612335155929&from=EN.

[34]*Permanent Stakeholders' Group*. (P. Dorey & S. Perry, Eds.), *The PSG Vision for ENISA* (2006). Diakses dari https://www.enisa.europa. eu/about-enisa/structure-organization/psg/files/psg-vision.

.

Gambar 6. Aksi Jangka Panjang ENISA

Sumber: *Permanent Stakeholders' Group*. (P. Dorey & S. Perry, Eds.), Visi PSG untuk ENISA (2006). Diakses dari https://www.enisa.europa. eu/about-enisa/structure-organization/psg/files/psg-vision.

1. **Bekerja sama dan mengoordinasikan jaringan nasional negara anggota dan otoritas keamanan informasi**

Kerja sama antar lembaga nasional saat ini sangat rendah. Banyak hal baik yang dapat dilakukan dengan meningkatkan komunikasi dan kerja sama antar lembaga nasional, terutama dalam berbagi praktik terbaik dari lembaga-lembaga maju kepada mereka yang masih baru saja memulai.

2. **Bekerja sama dengan berbagai lembaga penelitian**

Tujuan ENISA harus mengarahkan penelitian dasar dan pengembangan teknis yang ditargetkan agar fokus pada area-area paling bermanfaat untuk mengelola risiko keamanan aktual dalam sistem di dunia nyata. ENISA tidak perlu melakukan agenda penelitiannya sendiri, melainkan cukup melakukan penyelarasan proses dan prioritas dari program saat ini.

3. **Bekerja sama dengan vendor perangkat keras dan perangkat lunak**

Vendor perangkat keras dan perangkat lunak menurut definisi adalah pesaing dan mungkin sulit bagi mereka untuk menyetujui praktik bersama secara terbuka. ENISA dapat memberikan opini yang tidak bias dan menyediakan forum untuk pembahasan sensitif, di samping juga menjaga situasi yang sehat terhadap sikap anti persaingan.

Visi jangka panjang ENISA harus lebih fokus kepada pembuatan jaringan dan teknologi informasi andal yang tahan terhadap *worm* dan masalah lainnya, daripada sekadar mengembangkan tren keamanan hingga saat ini. Hal ini dapat dicapai dengan dukungan teknik untuk mengembangkan arsitektur dan perangkat lunak yang tepat, aman, dan andal.

4. Ikut serta dalam badan pengaturan standar

Dengan tujuan untuk mengidentifikasi dan mempublikasikan inisiatif nilai terbesar, ENISA harus melacak dan memantau topik terkait NIS dalam badan pengaturan standar, termasuk menindaklanjuti tugas dari berbagai badan akreditasi dan sertifikasi keamanan yang ada.

5. Ikut serta dalam proses legislatif melalui lobi dan opini

ENISA harus berusaha mendapatkan posisi sebagai badan konsultan tepercaya agar didengar pada awal proses penyusunan dan pengajuan arahan serta undang-undang lainnya dalam berbagai hal terkait NIS.

6. Memanfaatkan organisasi pengguna *(user organizations)*

Seringkali organisasi pengguna tidak terjelaskan dengan baik dalam badan legislatif dan pengaturan standar seperti halnya vendor. ENISA dapat memberikan wawasan kepada kelompok pengguna akhir *(end user)* mengenai pekerjaan standar dan kesempatan untuk menguasai pekerjaan tersebut.

7. Mengidentifikasi dan mempromosikan praktik terbaik negara anggota untuk industri pengguna akhir

ENISA seharusnya tidak hanya melindungi kepentingan bisnis, melainkan juga meningkatkan kepercayaan pengguna akhir dalam penggunaan internet dan media digital.

8. Mengupayakan solusi teknis dan politis untuk manajemen identitas

Kurangnya kepercayaan pada internet merupakan hambatan utama bagi bisnis elektronik *(e-business)* berorientasi konsumen skala besar. Mampu memeriksa identitas pemilik situs, alamat surel, atau beberapa layanan daring secara akurat merupakan suatu langkah besar dalam rangka memperbarui dan meningkatkan kepercayaan pengguna umum di internet. Solusi teknis di bidang ini harus dicari melalui proses yang dipimpin industri, selain ENISA dapat mengupayakan kebijakan di seluruh Uni Eropa untuk autentikasi entitas daring.

9. Menyeimbangkan upaya untuk masalah keamanan "informasi" dan "jaringan"

ENISA harus berkomunikasi dengan penyedia layanan internet dan jaringan (ISP/NSP) terbesar agar dapat membantu mereka mengidentifikasi praktik terbaik untuk kepentingan bisnis dan konsumen di seluruh Eropa. Hal ini penting karena ISP/NSP dapat berperan penting dalam meningkatkan keamanan internet secara luas. Kerja sama dan koordinasi yang memadai untuk langkah-langkah yang diambil ISP saat ini masih terbilang kurang.

Sumber: Abridged dari
Permanent Stakeholders' Group. (P. Dorey & S. Perry, Eds.), Visi PSG untuk ENISA (2006). DIakses dari https://www.enisa.europa. eu/about-enisa/structure-organization/psg/files/psg-vision.

ENISA merupakan badan keahlian yang dibentuk oleh Uni Eropa untuk melaksanakan tugas teknis dan ilmiah yang sangat spesifik di bidang keamanan informasi, sering disebut "Badan Komunitas Eropa". Badan ini juga membantu Komisi Eropa dalam langkah-langkah persiapan teknis untuk memperbarui dan mengembangkan undang-undang Komunitas di bidang NIS.

Tugas utama ENISA fokus kepada:

- Memberi nasihat dan membantu Komisi dan negara-negara anggota mengenai keamanan informasi dan pembahasan dengan industri untuk mengatasi masalah terkait dengan keamanan dalam produk perangkat keras dan perangkat lunak;
- Mengumpulkan dan menganalisis data mengnai insiden keamanan di Eropa dan risiko yang muncul;
- Mendorong penilaian risiko dan metode manajemen risiko untuk meningkatkan kemampuan menghadapi ancaman keamanan informasi; serta
- Peningkatan kesadaran dan kerja sama antar berbagai pelaku (actor) di bidang keamanan informasi, terutama dengan mengembangkan kemitraan publik-swasta dengan industri di bidang tersebut.

Strategi Keamanan Informasi Republik Korea

Pemerintah Korea menetapkan strategi komprehensif bernama “Strategi Dasar untuk Keamanan Informasi Di Mana pun” atau *Basic Strategy for Ubiquitous Information Security* pada Desember 2006. Tujuan utama strategi ini adalah untuk memastikan bahwa orang Korea dapat menggunakan layanan TIK dengan aman di semua bidang, termasuk layanan keuangan, pendidikan dan medis, privasi pribadi dilindungi, serta lingkungan penggunaan informasi yang baik diterapkan. Strategi Dasar untuk Keamanan Informasi Di Mana pun memperluas konsep perlindungan informasi yang mencakup *u-Security, u-Privacy, u-Trust,* dan *u-Clean*.

Pada pertengahan 1980-an, Republik Korea mengejar rencana informatisasi nasional. Akan tetapi, keamanan informasi sebagai tujuan nasional menjadi fokus baru yang dimulai pada pertengahan tahun 2000. Penelitian pada saat itu menyatakan bahwa sistem TIK/skala keuangan, infrastruktur yang relevan serta upaya penelitian dan pengembangan semuanya sangat lemah. Dengan demikian, pemerintah Korea memutuskan untuk membangun infrastruktur utama TIK secara bertahap melalui pencapaian rencana yang komprehensif. Pada bulan Juli 2008, pemerintah merilis Rencana Komprehensif Jangka Menengah untuk Keamanan Informasi. Rencana ini berisi enam agenda sebagai berikut:

1. Meningkatkan kemampuan negara dalam menangani serangan siber
2. Memperkuat perlindungan infrastruktur informasi kritis nasional
3. Memperkuat sistem perlindungan informasi pribadi
4. Mengembangkan infrastruktur keamanan informasi
5. Meningkatkan daya saing industri keamanan informasi
6. Membangun budaya keamanan informasi

Pada bulan April 2019, Biro Keamanan Nasional (National Security Office) menerbitkan Strategi Keamanan Siber Nasional yang menetapkan enam tugas strategis yang dipecah menjadi 18 tugas utama dan 73 tugas terperinci. Di bawah rencana tersebut, pemerintah

menjabarkan tujuannya untuk membangun masyarakat yang aman dan dapat dipercaya di mana pun dengan memastikan keandalan layanan *e-government*, menghilangkan kecemasan masyarakat dan mencapai integritas dalam kegiatan bisnis.

Enam tugas strategis dan 18 tugas utama adalah sebagai berikut:

1. Meningkatkan Keamanan Infrastruktur Inti Nasional
    a. Memperkuat keamanan jaringan informasi dan komunikasi nasional
    b. Meningkatkan lingkungan keamanan siber untuk infrastruktur kritis
    c. Mengembangkan infrastruktur keamanan siber generasi berikutnya

2. Meningkatkan Kemampuan Penanganan Serangan Siber
    a. Memastikan pencegahan serangan siber
    b. Memperkuat kesiapan menghadapi serangan siber secara masif
    c. Alat penanggulangan yang komprehensif dan aktif untuk serangan siber
    d. Meningkatkan kemampuan untuk menangani kejahatan siber

3. Membangun Tata Kelola Berdasarkan Kepercayaan dan Kerja Sama
    a. Memfasilitasi sistem kerja sama militer publik-swasta
    b. Membangun dan memfasilitasi sistem berbagi informasi nasional
    c. Memperkuat dasar hukum keamanan siber

4. Membangun Fondasi untuk Pertumbuhan Industri Keamanan Siber
    a. Mengembangkan investasi keamanan siber
    b. Memperkuat daya saing tenaga kerja dan teknologi keamanan siber
    c. Mendorong lingkungan pertumbuhan bagi perusahaan keamanan siber
    d. Menetapkan prinsip persaingan yang sehat di pasar keamanan siber

5. Memupuk Budaya Keamanan Siber
    a. Meningkatkan kesadaran keamanan siber dan memperkuat praktik keamanan siber
    b. Menyeimbangkan hak-hak fundamental dengan keamanan siber

6. Memimpin Kerja Sama Internasional dalam Keamanan Siber
    a. Memperkaya sistem kerja sama bilateral dan multilateral
    b. Kepemimpinan yang kuat dalam kerja sama internasional

Pemerintah Republik Korea percaya bahwa Keamanan Siber membutuhkan partisipasi bukan hanya dari pemerintah saja, melainkan juga dari individu dan bisnis. Pemerintah akan memperkuat kerja sama dan membuka pintu untuk hal tersebut, serta meningkatkan transparansi kebijakan dengan tujuan akhir terus menerapkan kebijakan keamanan siber berdasarkan kepercayaan publik.

Strategi Keamanan Informasi Jepang[35]

Strategi keamanan siber Jepang yang berlaku saat ini muncul pada bulan Juli 2018. Kantor Pusat Strategis Keamanan Siber (Cybersecurity Strategic Headquarters) didirikan pada November 2014 bertujuan untuk mendorong kebijakan keamanan siber secara efektif dan komprehensif yang dipimpin oleh Kepala Sekretaris Kabinet. Pusat Keamanan Informasi Nasional atau National Information Security Center (NISC) yang dibentuk sejak tahun 2005 telah diubah menjadi Pusat Nasional untuk Kesiapan Insiden dan Strategi Keamanan Siber atau National Center for Incident readiness and Strategy for Cybersecurity (NISC) yang bertindak sebagai Sekretariat Kantor Pusat Strategis Keamanan Siber bekerja sama dengan sektor publik dan swasta pada berbagai kegiatan untuk menciptakan "ruang siber yang bebas, adil, dan aman". NISC merupakan organisasi utama yang mengawasi seluruh tugas terkait keamanan informasi di Jepang.

NISC mengambil peran sebagai CERT pemerintah serta NISC dan JPCERT/CC, sebagai CERT yang mencakup entitas swasta, bekerja sama sebagai CERT nasional. NISC terdiri dari tujuh gugus. Masing-masing diminta untuk menetapkan peran dan rencananya sendiri serta menjalankannya (lihat Tabel 4).

Tabel 4. Peran dan Gugus yang Bertanggung Jawab Berdasarkan Strategi Nasional Keamanan Siber

Peran	Gugus
Merumuskan rencana jangka menengah-panjang mengenai kebijakan keamanan siber dan melakukan penelitian serta analisis tren teknologi keamanan siber, dan lain-lain.	Perencanaan Strategi dan Kebijakan
Mendorong kerja sama internasional dalam kebijakan keamanan siber	Strategi Internasional
Merumuskan dan mengoperasikan standar terpadu untuk mendorong langkah-langkah keamanan informasi lembaga pemerintah yang merupakan dasar audit	Langkah Komprehensif bagi Instansi Pemerintah
Mengumpulkan informasi terkini mengenai serangan siber dan mengoperasikan tim Koordinasi Operasi Keamanan Pemerintah (GSOC)	Integrasi dan Koordinasi Informasi Keamanan Siber
Membentuk kemitraan publik-swasta terkait langkah-langkah keamanan siber berdasarkan Kebijakan Keamanan Siber untuk Perlindungan Infrastruktur Kritis	Perlindungan Infrastruktur Kritis

[35] *Commitment to a Free,Fair and Secure Cyberspace.* NISC. (2018). Diakses dari https://www.nisc.go.jp/eng/.

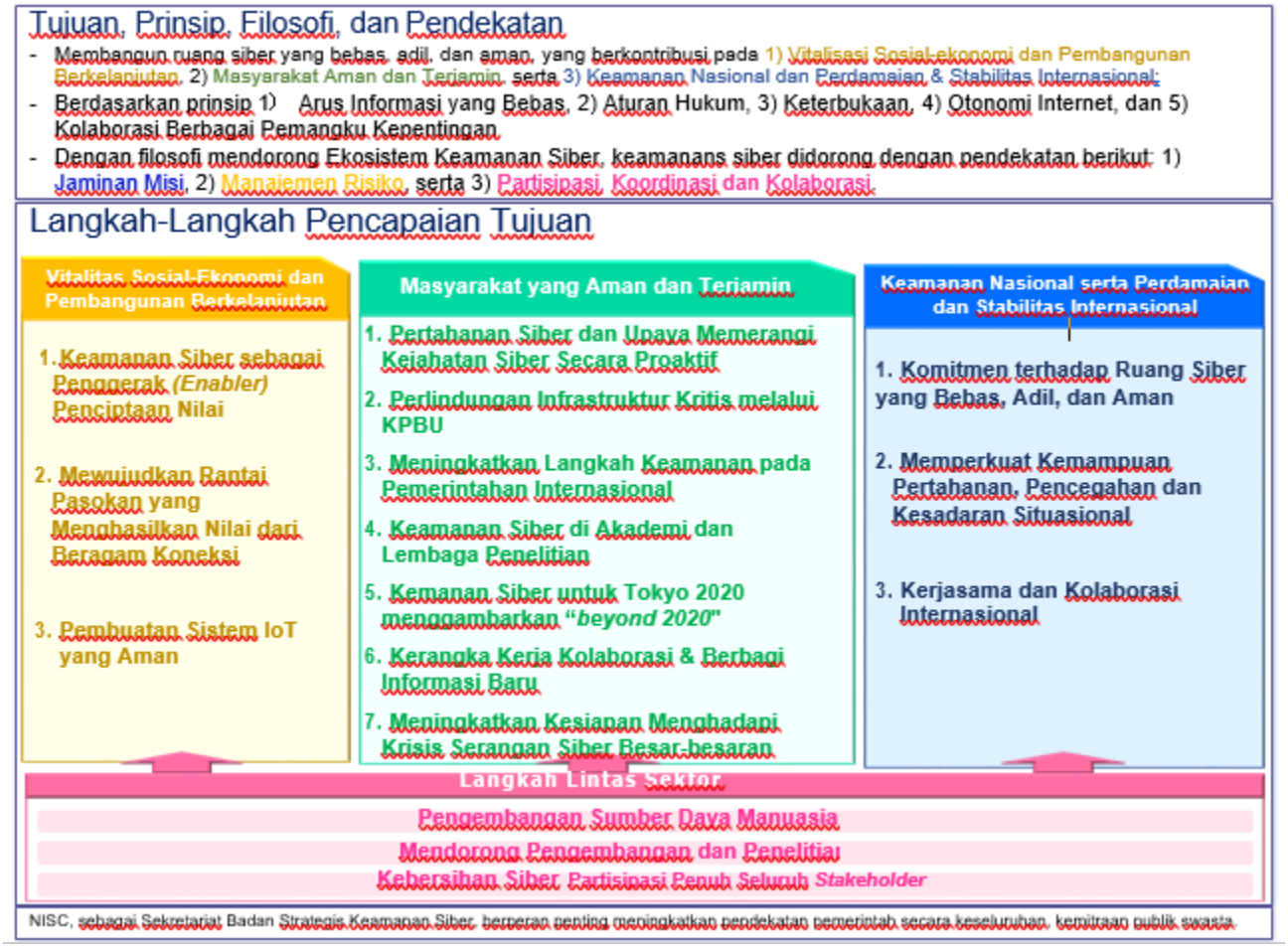
Menganalisis surel dan *malware* sasaran serta investigasi kasus serangan siber lainnya	Analisis dan Investigasi Insiden
Mendorong langkah-langkah keamanan siber untuk Olimpiade Tokyo dan Paralimpiade 2020	Tokyo 2020

Diambil (dengan modifikasi) dari: NISC, http://www.nisc.go.jp/eng/.

Strategi Keamanan Siber yang berlaku saat ini dan muncul pada Juli 2018 merupakan yang kedua berdasarkan Undang-Undang Dasar tentang Keamanan Siber. Undang-Undang Dasar tentang Keamanan Siber telah diterapkan sejak 2015 untuk mendorong kebijakan keamanan siber dengan cara:

- Menetapkan prinsip dasar kebijakan keamanan siber;
- Memperjelas tanggung jawab pemerintah, pihak swasta, dan masyarakat; serta
- Menetapkan kerangka kebijakan keamanan siber seperti perumusan strategi keamanan siber dan pembentukan Kantor Pusat Strategis Keamanan Siber.

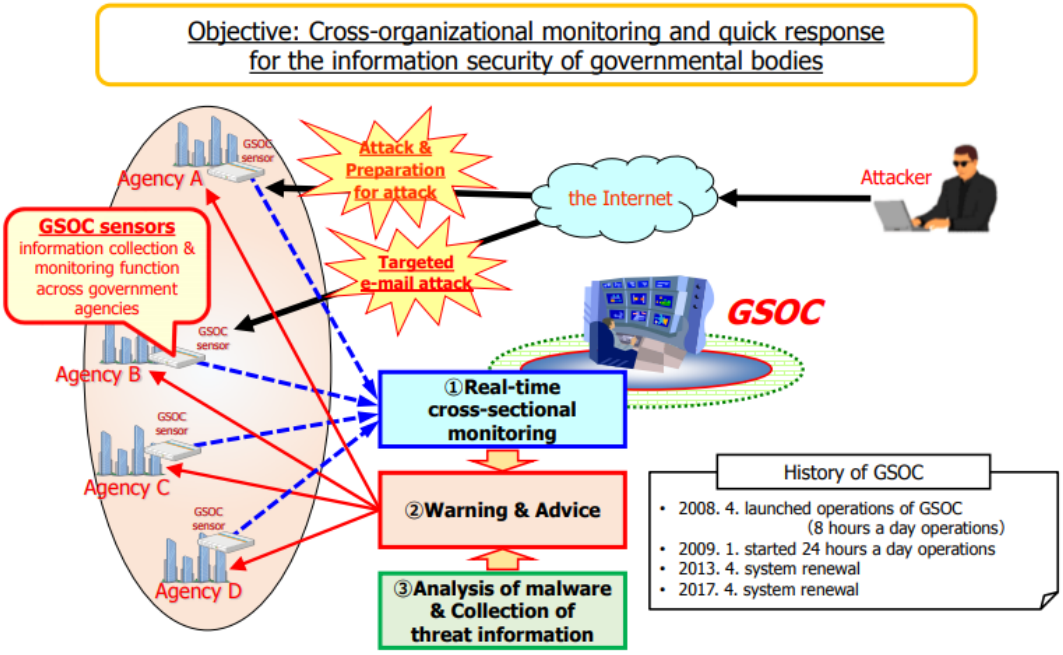
Tinjauan tentang Strategi Keamanan Siber saat ini adalah sebagai berikut (lihat Gambar 7 untuk garis besar strategi).



Gambar 7. Garis Besar Strategi Keamanan Siber Nasional

Jejaring Pemerintahan

NISC mengoperasikan tim pemantauan di seluruh pemerintahan secara *real time* yang disebut dengan tim Koordinasi Operasi Keamanan Pemerintah (GSOC). GSOC tidak hanya memantau komunikasi berbahaya yang masuk atau keluar dari sistem milik pemerintah, melainkan juga berfungsi sebagai kerangka kerja berbagi informasi antar entitas pemerintahan. GSOC memberikan peringatan dan saran pada entitas pemerintahan saat mereka mendeteksi sinyal yang mencurigakan atau *malware*.



Gambar 8. Tim Koordinasi Operasi Keamanan Pemerintah (GSOC)

Infrastruktur Kritis

Sejak tahun 2005, Kebijakan Keamanan Siber untuk Perlindungan Infrastruktur Kritis telah ditetapkan sebagai rencana aksi bersama oleh pemerintah yang memikul tanggung jawab untuk perlindungan infrastruktur kritis serta melakukan langkah-langkah perlindungan yang relevan secara independen oleh operator infrastruktur kritis. Edisi ke-4 dari dokumen kebijakan tersebut diterbitkan pada tahun 2017.

Dokumen tersebut mengidentifikasi 14 sektor sebagai infrastruktur kritis dan mengharapkan para pemangku kepentingan untuk melakukan lima langkah sebagaimana berikut.

- Pengembangan dan penetrasi prinsip keselamatan,
- Peningkatan sistem berbagi informasi,
- Penguatan kapasitas penanganan insiden,
- Manajemen risiko dan persiapan kesiagaan insiden, serta
- Membangun basis perlindungan infrastruktur kritis.

Pertanyaan:

1. Sejauh mana perbedaan aktivitas keamanan informasi di negara Anda dengan keadaan yang telah dijelaskan di atas?

2. Apakah terdapat aktivitas keamanan informasi yang sedang dijalankan di negara-negara yang telah disebutkan pada bab ini, tetapi tidak berlaku atau relevan dengan negara Anda? Jika ya, aktivitas keamanan informasi yang manakah dan apa alasannya?

3.3. Aktivitas Keamanan Informasi Internasional

Aktivitas Keamanan Informasi Perserikatan Bangsa-Bangsa

Pada **Konferensi Tingkat Tinggi (KTT) Dunia mengenai Masyarakat Informasi (WSIS)**[36] yang disponsori PBB, telah dilakukan sebuah deklarasi prinsip dan rencana aksi untuk pertumbuhan masyarakat informasi yang efektif dan penutupan "kesenjangan informasi". Rencana aksi menyatakan berbagai aksi berikut:

- Peran pemerintah dan seluruh pemangku kepentingan dalam mendukung TIK untuk pembangunan
- Infrastruktur informasi dan komunikasi sebagai landasan utama bagi masyarakat informasi yang inklusif
- Akses terhadap informasi dan pengetahuan
- Pengembangan kapasitas
- Membangun kepercayaan dan keamanan dalam penggunaan TIK
- Menciptakan lingkungan yang mendukung
- Penerapan TIK di semua aspek kehidupan
- Keragaman budaya dan identitas, keanekaragaman Bahasa, serta muatan lokal
- Media
- Dimensi etika dalam Masyarakat Informasi
- Kerja sama internasional dan regional[37]

Forum Tata Kelola Internet atau Internet Governance Forum (IGF) [38] merupakan organisasi pendukung Perserikatan Bangsa-Bangsa untuk masalah Tata Kelola Internet. IGF didirikan setelah fase kedua WSIS di Tunisia untuk menetapkan dan mengatasi masalah terkait tata kelola internet. Forum IGF kedua, yang diadakan di Rio de Janeiro pada 12-15 November 2007,

[36] International Telecommunications Union. (2006). *World Summit on the Information Society: About WSIS*. Diakses dari http://www.itu.int/wsis/basic/about.html.

[37] WSIS, WSIS: Plan of Action (2003). International Telecommunications Union. Diakses dari https://www.itu.int/net/wsis/docs/geneva/official/poa.html.

[38] Internet Governance Forum. (2021). Diakses dari http://www.intgovforum.org/.

berfokus pada isu-isu keamanan informasi seperti terorisme siber, kejahatan siber, dan keamanan anak-anak di internet.

Aktivitas Keamanan Informasi OECD[39]

Organisasi untuk Kerja Sama dan Pembangunan Ekonomi (OECD) merupakan forum khusus tempat pemerintah dari 30 negara demokrasi pasar bekerja sama dengan bisnis dan masyarakat sipil untuk mengatasi tantangan ekonomi, sosial, lingkungan, dan tata kelola yang dihadapi ekonomi dunia secara global. Dalam OECD, Kelompok Kerja terkait Privasi dan Keamanan Informasi (WPISP) bekerja di bawah naungan Komite Kebijakan Informasi, Komputer dan Komunikasi untuk memberikan analisis dampak TIK pada privasi dan keamanan informasi, serta untuk menghasilkan rekomendasi kebijakan melalui konsensus demi mempertahankan kepercayaan terhadap ekonomi internet.

Tugas WPISP terkait keamanan informasi: Pada tahun 2002, OECD mengeluarkan "Pedoman Keamanan Sistem dan Jaringan Informasi: Menuju Budaya Keamanan"[40] untuk mendorong "keamanan dalam pengembangan sistem dan jaringan informasi serta adopsi cara berpikir dan berperilaku baru saat menggunakan dan berinteraksi dalam sistem dan jaringan informasi."[41]

Untuk berbagi pengalaman dan praktik terbaik dalam keamanan informasi, Forum Global terkait Keamanan Jaringan dan Sistem Informasi digelar pada tahun 2003 serta Lokakarya OECD-APEC terkait Keamanan Sistem dan Jaringan Informasi juga digelar pada tahun 2005.

Sebuah proyek untuk meneliti metode melawan botnet dari perspektif privasi dan keamanan informasi diajukan pada tahun 2010. Sebuah kelompok sukarelawan telah dibentuk untuk menindaklanjuti proyek tersebut. Kelompok sukarelawan tersebut terdiri dari perwakilan dari Australia, Kanada, Jerman, Jepang, Republik Korea, Belanda, Swedia, Turki, Kerajaan Serikat, Amerika Serikat, dan Uni Eropa, serta Komite OECD (termasuk Komite Penasihat Bisnis dan Industri, Komite Penasihat Masyarakat Informasi Masyarakat Sipil, serta Komite Penasihat Teknis Internet). Republik Korea akan ikut serta dalam proyek ini dan juga akan memberi dukungan finansial.

Tugas WPISP terkait privasi: "Pedoman mengenai Perlindungan Privasi dan Arus Lintas Batas Data Pribadi" yang diterbitkan pada tahun 1980 mencerminkan konsensus internasional terkait penanganan informasi pribadi di sektor publik dan swasta. “Privasi *Online*: Pedoman OECD terkait Praktik dan Kebijakan” yang diterbitkan pada tahun 2002 berfokus pada teknologi peningkatan privasi, kebijakan privasi *online*, penegakan dan ganti rugi, dan sejenisnya terkait *e-commerce*. Saat ini, WPISP sedang menjalankan Kerja Sama Penegakan Hukum Privasi.

---

[39] OECD. (Mei 2006). OECD Working Party on Information Security and Privacy WPISP. Paris. Diakses dari https://www.gpdp.it/documents/10160/10704/Working+Party+on+Information+Security+and+Privacy.pdf/586b9ff2-0ae8-4cb1-873a-2025fb6f5a15?version=1.1

[40] OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (2002). Paris, Perancis. Diakses dari https://www.oecd.org/digital/ieconomy/15582260.pdf.

[41] Ibid., hlm. 8.

Proyek pengembangan indikator privasi dan keamanan informasi untuk statistik yang komparatif dan andal di antara anggota OECD telah diusulkan pada tahun 2011. Republik Korea akan berkontribusi pada proyek ini melalui partisipasi aktif dan dukungan keuangan.

Tugas lain: Pada tahun 1998, OECD menerbitkan "Pedoman Kebijakan Kriptografi" dan menggelar Deklarasi Menteri Ottawa terkait Autentikasi Perdagangan Elektronik *(e-Commerce)*. "Survei Kerangka Kerja Hukum dan Kebijakan untuk Layanan Autentikasi Elektronik *(e-Authentication)* dan Tanda Tangan Elektronik *(e-Signatures)* di Negara-Negara Anggota OECD" dilakukan dari tahun 2002 hingga tahun 2003. Pada tahun 2005, "Penggunaan Autentikasi Lintas Batas di Negara-negara OECD" diumumkan.

Pada tahun 2004, "Teknologi Berbasis Biometrik" lahir, dan pada tahun 2005, satuan tugas spam dibentuk. Tugas lain yang sedang berjalan adalah seputar manajemen identitas digital, *malware*, identifikasi frekuensi radio (RFID), sensor dan jaringan, dan kerangka kerja umum untuk menerapkan privasi dan keamanan informasi.

Aktivitas Keamanan Informasi APEC[42]

Kerja Sama Ekonomi Asia Pasifik (APEC) mengikuti aktivitas keamanan informasi di kawasan Asia-Pasifik melalui Telecommunications and Information Working Group (TEL) yang terdiri dari tiga kelompok pengarah: Kelompok Pengarah Liberalisasi *(Liberalization Steering Group)*, Kelompok Pengarah Pengembangan TIK *(ICT Development Steering Group)*, serta Kelompok Pengarah Keamanan dan Kesejahteraan *(Security and Prosperity Steering Group)*.

Sejak Pertemuan Tingkat Menteri APEC Ke-6 terkait Industri Telekomunikasi dan Informasi yang diadakan di Lima, Peru pada bulan Juni 2005, Kelompok Pengarah Keamanan dan Kesejahteraan makin meningkatkan pembahasan mengenai keamanan siber dan kejahatan siber. Strategi Keamanan Siber APEC, yang di antaranya memperkuat kepercayaan konsumen dalam penggunaan *e-commerce*, berfungsi untuk menyatukan upaya berbagai ekonomi. Upaya ini termasuk memberlakukan dan menerapkan undang-undang tentang keamanan siber yang sejalan dengan Resolusi Majelis Umum Perserikatan Bangsa-Bangsa 55/63[43] dan Konvensi terkait Kejahatan Siber.[44] Proyek Pengembangan Kapasitas Penegakan dan Inisiatif Legislasi Kejahatan Siber TEL dapat membantu berbagai lembaga dalam implementasi undang-undang baru.

Anggota APEC juga bekerja sama untuk menerapkan CERT sebagai sistem pertahanan peringatan dini terhadap serangan siber. Republik Korea memberikan pelatihan kepada anggota negara berkembang, sementara pedoman untuk menetapkan dan mengoperasikan CERT juga telah dikembangkan.

---

[42] *Telecommunications and Information*. Asia-Pacific Economic Cooperation. (2020, April). Diakses dari https://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information.

[43] *"Combating the criminal misuse of information", which recognizes that one of the implications of technological advances is increased criminal activity in the virtual world.*

[44] *An Agreement undertaken in Budapest that aims to uphold the integrity of computer systems by considering as criminal acts any action that violates said integrity*. Diakses dari http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

Perlindungan UKM dan pengguna rumahan *(home user)* dari serangan siber dan virus dianggap sebagai prioritas dan sejumlah alat telah dikembangkan untuk tujuan tersebut. Informasi mengenai cara menggunakan internet dengan aman, serta masalah keamanan terkait teknologi nirkabel dan pertukaran surel yang aman selalu tersedia.

Mengurangi tindak pidana penyalahgunaan informasi melalui kegiatan berbagi informasi, pengembangan prosedur dan hukum bantuan timbal balik *(mutual assistance laws)*, serta langkah-langkah lain untuk melindungi bisnis dan masyarakat, akan terus menjadi prioritas APECTEL. Sebagai bagian dari agendanya terkait masalah keamanan, APECTEL menyetujui *Pedoman Kebijakan dan Pendekatan Teknis terhadap Botnet* serta Lokakarya tentang Keamanan Siber dan Infrastruktur Informasi Kritis pada tahun 2007.

Sebagaimana didukung oleh Satgas Penanggulangan Terorisme atau APEC Counter-Terrorism Task Force (CTTF) dan APECTEL pada tahun 2009, *Seminar APEC Ke-3 tentang Perlindungan Ruang Siber Demi Mempertahankan Ekonomi yang Lebih Baik melalui Keamanan TI* digelar di Seoul, Republik Korea pada tanggal 7-8 September 2011 dengan diikuti 86 delegasi, moderator, dan pembicara dari 16 negara. Seminar ini diselenggarakan oleh Kementerian Luar Negeri dan Perdagangan, Kementerian Administrasi dan Keamanan Publik, serta KCC, yang disponsori oleh Korea Internet & Security Agency (KISA).

Seminar tersebut merupakan tindak lanjut dari dua proyek kerja sama CTTF-TEL sebelumnya, yaitu *Program Pelatihan APEC untuk Penguatan Keamanan Siber di Kawasan Asia-Pasifik* yang digelar pada tanggal 15-30 November 2007, di Seoul, dan *Seminar APEC tentang Perlindungan Ruang Siber dari Pemanfaatan dan Serangan Teroris* digelar pada 26-27 Juni 2008, di Seoul. Berdasarkan hasil program pelatihan dan seminar pertama, seminar ke-3 mempertemukan pejabat pemerintah dan pakar dari negara anggota APEC untuk membahas masalah keamanan siber seperti perlindungan infrastruktur kritis dari serangan teroris.

Aktivitas Keamanan Informasi ITU[45]

ITU merupakan Badan TIK terkemuka milik PBB. Berbasis di Jenewa, Swiss, ITU memiliki 191 negara anggota dan lebih dari 700 rekan dan anggota sektor dan asosiasi.

Peran ITU dalam membantu komunikasi dunia mencakup tiga sektor inti. Sektor Komunikasi Radio (ITU-R) berfokus pada pengelolaan sumber daya spektrum frekuensi radio internasional dan orbit satelit. Sektor Standardisasi Telekomunikasi (ITU-T) berfokus pada standarisasi jaringan dan layanan komunikasi informasi. Sektor Pembangunan (ITU-D) didirikan untuk membantu menyebarkan akses terhadap TIK yang adil, berkelanjutan dan terjangkau sebagai sarana untuk merangsang pembangunan sosial dan ekonomi yang lebih luas. ITU juga menyelenggarakan acara terkait telekomunikasi dan merupakan badan penyelenggara utama WSIS.

[45] International Telecommunications Union. (2021). ITU Cybersecurity Activities. http://www.itu.int/en/action/cybersecurity/Pages/default.aspx.

Peran mendasar ITU setelah WSIS adalah membangun kepercayaan dan keamanan dalam penggunaan TIK. Di WSIS, Kepala Negara dan para pemimpin dunia mempercayakan ITU untuk memimpin dalam koordinasi upaya internasional di bidang keamanan siber, sebagai fasilitator tunggal Poin Aksi C.5, yaitu “Membangun kepercayaan dan keamanan dalam penggunaan TIK”. Keamanan siber merupakan salah satu area fokus utama di bawah ITU-D.

Area yang menjadi fokus utama Poin Aksi C.5 WSIS adalah:

- CIIP
- Mendorong budaya keamanan siber global
- Harmonisasi pendekatan hukum nasional, serta koordinasi dan penegakan hukum internasional
- Melawan spam
- Mengembangkan kapabilitas pengawasan, peringatan, dan penanganan insiden
- Berbagi informasi mengenai pedoman, praktik yang baik, dan pendekatan nasional
- Perlindungan privasi, data, dan konsumen

Agenda Keamanan Siber Global ITU atau *ITU Global Cybersecurity Agenda* (GCA) merupakan kerangka kerja ITU untuk kerja sama internasional yang bertujuan mengusulkan solusi untuk meningkatkan kepercayaan dan keamanan dalam masyarakat informasi. GCA memiliki lima pilar strategis yang juga dikenal sebagai area kerja:

- Tindakan Hukum
- Tindakan Teknis & Prosedural
- Struktur Organisasi
- Pengembangan Kapasitas
- Kerja Sama internasional

Strategi tersebut dijabarkan melalui tujuan-tujuan berikut:

- Mengembangkan model hukum kejahatan siber yang dapat diterapkan secara global dan dapat dioperasikan dengan langkah legislatif nasional/regional yang ada;
- Membuat struktur organisasi serta kebijakan nasional dan regional terkait kejahatan siber;
- Menetapkan kriteria keamanan minimum serta skema akreditasi untuk sistem dan aplikasi perangkat lunak yang dapat diterima secara global;
- Menciptakan kerangka kerja global untuk pengawasan, peringatan dan penanganan insiden demi menjamin koordinasi inisiatif lintas batas;
- Membuat dan mendukung sistem identitas digital umum dan universal serta struktur organisasi yang diperlukan untuk menjamin pengakuan kredensial digital bagi individu di seluruh batas geografis;
- Mengembangkan strategi global untuk memfasilitasi pengembangan kapasitas manusia dan kelembagaan demi meningkatkan pengetahuan dan keterampilan lintas sektor di seluruh sektor yang telah disebutkan di atas; serta
- Memberi nasihat terkait kerangka kerja potensial untuk strategi multi pemangku kepentingan global dalam rangka kerja sama internasional, dialog dan koordinasi di semua sektor yang telah disebutkan di atas.

GCA telah mendorong berbagai inisiatif seperti Inisiatif Perlindungan Anak Secara Daring melalui kemitraannya dengan IMPACT dan dengan dukungan dari para pemain global terkemuka.

Inisiatif lainnya adalah Gerbang Keamanan Siber ITU *(ITU Cybersecurity Gateway)* yang berfungsi menyediakan sumber informasi yang mudah digunakan dan interaktif terhadap inisiatif-inisiatif yang berhubungan dengan keamanan siber nasional dan internasional. Gerbang keamanan tersebut tersedia untuk masyarakat, pemerintah, bisnis, dan organisasi internasional. Layanan yang disediakan oleh gerbang keamanan tersebut mencakup berbagi informasi, pengawasan dan peringatan, hukum dan undang-undang, privasi dan perlindungan, serta standar dan solusi industri.

ITU-D juga mengawasi Program Kerja Keamanan Siber ITU yang dibentuk dalam rangka membantu berbagai negara mengembangkan teknologi untuk keamanan ruang siber tingkat tinggi. Program kerja tersebut memberikan bantuan terkait dengan hal-hal sebagai berikut:

- Menetapkan strategi dan kapabilitas nasional untuk keamanan siber dan CIIP
- Menetapkan undang-undang kejahatan siber yang tepat sekaligus mekanisme pelaksanaannya
- Membangun kapabilitas pengawasan, peringatan dan penanganan insiden
- Melawan spam dan ancaman terkait
- Menjembatani kesenjangan standardisasi terkait keamanan antara negara berkembang dan negara maju
- Membuat Direktori Keamanan Siber/CIIP ITU, basis data kontak, dan publikasi *Who's Who*
- Menetapkan indikator keamanan siber
- Mendorong kegiatan kerja sama regional
- Berbagi informasi dan mendukung Gerbang Keamanan Siber ITU
- Penjangkauan dan promosi kegiatan terkait

Aktivitas terkait keamanan siber ITU-D lainnya adalah aktivitas gabungan bersama dengan StopSpamAlliance.org; kegiatan peningkatan kapasitas regional tentang undang-undang dan penegakan kejahatan siber; serta pengembangan dan distribusi sumber daya dan perangkat, seperti perangkat mitigasi botnet, [46] perangkat untuk model perundang-undangan kejahatan siber bagi negara-negara berkembang, perangkat penilaian mandiri keamanan siber nasional, [47] serta publikasi dan makalah keamanan siber/kejahatan siber. [48]

Sektor ITU-T juga berkontribusi pada bidang keamanan siber melalui pengembangan lebih dari 70 standar terkait keamanan (Rekomendasi ITU-T). Di simposium keamanan siber pada belakangan ini, peserta meminta ITU-T untuk mempercepat kerjanya di bidang ini. Sebagai

[46] Ramasubramanian, S., & Shaw, R. (2007, September). ITU Botnet Mitigation Project: Background & Approach. International Telecommunication Union. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-botnet-mitigation-toolkit.pdf

[47] ITU-D ICT Applications and Cybersecurity Division. (2009). ITU National Cybersecurity/CIIP Self-Assessment Tool. http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html.

[48] International Telecommunications Union. (2021). *ITU-D Cybersecurity*. ITU-D. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx.

balasan, ITU-T kini memberikan penekanan tambahan pada pengembangan standar keamanan. Untuk membantu proses tersebut, ITU-T mengembangkan *Roadmap Standar Keamanan TIK* yang menyatukan informasi terkait standar yang ada, standar yang sedang dikembangkan, dan bidang kerja standar keamanan di masa mendatang.[49]

Pekerjaan berstandar yang dilakukan oleh kelompok penelitian atau *study group* (SG) teknis dengan perwakilan dari keanggotaan ITU-T menyusun rekomendasi (standar) untuk berbagai bidang telekomunikasi internasional. SG lebih mengarahkan pekerjaan mereka dalam bentuk pertanyaan penelitian. Setiap pertanyaan membahas studi teknis di bidang standarisasi telekomunikasi tertentu.

Di dalam ITU-T, Kelompok Penelitian 17 (SG17) [50] mengoordinasikan pekerjaan terkait keamanan di seluruh kelompok penelitian.

SG17 bertanggung jawab atas penelitian terkait keamanan seperti keamanan siber, melawan spam, dan manajemen identitas. Ia juga bertanggung jawab untuk penerapan komunikasi sistem terbuka seperti pengenal *(identifier)* direktori dan objek, dan untuk bahasa teknis, metode penggunaannya, serta masalah lainnya terkait aspek perangkat lunak sistem telekomunikasi.

Struktur SG17 periode penelitian 2017-2020 adalah sebagai berikut:

- Kelompok Kerja 1. Keamanan Telekomunikasi/TIK
    - Pertanyaan 1 – Koordinasi keamanan Telekomunikasi/TIK
    - Pertanyaan 2 – Kerangka kerja dan Arsitektur Keamanan
    - Pertanyaan 3 – Manajemen keamanan informasi telekomunikasi
    - Pertanyaan 4 – Keamanan siber
    - Pertanyaan 5 – Melawan *spam* dengan langkah teknis
- Kelompok Kerja 2. Keamanan Ruang siber
    - Pertanyaan 6 – Aspek keamanan layanan telekomunikasi di mana pun
    - Pertanyaan 7 – Layanan aplikasi keamanan
    - Pertanyaan 8 – Keamanan arsitektur berorientasi layanan
    - Pertanyaan 9 – Telebiometrik
- Kelompok Kerja 3. Keamanan aplikasi
    - Pertanyaan 10 – Arsitektur dan mekanisme manajemen identitas
    - Pertanyaan 11 – Layanan direktori, sistem direktori, dan kunci publik/sertifikat atribut
    - Pertanyaan 12 – *Abstract Syntax Notation* One (ANS.1), Pengidentifikasi Objek dan registrasi terkait
    - Pertanyaan 13 – Bahasa formal dan perangkat lunak telekomunikasi
    - Pertanyaan 14 – Menguji bahasa, metodologi, dan kerangka kerja
    - Pertanyaan 15 – Interkoneksi Sistem Terbuka

[49] Persatuan Telekomunikasi Internasional (ITU). Roadmap Standar Keamanan TIK. Diakses dari http://www.itu.int/ITU-T/studygroups/com17/ict/index.html.

[50] Persatuan Telekomunikasi Internasional (ITU). *SG17 – Struktur Kelompok Penelitian (Periode Penelitian 2017-2020)*. ITU. Diakses dari http://www.itu.int/net4/ITU-T/lists/sgstructure.aspx?Group=17&Period=16.

Pekerjaan untuk membangun kepercayaan dan keamanan dalam penggunaan teknologi informasi dan komunikasi (TIK) terus ditingkatkan dalam upaya memfasilitasi infrastruktur jaringan, layanan, dan aplikasi yang lebih aman. Lebih dari 170 standar (Rekomendasi dan Pelengkap ITU-T) yang berfokus pada keamanan telah diterbitkan.

Kelompok Penelitian ITU-T 17 (SG17) mengoordinasikan pekerjaan terkait keamanan di seluruh Kelompok Penelitian ITU-T. SG17 menangani berbagai masalah standardisasi seringkali bekerja sama dengan organisasi pengembangan standar (SDO) dan berbagai konsorsium industri TIK lainnya.

Sebagai contoh, saat ini SG17 sedang mengerjakan keamanan siber; manajemen keamanan; arsitektur dan kerangka kerja keamanan; melawan spam; manajemen identitas; perlindungan informasi pengenal pribadi; serta keamanan aplikasi dan layanan untuk *internet of things* (IoT), jaringan cerdas *(smart grid)*, ponsel cerdas *(smartphone)*, jaringan yang ditentukan perangkat lunak (SDN), layanan web *(web service)*, analitik data besar *(big data analytics)*, jejaring sosial *(social networks)*, komputasi awan *(cloud computing)*, sistem keuangan seluler, IPTV, dan telebiometrik.

Referensi utama standar keamanan yang digunakan saat ini adalah Rekomendasi X.509 milik ITU-T yang berfungsi untuk autentikasi elektronik melalui jaringan publik. X.509 digunakan untuk merancang aplikasi yang berhubungan dengan infrastruktur kunci publik, serta banyak digunakan dalam berbagai aplikasi mulai dari pengamanan koneksi antara peramban dan *server* di web hingga menyediakan tanda tangan digital yang dapat digunakan untuk transaksi *e-commerce*. Pencapaian lain dari SG17 adalah Rekomendasi X.805, yang dapat membuat perusahaan dan operator jaringan telekomunikasi memberikan gambaran mengenai arsitektur ujung ke ujung *(end-to-end)* dari perspektif keamanan.[51]

SG17 juga merupakan tempat untuk mempelajari bahasa teknis dan teknik deskripsi. Contohnya adalah bahasa formal ASN.1, yaitu komponen penting untuk spesifikasi protokol atau rancangan sistem. ASN.1 merupakan bagian yang sangat penting dari jaringan saat ini. ASN.1 digunakan untuk sistem persinyalan oleh sebagian besar panggilan telepon, pelacakan paket, verifikasi kartu kredit dan sertifikat digital serta pada berbagai program perangkat lunak yang paling sering digunakan. Pekerjaan yang sedang berkembang saat ini adalah pengembangan profil bahasa pemodelan terpadu untuk bahasa ITU-T.[52]

Aktivitas Keamanan Informasi ISO/IEC

Sistem Manajemen Keamanan Informasi (SMKI) atau Information Security Management System (ISMS), sebagaimana namanya, merupakan sistem untuk mengelola keamanan informasi. ISMS terdiri dari berbagai sistem dan proses untuk memastikan kerahasiaan, keutuhan, dan ketersediaan aset informasi, di samping meminimalkan risiko keamanan.

[51] Persatuan Telekomunikasi Internasional. Sekilas tentang Kelompok Penelitian 17 (SG17). http://www.itu.int/net/ITU-T/info/sg17.aspx.
[52] Ibid.

Sertifikasi ISMS semakin populer di seluruh dunia, dengan tahun 2005 sebagai titik balik sejarah ISMS berstandar internasional karena dikeluarkannya dua dokumen: IS 27001 yang menjelaskan kebutuhan untuk membentuk ISMS, dan IS 17799: 2000, diterbitkan sebagai IS 17799: 2005, yang mengatur kontrol dasar untuk implementasi ISMS.

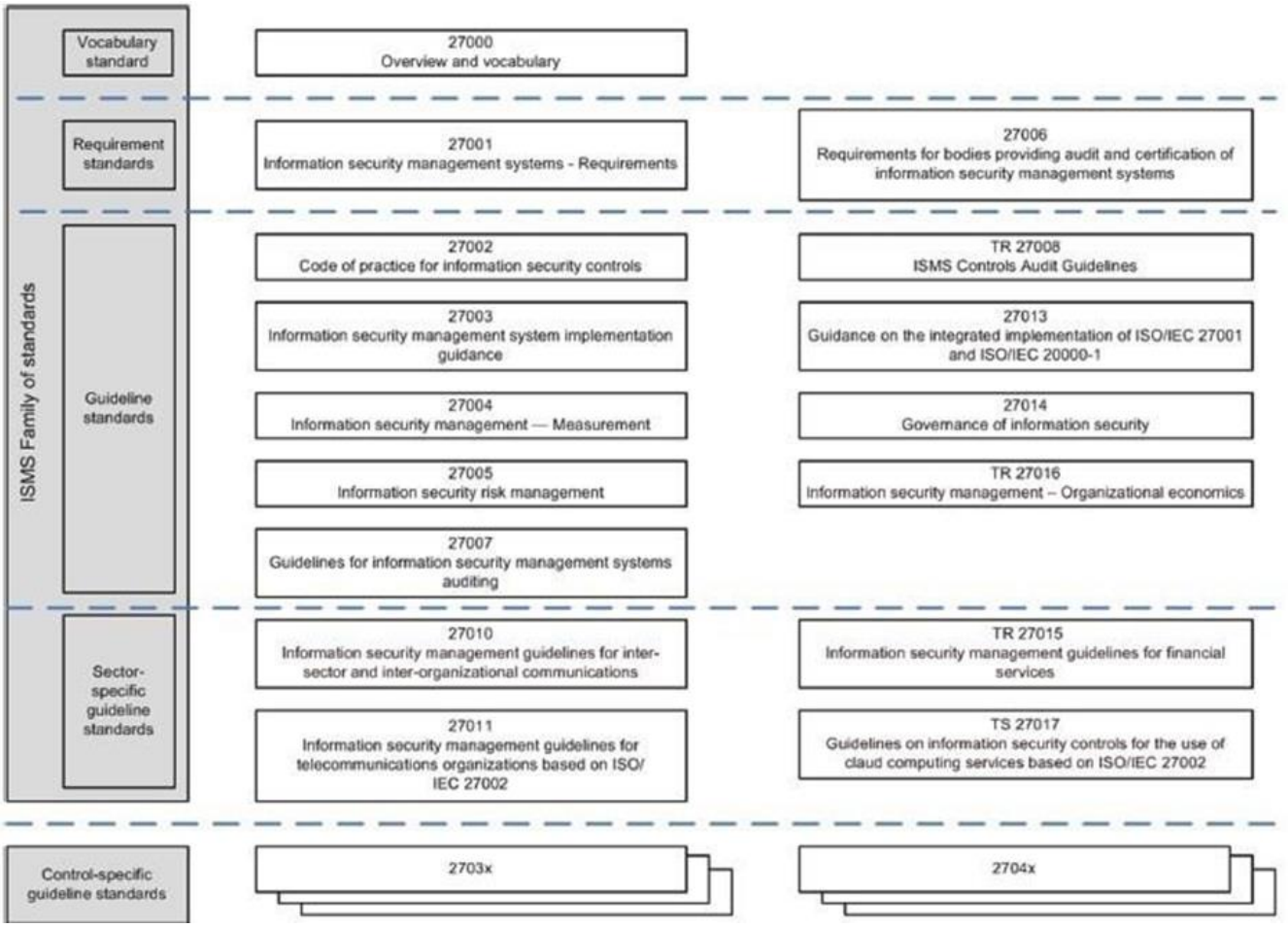
Standar ISMS sesungguhnya adalah BS 7799, yang pertama kali dikembangkan oleh British Standards Institution (BSI) pada tahun 1995 sebagai kode praktik untuk manajemen keamanan informasi. Pada tahun 1998, karena spesifikasi kebutuhan dikembangkan berdasarkan standar tersebut, "kode praktik untuk manajemen keamanan informasi" diubah menjadi Bab 1 dan spesifikasi kebutuhan menjadi Bab 2. Bab 1 menentukan kontrol manajemen keamanan informasi, sementara Bab 2 menjelaskan kebutuhan pembentukan ISMS serta menjelaskan proses keamanan informasi (Siklus *Plan-Do-Check-Act*) untuk perbaikan berkelanjutan dari landasan manajemen risiko.

Bab 1 ditetapkan sebagai IS 17799 oleh ISO/IEC JTC 1/SC27 WG1 pada tahun 2000. Sejak saat itu, IS 17799 terus ditnjau (dengan lebih dari 2.000 komentar) serta direvisi, dan versi akhirnya telah terdaftar dalam standar internasional pada bulan November 2005. IS 17799: 2000 memberikan 126 kontrol dalam 10 domain. IS 17799 yang direvisi pada tahun 2005 menyediakan 11 domain kontrol administratif dan 133 kontrol.

Bab 2 dari BS 7799 yang ditetapkan pada tahun 1999 telah digunakan sebagai standar untuk sertifikasi ISMS. Ia direvisi pada bulan September 2002 agar selaras dengan ISO 9001 dan ISO 14001. ISO mengadopsi Bab 2 BS7799: 2002 melalui metode jalur cepat *(fast track)* untuk mengatasi permintaan ISMS berstandar internasional dan mendaftarkannya sebagai standar internasional ISO27001 dengan sedikit revisi dalam waktu singkat. Perubahan signifikan yang dilakukan di antaranya adalah menambahkan konten mengenai efektivitas dan memodifikasi lampiran.

Karena dua dokumen penting terkait ISMS telah berstandar internasional, sekumpulan standar keamanan internasional juga muncul di bawah skema nomor seri 27000, yang sama dengan sistem manajemen lainnya (Bisnis kualitas: seri 9000, Manajemen lingkungan: seri 14000). IS 27001, versi revisi dari IS 17799: 2005, yang mencakup kebutuhan untuk pembentukan ISMS serta IS17799: 2005, yang mencakup kontrol dasar untuk implementasi ISMS, telah diubah menjadi IS27002 pada tahun 2007. Pedoman untuk penerapan ISMS, standar untuk manajemen risiko keamanan informasi, serta pengukuran manajemen keamanan informasi yang dikembangkan oleh JTC1 SC27 berada pada seri 27000.

Gambar 9 menunjukkan kumpulan standar terkait ISMS. Kegiatan sertifikasi ISMS mendapatkan momentum dan diharapkan standar atau pedoman ISMS yang sesuai untuk industri tertentu dikembangkan berdasarkan ISMS umum untuk sistem pada umumnya. Contohnya adalah upaya mengembangkan pedoman ISMS yang mencerminkan karakteristik industri komunikasi.



Gambar 9. Kumpulan ISO/IEC 27000

Pertanyaan:

Dari beberapa aktivitas keamanan informasi yang dipelopori oleh organisasi internasional, aktivitas manakah yang telah atau sedang diadopsi oleh negara Anda? Bagaimana penerapannya?

Uji Kompetensi

1. Apakah kesamaan aktivitas keamanan informasi yang dilakukan oleh berbagai negara yang dijelaskan dalam bab ini? Apa pula perbedaannya?

2. Apa prioritas keamanan informasi organisasi internasional yang dijelaskan dalam bab ini?

4. Metodologi Keamanan Informasi

Bab ini bertujuan untuk menjelaskan metodologi keamanan informasi administratif, fisik, dan teknis yang digunakan secara internasional.

4.1. Berbagai Aspek Keamanan Informasi

Metodologi keamanan informasi berfungsi untuk meminimalkan kerugian dan menjaga kontinuitas bisnis dengan mempertimbangkan segala kemungkinan kerentanan dan ancaman terhadap aset informasi. Untuk menjamin kontinuitas bisnis, metodologi keamanan informasi berupaya memastikan kerahasiaan, keutuhan, dan ketersediaan aset informasi internal. Hal ini melibatkan penerapan metode dan kontrol penilaian risiko. Pada dasarnya, yang dibutuhkan adalah perencanaan yang baik yang mencakup aspek administratif, fisik, dan teknis dari keamanan informasi.

Aspek administratif

Terdapat banyak ISMS yang menitikberatkan pada aspek administratif. ISO/IEC 27001 merupakan salah satu standar ISMS yang paling umum digunakan.

ISO/IEC27001, standar ISMS internasional yang ditetapkan oleh BSI, diambil dari BS7799. BS7799 menetapkan kebutuhan untuk penerapan dan pengelolaan ISMS serta standar umum yang diterapkan pada standar keamanan berbagai organisasi dan manajemen keamanan yang efektif. Bab 1 BS7799 menjelaskan aktivitas keamanan yang diperlukan berdasarkan praktik terbaik aktivitas keamanan dalam organisasi. Bab 2, yang telah menjadi ISO/IEC27001 saat ini, menyarankan kebutuhan minimum yang diperlukan untuk pengoperasian dan penilaian aktivitas keamanan ISMS.

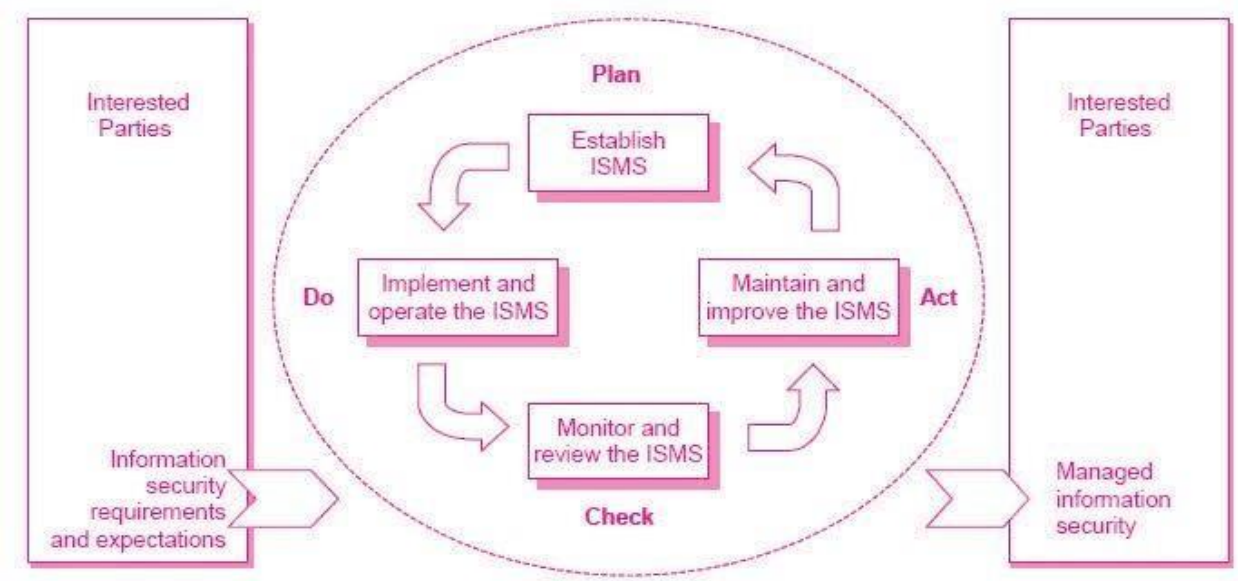
Aktivitas keamanan dalam ISO/IEC27001 terdiri dari 114 kontrol dalam 14 domain (Tabel 5).

Tabel 5. Kontrol dalam ISO/IEC27001

Domain	Butir
A5.	Kebijakan keamanan informasi
A6.	Organisasi keamanan informasi
A7.	Keamanan sumber daya manusia
A8.	Manajemen aset
A9.	Kontrol akses
A10.	Kriptografi
A11.	Keamanan lingkungan dan fisik
A12.	Keamanan operasi

A13.	Keamanan komunikasi
A14.	Akuisisi, pengembangan dan pemelihataan sistem
A15.	Hubungan pemasok
A16.	Manajemen insiden keamanan informasi
A17.	Aspek keamanan informasi dari manajemen kontinuitas bisnis
A18.	Kepatuhan *(compliance)*

ISO/IEC27001 mengadopsi model proses *Plan-Do-Check-Act*, yang diterapkan untuk menyusun seluruh proses ISMS. Dalam ISO/IEC27001, seluruh bukti penilaian ISMS harus didokumentasikan; sertifikasi harus diaudit secara eksternal setiap enam bulan; dan seluruh proses harus diulangi setelah tiga tahun untuk pengelolaan ISMS berkesinambungan.



Gambar 10. Model proses *Plan-Do-Check-Act* yang diterapkan pada proses ISMS
Sumber: ISO/IEC JTC 1/SC 27.

Kontrol keamanan harus direncanakan dengan mempertimbangkan kebutuhan keamanan *(security requirements)*. Seluruh sumber daya manusia, termasuk pemasok, kontraktor, pelanggan, dan spesialis dari luar, harus berpartisipasi dalam aktivitas ini. Menyiapkan kebutuhan keamanan didasarkan pada tiga faktor berikut:

- Penilaian risiko
- Kebutuhan hukum dan ketentuan kontrak
- Proses informasi untuk menjalankan organisasi

Analisis kesenjangan mengacu pada proses pengukuran tingkat keamanan informasi saat ini dan menentukan arah keamanan informasi di masa mendatang. Hasil analisis kesenjangan diperoleh dari jawaban para pemilik aset terhadap 133 kontrol dan 11 domain. Saat area yang kurang baik teridentifikasi melalui analisis kesenjangan, kontrol yang sesuai untuk masing-masing area dapat ditetapkan.

Penilaian risiko dibagi menjadi penilaian nilai aset serta penilaian ancaman dan kerentanan. Penilaian nilai aset merupakan penilaian kuantitatif dari aset informasi. Penilaian ancaman mencakup pemeringkatan ancaman terhadap kerahasiaan, keutuhan, dan ketersediaan informasi. Contoh di bawah ini menunjukkan perhitungan yang dilakukan dalam penilaian risiko.

Nama aset	Nilai aset	Ancaman			Kerentanan			Risiko		
		C	I	A	C	I	A	C	I	A
Nama aset #1	2	3	3	1	3	1	1	8	6	5

- Nilai Aset + Ancaman + Kerentanan = Risiko
- Kerahasiaan/*Confidentiality* (C): Nilai Aset(2) + Ancaman(3) + Kerentanan(3) = Risiko(8)
- Keutuhan/*Integrity* (I): Nilai Aset(2) + Ancaman(3) + Kerentanan(1) = Risiko(6)
- Ketersediaan/*Availability* (A): Nilai Aset(2) + Ancaman(1) + Kerentanan(1) = Risiko(5)

Penerapan kontrol: Setiap nilai risiko akan berbeda sesuai dengan hasil penilaian risiko. Keputusan diperlukan untuk menerapkan kontrol yang sesuai pada aset-aset dengan nilai beragam. Risiko harus dipecah menjadi risiko yang dapat diterima dan risiko yang tidak dapat diterima sesuai dengan kriteria Tingkat Jaminan *(Degree of Assurance)*. Kontrol perlu diterapkan pada aset informasi yang memiliki risiko tidak dapat diterima. Kontrol diterapkan berdasarkan kontrol ISO/IEC, tetapi akan lebih efektif menerapkan kontrol berdasarkan pada keadaan organisasi yang sebenarnya.

Aspek Teknis
Tidak ada ISMS untuk aspek teknis. Standar evaluasi umum internasional seperti sertifikasi *Common Criteria* (CC) [53] dapat digunakan sebagai gantinya.

Sertifikasi CC memiliki potensi komersial. Ia dibentuk untuk mengatasi kekhawatiran mengenai perbedaan tingkat keamanan produk TI dari berbagai negara. Standar internasional untuk evaluasi produk IT tersebut ditetapkan oleh Kanada, Perancis, Jerman, Kerajaan Serikat, dan Amerika Serikat.

Secara khusus, CC menjelaskan kebutuhan keamanan TI suatu produk atau sistem mengikuti kategori kebutuhan fungsional dan kebutuhan jaminan yang berbeda. Kebutuhan fungsional CC menentukan langkah keamanan yang diinginkan. Kebutuhan jaminan merupakan dasar untuk mendapatkan keyakinan bahwa langkah keamanan yang diklaim efektif dan telah diterapkan dengan benar. Fungsi keamanan CC terdiri dari 134 komponen dari 11 kelas yang terdiri dari 65 kelompok. Kebutuhan jaminan mengacu pada 81 komponen dari delapan kelas yang terdiri dari 38 kelompok.

Kebutuhan fungsional keamanan (SFR): SFR menentukan seluruh fungsi keamanan untuk Target Evaluasi (TOE). Tabel 6 menjelaskan kelas-kelas fungsi keamanan yang termasuk dalam SFR.

[53] Common Criteria. *Common Criteria : New CC Portal*. Diakses dari http://www.commoncriteriaportal.org/.

Tabel 6. Komposisi Kelas dalam SFR

Kelas		Detail
FAU	Audit keamanan	Mengacu pada fungsi yang mencakup perlindungan data audit, format rekaman/catatan, dan pemilihan kegiatan, juga alat analisis, peringatan dan analisis langsung *(real time)* pelanggaran.
FCO	Komunikasi	Menjelaskan kebutuhan khusus yang menarik untuk TOE yang digunakan untuk pengangkutan informasi.
CS	Dukungan kriptografi	Menentukan penggunaan manajemen kunci kriptografi dan operasi kriptografi
FDP	Perlindungan data pengguna	Menetapkan kebutuhan terkait dengan perlindungan data pengguna
FIA	Identifikasi dan autentikasi	Menangani kebutuhan untuk menetapkan dan memverifikasi identitas pengguna yang diklaim
FMT	Manajemen keamanan	Menentukan pengelolaan beberapa aspek Fungsi Keamanan TOE (TSF): atribut keamanan, data dan fungsi TSF
FPR	Privasi	Menjelaskan kebutuhan yang dapat diadakan untuk memenuhi kebutuhan privasi pengguna, di samping tetap memungkinkan fleksibilitas sistem sejauh mungkin untuk mempertahankan kontrol yang memadai atas pengoperasian sistem
FPT	Perlindungan TSF	Berisi kelompok kebutuhan fungsional yang berhubungan dengan integritas dan manajemen mekanisme yang membentuk TSF dan keutuhan data TSF
FRU	Pemanfaatan sumber daya	Berisi ketersediaan sumber daya yang diperlukan seperti kemampuan pemrosesan, dan/atau kapasitas penyimpanan
FTA	Akses TOE	Menentukan kebutuhan fungsional untuk mengontrol pembentukan sesi pengguna
FTP	Saluran/jalur tepercaya	Menyediakan kebutuhan untuk jalur komunikasi tepercaya antara pengguna dan TSF

Sumber:
Common Criteria. (2009). (publikasi). *Common Criteria for Information Technology Security Evaluation*. Diakses dari https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.pdf

Komponen jaminan keamanan atau *security assurance components* (SAC): Filosofi CC membutuhkan penjelasan ancaman keamanan dan komitmen terhadap kebijakan keamanan organisasi melalui langkah-langkah keamanan yang sesuai dan memadai. Langkah-langkah yang akan diambil harus dapat membantu mengidentifikasi kerentanan, mengurangi potensi kerentanan dimanfaatkan dan memitigasi tingkat kerusakan jika kerentanan dimanfaatkan.[54] Tabel 7 menjelaskan kelas-kelas yang termasuk dalam SAC.

Tabel 7. Komposisi Kelas dalam SAC

Kelas		**Detail**
APE	Evaluasi Profil Perlindungan (PP)	Hal ini diperlukan untuk menunjukkan bahwa PP tersebut kuat dan konsisten secara internal serta apakah PP tersebut didasarkan pada satu atau lebih PP atau paket lainnya sehingga PP tersebut merupakan contoh yang benar dari beberapa PP dan paket tersebut.
ASE	Evaluasi Target Keamanan (ST)	Hal ini diperlukan untuk menunjukkan bahwa ST kuat dan konsisten secara internal, serta apakah ST didasarkan pada satu atau lebih PP atau paket lainnya sehingga ST merupakan instansiasi *(instantiation)* yang benar dari beberapa PP dan paket tersebut.
ADV	Pengembangan	Ia menyediakan informasi mengenai TOE. Pengetahuan yang diperoleh digunakan sebagai dasar untuk melakukan analisis kerentanan dan pengujian terhadap TOE, sebagaimana yang dijelaskan dalam kelas ATE dan AVA.
AGD	Dokumen Pedoman	Untuk persiapan dan pengoperasian TOE yang aman, perlu dijelaskan seluruh aspek relevan untuk penanganan TOE yang aman. Kelas tersebut juga membahas kemungkinan konfigurasi yang salah atau penanganan TOE yang tidak diinginkan.
ALC	Dukungan siklus hidup	Dalam siklus hidup produk, yang mencakup kapabilitas manajemen konfigurasi (CM), cakupan CM, penyampaian *(delivery)*, keamanan

[54] Common Criteria. (2009). (publication). *Common Criteria for Information Technology Security Evaluation*. Retrieved from https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.pdf
.

		pengembangan, perbaikan cacat/kerusakan, definisi siklus hidup, alat dan teknik, perlu dibedakan apakah TOE berada di bawah tanggung jawab pengembang atau pengguna.
ATE	Pengujian	Penekanan dalam kelas ini adalah penegasan bahwa TSF beroperasi sesuai deskripsi desainnya. Kelas ini tidak membahas pengujian penetrasi *(penetration testing)*.
AVA	Penilaian kerentanan	Aktivitas penilaian kerentanan meliputi berbagai kerentanan dalam pengembangan dan pengoperasian TOE.
ACO	Komposisi	Menetapkan kebutuhan jaminan yang dirancang untuk memberikan keyakinan bahwa TOE yang dibuat akan beroperasi dengan aman saat mengandalkan fungsionalitas keamanan yang disediakan oleh komponen perangkat lunak, *firmware*, atau perangkat keras yang telah dievaluasi sebelumnya.

Sumber:
Common Criteria. (2009). (publikasi). *Common Criteria for Information Technology Security Evaluation*. Diakses dari https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.pdf

Metode evaluasi CC

1. **Evaluasi PP (APE)**: PP menjelaskan serangkaian kebutuhan keamanan yang tidak bergantung pada implementasi untuk kategori TOE dan berisi laporan masalah keamanan yang ingin dipecahkan oleh produk yang sesuai. PP menetapkan kebutuhan fungsional dan jaminan CC serta memberikan alasan untuk komponen fungsional dan jaminan yang dipilih. Ia biasanya dibuat oleh konsumen atau komunitas konsumen untuk kebutuhan keamanan TI.

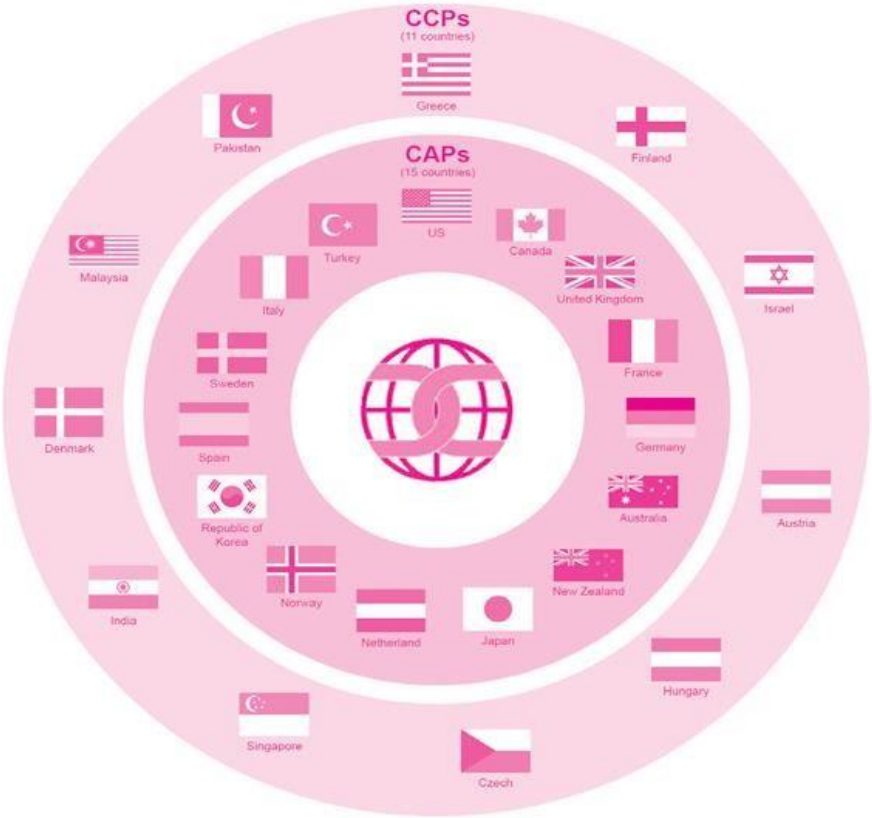
2. **Evaluasi ST (ASE)**: ST merupakan hal mendasar untuk kesepakatan antara pengembang TOE, konsumen, penilai, dan otoritas evaluasi mengenai keamanan yang ditawarkan TOE, serta ruang lingkup evaluasi. Audiens ST juga dapat mencakup mereka yang mengelola, memasarkan, membeli, menginstal, mengonfigurasi, mengoperasikan, dan menggunakan TOE. ST berisi beberapa informasi khusus implementasi yang menunjukkan bagaimana produk memenuhi kebutuhan keamanan. ST mungkin mengacu pada satu PP atau lebih. Dalam hal ini, ST harus memenuhi kebutuhan keamanan umum dalam masing-masing PP tersebut dan mungkin menentukan kebutuhan lebih lanjut.

3. **Lainnya**: Evaluasi ADV, AGD, ALC, ATE, AVA dan ACO.

Pengaturan Pengenalan Common Criteria (Common Criteria Recognition Arrangement)

Pengaturan Pengenalan *Common Criteria* atau *Common Criteria Recognition Arrangement* (CCRA) diadakan untuk mengesahkan sertifikasi CC antar negara. CCRA bertujuan untuk memastikan evaluasi CC dilakukan dengan standar yang konsisten, menghilangkan atau mengurangi evaluasi rangkap produk TI atau profil perlindungan (PP), dan meningkatkan peluang pasar global untuk industri TI dengan mengesahkan sertifikasi di antara negara-negara anggota.

CCRA terdiri dari 26 negara anggota dengan 15 negara di antaranya merupakan Peserta Yang Mengesahkan Sertifikat atau *Certificate Authorizing Participants* (CAP) dan 11 negara merupakan Peserta Yang Menggunakan Sertifikat atau *Certificate Consuming Participants* (CCP). CAP merupakan produsen sertifikat evaluasi. Mereka adalah sponsor dari badan sertifikasi kepatuhan yang beroperasi di negara mereka sendiri dan mengesahkan sertifikat yang diterbitkannya. Sebuah negara harus menjadi anggota CCRA sebagai CCP selama minimal dua tahun sebelum dapat mengajukan permohonan untuk menjadi CAP. CCP merupakan konsumen sertifikat evaluasi. Meskipun mereka mungkin tidak mempertahankan kemampuan evaluasi keamanan TI, mereka memiliki minat yang jelas dalam penggunaan produk yang disertifikasi/divalidasi serta profil perlindungan (PP). Untuk menjadi anggota CCRA, sebuah negara harus mengajukan permohonan tertulis kepada Komite Manajemen.



Gambar 11. CAP dan CCP

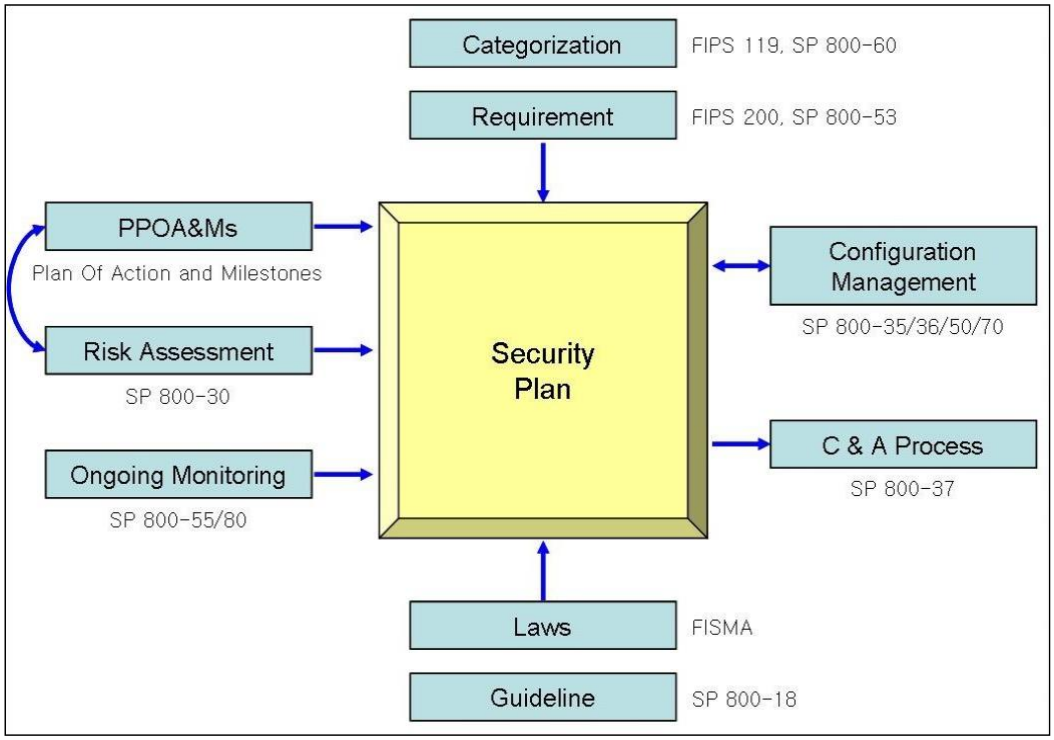
4.2. Contoh Metodologi Keamanan Informasi

Badan Nasional Standar dan Teknologi Amerika Serikat (NIST)

Berdasarkan FISMA, Badan Standar dan Teknologi Nasional Amerika Serikat (NIST) telah mengembangkan pedoman dan standar untuk memperkuat keamanan informasi dan sistem informasi yang dapat digunakan oleh lembaga-lembaga Federal. Pedoman dan standar tersebut bertujuan untuk:

- Memberikan spesifikasi untuk kebutuhan keamanan minimum dengan mengembangkan standar yang dapat digunakan untuk kategorisasi informasi dan sistem informasi Federal;
- Memperbolehkan kategorisasi keamanan informasi dan sistem informasi;
- Memilih dan menentukan kontrol keamanan untuk sistem informasi yang mendukung berbagai badan eksekutif Pemerintahan Federal; serta
- Memverifikasi efisiensi dan efektivitas kontrol keamanan terhadap kerentanan.

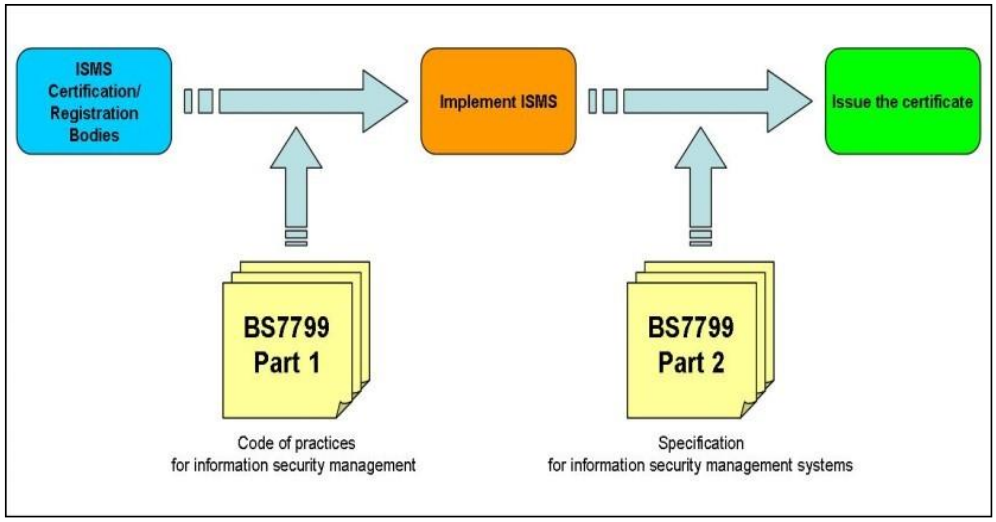
Pedoman terkait FISMA diterbitkan sebagai publikasi khusus dan Publikasi Standar Pemrosesan Informasi Federal. Terdapat dua seri publikasi khusus: seri 500 untuk teknologi informasi dan seri 800 untuk keamanan komputer. Gambar 12 menunjukkan proses yang diikuti oleh lembaga pemerintah Amerika Serikat untuk menetapkan rencana keamanannya berdasarkan standar tersebut.



Gambar 12. Masukan/Keluaran Proses Perencanaan Keamanan

Kerajaan Serikat (BS7799)

Sebagaimana penjelasan sebelumnya, BSI menganalisis aktivitas keamanan organisasi di Kerajaan Serikat (UK) dan memberikan sertifikasi BS7799 yang kini telah dikembangkan menjadi ISO27001 (BS7799 Bab 2) dan ISO27002 (BS7799 Bab 1). Gambar 13 berikut menunjukkan prosedur yang diikuti.



Gambar 13. Proses Sertifikasi BS7799

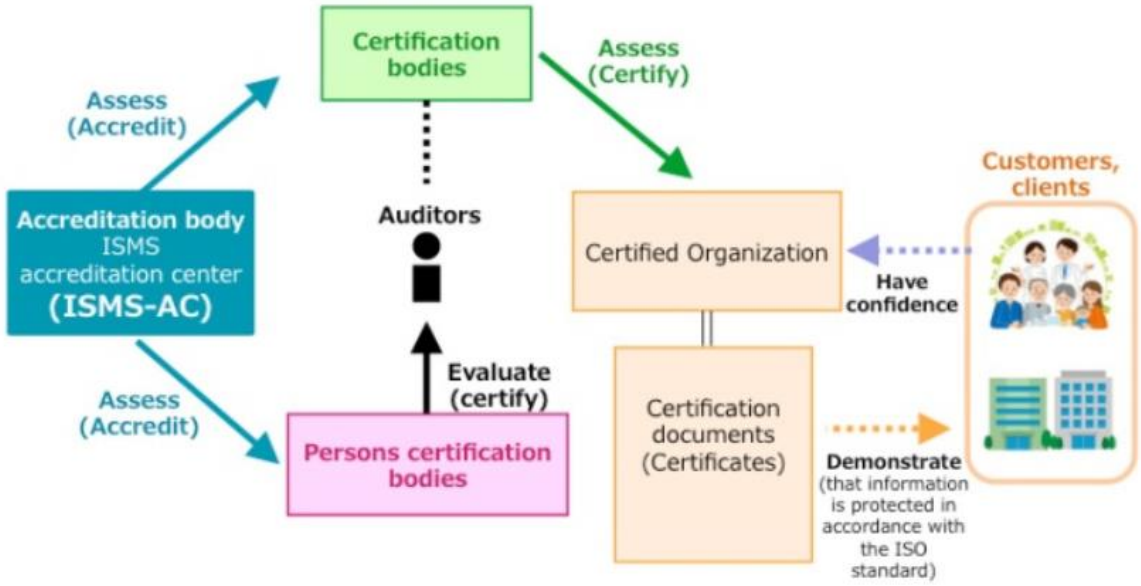
Jepang (dari ISMS Ver2.0 menjadi JIS Q 27001:2014)[55]

ISMS Ver2.0 Perusahaan Pengembangan Pemrosesan Informasi Jepang (JIPDEC) telah beroperasi di Jepang sejak April 2002. Sejak saat itu, ISMS Ver2.0 telah diganti oleh Bab 2 BS7799: 2002, yaitu JIS Q 27001: 2006 pada Maret 2006 yang sejalan dengan penerbitan ISO/IEC 27001: 2005 dan kemudian direvisi serta diterbitkan pada Maret 2014 sebagai JIS Q 27001: 2014 berdasarkan revisi ISO/IEC 27001.

Skema penilaian kepatuhan ISMS di Jepang memiliki struktur komprehensif yang terdiri dari "badan sertifikasi" yang menilai dan melakukan sertifikasi ISMS organisasi pemohon berdasarkan ISO/IEC 27001, "badan sertifikasi personel" yang melakukan sertifikasi dan mendaftarkan auditor ISMS, serta "badan akreditasi" yang menilai kompetensi badan-badan tersebut dalam melaksanakan tugas-tugasnya. Terkait dengan "lembaga pelatihan auditor", lembaga sertifikasi personel melakukan penilaian terhadap lembaga-lembaga tersebut dan memberikan persetujuan berdasarkan hasil penilaian.

Gambar 14 menunjukkan sistem sertifikasi ISMS di Jepang.

[55] ISMS Accreditation Centre. *Overview of the ISMS conformity assessment scheme*. ISMS-AC. https://isms.jp/english/isms/about.html.



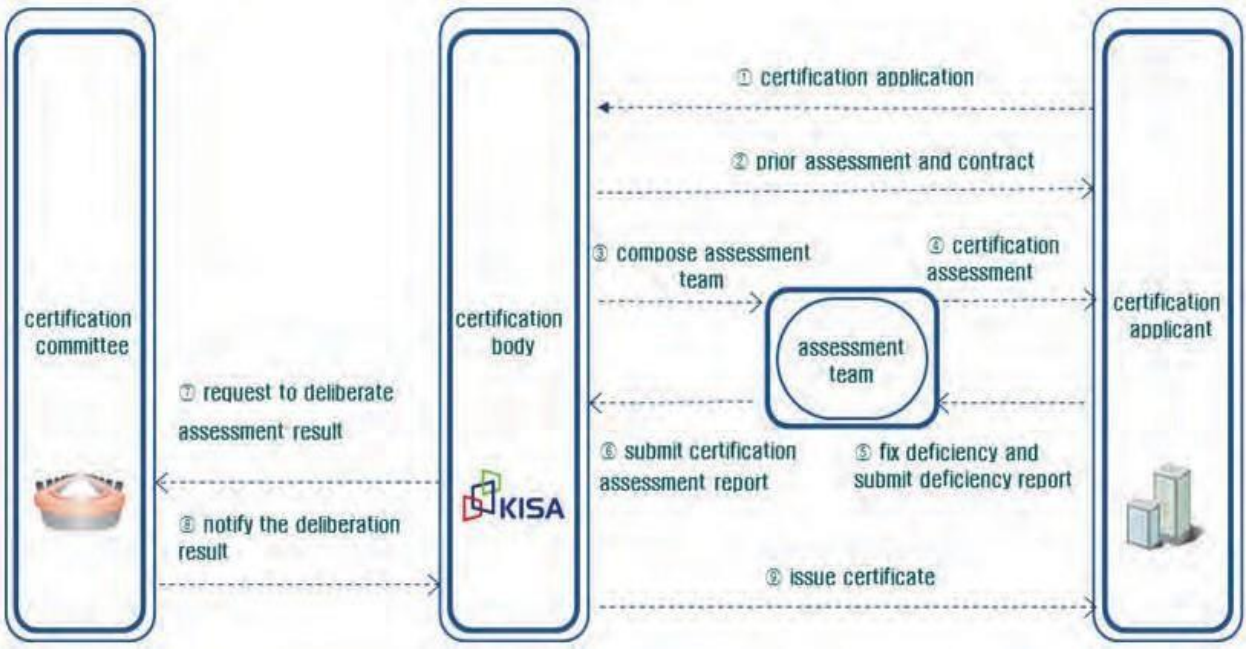
Gambar 14. Sistem Sertifikasi ISMS di Jepang

Sumber: ISMS Accreditation Centre. Overview of the ISMS conformity assessment scheme. ISMS-AC. Diakses dari https://isms.jp/english/isms/about.html.

Republik Korea (KISA ISMS)

Sejak 2002, KCC dan KISA telah memperkenalkan dan menjalankan program sertifikasi ISMS. KCC dan KISA telah berupaya keras untuk mempromosikan program sertifikasi ISMS, dan saat ini program tersebut dianggap sebagai program yang sangat sukses. Skema dan prosedur sertifikasi ISMS masing-masing ditunjukkan pada Gambar 15 dan 16. Pada tahun 2011, jumlah sertifikat ISMS mencapai 114. Dengan meningkatnya jumlah tersebut, tingkat keamanan informasi dari masing-masing organisasi yang disertifikasi diperkirakan akan meningkat drastis. Organisasi yang telah tersertifikasi merupakan perusahaan terkemuka di berbagai bidang bisnis seperti KT, Korean Air, NHN, Daum, dan lain-lain.

Gambar 15. Skema Sertifikasi ISMS di Republik Korea



Gambar 16. Prosedur Sertifikasi ISMS di Republik Korea

Jerman

BSI Jerman (Bundesamt fűr Sicherheit in der Informationstechnik) merupakan badan nasional untuk keamanan informasi. BSI adalah penyedia layanan keamanan TI pusat pertama dan terpenting bagi pemerintah federal di Jerman. BSI menyediakan layanan keamanan TI kepada para individu, organisasi, kota, dan pemerintah Jerman di Jerman.

BSI telah menetapkan Kualifikasi Perlindungan Dasar TI *(IT-Grundschutz)* berdasarkan standar internasional, *ISO Guide 25* [GUI25] dan standar Eropa EN45001 yang diakui oleh Komite Eropa untuk Pengujian dan Sertifikasi TI. Jenis-jenis sertifikasinya meliputi Sertifikat Perlindungan Dasar TI *(IT Baseline Protection)* serta Sertifikat Perlindungan Dasar TI tingkat atas dan Sertifikat Perlindungan Dasar TI tingkat pemula yang dinyatakan sendiri. Pada tahun 1999, EN45001 diganti dengan ISO/IEC/EN 17025.

Selain itu, manual perlindungan dasar (BPM) dan sub-manual Standar BSI Serie: 100-X telah dikembangkan. Hal tersebut mencakup Standar BSI 100-1 ISMS, Standar BSI 100-2 Metodologi BPM, dan Analisis Risiko BSI Standar 100-3.

Pada tahun 2011, Jerman secara resmi membuka Pusat Pertahanan Siber Nasional atau German Nationales Cyber-Abwehrzentrum (NCAZ) Jerman yang berlokasi di Bonn. NCAZ sangat erat kerja samanya dengan BSI, BKA (Organisasi Polisi Federal), BND (Badan Intelijen Federal), MAD (Badan Intelijen Militer) dan organisasi nasional lainnya di Jerman untuk menjaga aspek keamanan nasional. Tugas utama NCAZ adalah mendeteksi dan mencegah serangan terhadap infrastruktur nasional. Jerman juga telah mendirikan lembaga penelitian terbesar untuk keamanan TI di Eropa, Pusat Penelitian Keamanan dan Privasi (CRISP) di Darmstadt.

Lainnya

Tabel 8 mencantumkan sertifikasi ISMS lainnya yang ada saat ini.

Tabel 8. Sertifikasi ISMS Negara Lainnya

	Lembaga Akreditasi	Standar
Kanada	Lembaga Keamanan Komunikasi (CSE)	Pedoman Sertifikasi & Akreditasi untuk Sistem Teknologi Informasi MG-4 A
Jerman	Die Deutsche Akkreditierungsstelle GmbH (DAkkS)	
India	Badan Akreditasi Nasional untuk Laboratorium Pengujian dan Kalibrasi (NABL)	
Indonesia	Komite Akreditasi Nasional (KAN)	
Irlandia	Badan Akreditasi Nasional Irlandia (INAB)	
Selandia Baru	Akreditasi Internasional Selandia Baru (IANZ)	
Provinsi Taiwan, Cina	Biro Standar, Meteorologi dan Pemeriksaan	CNS 17799 & CNS 17800
Belanda	Dewan Akreditasi Belanda (DAC)	
Singapura	Komite Standar Teknologi Informasi	SS493: Bab 1 (Kerangka Standar Keamanan TI) & SS493: Bab 2 (Layanan Keamanan) dalam pengembangan
Republik Korea	Skema Akreditasi Laboratorium Korea (KOLAS)	
Vietnam	Biro Akreditasi	

5. Perlindungan Privasi

Bab ini bertujuan untuk:
- Melacak perubahan dalam konsep privasi;
- Menjelaskan tren internasional dalam perlindungan privasi; serta
- Memberikan contoh dan gambaran umum mengenai Penilaian Dampak Privasi

5.1. Konsep Privasi

Informasi pribadi adalah informasi apa pun yang berkaitan dengan individu yang dapat dikenali[56] atau orang yang dapat didentifikasi atau teridentifikasi.[57] Informasi pribadi mencakup berbagai informasi seperti nama individu, nomor telepon, alamat, alamat surel, nomor lisensi mobil, karakteristik fisik (dimensi wajah, sidik jari, tulisan tangan, dan lain-lain), nomor kartu kredit, serta hubungan keluarga.

Akses, pengumpulan, analisis, hingga penggunaan informasi pribadi seseorang yang tidak semestisnya dapat memengaruhi perilaku orang lain terhadap individu tersebut, dan pada akhirnya berdampak negatif pada status sosial, kekayaan, dan keamanannya. Oleh karena itu, informasi pribadi harus dilindungi dari akses, pengumpulan, penyimpanan, analisis, serta penggunaan yang tidak sah. Dalam pengertian ini, informasi pribadi merupakan subjek perlindungan.

Saat subjek perlindungan merupakan hak atas informasi pribadi daripada informasi pribadi itu sendiri, inilah yang disebut konsep privasi. Terdapat lima hal untuk menjelaskan hak atas privasi:

- Hak agar terbebas dari akses yang tidak diinginkan (misalnya, akses fisik dan akses melalui layanan pesan singkat);
- Hak untuk tidak mengizinkan informasi pribadi digunakan dengan cara yang tidak dikehendaki (misalnya, penjualan informasi, serta pembocoran dan pencocokan informasi);
- Hak untuk tidak mengizinkan informasi pribadi dikumpulkan oleh orang lain tanpa sepengetahuan dan persetujuan yang bersangkutan (misalnya, melalui penggunaan CCTV dan *cookies*);
- Hak untuk menyampaikan informasi pribadi secara akurat dan benar (integritas); serta
- Hak untuk mendapatkan imbalan atas nilai informasinya sendiri.

[56] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. (1995). *Official Journal of the European Communities*, *38*(281), 31–50. Diakses dari https://doi.org/https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN

[57] Organisation for Economic Co-operation and Development. *Privacy Online: OECD Guidance on Policy and Practice*. OECD. Diakses dari https://www.oecd.org/digital/ieconomy/privacyonlineoecdguidanceonpolicyandpractice.htm.

Konsep pasif privasi mencakup hak untuk membiarkan saja dan hak kodrati yang berkaitan dengan martabat manusia. Konsep ini terkait dengan hukum yang mencegah penyalahgunaan.

Konsep aktif privasi mencakup pengendalian diri atas informasi pribadi atau hak untuk mengelola/mengendalikan informasi pribadi secara positif, termasuk hak melakukan koreksi terhadap efek yang ditimbulkan oleh informasi pribadi yang tidak benar.

5.2. Berbagai Tren dalam Kebijakan Privasi

Pedoman OECD tentang Perlindungan Privasi

Pada tahun 1980, OECD mengadopsi *Pedoman terkait Perlindungan Privasi dan Arus Lintas Batas Data Pribadi*, yang juga dikenal sebagai *Praktik Informasi yang Adil (Fair Information Practices) OECD*. Pada tahun 2002, *Privasi Online: Pedoman OECD terkait Praktik dan Kebijakan* diumumkan.[58] Pedoman ini berlaku untuk data pribadi, baik di sektor publik atau swasta, yang dapat membahayakan privasi dan kebebasan individu karena cara informasi tersebut diproses atau karena sifat ataupun konteks penggunaannya. Prinsip OECD dalam Pedoman tersebut menjelaskan hak dan kewajiban individu dalam konteks pemrosesan data pribadi secara otomatis, serta hak dan kewajiban mereka yang terlibat dalam pemrosesan tersebut. Selanjutnya, prinsip-prinsip dasar yang dijelaskan dalam Pedoman tersebut dapat diterapkan di tingkat nasional dan internasional.

Delapan prinsip yang membentuk Pedoman OECD tentang Perlindungan Privasi adalah sebagai berikut:

1. **Prinsip pembatasan pengumpulan (data)**

Harus terdapat batasan dalam pengumpulan data pribadi. Data tersebut harus diperoleh dengan cara yang sah dan adil, tepat, serta dengan sepengetahuan atau persetujuan dari subjek data.

2. **Prinsip kualitas data**

Data pribadi harus relevan dengan tujuan penggunaannya, sejauh yang diperlukan tujuannya, serta harus akurat, lengkap, dan mutakhir *(up-to-date)*.

3. **Prinsip spesifikasi tujuan**

Tujuan pengumpulan data pribadi harus ditentukan paling tidak pada saat pengumpulan data. Untuk penggunaan selanjutnya terbatas pada pemenuhan tujuan atau hal lain yang tidak sesuai dengan tujuan, sebagaimana ketentuan di setiap alasan perubahan tujuan.

[58] OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* 9–17 (2013). Paris, Perancis. Diakses dari https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

4. Prinsip batasan penggunaan

Data pribadi tidak boleh diperlihatkan, disediakan atau digunakan untuk tujuan selain yang ditentukan sesuai dengan prinsip spesifikasi tujuan kecuali dengan persetujuan subjek data atau oleh otoritas hukum.

5. Prinsip jaminan keamanan

Data pribadi harus dilindungi oleh jaminan keamanan yang layak terhadap risiko seperti kehilangan atau akses tidak sah, perusakan, pemanfaatan, perubahan, atau pembukaan data.

6. Prinsip keterbukaan

Harus ada kebijakan umum keterbukaan terkait perkembangan, praktik, dan kebijakan yang berhubungan dengan data pribadi. Sarana harus tersedia untuk menentukan wujud dan sifat data pribadi, serta tujuan utama penggunaannya, sekaligus identitas dan tempat tinggal pengendali data *(data controller)* pada umumnya.

7. Prinsip partisipasi individu

Setiap individu harus memiliki hak untuk:

a. Memperoleh konfirmasi dari pengendali data apakah ia memiliki data yang berhubungan dengan dirinya;
b. Menerima komunikasi terkait data tentang dirinya dalam waktu yang wajar, dengan biaya yang tidak berlebihan (jika ada), dengan cara yang wajar, dan dalam bentuk yang mudah dimengerti oleh dirinya;
c. Menerima alasan saat permintaan terkait poin (a) dan (b) ditolak, dan dapat mengajukan keberatan terhadap penolakan tersebut; serta
d. Mengajukan keberatan atas data yang berkaitan dengannya dan meminta agar data tersebut dihapus, diperbaiki, dilengkapi, atau diubah saat pengajuan keberatannya berhasil dikabulkan.

8. Prinsip akuntabilitas

Seorang pengendali data harus bertanggung jawab untuk mematuhi langkah-langkah yang memengaruhi prinsip-prinsip yang telah disebutkan di atas.[59]

Pedoman PBB Terkait Perlindungan Privasi

Sejak akhir 1960-an, dunia telah mengamati efek privasi pemrosesan informasi secara otomatis. Organisasi Pendidikan, Keilmuan, dan Kebudayaan Perserikatan Bangsa-Bangsa

[59] UN General Assembly, Guidelines for the Regulation of Computerized Personal Data Files (1990). https://www.refworld.org/docid/3ddcafaac.html. Adopted by General Assembly resolution 45/95 of 14 December 1990. Contain procedures for implementing regulations concerning computerized personal data files.

(UNESCO) secara khusus memperhatikan privasi dan perlindungan privasi sejak *Pedoman PBB untuk Regulasi File Data Pribadi Terkomputerisasi* diadopsi oleh Majelis Umum PBB pada tahun 1990.

Pedoman Perserikatan Bangsa-Bangsa diterapkan pada berbagai dokumen (kertas) serta *file* data terkomputerisasi di sektor publik atau swasta. Pedoman tersebut menetapkan serangkaian prinsip mengenai jaminan minimum yang perlu disediakan undang-undang nasional atau dalam undang-undang internal organisasi internasional, sebagaimana berikut:

1. **Prinsip keabsahan dan keadilan**

Informasi terkait seseorang tidak boleh dikumpulkan atau diproses dengan cara yang tidak wajar atau melanggar hukum. Ia juga tidak boleh digunakan untuk tujuan yang bertentangan dengan tujuan dan prinsip Piagam Perserikatan Bangsa-Bangsa.

2. **Prinsip akurasi**

Orang yang bertanggung jawab atas penghimpunan *file* atau mereka yang bertanggung jawab menyimpannya berkewajiban melakukan pemeriksaan rutin terkait keakuratan dan relevansi data yang terekam (tercatat) serta memastikan bahwa *file* tersebut disimpan selengkap mungkin untuk menghindari kesalahan karena kelalaian *(error of omission).* Ia juga harus memastikan bahwa *file* tersebut harus selalu diperbarui secara teratur atau saat informasi yang terkandung dalam sebuah *file* tersebut digunakan atau diproses.

3. **Prinsip spesifikasi tujuan**

Tujuan penyediaan *file* serta penetapan, pengesahan, dan waktu penetapan tujuan pemanfaatannya adalah terpublikasikan atau diketahui orang yang bersangkutan, dalam rangka memastikan setelahnya bahwa:

a. Seluruh data pribadi yang terkumpul dan tercatat tetap relevan dan memadai untuk tujuan yang sudah ditetapkan;
b. Tak satu pun dari data pribadi tersebut digunakan atau diperlihatkan untuk tujuan yang tidak sesuai dengan yang telah ditentukan kecuali dengan persetujuan dari orang yang bersangkutan; serta
c. Periode penyimpanan data pribadi tidak melampaui waktu untuk mencapai tujuan yang ditentukan.

4. **Prinsip akses orang yang berkepentingan**

Setiap orang yang dapat memberikan bukti identitas berhak mengetahui apakah informasi mengenai dirinya sedang diproses dan bisa mendapatkannya dalam bentuk yang dapat dipahami, tanpa penundaan atau biaya yang tidak semestinya, serta mendapatkan perbaikan atau penghapusan yang sesuai jika terjadi pelanggaran hukum, entri yang tidak akurat atau tidak perlu dan kapan ia dikomunikasikan agar diinformasikan kepada si penerima.

5. Prinsip non-diskriminasi

Perihal beberapa pengecualian yang secara terbatas dipertimbangkan berdasarkan prinsip 6, yaitu data yang kemungkinan besar dapat menimbulkan diskriminasi yang melanggar hukum atau sewenang-wenang, seperti informasi terkait asal ras atau etnis, warna kulit, kehidupan seks, opini politik, agama, filosofis, dan anggapan lainnya serta keanggotaan dalam sebuah asosiasi atau serikat pekerja, tidak boleh dikompilasi (dihimpun).

6. Kemampuan untuk membuat pengecualian

Penyimpangan dari prinsip 1 hingga 4 diperbolehkan hanya jika diperlukan untuk melindungi keamanan nasional, ketertiban umum, moralitas atau kesehatan publik, sekaligus di antaranya, hak dan kebebasan orang lain, terutama orang yang dianiaya (pasal kemanusiaan), dengan catatan penyimpangan tersebut ditentukan secara tegas dalam undang-undang atau peraturan setara yang diberlakukan sesuai dengan sistem hukum internal yang secara jelas menyatakan batasannya dan menetapkan perlindungan yang sesuai.

Pengecualian terhadap prinsip 5 terkait larangan diskriminasi, selain bergantung pada perlindungan yang sama sebagaimana yang ditetapkan untuk pengecualian terhadap prinsip 1 dan 4, dapat diizinkan hanya dalam batas yang ditentukan oleh Undang-Undang Hak Asasi Manusia Internasional dan instrumen terkait lainnya di bidang perlindungan hak asasi manusia dan pencegahan diskriminasi.

7. Prinsip keamanan

Langkah yang tepat harus diambil untuk melindungi *file* dari bahaya yang lazim *(natural dangers)*, seperti kehilangan atau kerusakan yang tidak disengaja, dan bahaya karena ulah manusia *(human dangers)*, seperti akses yang tidak sah, penyalahgunaan data secara curang atau terkontaminasi oleh virus komputer.

8. Pengawasan dan sanksi

Hukum setiap negara akan menunjuk pihak yang berwenang, sesuai dengan sistem hukum yang berlaku di dalam negeri, untuk bertanggung jawab mengawasi ketaatan terhadap prinsip-prinsip yang ditetapkan di atas. Pihak berwenang tersebut harus memberikan jaminan ketidakberpihakan, terbebas dari orang atau badan yang bertanggung jawab untuk memproses dan menetapkan data, serta kewenangan yang bersifat teknis. Jika terjadi pelanggaran terhadap ketentuan hukum nasional yang menerapkan prinsip-prinsip di atas, maka hukuman pidana atau lainnya harus dipertimbangkan bersamaan dengan penegakan hukum yang sesuai.

9. Arus data lintas batas

Ketika undang-undang dua negara atau lebih yang berkaitan dengan aliran data lintas batas menawarkan perlindungan yang berimbang untuk perlindungan privasi, informasi harus dapat beredar secara bebas sebagaimana dalam setiap wilayah terkait. Jika tidak ada perlindungan timbal balik, pembatasan terhadap peredaran informasi semacam itu tidak boleh dipaksakan secara berlebihan dan hanya sejauh tuntutan perlindungan privasi saja.

10. Bidang penerapan

Prinsip-prinsip tersebut harus dapat diterapkan terlebih dahulu untuk seluruh *file* publik dan swasta terkomputerisasi serta *file* manual dengan cara tambahan opsional dan bergantung pada penyesuaian yang tepat. Ketentuan khusus, juga opsional, dapat dibuat untuk memperluas seluruh atau sebagian prinsip-prinsip tersebut terhadap berbagai *file* terkait subjek hukum, khususnya saat berisi informasi terkait berbagai individu.[60]

Privasi, etika, dan perlindungan data dirilis oleh Kelompok Pembangunan Perserikatan Bangsa-Bangsa (UNDG) dan berlaku untuk berbagai entitias UNDG.

Dokumen ini menjelaskan pedoman umum tentang privasi data, perlindungan data, dan etika data terkait penggunaan data besar, yang dikumpulkan secara *real time* oleh berbagai pihak swasta sebagai bagian dari penawaran bisnis mereka, dan dibagikan kepada anggota-anggota UNDG untuk tujuan memperkuat implementasi operasional program mereka demi mendukung suksesnya Agenda 2030.

Pedoman tersebut menjelaskan hal-hal sebagai berikut:

1. Penggunaan yang wajar, sah, dan diperbolehkan

Akses data, analisis data atau penggunaan data lainnya harus selaras dengan Piagam Perserikatan Bangsa-Bangsa dan dalam mendorong Tujuan Pembangunan Berkelanjutan.

2. Spesifikasi tujuan, batasan penggunaan, dan kesesuaian tujuan

Setiap penggunaan data harus sesuai atau relevan dan tidak melampaui batas kaitannya dengan tujuan data tersebut didapatkan.

3. Penilaian keuntungan dan kerugian risiko, serta mitigasi risiko

Penilaian keuntungan dan kerugian risiko yang memperhitungkan perlindungan dan privasi data serta etika penggunaan data harus dilakukan sebelum menggunakan data baru atau data yang berubah secara substansial.

4. Data sensitif dan konteks sensitif

Standar perlindungan data yang lebih ketat harus diterapkan saat memperoleh, mengakses, mengumpulkan, menganalisis atau menggunakan data terkait populasi dan orang-orang yang rentan terkena risiko, anak-anak dan remaja, atau data sensitif lainnya.

[60] Tan, D. R. (1999). Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United Stats and European Union. *Loyola of Los Angeles International and Comparative Law Review*, *21*(4). Diakses dari https://digitalcommons.lmu.edu/ilr/vol21/iss4/5.

5. Keamanan data

Keamanan data sangat penting dalam rangka memastikan privasi dan perlindungan data. Dengan mempertimbangkan teknologi yang tersedia dan biaya implementasi, pengamanan dan prosedur teknis serta organisasi yang kuat (termasuk pemantauan yang efisien terhadap akses data dan prosedur pemberitahuan pelanggaran data) harus diterapkan untuk memastikan pengelolaan data yang tepat sepanjang siklus hidup data sekaligus mencegah penggunaan, penyingkapan, atau pelanggaran data pribadi apapun yang tidak sah.

6. Retensi data dan minimalisasi data

Akses data, analisis data atau penggunaan data lainnya harus dijaga seminimal mungkin untuk memenuhi tujuannya. Jumlah data, termasuk perinciannya, harus dibatasi seminimal mungkin. Penggunaan data harus dipantau untuk memastikan bahwa data tersebut tidak melampaui kebutuhan penggunaannya yang sah.

7. Kualitas data

Semua aktivitas terkait data harus dirancang, dilaksanakan, dilaporkan, dan didokumentasikan dengan tingkat kualitas dan transparansi yang memadai. Terlebih, perlu adanya validasi keakuratan, relevansi, kecukupan, integritas, kelengkapan, kegunaan, validitas, koherensi, dan kemutakhiran data jika memungkinkan.

8. Data terbuka, transparansi, dan akuntabilitas

Mekanisme tata kelola dan akuntabilitas yang tepat harus ditetapkan dalam rangka memantau kepatuhan terhadap hukum yang relevan, termasuk undang-undang privasi dan standar kerahasiaan tertinggi, kode etik dan moral sehubungan dengan penggunaan data.

9. Uji tuntas *(due diligence)* untuk kolaborator pihak ketiga

Kolaborator pihak ketiga yang terlibat dalam penggunaan data harus bertindak sesuai dengan hukum yang relevan, seperti undang-undang privasi, sekaligus standar kerahasiaan serta kode etik dan moral tertinggi.

Perlindungan Data Uni Eropa[61]

Dewan Menteri atau Dewan Uni Eropa (UE) pada awalnya mengadopsi *Pedoman Eropa tentang Perlindungan Individu yang Menyangkut Pemrosesan dan Pergerakan Bebas Data Pribadi* (Pedoman UE 95/46/EC) pada tanggal 24 Oktober 1995 untuk menyediakan kerangka peraturan demi menjamin pergerakan data pribadi yang aman dan bebas melintasi perbatasan

[61] EUR-Lex, Peraturan (UE) 2016/679 Parlemen dan Dewan Eropa pada 27 April 2016 tentang perlindungan perorangan terkait dengan pemrosesan dan pergerakan bebas data pribadi, serta pencabutan Pedoman 95/46/EC (Peraturan Perlindungan Data Umum) (2016). Diakses dari https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504.

nasional negara-negara anggota Uni Eropa, selain menetapkan dasar keamanan informasi pribadi di mana pun ia disimpan, dikirim, atau diproses.

Pedoman ini dicabut pada April 2016 dengan adanya Peraturan (UE) 2016/679 yang memperkuat hak-hak dasar individu di era digital dan memfasilitasi bisnis dengan mengklarifikasi aturan untuk berbagai perusahaan dan badan publik di pasar digital tunggal. Sebuah undang-undang juga akan menghapus fragmentasi saat ini dalam berbagai sistem nasional, sekaligus hal administratif tidak penting lainnya. Peraturan (UE) 2016/679 mulai muncul pada 24 Mei 2016 dan berlaku sejak 25 Mei 2018.

Perlindungan Privasi di Amerika Serikat

Amerika Serikat (AS) mempercayakan aktivitas perlindungan privasi ke pasar yang ada karena terlalu banyak pembatasan pemerintah yang menghambat aktivitas *e-commerce*. Akibatnya, segel privasi *(privacy seals)* seperti *Trust-e* atau *Better Business Bureau Online* muncul, dan undang-undang tentang perlindungan privasi belum terintegrasi. Undang-Undang Privasi tahun 1974 memberikan perlindungan privasi informasi di sektor publik sementara undang-undang yang berbeda mengatur privasi di sektor swasta. Belum ada organisasi yang menangani masalah perlindungan privasi di sektor swasta. Di sektor publik, Kantor Manajemen dan Anggaran AS (OMB) berperan dalam penetapan kebijakan privasi pemerintah federal sesuai dengan Undang-Undang Privasi. Di sektor swasta, Komisi Perdagangan Federal berwenang untuk menjalankan undang-undang yang melindungi privasi daring anak-anak, informasi kredit pelanggan, dan praktik perdagangan yang adil.

Undang-undang Amerika Serikat terkait dengan perlindungan privasi meliputi:

- Undang-Undang Privasi, 1974
- Undang-Undang Perlindungan Kredit Konsumen (CCPA), 1984
- Undang-Undang Privasi Komunikasi Elektronik (ECPA), 1986
- Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan (HIPAA), 1996
- Undang-Undang Perlindungan Privasi Online Anak-anak (COPPA), 1998
- Undang-Undang *Gramm-Leach-Bliley* (GLBA), 1999
- Undang-Undang *Sarbanes-Oxley* (SOx), 2002
- Undang-Undang Manajemen Keamanan Informasi Federal (FISMA), 2002

Di samping itu, terdapat pula undang-undang privasi yang diberlakukan untuk setiap negara bagian di Amerika Serikat.

Pertanyaan:

1. Di negara Anda, undang-undang dan kebijakan apakah yang berlaku untuk melindungi privasi informasi?

2. Isu atau pertimbangan apakah yang membuat kebijakan dan undang-undang tersebut diberlakukan dan/atau diterapkan?

3. Prinsip apakah (lihat Pedoman OECD dan Pedoman PBB) yang menurut Anda mendukung kebijakan dan undang-undang mengenai perlindungan privasi di negara Anda?

5.3. Penilaian Dampak Privasi (PIA)

Apa itu PIA?

Penilaian Dampak Privasi atau *Privacy Impact Assessment* (PIA) merupakan proses sistematis dari penyelidikan, analisis, dan evaluasi pengaruh pengenalan sistem informasi baru atau modifikasi sistem informasi yang ada terhadap privasi pelanggan atau negara. PIA didasarkan pada prinsip pencegahan awal, artinya mencegah lebih baik daripada mengobati. PIA bukan hanya evaluasi sistem, melainkan juga pertimbangan efek serius terhadap privasi dalam memperkenalkan atau mengubah sistem baru. Dengan demikian, PIA berbeda dengan audit perlindungan privasi yang berfungsi untuk memastikan kepatuhan terhadap kebijakan internal dan kebutuhan eksternal untuk privasi.

Karena PIA dilakukan untuk menganalisis faktor pelanggaran privasi saat sistem baru dibangun, PIA harus dilakukan pada tahap awal pengembangan, saat penyesuaian spesifikasi pengembangan sistem masih memungkinkan. Namun, saat terdapat risiko pelanggaran serius dalam pengumpulan, penggunaan, dan pengelolaan informasi pribadi saat mengoperasikan layanan yang ada, sebaiknya lakukan PIA dan selanjutnya modifikasi sistem yang sesuai.

Proses PIA[62]

PIA umumnya terdiri dari tiga langkah (lihat Tabel 9).

[62] Komisaris Privasi dan Informasi Ontario, Rencana Sukses: Pedoman Penilaian Dampak Privasi (2015). Diakses dari https://www.ipc.on.ca/wp-content/uploads/2015/05/planning-for-success-pia-guide.pdf.

Tabel 9. Proses PIA

Analisis Konseptual	Analisis Aliran Data	Analisi Tindak Lanjut
Menyiapkan deskripsi bahasa sederhana mengenai ruang lingkup serta dasar atau alasan bisnis dari inisiatif yang diusulkan. Mengidentifikasi sejak dini potensi masalah dan risiko privasi, serta pemangku kepentingan utama *(key stakeholders)*. Memberikan penjelasan rinci mengenai aspek-aspek penting usulan, termasuk analisis kebijakan dari berbagai masalah penting. Mendokumentasikan arus utama informasi pribadi. Mengumpulkan tinjauan masalah lingkungan untuk meninjau ulang bagaimana yurisdiksi lain menangani inisiatif serupa. Mengidentifikasi kepentingan dan persoalan para pemangku kepentingan. Mengkaji reaksi publik.	Menganalisis aliran data melalui diagram proses bisnis dan mengidentifikasi elemen data pribadi atau kelompok data tertentu. Menilai kesesuaian usulan dengan kebebasan informasi (FOI) serta undang-undang privasi dan undang-undang program yang relevan. Menilai kesesuaian usulan yang lebih luas dengan prinsip privasi secara umum. Menganalisis risiko berdasarkan analisis privasi inisiatif dan mengidentifikasi solusi yang mungkin. Meninjau opsi desain dan identifikasi masalah/persoalan privasi yang belum tertangani. Mempersiapkan respons atau penanganan untuk masalah privasi yang belum terselesaikan.	Meninjau dan menganalisis perangkat keras dan rancangan sistem dari inisiatif yang diusulkan untuk memastikan kesesuaian dengan kebutuhan rancangan privasi. Memberikan tinjauan akhir dari inisiatif yang diusulkan. Melakukan analisis privasi dan risiko dari setiap perubahan baru terhadap inisiatif usulan desain perangkat keras dan perangkat lunak untuk memastikan kesesuaian dengan FOI dan undang-undang privasi, undang-undang program yang relevan, serta prinsip privasi secara umum. Menyiapkan rencana komunikasi.

Sumber: Komisaris Informasi dan Privasi Ontario, Rencana Sukses: Pedoman Penilaian Dampak Privasi (PIA) (2015) 5. Diakses dari https://www.ipc.on.ca/wp-content/uploads/2015/05/planning-for-success-pia-guide.pdf.

Ruang Lingkup Penilaian PIA

PIA dilaksanakan saat:
1. Membangun sistem informasi baru yang akan menampung dan mengelola informasi pribadi dalam jumlah besar;
2. Menggunakan teknologi baru yang dapat mengganggu privasi;
3. Memodifikasi sistem informasi yang ada saat ini yang menyimpan dan mengelola informasi pribadi; serta
4. Mengumpulkan, menggunakan, menyimpan dan/atau menghancurkan informasi pribadi yang berarti risiko pelanggaran privasi dapat terjadi.

Akan tetapi, PIA tidak perlu dilakukan pada seluruh sistem informasi. PIA tidak perlu dilakukan jika hanya terjadi sedikit perubahan pada program dan sistem yang ada.

Contoh-Contoh Penerapan PIA

Kebutuhan PIA di Amerika Serikat
Undang-Undang *E-Government* 2002 *(E-Government Act of 2002)*, Bab 208, menetapkan kebutuhan lembaga untuk melakukan penilaian dampak privasi (PIA) terhadap sistem dan kumpulan informasi elektronik. Penilaian tersebut merupakan metode praktis untuk mengevaluasi privasi dalam sistem dan kumpulan informasi, serta jaminan terdokumentasi bahwa masalah privasi telah teridentifikasi dan cukup tertangani.

Kebutuhan PIA di Uni Eropa
Peraturan (UE) 2016/679 alias Peraturan Perlindungan Data Umum (GDPR) mengharuskan penilaian dampak perlindungan data (DPIA) dalam beberapa kasus. Selain sistem dan proyek TI baru, pendekatan PIA juga perlu untuk tinjauan atau audit berkala terstruktur atas aturan privasi organisasi.

Tabel 10 berikut menunjukkan berbagai sistem PIA di tiga negara.

Tabel 10. Contoh PIA Nasional

	Amerika Serikat	Kanada	Australia/Selandia Baru
Dasar Hukum	Bab 208 Undang-Undang *e-Government* tahun 2002. OMB menyediakan kebutuhan PIA dalam OMB-M-03-22.	Memperkenalkan kebijakan dan pedoman PIA pada Mei 2002. Pelaksanaan PIA wajib atas dasar hukum umum terkait privasi.	Melakukan PIA secara sukarela (tidak ada dasar hukum). Buku Pegangan PIA untuk menunjang PIA (2004, Selandia Baru), pedoman untuk PIA (2004, Australia).

Subjek	Seluruh departemen dan lembaga cabang eksekutif serta kontraktor yang menggunakan TI atau yang mengoperasikan situs web untuk tujuan berinteraksi dengan publik; inisiatif lintas-lembaga yang relevan, termasuk yang mendorong *e-government*.	Seluruh program dan layanan yang disediakan lembaga pemerintah.	Tidak ada kewajiban atau batasan.
Pelaku	Berbagai instansi yang melakukan proyek *e-government* terkait informasi pribadi.	Instansi pemerintah yang mengembangkan atau menjalankan berbagai program dan layanan.	Instansi terkait atau dengan meminta intansi atau lembaga konsultasi eksternal.
Publikasi	Menyediakan PIA untuk umum melalui situs web instansi tertentu, publikasi di Daftar Federal *(Federal Register)* atau cara lain yang dapat diubah atau dikecualikan untuk alasan keamanan, atau untuk melindungi informasi yang bersifat pribadi, rahasia, atau sensitif yang terkandung dalam penilaian. Berbagai instansi harus memberikan salinan PIA kepada Direktur OMB untuk setiap sistem yang meminta pendanaan.	Menyediakan ringkasan PIA untuk umum. Memberikan salinan PIA versi akhir dan melapor sebelumnya ke Kantor Komisaris Privasi (Office of the Privacy Commissioner) untuk mendapatkan saran atau pedoman yang tepat terkait dengan strategi perlindungan yang tepat.	Hasil PIA biasanya tidak tersedia untuk publik (tidak ada kewajiban untuk melaporkan dan mempublikasikan).

Uji Kompetensi

1. Apa perbedaan antara informasi pribadi dengan jenis informasi lainnya?
2. Mengapa informasi pribadi harus dilindungi?
3. Apa pentingnya prinsip PBB dan OECD terhadap perlindungan privasi?
4. Mengapa penilaian dampak privasi (PIA) dilakukan?

6. Pembentukan dan Operasi CSIRT

Bab ini bertujuan untuk:

- Menjelaskan cara membentuk dan mengoperasikan Tim Tanggap Insiden Keamanan Komputer (CSIRT) nasional; dan
- Menyajikan berbagai model CSIRT dari berbagai negara.

Kejahatan siber dan berbagai ancaman terhadap keamanan informasi perlu ditanggapi serius karena dampak ekonominya yang sangat besar. Group-IB, sebuah perusahaan keamanan Rusia, memperkirakan bahwa pasar kejahatan siber secara global akan mencapai 2,5 miliar USD dan bergerak naik hingga lebih dari 7 miliar USD. Menurut survei penelitian IDC, hampir setengah perusahaan dari segala ukuran melaporkan bahwa dampak keseluruhan kerugian finansial dari setiap kejadian lebih dari 100.000 USD, sementara 8,5% perusahaan melaporkan kerugian finansial lebih dari 1 juta USD.

Pembentukan CSIRT merupakan cara efektif untuk mengurangi dan meminimalkan dampak serangan terhadap sistem informasi, serta pelanggaran keamanan informasi.

6.1. Pengembangan dan Operasi CSIRT

Tim Tanggap Keamanan Komputer (CSIRT) merupakan organisasi, semacam yang diformalkan atau *ad-hoc*, yang bertanggung jawab untuk menerima, meninjau, dan menanggapi laporan dan aktivitas insiden keamanan komputer. Tujuan dasar CSIRT adalah menyediakan layanan penanganan insiden keamanan komputer untuk meminimalkan dampak kerugian atau kerusakan dan perbaikan atau pemulihan dari insiden keamanan komputer secara efisien.[63]

Pada tahun 1988, wabah *worm* pertama bernama Morris terjadi dan menyebar dengan cepat ke seluruh dunia. Setelah kejadian tersebut, Badan Proyek Penelitian Lanjutan Pertahanan (DARPA) mendirikan Institut Rekayasa Perangkat Lunak dan kemudian membentuk CERT/CC di Universitas Carnegie Mellon di bawah kontrak Pemerintah Amerika Serikat. Sejak saat itu, setiap negara di Eropa membentuk organisasi serupa. Karena tidak ada satu pun CSIRT yang mampu menyelesaikan insiden kerentanan yang sangat luas, Forum Tim Keamanan dan Penanganan Insiden (FIRST) dibentuk pada tahun 1990. Melalui FIRST, banyak lembaga keamanan informasi dan CSIRT dapat bertukar pendapat dan berbagi informasi.

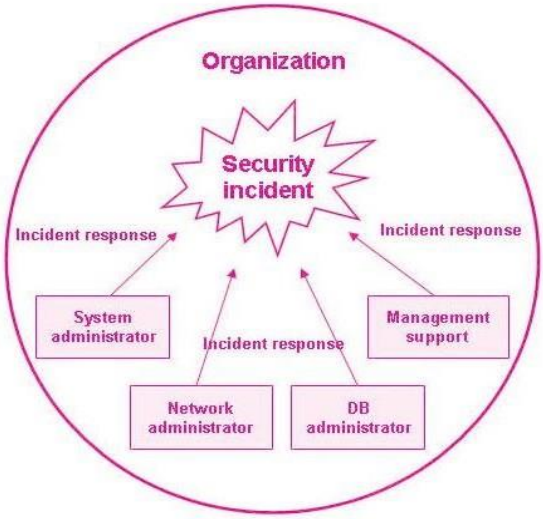
[63] Universitas Carnegie Mellon. (18 Januari 2017). Pertanyaan yang Sering Diajukan (FAQ) CSIRT. Diakses dari https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=485652.

Pemilihan Model CSIRT yang Tepat[64]

Terdapat lima model organisasi umum untuk CSIRT. Model yang paling sesuai untuk organisasi—sebagaimana pertimbangan berbagai kondisi seperti lingkungan, status keuangan, dan sumber daya manusia—harus diadopsi.

1. Model Tim Keamanan (Menggunakan Staf IT yang Ada Saat Ini)

Model tim keamanan bukanlah model CSIRT biasa. Faktanya, model tersebut merupakan kebalikan dari CSIRT biasa. Dalam model tersebut, tidak ada organisasi terpusat yang diberi tanggung jawab untuk menangani insiden keamanan komputer. Sebaliknya, tugas penanganan insiden dilakukan oleh administrator sistem dan jaringan atau oleh spesialis sistem keamanan lainnya.



Gambar 17. Model Tim Keamanan

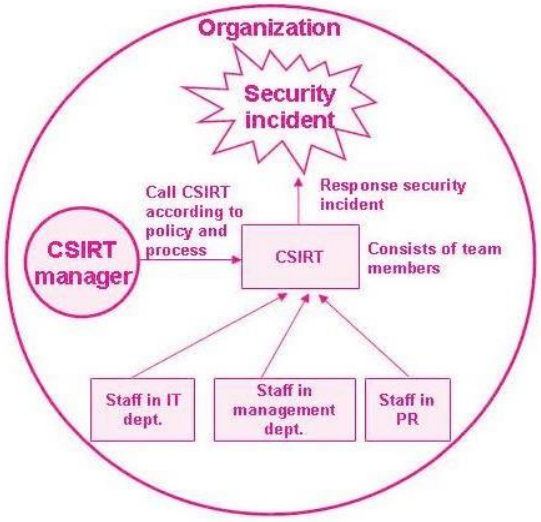
2. Model CSIRT Terdistribusi Internal

Model ini juga disebut sebagai “CSIRT terdistribusi”. Tim dalam model ini terdiri dari administrator CSIRT yang bertanggung jawab untuk pelaporan dan manajemen secara keseluruhan, serta staf dari divisi lain perusahaan/lembaga terkait. Model CSIRT ini merupakan organisasi yang diakui secara resmi yang bertanggung jawab menangani semua aktivitas penanganan insiden. Karena tim tersebut dibentuk di dalam sebuah perusahaan atau lembaga, maka ia disebut "internal".

Model CSIRT terdistribusi internal berbeda dengan model tim keamanan dalam beberapa hal berikut:

[64] Killcrece, G., Kossakowski, K.-P., Ruefle, R., & Zajicek, M. (2003). *Model Organisasi untuk Tim Respons Insiden Keamanan Komputer (CSIRTs)*. Institut Rekayasa Perangkat Lunak. Diakses dari 10.1184/R1/6575921.v1

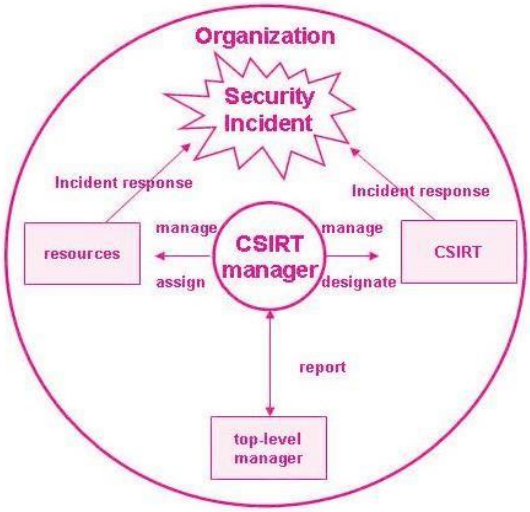
- Adanya kebijakan, prosedur dan proses penanganan insiden yang lebih formal;
- Metode komunikasi yang mapan dengan seluruh perusahaan terkait ancaman keamanan dan strategi penanganan; serta
- Manajer CSIRT yang ditunjuk dan anggota tim yang secara khusus ditugaskan untuk menangani insiden.



Gambar 18. Model CSIRT Terdistribusi Internal

3. Model CSIRT Terpusat Internal

Dalam model CSIRT terpusat internal, tim yang berlokasi di pusat mengontrol dan membantu organisasi. CSIRT bertanggung jawab secara keseluruhan terhadap seluruh pelaporan insiden, analisis dan tanggapan. Dengan demikian, anggota tim tidak dapat menangani pekerjaan lain dan menghabiskan seluruh waktu bekerja mereka untuk tim dan menangani semua insiden yang ada. Selain itu, manajer CSIRT melapor kepada manajemen puncak seperti *Chief Information Officer* (CIO), *Chief Security Officer* (CSO), atau *Chief Risk Officer* (CRO).

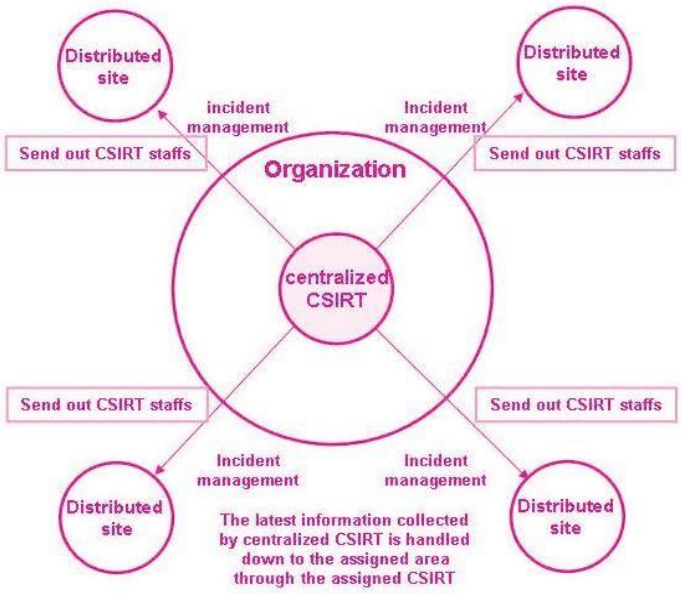


Gambar 19. Model CSIRT Terpusat Internal

4. Model CSIRT Gabungan Terdistribusi dan Terpusat

Model ini juga dikenal dengan sebutan "CSIRT Gabungan". Saat CSIRT terpusat tidak dapat mengontrol dan mendukung seluruh organisasi, beberapa anggota tim disebar di berbagai lokasi/cabang/divisi organisasi untuk memberikan tingkat layanan yang sama dalam wilayah tanggung jawab mereka sebagaimana layanan yang disediakan oleh CSIRT terpusat.

Model tim terpusat menyediakan analisis data tingkat tinggi, metode pemulihan atau perbaikan, dan strategi mitigasi. Model ini juga membekali anggota tim yang tersebar dengan dukungan penanganan insiden, kerentanan, dan artefak. Anggota tim yang tersebar di setiap lokasi menerapkan strategi dan mengerahkan keahlian di bidangnya.



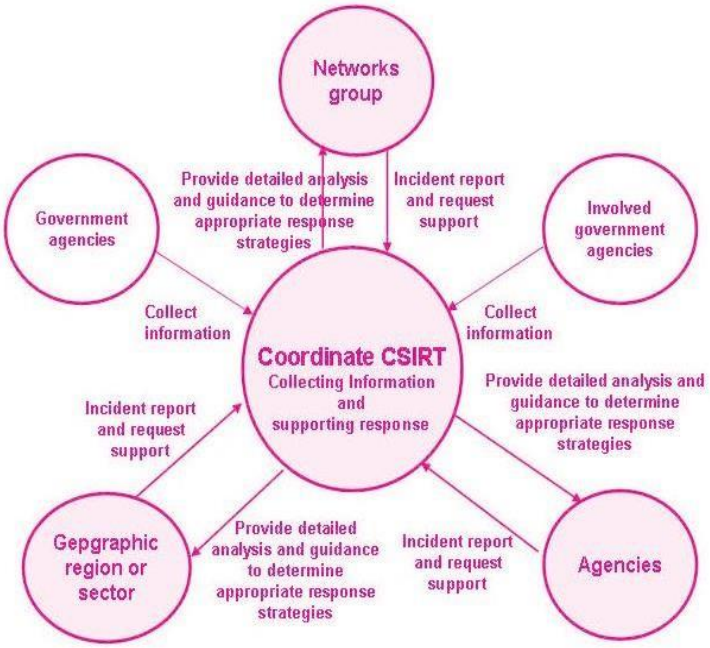
Gambar 20. CSIRT Gabungan

5. Model CSIRT Terkoordinasi

CSIRT terkoordinasi memperkuat fungsi tim yang tersebar dalam CSIRT gabungan. Dalam model CSIRT terkoordinasi, anggota tim dalam CSIRT gabungan dikelompokkan menjadi CSIRT independen berdasarkan karakteristik seperti konektivitas jaringan, batas geografis, dan sejenisnya. Mereka diatur oleh CSIRT terpusat.

Model CSIRT terkoordinasi cocok untuk sistem CSIRT nasional. Model ini dapat diterapkan pada kegiatan internal di sebuah organisasi dan untuk mendukung dan mengoordinasikan badan-badan eksternal secara erat.

Kegiatan koordinasi dan fasilitasi meliputi berbagi informasi, penyediaan strategi mitigasi, penanganan insiden, metode pemulihan, penelitian/analisis tren dan pola aktivitas insiden, basis data kerentanan, *clearing house* untuk perangkat keamanan, serta layanan konsultasi dan peringatan.



Gambar 21. CSIRT Terkoordinasi

Pembentukan CSIRT: Langkah-Langkah Membentuk CSIRT Nasional[65]

Terdapat lima tahapan dalam membentuk CSIRT. Tujuan, visi atau peran CSIRT harus menjadi pedoman sepanjang tahapan pengembangan yang ada.

Tahap 1 – Mengedukasi pemangku kepentingan terkait pengembangan tim nasional

Tahap 1 adalah tahap kesadaran, di mana para pemangku kepentingan membangun pemahaman mengenai apa saja yang terlibat dalam pembentukan CSIRT. Melalui berbagai metode edukasi, mereka belajar tentang:

a. Penggerak dan motivator bisnis di balik kepentingan CSIRT nasional;
b. Kebutuhan untuk membangun kemampuan penanganan insiden CSIRT nasional;
c. Mengidentifikasi orang-orang yang akan terlibat dalam pembahasan pembentukan tim nasional;
d. Sumber daya utama dan infrastruktur penting yang ada di dalam negeri;
e. Jenis-jenis saluran komunikasi yang perlu ditentukan untuk berkomunikasi dengan para konstituen CSIRT;
f. Undang-undang, peraturan dan kebijakan khusus lainnya yang akan memengaruhi pengembangan CSIRT nasional;
g. Strategi pendanaan yang dapat digunakan untuk mengembangkan, merencanakan, melaksanakan, dan mengoperasikan kemampuan penanganan;

[65] Killcrece, G. (2004). Steps for Creating National CSIRTs. Software Engineering Institute. Retrieved from https://resources.sei.cmu.edu/asset_files/WhitePaper/2004_019_001_53064.pdf

h. Infrastruktur teknologi dan jaringan informasi yang akan dibutuhkan untuk mendukung operasional tim nasional;
i. Rencana penanganan dasar dan interpendensi saat semuanya diterapkan di berbagai sektor;
j. Seperangkat layanan inti potensial yang dapat CSIRT nasional berikan kepada konstituennya; serta
k. Pedoman dan praktik terbaik *(best practices)*

Tahap 2 - Perencanaan CSIRT: Membangun pengetahuan dan informasi yang diperoleh selama Tahap 1

Tahap 2 menyangkut perencanaan CSIRT berdasarkan pengetahuan dan informasi yang diperoleh selama Tahap 1. Masalah-masalah yang dibahas dalam Tahap 1 ditinjau dan dibahas lebih lanjut, serta kemudian menetapkan detail yang tepat untuk diterapkan pada rencana implementasi. Rencana tersebut dibuat dengan mempertimbangkan hal-hal berikut:

a. Mengidentifikasi kebutuhan dan kepentingan CSIRT nasional —
   - Hukum dan regulasi yang dapat memengaruhi operasi tim nasional;
   - Sumber daya penting yang perlu diidentifikasi dan dilindungi;
   - Insiden dan tren terkini yang sedang dilaporkan atau harus dilaporkan; serta
   - Kemampuan penanganan insiden yang ada dan keahlian keamanan komputer.
b. Menetapkan visi CSIRT nasional.
c. Menetapkan misi tim nasional.
d. Menentukan konstituen yang akan dilayaninya.
e. Mengidentifikasi antarmuka komunikasi antara konstituen dan tim nasional.
f. Mengenali jenis sponsor, kepemimpinan, dan izin nasional (pemerintah).
g. Mengidentifikasi jenis keterampilan dan pengetahuan staf yang diperlukan untuk mengoperasikan tim.
h. Mendefinisikan jenis peran dan tanggung jawab CSIRT nasional.
i. Menentukan proses manajemen insiden CSIRT serta menentukan hubungannya dengan proses serupa di salah satu organisasi konstituen eksternal.
j. Mengembangkan seperangkat kriteria standar dan terminologi yang konsisten untuk mengategorikan dan mendefinisikan aktivitas dan kejadian insiden.
k. Menentukan bagaimana CSIRT nasional akan berinteraksi dengan konstituen dan CSIRT global lainnya atau mitra eksternal.
l. Menentukan proses apa saja yang diperlukan untuk integrasi dengan rencana pemulihan bencana *(disaster recovery)* yang ada, rencana penanganan insiden, rencana kontinuitas bisnis, manajemen krisis atau rencana manajemen darurat lainnya.
m. Membuat jadwal proyek.
n. Membuat rencana CSIRT nasional berdasarkan hasil dari kegiatan perencanaan, visi dan kerangka kerja yang sesuai.

Tahap 3 – Penerapan CSIRT

Pada Tahap 3, tim proyek memanfaatkan informasi dan rencana dari Tahap 1 dan 2 untuk mengimplementasikan CSIRT. Proses implementasinya adalah sebagai berikut:

a. Mendapatkan dana dari sumber yang diketahui selama tahap perencanaan.
b. Mengumumkan secara luas bahwa CSIRT nasional sedang dibuat dan di mana bisa mendapatkan informasi tambahan (mengenai progres pengembangan, kebutuhan pelaporan, dll.).
c. Menyusun mekanisme koordinasi dan komunikasi dengan para pemangku kepentingan dan koneksi lainnya.
d. Menerapkan sistem informasi dan infrastruktur jaringan yang aman untuk mengoperasikan CSIRT nasional (misalnya, server, aplikasi, alat telekomunikasi, dan sumber daya pendukung infrastruktur lainnya yang aman).
e. Mengembangkan operasi dan proses untuk staf CSIRT, seperti standar yang disepakati dalam tahap perencanaan dan pedoman pelaporan.
f. Mengembangkan kebijakan dan prosedur internal untuk akses dan pengoperasian peralatan CSIRT dan perlengkapan diri, serta kebijakan penggunaan yang dapat diterima.
g. Menerapkan proses interaksi CSIRT nasional dengan konstituennya.
h. Mengidentifikasi dan mempekerjakan (atau menugaskan kembali) personel, mencarikan pelatihan dan pendidikan yang sesuai untuk staf CSIRT, serta menentukan upaya dalam menjangkau potensi lainnya untuk melatih dan mengedukasi konstituen.

Tahap 4 – Pengoperasian CSIRT

Pada tahap operasional, perlu adanya penetapan layanan dasar yang harus CSIRT nasional berikan serta evaluasi efisiensi operasional untuk memanfaatkan kemampuan manajemen insiden. Berdasarkan hasil tersebut, detail operasional ditetapkan dan ditingkatkan. Adapun kegiatan-kegiatan pada tahap ini adalah:

a. Secara aktif melaksanakan berbagai layanan yang diberikan oleh CSIRT nasional.
b. Mengembangkan dan menerapkan mekanisme untuk mengevaluasi efektivitas operasi CSIRT nasional.
c. Perbaikan CSIRT nasional sesuai hasil evaluasi.
d. Mengembangkan misi, layanan, dan staf yang sesuai dan dapat dipertahankan untuk meningkatkan layanan kepada konstituen.
e. Terus mengembangkan dan menyempurnakan kebijakan dan prosedur CSIRT.

Tahap 5 – Kolaborasi

CSIRT nasional dapat membangun hubungan tepercaya dengan para pemangku kepentingan utama melalui operasi yang efisien (Tahap 4). Akan tetapi, CSIRT nasional juga perlu bertukar pengalaman penanganan insiden dan informasi penting melalui pertukaran jangka panjang dengan lembaga yang bekerja sama, yaitu CSIRT nasional dan CSIRT internasional. Adapun kegiatan pada tahap ini antara lain:

a. Berpartisipasi dalam kegiatan berbagi data dan informasi serta mendukung pengembangan standar untuk berbagi data dan informasi antara mitra, CSIRT lain, konstituen, dan para pakar keamanan komputer lainnya.
b. Berpartisipasi dalam kegiatan *watch and warning* global untuk mendukung komunitas CSIRT.

c. Meningkatkan kualitas kegiatan CSIRT dengan memberikan pelatihan, lokakarya, dan konferensi yang membahas tren serangan dan strategi penanganan.
d. Berkolaborasi dengan komunitas lainnya untuk mengembangkan dokumen dan pedoman praktik terbaik.
e. Meninjau dan merevisi proses manajemen insiden sebagai bagian dari proses perbaikan yang berkelanjutan.

Layanan CSIRT[66]

Layanan yang disediakan CSIRT dapat diklasifikasikan menjadi layanan reaktif, layanan proaktif, dan layanan manajemen kualitas layanan.

Layanan reaktif merupakan layanan inti CSIRT. Layanan tersebut antara lain:

1. **Siaga dan Peringatan *(Alerts and warnings)*** – Layanan ini mencakup penyediaan informasi dan metode penananganan masalah seperti kerentanan keamanan, peringatan gangguan, virus komputer, atau hoaks.

2. **Penanganan insiden** – Layanan ini mencakup penerimaan, penentuan seleksi (triase) dan respons permintaan dan laporan, serta analisis dan pemrioritasan kejadian dan peristiwa. Adapun aktivitas penanganan khusus adalah sebagai berikut:

    - **Analisis insiden** – Pemeriksaan atas seluruh informasi dan bukti pendukung yang tersedia atau artefak yang terkait dengan suatu insiden atau peristiwa. Tujuan dari analisis ini adalah untuk mengidentifikasi ruang lingkup insiden, tingkat kerusakan yang disebabkan oleh insiden tersebut, sifat insiden dan strategi penanganan atau solusi yang tersedia.

    - **Pengumpulan bukti forensik** – Pengumpulan, pemeliharaan, dokumentasi, dan analisis bukti dari sistem komputer yang disusupi *(compromised computer system)* untuk menentukan perubahan pada sistem serta untuk membantu rekonstruksi peristiwa yang mengarah pada penyusupan tersebut.

    - **Pelacakan atau penelusuran** – Mencakup pelacakan atau penelusuran bagaimana cara penyusup memasuki sistem dan jaringan terkait yang telah disusupinya. Kegiatan ini termasuk melacak asal-usul penyusup atau mengidentifikasi sistem yang aksesnya dimiliki penyusup.

3. **Penanganan insiden di tempat *(on site)*** – CSIRT memberikan bantuan langsung di tempat untuk membantu konstituen pulih dari insiden.

4. **Dukungan penanganan insiden** – CSIRT membantu dan membimbing korban serangan agar dapat pulih dari insiden melalui telepon, surel, faksimile, atau dokumentasi.

[66] CERT. (2002). Layanan CSIRT. Institut Rekayasa Perangkat Lunak. Diakses dari https://resources.sei.cmu.edu/asset_files/WhitePaper/2002_019_001_53048.pdf

5. **Koordinasi penanganan insiden** – Upaya penanganan di antara pihak-pihak yang terlibat dalam insiden tersebut terkoordinasi. Hal ini biasanya mencakup korban serangan, lokasi lain yang terlibat dalam serangan tersebut, dan di manapun yang membutuhkan bantuan analisis serangan. Hal ini mungkin juga termasuk pihak-pihak yang memberikan dukungan IT kepada korban, seperti ISP dan CSIRT lainnya.

6. **Penanganan kerentanan** – Layanan ini mencakup penerimaan informasi dan laporan tentang kerentanan perangkat keras dan perangkat lunak, menganalisis efek kerentanan, dan mengembangkan strategi penanganan untuk mendeteksi dan memperbaiki kerentanan.

    - **Analisis kerentanan** – Mengacu pada analisis teknis dan pemeriksaan kerentanan dalam perangkat keras atau perangkat lunak. Termasuk pula dalam analisis ini adalah meninjau kode sumber, menggunakan *debugger* untuk menentukan lokasi terjadinya kerentanan, atau berupaya meniru ulang *(reproduce)* permasalahan pada sistem pengujian.

    - **Penanganan kerentanan** – Mencakup penentuan respons atau penanganan yang tepat untuk memitigasi atau memperbaiki kerentanan. Layanan ini dapat mencakup tindakan penanganan dengan memasang tambalan *(patch)*, perbaikan, atau solusi sementara *(workaround)*. Layanan ini juga menginformasikan strategi mitigasi, laporan atau peringatan lainnya.

    - **Koordinasi penanganan kerentanan** – CSIRT menginformasikan berbagai macam perusahaan atau konstituen mengenai kerentanan dan berbagi informasi serta bagaimana cara memperbaiki atau memitigasinya. CSIRT juga melakukan klasifikasi strategi penanganan kerentanan yang berhasil. Kegiatannya mencakup analisis kerentanan atau laporan kerentanan dan menyintesis analisis teknis yang dilakukan oleh berbagai pihak. Layanan ini juga dapat mencakup pemeliharaan arsip publik atau pribadi atau basis pengetahuan informasi kerentanan dan strategi penanganan yang sesuai.

7. **Penanganan artefak** – Layanan ini mencakup analisis, penanganan, koordinasi, dan penanganan artefak-artefak seperti virus komputer, program *trojan horse*, *worm, exploit scripts*, dan *toolkit*.

    - Analisis artefak – CSIRT melakukan pemeriksaan teknis dan analisis artefak yang ditemukan dalam sistem.

    - Penanganan artefak – Mencakup penentuan langkah yang tepat untuk mendeteksi dan menghapus artefak dari sistem.

    - Koordinasi penanganan artefak – Mencakup kegiatan berbagi dan menyintesis hasil analisis dan strategi penanganan terkait artefak dengan peneliti lainnya, CSIRT, vendor, dan pakar keamanan lainnya.

Layanan proaktif adalah meningkatkan infrastruktur dan proses keamanan konstituen sebelum insiden atau peristiwa apa pun terjadi atau terdeteksi. Yang termasuk dalam layanan ini antara lain:

1. **Pemberitahuan** – Termasuk dalam hal ini adalah peringatan intrusi (gangguan), peringatan kerentanan, laporan keamanan, dan sejenisnya. Pemberitahuan tersebut memberi tahu konstituen mengenai berbagai perkembangan baru dengan dampak jangka menengah hingga panjang, seperti kerentanan yang baru ditemukan atau perangkat penyusup. Pemberitahuan dapat membuat konstituen melindungi sistem dan jaringan mereka dari masalah yang baru ditemukan sebelum akhirnya dapat dimanfaatkan.

2. **Pengawasan teknologi** – Layanan ini mencakup pemantauan dan pengamatan pengembangan teknis yang baru, aktivitas penyusup dan tren terkait dalam rangka membantu mengidentifikasi ancaman di masa mendatang. Hasil dari layanan ini dapat berupa beberapa jenis pedoman atau rekomendasi yang berfokus pada masalah keamanan jangka menengah hingga panjang.

3. **Audit atau penilaian keamanan** – Layanan ini memberikan tinjauan terperinci serta analisis infrastruktur keamanan organisasi, berdasarkan kebutuhan yang ditetapkan oleh organisasi atau oleh standar industri lain yang berlaku.

4. **Konfigurasi serta pemeliharaan perangkat, aplikasi, infrastruktur dan layanan keamanan** – Layanan ini memberikan pedoman yang sesuai mengenai cara konfigurasi serta pemeliharaan perangkat, aplikasi, dan infrastruktur komputasi umum secara aman.

5. **Pengembangan perangkat keamanan** – Layanan ini mencakup pengembangan alat (*tools)*, perangkat lunak, *plug-in*, dan *patch* baru khusus untuk konstituen yang dikembangkan dan didistribusikan untuk keamanan.

6. **Layanan deteksi gangguan (penyusupan)** – CSIRT yang melakukan layanan ini meninjau log IDS yang ada, menganalisisnya, dan memulai langkah penanganan untuk kejadian-kejadian yang mencapai ambang batas yang telah ditentukan.

7. **Penyebaran informasi terkait keamanan** – Layanan ini membuat konstituen mendapatkan kumpulan informasi berguna serta lengkap dan mudah ditemukan yang dapat membantu meningkatkan keamanan.

Layanan manajemen kualitas keamanan dirancang untuk mendapatkan pengetahuan dari hasil penanganan insiden, kerentanan, dan serangan secara sintetis. Layanan-layanan tersebut meliputi:

1. **Analisis risiko** – Layanan ini mencakup peningkatan kemampuan CSIRT untuk menilai ancaman nyata, memberikan penilaian risiko kualitatif dan kuantitatif yang realistis terhadap aset informasi, serta mengevaluasi strategi perlindungan dan penanganan.

2. **Perencanaan kontinuitas bisnis (BCP) dan pemulihan bencana (DRP)** – Kontinuitas bisnis dan pemulihan dari bencana yang disebabkan oleh serangan keamanan komputer dipastikan melalui perencanaan yang cukup memadai.

3. **Konsultasi keamanan** – CSIRT juga dapat memberikan saran dan pedoman praktis untuk operasi bisnis.

4. **Membangun kesadaran** – CSIRT dapat meningkatkan kesadaran keamanan dengan mengidentifikasi dan memberikan informasi serta pedoman tentang praktik dan kebijakan keamanan yang diperlukan oleh konstituen.

5. **Edukasi/Pelatihan** – Layanan ini mencakup pemberian pendidikan dan pelatihan tentang topik-topik seperti pedoman pelaporan insiden, metode penanganan yang tepat, perangkat penanganan insiden, metode pencegahan insiden, dan informasi lain yang diperlukan untuk melindungi, mendeteksi, melaporkan, dan menangani insiden keamanan komputer. Adapun jenis pelatihannya meliputi seminar, lokakarya, kursus, dan tutorial.

6. **Evaluasi atau sertifikasi produk** – CSIRT dapat melakukan evaluasi produk pada perangkat, aplikasi, atau layanan lain untuk memastikan keamanan produk dan kesesuaiannya dengan CSIRT atau praktik keamanan organisasi yang sesuai.

Tabel 11 menunjukkan tingkat setiap layanan CSIRT — apakah ia termasuk layanan inti, layanan tambahan, atau layanan tidak biasa —dalam setiap model CSIRT.

Tabel 11. Layanan CSIRT

Kategori Layanan	Layanan		Tim Keamanan	Model Terdistribusi	Model Terpusat	Model Gabungan	Model Terkoordinasi
Reaktif	Siaga dan Peringatan		Tambahan	Inti	Inti	Inti	Inti
	Penanganan Insiden	Analisis insiden	Inti	Inti	Inti	Inti	Inti
		Penanganan Insiden di Tempat	Inti	Tambahan	Tambahan	Tambahan	Tidak biasa
		Dukungan Penanganan Insiden	Tidak biasa	Inti	Inti	Inti	Inti
		Koordinasi Penanganan Insiden	Inti	Inti	Inti	Inti	Inti
	Penanganan Artefak	Analisis Kerentanan	Tambahan	Tambahan	Tambahan	Tambahan	Tambahan
		Penanganan Kerentanan	Inti	Tambahan	Tidak biasa	Tambahan	Tambahan
		Koordinasi Penanganan Kerentanan	Tambahan	Inti	Inti	Inti	Inti
		Analisis Artefak	Tambahan	Tambahan	Tambahan	Tambahan	Tambahan
		Penanganan Artefak	Inti	Tambahan	Tambahan	Tambahan	Tambahan

		Koordinasi Penanganan Artefak	Tambahan	Tambahan	Inti	Inti	Inti
Proaktif	Pemberitahuan		Tidak biasa	Inti	Inti	Inti	Inti
	Pengawasan Teknologi		Tidak biasa	Tambahan	Inti	Inti	Inti
	Audit atau Penilaian Keamanan		Tidak biasa	Tambahan	Tambahan	Tambahan	Tambahan
	Konfigurasi dan Pemeliharaan Perangkat, Aplikasi, Infrastruktur, dan Layanan Keamanan		Inti	Tambahan	Tambahan	Tambahan	Tidak biasa
	Pengembangan Perangkat Keamanan		Tambahan	Tambahan	Tambahan	Tambahan	Tambahan
	Layanan Deteksi Gangguan (Penyusupan)		Inti	Tambahan	Tambahan	Tambahan	Tidak biasa
	Penyebaran Informasi Terkait Keamanan		Tidak biasa	Tambahan	Inti	Inti	Inti
Manajemen kualitas keamanan	Analisis Risiko		Tidak biasa	Tambahan	Tambahan	Tambahan	Tambahan
	Perencanaan Kontinuitas Bisnis (BRP) dan Pemulihan Bencana (DRP)		Tidak biasa	Tambahan	Tambahan	Tambahan	Tambahan
	Konsultasi Keamanan		Tidak biasa	Tambahan	Tambahan	Tambahan	Tambahan
	Membangun Kesadaran		Tidak biasa	Tambahan	Tambahan	Tambahan	Inti
	Edukasi/Pelatihan		Tidak biasa	Tambahan	Tambahan	Tambahan	Inti
	Evaluasi atau Sertifikasi Produk		Tidak biasa	Tambahan	Tambahan	Tambahan	Tambahan

Sumber:
Killcrece, G., Kossakowski, K.-P., Ruefle, R., & Zajicek, M. (2003). *Organizational Models for Computer Security Incident Response Teams (CSIRTs)*. Software Engineering Institute. Diakses dari 10.1184/R1/6575921.v1

6.2. Asosiasi CSIRT Internasional

Saat ini, terdapat sejumlah CSIRT internasional yang khusus dibentuk untuk menangani insiden keamanan komputer di seluruh dunia. Ketika CSIRT nasional dapat menangani serangan dan melaksanakan fungsi lainnya, serangan internasional membutuhkan perhatian dari CSIRT internasional.

Forum Tim Keamanan dan Penanganan Insiden (FIRST)[67]

Forum Tim Keamanan dan Penanganan Insiden atau Forum of Incident Response Security Teams (FIRST) terdiri dari CERT, lembaga pemerintah dan perusahaan keamanan dari 52 negara. Keanggotaannya mencakup 248 organisasi, termasuk CERT/CC dan US-CERT (per

[67] Forum of Incident Response and Security Teams, Inc. (2020). *About FIRST*. FIRST. http://www.first.org/about.

September 2011). FIRST merupakan lembaga untuk kegiatan berbagi informasi dan kerja sama di antara tim penanganan insiden. Tujuannya adalah untuk mengaktifkan kegiatan perlindungan dan penanganan insiden serta mendorong kerja sama antar anggota dengan membekali mereka teknologi, pengetahuan dan perangkat untuk penanganan insiden. Adapun aktivitas FIRST adalah sebagai berikut:

- Mengembangkan dan berbagi praktik terbaik, prosedur, perangkat, informasi teknis, dan metodologi untuk perlindungan dan penanganan insiden;
- Mendorong pengembangan kebijakan, pelayanan dan keamanan produk yang berkualitas baik;
- Mendukung dan mengembangkan pedoman keamanan komputer yang sesuai;
- Membantu pemerintah, perusahaan, dan lembaga pendidikan untuk membentuk tim tanggap insiden dan mengembangkannya; serta
- Memfasilitasi kegiatan berbagi teknologi, pengalaman dan pengetahuan di antara anggota untuk lingkungan elektronik yang lebih aman.

6.3. Asosiasi CSIRT Regional

CERT Asia-Pasifik[68]

Tim Tanggap Darurat Komputer Asia-Pasifik atau Asia-Pacific Computer Emergency Response Team (APCERT) yang dibentuk pada bulan Februari 2003 berfungsi sebagai jaringan para ahli keamanan, memperkuat penanganan insiden, dan meningkatkan kesadaran keamanan di Kawasan Asia-Pasifik. Konferensi CSIRT Asia-Pasifik pertama digelar di Jepang pada tahun 2002. APCERT terbentuk setahun kemudian di sebuah konferensi di Taipei yang dihadiri oleh 14 CSIRT Asia-Pasifik. Per September 2011, APCERT telah memiliki 18 anggota tetap dan 9 anggota umum dari 18 negara.

Anggota APCERT sepakat bahwa insiden keamanan komputer saat ini sangat banyak, kompleks, dan sulit dikendalikan oleh satu organisasi atau negara mana pun, sementara penanganan yang lebih efektif dapat diterapkan dengan kerja sama antar anggota APCERT lainnya. Sebagaimana di FIRST, konsep terpenting dalam APCERT adalah hubungan saling percaya antar anggota untuk bertukar informasi dan bekerja sama satu sama lain. Dengan demikian, aktivitas APCERT dirancang untuk:

- Meningkatkan kerja sama internasional dan regional Asia-Pasifik;
- Bersama-sama mengembangkan langkah-langkah penanganan insiden keamanan jaringan skala besar atau regional;
- Meningkatkan pertukaran teknologi dan berbagi informasi keamanan, termasuk informasi mengenai virus komputer, *exploit scripts*, dan sejenisnya;
- Meningkatkan kerja sama penelitian masalah umum;
- Membantu CERT lainnya di kawasan tersebut dalam menangani insiden keamanan komputer secara efektif; serta

[68] Asia Pacific Computer Emergency Response Team. *Background*. Background: About APCERT. Diakses dari http://www.apcert.org/about/background/index.html.

- Memberikan saran dan solusi untuk masalah hukum yang berkaitan dengan keamanan informasi dan penanganan insiden regional.

CERT Pemerintah Eropa[69]

CERT Pemerintah Eropa atau European Government CERT (EGC) merupakan komite non-resmi yang berhubungan dengan CSIRT pemerintah di negara-negara Eropa. Anggotanya antara lain Finlandia, Perancis, Jerman, Hongaria, Belanda, Norwegia, Swedia, Swiss, dan Kerajaan Serikat (UK). Peran dan tanggung jawabnya adalah untuk:

- Mengembangkan bersama langkah penanganan insiden keamanan jaringan skala besar atau regional;
- Mendorong kegiatan berbagi informasi dan pertukaran teknologi yang berhubungan dengan insiden keamanan serta ancaman dan kerentanan kode berbahaya *(malicious code)*;
- Identifikasi bidang pengetahuan dan keahlian yang dapat dibagikan di dalam kelompok;
- Mengidentifikasi bidang untuk kerja sama penelitian dan pengembangan subjek yang menarik perhatian anggota; serta
- Mendorong pembentukan CSIRT pemerintah di negara-negara Eropa.

Badan Keamanan Jaringan dan Informasi Eropa[70]

Tujuan Badan Keamanan Jaringan dan Informasi Eropa atau European Network and Information Security Agency (ENISA) adalah untuk meningkatkan keamanan jaringan dan keamanan informasi di Uni Eropa melalui pembentukan budaya NIS. Ia dibentuk pada Januari 2004 oleh Dewan Menteri dan Parlemen Eropa untuk menangani kejahatan berteknologi tinggi. NIS memiliki peran sebagai berikut:

- Memberikan dukungan untuk memastikan NIS bagi anggota ENISA atau Uni Eropa;
- Mendorong pertukaran informasi yang stabil di antara para pemangku kepentingan; serta
- Meningkatkan koordinasi pekerjaan yang berkaitan dengan NIS.

ENISA diharapkan dapat berkontribusi terhadap upaya internasional dalam memitigasi virus dan peretasan serta melakukan pemantauan ancaman secara daring.

AfricaCERT

Tujuan dari forum tim penanganan insiden komputer di Afrika adalah mengusulkan solusi terhadap berbagai tantangan kesehatan internet dalam Ekosistem Internet Afrika. Tujuan AfricaCERT meliputi:

- Mengoordinasikan kerja sama antar CSIRTS;
- Membantu negara-negara Afrika dalam pembentukan CSIRT dengan memberi saran dan keahlian; serta

[69] EGC Group. *EGC group*. European Government CERTs (EGC) group. Diakses dari http://www.egc-group.org/.
[70] ENISA. (15 Januari 2021). About ENISA - The European Union Agency for Cybersecurity. ENISA. Diakses dari http://www.enisa.europa.eu/about-enisa.

- Menjaga dan mendukung program pendidikan dan penjangkauan dalam Keamanan TIK antar negara-negara di Afrika.

6.4. CSIRT Nasional

Beberapa negara telah membentuk CSIRT Nasional. Tabel 12 berikut menyajikan data berbagai negara beserta masing-masing CSIRT dan situs webnya.

Tabel 12. Daftar CSIRT Nasional

Negara	Nama Resmi	Situs Web
Abu Dhabi	Abu Dhabi Police Computer Emergency Response Team	https://adsic.abudhabi.ae
Amerika Serikat	United States Computer Emergency Readiness Centre	https://www.us-cert.gov
Arab Saudi	Computer Emergency Response Team – Saudi Arabia	http://www.cert.gov.sa
Argentina	ICIC-CERT	http://www.icic.gob.ar
Australia	Australia Computer Emergency Response Team	http://www.auscert.org.au
Australia	Australia Cyber Security Centre	http://www.cyber.gov.au
Austria	CERT.at	https://www.cert.at
Azerbaijan	CERT.AZ	http://www.cert.az
Bangladesh	Bangladesh e-Government Computer Incident Response Team	https://www.cirt.gov.bd
Brazil	Computer Emergency Response Team Brazil	http://www.cert.br
Brunei Darussalam	Brunei Computer Emergency Response Team	http://www.brucert.org.bn
Belanda	National Cyber Security Centre of The Netherlands	http://www.ncsc.nl
Belarusia	CERT.BY	http://cert.by
Belgia	Belgian Federal Cyber Emergency Team	http://www.cert.be
Bhutan	Bhutan Computer Incident Response Team	http://www.btcirt.bt

Negara	Nama Resmi	Situs Web
Bolivia	Cenro de Gestion de Incidentes Informaticos	https://cgii.gob.bo/
Brazil	Computer Emergency Response Team Brazil	http://www.cert.br
Brunei	Brunei Computer Emergency Response Team	http://www.brucert.org.bn
Chili	Chilean Computer Emergency Response Team	http://www.clcert.cl
Cina	National Computer Network Emergency Response Technical Ream – Coordination Center of China	http://www.cert.org.cn
Denmark	Danish Computer Emergency Response Team	http://www.cert.dk
Estonia	CERT-EE	https://ria.ee
Filipina	Philippines Computer Emergency Response Team	http://www.phcert.org
Finlandia	National Cyber Security Centre Finland	http://www.ncsc.fi
Ghana	CERT-GH National Cyber Security Centre of Ghana	https://cybersecurity.gov.gh
Hong Kong, Cina	Hong Kong Computer Response Coordination Centre	http://www.hkcert.org
Hongaria	CERT-Hungary National Cyber Security Center	https://nki.gov.hu
India	CERT-In Indian Computer Emergency Response Team	http://www.cert-in.org.in
Indonesia	Indonesia Security Incident Response Team on Internet Infrastructure	http://www.idsirtii.or.id
Iran	CERT CC Maher	https://www.ircert.com
Islandia	CERT-IS Computer Incident Response Team Iceland	https://www.cert.is
Italia	CSIRT Italia	https://www.csirt-ita.it/
Jepang	JP CERT Coordination Center	http://www.jpcert.or.jp
Jerman	CERT-Bund	http://www.bsi.bund.de/certbund

Negara	Nama Resmi	Situs Web
Kanada	Canadian Centre for Cyber Security	http://www.cyber.gc.ca
Kazakhstan	Kazakhstan Computer Emergency Response	http://www.cert.kz
Kerajaan Serikat (UK)	National Cyber Security Centre	http://www.ncsc.gov.uk
Kroasia	CarNet CERT	http://www.carnet.hr
Lithuania	LITNET CERT	http://cert.litnet.lt
Makau	MOCERT	http://www.mocert.org
Malaysia	Malaysian Computer Emergency Response Team	http://www.mycert.org.my
Maroko	maCERT	https://www.dgssi.gov.ma
Meksiko	Universidad Nacional Autonoma de Mexico	http://www.cert.org.mx
Mesir	Danish Computer Emergency Response Team	http://www.egcert.eg
Mongolia	Mongolian Cyber Emergency Response / Coordination Centre	http://www.mncert.org
Nigeria	ngCERT Nigerian Computer Emergency Response Team	http://www.cert.gov.ng
Norwegia	Norwegian Computer Emergency Response Team	https://nsm.stat.no/norcert
Pakistan	PakCERT	http://www.pakcert.org
Papua Nugini	PNGCERT	https://www.pngcert.org.pg
Perancis	CERT-FR	http://www.cert.ssi.gouv.fr
Polandia	Computer Emergency Response Team Polska	http://www.cert.pl
Portugal	CERT.PT	https://www.cncs.gov.pt
Provinsi Taiwan, Cina	Taiwan Computer Emergency Response Team/Coordination Center	http://www.twcert.org.tw
Qatar	Qatar National Center for Information Security	http://www.qcert.org
Republik Ceko	CSIRT.CZ	http://www.clcert.cl

Negara	Nama Resmi	Situs Web
Republik Irlandia	CSIRT-IE	https://ncsc.gov.ie/csirt
Republik Korea	CERT Coordination Center Korea	http://www.krcert.or.kr
Rumania	Romanian National Computer Security Incident Response Team	http://cert.ro
Rusia	RU-CERT Computer Security Incident Response Team	http://www.cert.ru
Selandia Baru	CERT NZ	http://www.cert.govt.nz
Singapura	Singapore Computer Emergency Response Team	https://www.csa.gov.sg/singcert
Slovenia	Slovenia Computer Emergency Response Team	http://www.cert.si
Slowakia	SK-CERT	https://www.sk-cert.sk
Spanyol	INCIBE-CERT Spanish National Cybersecurity Institute - National CSIRT	https://www.incibe-cert.es
Sri Lanka	SL CERT | CC	http://www.cert.gov.lk
Swedia	CERT-SE	http://www.cert.se
Swiss	Computer Emergency Response Team of the Swiss Government	http://www.melani.admin.ch
Tonga	CERT Tonga	http://www.cert.gov.to
Tunisia	TunCERT – Tunisian Computer Emergency Response Team	https://www.ansi.tn
Turki	TP-CERT National Cyber Security Incident Response Team	http://www.uekae.tubitak.gov.tr
Uganda	CERT.UG Uganda Computer Emergency Response Team	http://www.ug-cert.ug
Ukraina	Computer Emergency Response Team of Ukraine	https://cert.gov.ua

Negara	Nama Resmi	Situs Web
Uni Emirat Arab	The United Arab Emirates Computer Emergency Response Team	http://www.aecert.ae
Uzbekistan	Computer Emergency Response Team of Uzbekistan	http://uzcert.uz
Vietnam	Vietnam Computer Emergency Response Team	http://www.vncert.gov.vn

Pertanyaan

Apakah terdapat CSIRT nasional di negara Anda?

1. Jika ya, jelaskan model dan cara kerjanya. Kemudian evaluasi seberapa efektif CSIRT tersebut dalam menjalankan fungsinya.
2. Jika tidak ada, tentukan model CSIRT manakah yang sesuai untuk negara Anda dan jelaskan apa yang diperlukan untuk membentuk CSIRT nasional di negara Anda.

Latihan

1. Apa fungsi utama CSIRT?

2. Apa perbedaan antara CSIRT internasional dan CSIRT nasional?

3. Apa saja yang diperlukan untuk membentuk CSIRT?

7. Siklus Hidup Kebijakan Keamanan Informasi

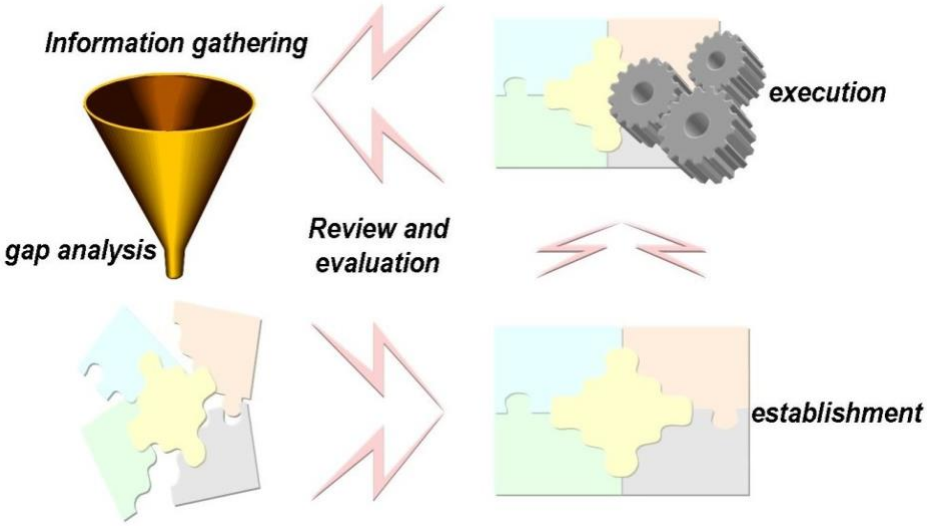
Bab ini bertujuan untuk:

- Memberikan gambaran umum tentang proses pembuatan kebijakan keamanan informasi; dan
- Membahas masalah yang harus dipertimbangkan oleh pembuat kebijakan dalam pembuatan kebijakan keamanan informasi

Para pembuat kebijakan perlu memerhatikan beberapa pertimbangan, antara lain alasan kebijakan, sumber daya yang tersedia, arah kebijakan, kebutuhan hukum dan anggaran, serta hasil kebijakan yang diharapkan. Pada bab ini, pertimbangan tersebut dibahas dalam konteks berbagai tahapan penyusunan kebijakan keamanan informasi.

Perlu dicatat bahwa setiap negara akan memiliki pertimbangan dan konteks kebijakan yang sedikit berbeda. Proses penyusunan kebijakan yang dijelaskan di bab ini bersifat umum dan berdasarkan asumsi bahwa belum ada kebijakan keamanan informasi nasional.

Seperti kebijakan lainnya, siklus hidup kebijakan keamanan informasi dapat dibagi menjadi empat tahap: (1) pengumpulan informasi dan analisis kesenjangan; (2) penetapan kebijakan; (3) implementasi kebijakan; serta (4) kontrol dan umpan balik (Gambar 22). Selain itu, kebijakan keamanan informasi nasional harus mencakup strategi keamanan informasi, hubungan resmi, organisasi keamanan informasi, teknologi keamanan informasi, dan hubungan di antara mereka.



Gambar 22. Siklus Hidup Kebijakan Keamanan Informasi

7.1. Pengumpulan Informasi dan Analisis Kesenjangan

Tahap pertama dalam merumuskan kebijakan keamanan informasi adalah pengumpulan informasi dan analisis kesenjangan.

Dalam pengumpulan informasi, penting untuk mempertimbangkan contoh keamanan informasi dan kebijakan terkait hal tersebut dari negara-negara lain, termasuk berbagai kebijakan di dalam negara itu sendiri.

Dalam analisis kesenjangan, penting untuk memahami infrastruktur yang ada saat ini terkait dengan keamanan informasi, seperti sistem dan hukum saat ini, serta bidang atau kesenjangan yang perlu diisi. Ini merupakan langkah penting karena hal tersebut dapat menentukan arah atau prioritas kebijakan keamanan informasi yang akan ditetapkan.

Pengumpulan Informasi

Pengumpulan kasus luar negeri: Dalam menemukan kasus yang relevan di negara lain, pembuat kebijakan harus mempertimbangkan kesamaan dalam hal —

- Tingkat keamanan informasi nasional
- Arah penetapan kebijakan
- Infrastruktur sistem dan jaringan

Berdasarkan kesamaan tersebut, beberapa materi berikut dapat dikumpulkan —

- Informasi tentang pembentukan dan pengoperasian organisasi yang berhubungan dengan keamanan informasi (lihat Bab 3 dan Bab 6 pada modul ini)
- Kebijakan, hukum dan peraturan keamanan informasi (lihat Bab 3)
- Metodologi keamanan informasi yang digunakan secara internasional dan contoh-contoh dari berbagai negara (lihat Bab 4)
- Tren ancaman dan tindakan pencegahan atau kontrol yang sesuai dengan jenis serangan (lihat Bab 2 dan Bab 6)
- Penanggulangan untuk perlindungan privasi (lihat Bab 5)

Pengumpulan materi dalam negeri: Meskipun sebagian besar pembuat kebijakan bukan ahli dalam keamanan informasi, mereka melakukan berbagai kegiatan yang berhubungan atau relevan dengan keamanan informasi. Secara khusus, mereka menyusun undang-undang, peraturan, dan kebijakan di berbagai bidang terkait dengan keamanan informasi. Namun, karena undang-undang, peraturan, dan kebijakan cenderung berfokus pada bidang tertentu, korelasi di antara mereka mungkin tidak langsung terlihat oleh pembuat kebijakan. Oleh karena itu, penting untuk mengumpulkan, menganalisis, dan mengevaluasi seluruh undang-undang, peraturan dan kebijakan yang berhubungan atau relevan dengan keamanan informasi.

Analisis Kesenjangan

Dalam buku *Art of War* karya Sun Tzu disebutkan, "Kenali musuhmu". Artinya kita harus mengetahui keterbatasan kita serta keterbatasan musuh. Dalam hal penyusunan kebijakan

keamanan informasi, hal tersebut berarti kita harus mengetahui apa yang perlu dilindungi melalui kebijakan keamanan informasi serta kerentanan dan ancaman terhadap keamanan informasi.

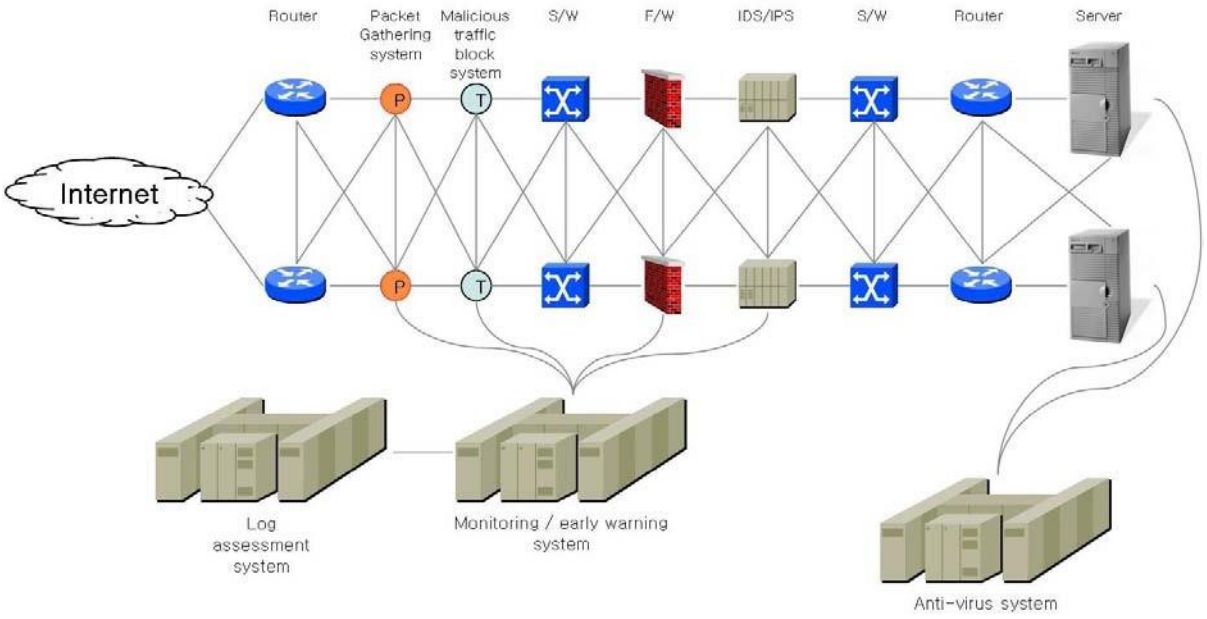
Analisis kesenjangan dibagi menjadi dua fase:

1. Memahami kemampuan dan kapasitas negara — yaitu organisasi dan sumber daya manusianya, serta infrastruktur informasi dan komunikasinya — di bidang umum keamanan informasi; serta
2. Mengidentifikasi ancaman eksternal terhadap keamanan informasi.

Pembuat kebijakan perlu mengenal organisasi keamanan informasi dan sumber daya manusianya, yaitu lembaga publik dan swasta di bidang yang berhubungan dengan keamanan informasi. Mereka harus mengetahui organisasi yang terlibat dalam pekerjaan terkait keamanan informasi dan memahami ruang lingkup pekerjaan, peran dan tanggung jawabnya. Hal ini penting agar tidak terjadi duplikasi dalam struktur keamanan informasi yang ada.

Pada fase ini juga, para pakar keamanan informasi yang memiliki latar belakang hukum, kebijakan, teknologi, pendidikan, dan bidang terkait harus teridentifikasi dan termanfaatkan.

Infrastruktur informasi-komunikasi mengacu pada struktur TI yang mengumpulkan, memproses, menyimpan, mencari, mengirim, dan menerima informasi dan sistem manajemen kontrol elektronik. Singkatnya, inilah sistem informasi dan jaringan. Memahami status infrastruktur informasi-komunikasi saat ini sangat penting dari sudut pandang ekonomi. Karena investasi besar diperlukan untuk menghubungkan seluruh negeri, memanfaatkan fasilitas informasi-komunikasi yang ada akan menguntungkan. Gambar 23 menunjukkan contoh infrastruktur informasi-komunikasi untuk keamanan informasi. Ini belum mencakup seluruh *item* yang mungkin diperlukan dan yang tersaji di sini hanya untuk tujuan ilustrasi. Perhatikan hubungan antara berbagai komponen jaringan.



Gambar 23. Contoh Struktur Sistem dan Jaringan

Pembuat kebijakan perlu memahami bagaimana cara membuat jaringan dan sistem keamanan informasi secara umum.

Fase kedua dalam analisis kesenjangan adalah mengidentifikasi ancaman eksternal terhadap keamanan informasi. Sebagaimana yang dijelaskan pada Bab 2, ancaman terhadap informasi penting tidak hanya meningkat, melainkan juga menjadi lebih canggih. Pembuat kebijakan perlu memahami ancaman ini agar dapat memutuskan langkah penanggulangan apa yang diperlukan. Secara khusus, pembuat kebijakan harus memahami:

- Tingkat penetrasi ancaman terhadap keamanan informasi
- Jenis serangan terbaru dan yang paling umum
- Jenis ancaman dan tingkat kekuatannya di masa mendatang

Setelah menganalisis organisasi nasional, sumber daya manusia dan infrastruktur informasi-komunikasi, serta memahami komponen ancaman di bidang keamanan informasi, penting untuk menentukan komponen yang rentan. Hal ini menentukan sejauh mana negara dapat menangkal komponen ancaman eksternal. Penentuan tersebut dapat dilakukan dengan memperhatikan hal-hal berikut:

- Status CERT saat ini dan kemampuannya untuk bereaksi
- Status ahli keamanan informasi saat ini
- Tingkat konstruksi dan intensitas sistem keamanan informasi
- Perlindungan hukum terhadap pelanggaran aset informasi
- Lingkungan fisik untuk melindungi aset informasi

Tujuan dari analisis kesenjangan adalah untuk dapat mengidentifikasi langkah penanggulangan praktis yang harus dilakukan. Perlu ditekankan pula bahwa ini merupakan langkah paling mendasar dalam penyusunan kebijakan keamanan informasi.

7.2. Perumusan Kebijakan Keamanan Informasi

Perumusan kebijakan keamanan informasi nasional meliputi: (1) menetapkan arah kebijakan; (2) mendirikan organisasi keamanan informasi serta menentukan peran dan tanggung jawabnya; (3) menetapkan kerangka kebijakan keamanan informasi; (4) melembagakan dan/atau merevisi hukum agar sesuai dengan kebijakan; serta (5) mengalokasikan anggaran untuk implementasi kebijakan informasi.

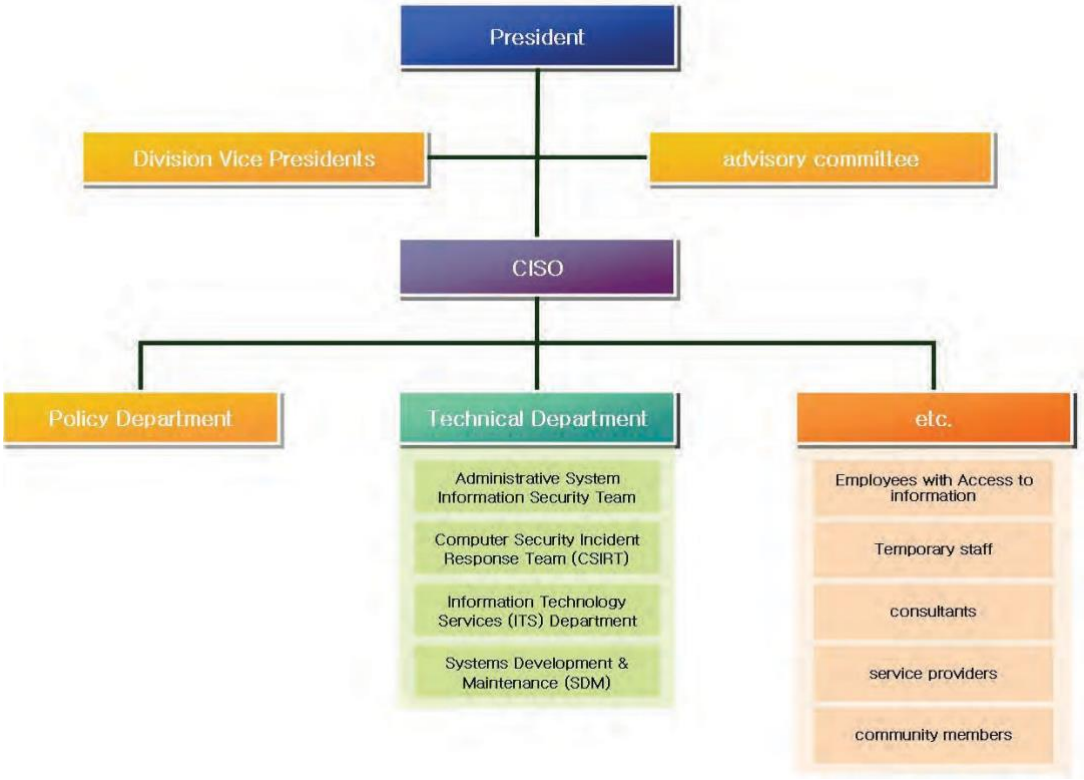
1. Menetapkan Arah Kebijakan dan Mendorongnya

Dalam banyak kasus, penyusunan kebijakan keamanan informasi harus dipelopori oleh pemerintah daripada menyerahkannya kepada sektor swasta. Secara khusus, pemerintah perlu menetapkan kebijakan, berperan penting dalam menempatkan infrastruktur yang diperlukan dan memberikan dukungan jangka panjang. Selanjutnya, sektor swasta bergabung dengan proyek tersebut, terutama untuk mengambil bagian dalam penelitian dan pengembangan, serta konstruksi sistem.

Rencana partisipasi sektor swasta meliputi kegiatan peningkatan kesadaran sekaligus dengan pembangunan dan penguatan infrastruktur informasi-komunikasi. Jika pemerintah ingin mendorong sektor swasta menerima strategi keamanan informasi, pemerintah harus berperan sebagai pendukung daripada pengatur. Termasuk dalam hal ini adalah menyebarkan pedoman keamanan informasi.

2. Susunan Organisasi Keamanan Informasi, serta Penentuan Peran dan Tanggung Jawab[71]

Saat arah kebijakan keamanan informasi ditetapkan, organisasi pelaksana harus dibentuk. Gambar 24 menunjukkan struktur umum organisasi keamanan informasi nasional.



Gambar 24. Struktur Umum Organisasi Keamanan Informasi Nasional

Organisasi keamanan informasi nasional setiap negara agak berbeda, sesuai dengan karakteristik dan budayanya masing-masing. Namun, prinsip dasarnya adalah memastikan bahwa peran dan tanggung jawab tergambar dengan jelas.

[71] Sinclair Community College. *Information Security Organization – Roles and Responsibilities*. Information Security Policy. Diakses dari https://it.sinclair.edu/index.cfm/services/student-and-guests-services/policies-and-security-information/information-security-policy/.

Organisasi Administratif

Division Vice Presidents memiliki tanggung jawab utama agar informasi yang digunakan atau dimiliki oleh divisinya masing-masing dikumpulkan, dipelihara dan/atau diidentifikasi. Mereka dapat menunjuk seorang Petugas Keamanan Informasi atau *Information Security Officer* (ISO) serta individu lain untuk membantu ISO dalam menerapkan kebijakan keamanan informasi. Petugas yang ditunjuk harus dapat memastikan bahwa aset informasi yang berada dalam kendali mereka telah ditunjuk pemiliknya, penilaian risiko telah dilaksanakan, dan proses mitigasi berdasarkan risiko-risiko tersebut telah diimplementasikan.

Supervisor (Direktur, Ketua, Manajer, dan lain-lain) mengelola karyawan yang memiliki akses terhadap informasi dan sistem informasi serta menentukan, menerapkan, dan menegakkan kontrol keamanan informasi yang berlaku di area masing-masing. Mereka harus memastikan bahwa setiap karyawan memahami tanggung jawabnya terkait dengan keamanan informasi dan mereka memiliki akses yang diperlukan untuk melakukan pekerjaannya. Pengawas harus meninjau secara berkala semua tingkat akses pengguna untuk memastikan kesesuaiannya dan mengambil langkah yang tepat untuk memperbaiki ketidaksesuaian atau kekurangannya.

Chief Information Security Officer **(CISO)** bertanggung jawab untuk mengoordinasikan dan mengawasi kebijakan keamanan informasi. Bekerja sama dengan berbagai divisi, CISO dapat memberi rekomendasi bahwa supervisor dari divisi tertentu menunjuk perwakilan lain untuk mengawasi dan mengoordinasikan unsur tertentu dari kebijakan tersebut. CISO juga memberi pemilik informasi praktik terbaik keamanan informasi dalam hal:

- Menetapkan dan menyebarluaskan aturan yang dapat diterapkan terkait akses dan penggunaan sumber informasi yang diizinkan;
- Melakukan/mengoordinasikan penilaian dan analisis risiko keamanan informasi;
- Menetapkan pedoman dan langkah keamanan yang tepat untuk melindungi data dan sistem;
- Membantu pemantauan dan pengelolaan kerentanan keamanan sistem;
- Melakukan/mengoordinasikan audit keamanan informasi; serta
- Membantu penyelidikan/penyelesaian masalah dan/atau dugaan pelanggaran kebijakan keamanan informasi nasional.

Organisasi Teknis

Administrative System Information Security Team mengembangkan dan menerapkan berbagai langkah untuk memastikan bahwa kontrol keamanan aplikasi administratif memberi pemangku kepentingan akses yang tepat terhadap informasi sekaligus memenuhi kewajiban etis dan hukum nasional dalam rangka perlindungan informasi pribadi, sensitif, dan sangat penting. Tim tersebut mengembangkan proses dan standar untuk menghasilkan ketersediaan, keutuhan, dan kerahasiaan informasi sistem administrasi yang optimal, termasuk proses meminta dan perubahan akses oleh pengguna; dokumentasi akses pengguna yang sah, serta hak dan tanggung jawab pengguna/supervisor; serta penyelesaian konflik dan permasalahan terkait keamanan.

Termasuk di dalam tim tersebut adalah *Division Information Security Officers* dan CISO. Tim tersebut diberi arahan oleh *Department Information Security Officers* dan *Administrative Systems Administrators*.

CSIRT memberikan informasi dan membantu pemangku kepentingan dalam melakukan langkah proaktif untuk mengurangi risiko insiden keamanan komputer, serta dalam menyelidiki, menangani, dan meminimalkan kerugian akibat insiden tersebut. CSIRT juga menentukan dan merekomendasikan aksi tindak lanjut. CSIRT dua lapis terdiri dari tim operasional yang bertugas melakukan identifikasi awal, penanganan, triase, dan penentuan kebutuhan eskalasi, serta tim manajemen yang bertugas memelopori penanganan nasional terhadap insiden besar atau signifikan. CISO dan anggota staf TI yang didelegasikan dari Departemen Layanan TI serta Pemeliharaan dan Pengembangan Sistem merupakan bagian dari CSIRT operasional. Tim manajemen CSIRT terdiri dari *Chief Information Officer* (CIO), Kepala Polisi, Direktur Informasi Publik, Direktur Layanan TI, Direktur Pemeliharaan dan Pengembangan Sistem, CISO, manajer sistem dan jaringan, penasihat hukum, penasihat sumber daya manusia, dan delegasi yang memiliki keahlian teknis yang ditunjuk secara khusus oleh *Vice President*.

Staf Layanan TI meliputi administrator sistem dan jaringan beserta jajarannya, serta penyedia layanan teknis seperti *IT Help Desk*, teknisi pendukung pengguna, dan administrator komunikasi suara. Mereka bertanggung jawab atas integrasi perangkat, kontrol, dan praktik keamanan informasi teknis di lingkungan jaringan. Mereka menerima laporan dugaan kegagalan atau insiden keamanan informasi dari pengguna akhir *(end user)*.

Staf Pengembangan dan Pemeliharaan Sistem meliputi pengembang dan administrator basis data. Mereka mengembangkan, mempraktikkan, mengintegrasikan, dan menerapkan praktik terbaik keamanan untuk aplikasi nasional, dan melatih pengembang aplikasi web dalam menggunakan prinsip keamanan aplikasi.

Lainnya

Pegawai yang memiliki akses terhadap informasi dan sistem informasi harus mematuhi kebijakan dan prosedur nasional yang berlaku, serta praktik atau prosedur tambahan yang ditetapkan oleh kepala unit atau direktur mereka. Termasuk dalam hal ini adalah melindungi sandi akun mereka dan melaporkan dugaan penyalahgunaan informasi atau insiden keamanan informasi kepada pihak yang tepat (biasanya supervisor mereka).

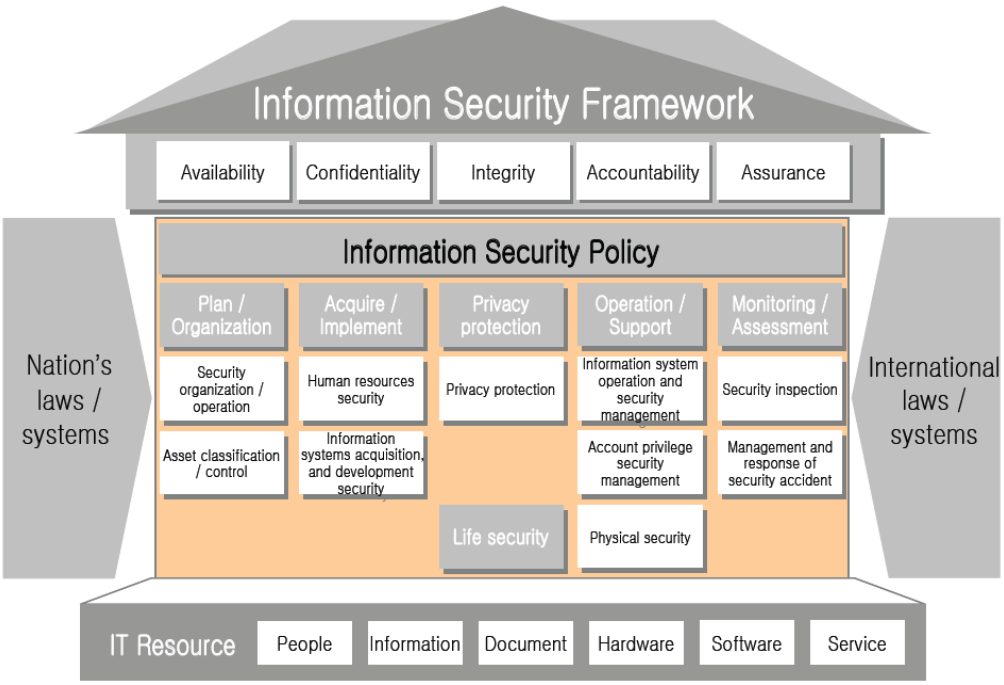
Pegawai tidak tetap dianggap sebagai pegawai yang memiliki tanggung jawab yang sama dengan pegawai penuh atau paruh waktu yang memiliki akses terhadap informasi dan sistem informasi.

Konsultan, penyedia layanan, dan pihak ketiga yang dikontrak lainnya diberi akses terhadap informasi atas dasar "perlu mengetahuinya". Akun jaringan yang dibutuhkan oleh pihak ketiga harus diminta "sponsor" organisasi yang akan memastikan bahwa pengguna pihak ketiga memahami tanggung jawab individu terkait dengan akun jaringan, serta telah disetujui oleh *Vice President* atau direktur yang berwenang. Pengguna harus menjaga kata sandinya agar tetap aman dan bertanggung jawab atas aktivitas apa pun yang dihasilkan dari pemanfaatan ID pengguna tersebut dalam lingkup kendalinya.

3. Menetapkan Kerangka Kebijakan Keamanan Informasi

Kerangka kerja keamanan informasi

Kerangka kerja keamanan informasi menetapkan parameter untuk kebijakan keamanan informasi dan memastikan bahwa kebijakan tersebut memperhitungkan sumber daya TI (orang, dokumen informasi, perangkat keras, perangkat lunak, layanan); mencerminkan hukum dan peraturan internasional; serta memenuhi prinsip ketersediaan, kerahasiaan, keutuhan, akuntabilitas dan jaminan informasi. Gambar 25 menunjukkan kerangka kerja keamanan informasi.



Gambar 25. Kerangka Kerja Keamanan Informasi

Kebijakan keamanan informasi adalah bagian terpenting dari kerangka kerja keamanan informasi. Kebijakan tersebut meliputi lima bidang sebagaimana pembahasan berikut.

a. Rencana dan Organisasi: Bidang ini meliputi organisasi dan operasi keamanan, serta klasifikasi dan kontrol aset.

Organisasi dan operasi keamanan mencakup —

- Organisasi dan sistem organisasi keamanan informasi nasional
- Prosedur masing-masing organisasi keamanan informasi
- Konstitusi dan manajemen keamanan informasi nasional
- Kerja sama dengan lembaga internasional terkait
- Kerja sama dengan kelompok ahli

Klasifikasi dan kontrol aset mencakup —

- Penyerahan kepemilikan dan standar klasifikasi untuk aset informasi penting
- Instruksi pendaftaran dan penilaian risiko aset informasi penting
- Manajemen hak akses terhadap aset informasi penting
- Publikasi dan ekspor aset informasi penting
- Pengurusan dan penilaian ulang aset informasi penting
- Manajemen keamanan dokumen

b. Akuisisi dan Implementasi: Bidang ini meliputi keamanan sumber daya manusia, serta keamanan pengembangan dan akuisisi sistem informasi.

Keamanan sumber daya manusia menyangkut penetapan metode manajemen untuk penerimaan pegawai baru yang mencakup—

- Langkah keamanan sumber daya manusia dan pelatihan keamanan
- Pemrosesan pelanggaran hukum dan peraturan keamanan
- Manajemen keamanan akses pihak ketiga
- Manajemen keamanan akses personel alih daya *(outsource)*
- Tugas dan manajemen pihak ketiga serta mengalihdayakan *(outsourcing)* pegawai
- Manajemen keamanan ruangan dan perlengkapan komputer
- Akses terhadap bangunan dan fasilitas utama
- Pemrosesan insiden keamanan

Keamanan pengembangan dan akuisisi sistem informasi mencakup —

- Pemeriksaan keamanan saat sistem informasi didapatkan
- Manajemen keamanan program aplikasi *in-house* maupun alih daya *(outsource)*
- Sistem enkripsi nasional (program dan kunci enkripsi, dan sebagainya)
- Pengujian setelah pengembangan program
- Kebutuhan keamanan yang dianjurkan saat pengembangan alih daya *(outsourcing)*
- Verifikasi keamanan selama pengembangan dan akuisisi

c. Perlindungan Privasi: Menyertakan perlindungan privasi dalam kebijakan keamanan informasi bersifat tidak wajib. Namun, akan lebih baik menyertakannya mengingat perlindungan privasi merupakan isu internasional. Perlindungan privasi harus mencakup hal-hal berikut —

- Pengumpulan dan penggunaan informasi pribadi
- Permintaan izin sebelumnya saat memanfaatkan privasi seseorang
- PIA

d. Operasi dan Dukungan: Bidang ini terkait dengan keamanan teknis dan fisik. Penggunaan jaringan dan sistem diatur secara rinci, serta keamanan fisik insfrastruktur informasi dan komunikasi ditetapkan.

Manajemen keamanan dan operasi sistem informasi menyangkut penetapan beberapa hal berikut —

- Manajemen keamanan dan operasi server, jaringan, aplikasi dan basis data
- Pengembangan sistem keamanan informasi
- Catatan *(log)* dan cadangan (*back-up)* tindakan yang sah
- Manajemen penyimpanan informasi
- Komputasi bergerak (*mobile computing)*
- Standar penjagaan dan pengamanan data komputer
- Layanan *e-commerce*

Manejemen keamanan hak akun – Kontrol akses dan manajemen akun harus dibuat untuk menjamin kerahasiaan penggunaan tempat penyimpanan informasi nasional. Hal ini mencakup —

- Registrasi, penghapusan, manajemen hak pengguna sistem informasi nasional
- Manajemen akun dan hak dalam jaringan terenkripsi

Keamanan fisik – Keamanan fisik mengacu pada perlindungan fasilitas informasi dan komunikasi yang menyimpan informasi penting. Hal ini mencakup —

- Konfigurasi dan pengelolaan metode bidang keamanan
- Kontrol akses dan pengiriman untuk pusat komputer
- Pencegahan kerusakan akibat bencana alam dan bencana lainnya

e. Pemantauan dan Penilaian: Bidang kebijakan keamanan informasi ini membutuhkan formulasi standar dan proses pencegahan insiden keamanan serta pengelolaan dan penanganan insiden keamanan.

Inspeksi keamanan mencakup —

- Penetapan rencana inspeksi keamanan
- Pelaksanaan inspeksi keamanan secara rutin
- Pengorganisasian/penyusunan berbagai bentuk laporan
- Pengidentifikasian subjek target inspeksi dan laporan keamanan

Manajemen dan penanganan insiden keamanan menyangkut penetapan —

- Tugas dan peran tiap organisasi dalam pemrosesan insiden keamanan
- Prosedur untuk memantau dan mengenali gejala insiden keamanan
- Prosedur pemrosesan insiden keamanan dan metode penanganan
- Langkah yang perlu diambil setelah pemrosesan insiden keamanan

4. Penyusunan dan/atau revisi hukum agar sesuai kebijakan keamanan informasi

Hukum harus sesuai dengan kebijakan keamanan informasi. Perlu adanya hukum yang mengatur organisasi pemerintah dan perusahaan swasta. Tabel 13-15 menunjukkan hukum terkait keamanan informasi di Jepang, Uni Eropa dan Amerika Serikat. Di Jepang, perwakilan

hukum TI adalah *Basic Act on the Formation of an Advanced Information and Telecommunications Network Society*. Hukum ini merupakan standar dasar untuk keamanan informasi di negara tersebut dan seluruh hukum terkait harus sejalan dengannya.

Tabel 13. Hukum Terkait Keamanan Informasi di Jepang

Undang-Undang	Target Industri	Target Peraturan	Hukuman
Unauthorized Computer Access Law	Semua industri	Tindakan yang mendorong adanya akses tidak sah dan memberikan informasi ID orang lain tanpa pemberitahuan	
Act on the Protection of Personal Information	Perusahaan swasta yang menggunakan informasi pribadi untuk tujuan bisnis	Manajemen informasi privasi (alamat, nomor ponsel, surel, dan lain-lain)	Hukum pidana, denda
Act on Electronic Signatures and Certification		Pemfasilitasan *e-commerce* yang memanfaatkan internet dan aktivitas ekonomi melalui jaringan	

Tabel 14. Hukum Terkait Keamanan Informasi di Uni Eropa

Undang-Undang	Rincian
A Common Regulatory Framework (Directive 2002/21/ EC)	• Memberikan kerangka kerja pengaturan jaringan dan layanan telekomunikasi • Bertujuan untuk melindungi privasi melalui jaringan komunikasi yang aman

EU Directive on Data Protection (Directive 1995/46/ EC)	• Pedoman pemrosesan dan penghapusan gratis informasi pribadi • Hukum dasar yang menetapkan tanggung jawab negara anggota dan pengakuan kewenangan penuh individu atas informasi pribadi • Lebih ketat daripada standar Amerika Serikat
EU Directive on Electronic Signatures (Directive 1999/93/EC) *EU Directive on Electronic Commerce* (Directive 2000/31/EC)	• Mengatur penggunaan tanda tangan elektronik • Mengatur pelaksanaan *e-commerce*
Cybercrime Treaty	• Perjanjian internasional paling komprehensif mengenai kejahatan siber • Mendefinisikan secara rinci seluruh tindakan kriminal menggunakan internet beserta hukuman/denda yang setimpal
Data Preservation Guideline on Communication and Networks	• Mensyaratkan penyediaan layanan komunikasi untuk mempertahankan data panggilan dari 6 bulan sampai 24 bulan (diumumkan setelah serangan teroris di Madrid dan London pada tahun 2004 dan 2005)

Tabel 15. Undang-Undang Terkait Keamanan Informasi di Amerika Serikat

Undang-Undang	Target Industri	Target Peraturan	Hukuman
Federal Information Security Management Act of 2002	Lembaga administratif federal	Informasi lembaga administratif, sistem TI, program keamanan informasi	-
Health Insurance Privacy and Accountability Act of 1996	Lembaga keseharan dan penyedia layanan kesehatan	Data elektronik tentang informasi kesehatan pribadi seseorang	Hukum pidana, denda

Gramm-Leach-Bliley Act of 1999	Lembaga keuangan	Informasi pribadi konsumen	Hukum pidana, denda
Sarbanes-Oxley Act of 2002	Perusahaan terdaftar di Bursa Efek Amerika Serikat	Kontrol internal dan catatan keuangan publik	Hukuman pidana, denda
California Database Security Breach Information Act of 2003	Lembaga administratif dan perusahaan swasta di California	Informasi pribadi terenkripsi	Denda dan pemberitahuan pada korban

5. Mengalokasikan Anggaran untuk Penerapan Kebijakan Informasi

Penerapan kebijakan membutuhkan anggaran. Tabel 16 berikut menunjukkan anggaran untuk keamanan informasi di Kerajaan Serikat (UK) dan Amerika Serikat dalam beberapa tahun belakangan ini.

Tabel 16. Anggaran Keamanan Informasi UK dan AS

(Satuan: UK – juta pounds; AS – juta dolar)

UK	**2016**	**2017**	**2018**	**2019**	**2020**
Anggaran keamanan informasi	1.092	1.137	-	-	-
AS	**2016**	**2017**	**2018**	**2019**	**2020**
Total anggaran TI tahunan	-	81.495	137.489	-	-
Anggaran keamanan informasi	-	13.150	14.980	16.650	17.430
Persentase total anggaran TI	-	16,13	10,89	9,10	-

Sumber: Statista.co untuk perhitungan statistik UK & AS.

Latihan:

Jika negara Anda memiliki kebijakan keamanan informasi, telusuri perkembangannya berdasarkan lima (5) aspek penyusunan kebijakan keamanan informasi sebagaimana penjelasan di atas. Artinya, jelaskan:

1. Arah kebijakan

2. Organisasi keamanan informasi

3. Kerangka kebijakan

4. Hukum/Undang-Undang yang mendukung kebijakan keamanan informasi

5. Alokasi anggaran untuk keamanan informasi

Jika negara Anda belum memiliki kebijakan keamanan informasi, uraikan kemungkinan dari masing-masing lima (5) aspek di atas dalam penyusunan kebijakan. Gunakan pertanyaan berikut sebagai panduan:

1. Apa yang seharusnya menjadi arah kebijakan keamanan informasi di negara Anda?

2. Bagaimana pengaturan organisasi yang harus ada? Organisasi mana saja yang harus terlibat dalam pengembangan dan implementasi kebijakan keamanan informasi di negara Anda?

3. Isu khusus apakah yang perlu ditangani kerangka kerja kebijakan tersebut?

4. Hukum/undang-undang apakah yang perlu ditetapkan atau dicabut untuk mendukung kebijakan informasi?

5. Anggaran apa saja yang harus dipertimbangkan? Dari manakah sebaiknya anggaran tersebut didapatkan?

Peserta pelatihan dari negara yang sama dapat melakukan kegiatan ini bersama-sama.

7.3. Implementasi/Pelaksanaan Kebijakan

Implementasi kebijakan keamanan informasi yang berjalan mulus membutuhkan kerja sama antara pemerintah, pihak swasta dan lembaga internasional. Gambar 26 menunjukkan bidang spesifik dari implementasi kebijakan informasi dengan kerja sama merupakan hal yang sangat krusial.

Gambar 26. Bidang Kerja Sama dalam Implementasi Kebijakan Keamanan Informasi

Pengembangan Kebijakan Keamanan Informasi

Tabel 17 di bawah ini menunjukkan bagaimana pemerintah, pihak swasta, dan organisasi internasional dapat berkontribusi pada pengembangan kebijakan keamanan informasi nasional.

Tabel 17. Contoh Kerja Sama Pengembangan Kebijakan Keamanan Informasi

Sektor	Kontribusi pada Pengembangan Kebijakan
Pemerintah	• Organisasi perencanaan dan strategi nasional: memastikan kecocokan antara kebijakan informasi dengan rencana nasional • Organisasi TIK: memastikan kerja sama pembentukan standar teknologi keamanan informasi nasional • Organisasi analisis tren keamanan informasi: mencerminkan analisis dan tren kebijakan keamanan nasional dan internasional • Organisasi analisis hukum: memeriksa kecocokan antara kebijakan keamanan informasi dengan hukum atau undang-undang yang ada • Organisasi informasi nasional: Bekerja sama dalam penentuan arah dan strategi • Lembaga investigasi: Bekerja sama dalam pemrosesan insiden keamanan

Pihak swasta	• Perusahaan konsultasi keamanan informasi: memanfaatkan agen profesional dalam penyusunan kebijakan keamanan informasi • Laboratorium teknologi keamanan informasi swasta: menetapkan standar teknologi terkait dengan keamanan informasi • Jurusan keamanan informasi di perguruan tinggi: memberikan keahlian dalam penyusunan kebijakan
Organisasi internasional	• Memastikan kesesuaian dengan standar kebijakan nasional • Mengoordinasikan penanganan ancaman dan insiden internasional

Manajemen dan Perlindungan Infrastruktur Informasi dan Komunikasi

Penggunaan informasi yang efektif (pengumpulan, pemeliharaan, dan lain-lain) memerlukan administrasi dan perlindungan infrastruktur TI yang tepat. Sebuah kebijakan keamanan informasi yang baik tidak akan bermanfaat jika tidak didukung dengan hadirnya infrastruktur TI yang baik.

Manajemen dan perlindungan infrastruktur informasi dan komunikasi yang efektif membutuhkan kerja sama antara manajer bidang TI, sistem, dan jaringan. Kerja sama institusi publik dan swasta juga memberikan keuntungan (lihat Tabel 18).

Tabel 18. Kerja Sama dalam Administrasi dan Perlindungan Informasi

Sektor	Kontribusi terhadap Administrasi dan Perlindungan Infrastruktur Informasi dan Komunikasi
Pihak pemerintah	• Organisasi terkait jaringan informasi dan komunikasi: menentukan komposisi dan tingkat keamanan jaringan informasi dan komunikasi nasional • Laboratorium TIK: menyebarkan standar publik dan mengadopsi teknologi yang berguna
Pihak swasta	• Penyedia ISP: Kerja sama dalam komposisi jaringan informasi dan komunikasi nasional • Laboratorium TIK: memberikan layanan pengembangan teknis dan bekerja sama dalam operasi teknologi keamanan dan infrastruktur informasi dan komunikasi yang stabil
Organisasi internasional	• Bekerja sama dengan organisasi standar teknologi internasional untuk informasi dan komunikasi internasional, serta mendapatkan teknologi baru

Pencegahan serta Penanganan Ancaman dan insiden

Penanganan secara efektif terhadap ancaman dan gangguan keamanan informasi membutuhkan kerja sama di antara organisasi informasi nasional, lembaga investigasi, dan lembaga hukum, serta organisasi yang melakukan inspeksi insiden keamanan dan mengestimasi kerusakan. Selain itu, perlu juga bekerja sama dengan organisasi yang mampu menganalisis kerentanan secara teknis dan memberikan langkah penanganan teknis.

Tabel 19. Contoh Kerja Sama dalam Penanganan Insiden Keamanan Informasi

Sektor	Kontribusi
Organisasi pemerintah	• Organisasi penanganan insiden keamanan: memberikan analisis situasi, menangani insiden peretasan, dan teknologi untuk menangani pelanggaran dan insiden • Organisasi informasi nasional: menganalisis dan menginspeksi keamanan informasi terkait pelanggaran dan insiden • Lembaga investigasi: Bekerja sama dengan organisasi yang terlibat dalam penahanan dan penuntutan tersangka pelaku insiden keamanan • Organisasi yang memberikan evaluasi keamanan: menguji keamanan dan keandalan produksi berbasis keamanan informasi dan jaringan informasi • Organisasi pendidikan keamanan informasi: menganalisis penyebab insiden keamanan informasi dan mengedukasi masyarakat untuk mencegah terulangnya insiden
Kelompok swasta	• Organisasi penanganan insiden swasta: memberikan dukungan dan penanganan teknis • Lembaga investigasi swasta: bekerja sama dengan lembaga investigasi pemerintah
Organisasi internasional	• Dalam kasus insiden dan ancaman internasional, melapor dan bekerja sama dengan Interpol, CERT/CC.

Pencegahan Insiden Keamanan Informasi

Pencegahan pelanggaran dan insiden keamanan informasi mencakup pengawasan, pendidikan dan manajemen perubahan. CSIRT nasional merupakan organisasi pengawas utama. Hal yang penting adalah menyesuaikan kebijakan informasi dan pengawasan data sesungguhnya. Oleh karena itu, penting untuk membahas ruang lingkup pengawasan kebijakan informasi. Lebih lanjut, penting untuk mengedukasi para pegawai pemerintah dan pihak swasta, serta masyarakat umum, mengenai kebijakan keamanan informasi. Hal ini

mungkin diperlukan untuk mengubah sikap tertentu terhadap informasi dan perilaku yang berdampak pada keamanan informasi. Manajemen perubahan dan pendidikan keamanan informasi ditetapkan dalam US SP 800-16 *(Information Technology Security Training Requirements)*.

Tabel 20. Contoh Kerja Sama Pencegahan Insiden & Pelanggaran Keamanan Informasi

Sektor	Koordinasi
Organisasi pemerintah	• Agen pengawasan: pengawasan jaringan berkelanjutan dan deteksi ancaman keamanan yang lebih canggih • Agen pengumpulan: berbagi informasi dengan organisasi internasional dan situs-situs keamanan • Lembaga pelatihan: pelatihan simulasi secara rutin untuk mengembangkan kemampuan menangani pelanggaran dan insiden keamanan informasi secara cepat
Organisasi swasta	• Penyedia ISP, kontrol keamanan dan perusahaan anti-virus: menyediakan statistik lalu lintas, informasi jenis serangan dan profil *worm*/virus
Organisasi internasional	• Memberikan informasi jenis serangan, profil *worm*/virus, dan lain-lain

Keamanan Privasi

Dibutuhkan kerja sama untuk menetapkan langkah perlindungan privasi internet, pencegahan insiden informasi lokasi pribadi, perlindungan informasi biologis, dan pelaporan pelanggaran privasi.

Tabel 21. Contoh Koordinasi dalam Perlindungan Privasi

Sektor	Koordinasi
Lembaga pemerintah	• Organisasi analis sistem: menjalankan bisnis terkait informasi lokasi pribadi, dan analisis tren dalam perlindungan informasi pribadi internal dan eksternal • Organisasi perencanaan: memperbaiki sistem/hukum, langkah teknis/administratif dan manajemen standar • Dukungan teknis: koordinasi sertifikasi pengguna siber untuk bisnis • Organisasi pelayanan: Mengoordinasikan dukungan untuk penanganan pelanggaran privasi dan *spam*

Organisasi swasta	• Organisasi keamanan informasi pribadi: menunjukkan kebutuhan dan mengatur asosiasi kerja sama untuk keamanan informasi pribadi • Konsultasi keamanan informasi pribadi
International organizations	• Bekerja sama untuk menerapkan standar kemanan informasi pribadi internasional

Kerja Sama Internasional

Keamanan informasi tidak dapat tercapai melalui upaya satu negara saja karena pelanggaran keamanan informasi cenderung berskala internasional. Oleh karena itu, kerja sama internasional dalam perlindungan keamanan informasi, baik di sektor pemerintahan maupun swasta, harus dilakukan.

Bagi sektor swasta, organisasi internasional yang relevan untuk kemajuan dan perlindungan keamanan informasi adalah CERT/CC. Di kalangan pemerintahan, ENISA (untuk Uni Eropa) dan ITU berfungsi untuk menumbuhkan kerja sama keamanan informasi antar berbagai negara.

Di setiap negara, harus terdapat lembaga pemerintahan yang berperan untuk membantu kerja sama organisasi pemerintah dan swasta dengan lembaga dan institusi internasional.

7.4. Tinjauan dan Evaluasi Keamanan Informasi

Langkah terakhir dalam penyusunan kebijakan keamanan informasi adalah mengevaluasi kebijakan dan melengkapi bidang yang kurang dikembangkan. Revisi kebijakan merupakan hal penting setelah efesiensi kebijakan keamanan informasi ditetapkan.

Metode evaluasi kebijakan dalam negeri dapat diterapkan untuk menentukan efesiensi kebijakan keamanan informasi nasional. Aspek-aspek metode ini dibahas sebagaimana penjelasan berikut.

Pemanfaatan lembaga audit

Terdapat berbagai lembaga yang berfungsi melakukan penilaian dan evaluasi kebijakan. Lembaga tersebut harus melakukan audit rutin terhadap kebijakan keamanan informasi nasional. Lebih lanjut, lembaga ini harus tidak terikat dengan lembaga penyusun kebijakan keamanan informasi dan lembaga yang menerapkan kebijakan tersebut.

Revisi kebijakan keamanan informasi

Berbagai permasalahan biasanya ditemukan selama proses audit kebijakan. Perlu ada proses untuk merevisi kebijakan dalam rangka mengatasi permasalahan tersebut

Perubahan lingkungan

Penting untuk bereaksi secara sensitif terhadap perubahan dalam lingkungan kebijakan. Perubahan yang timbul dari ancaman (serangan) dan kerentanan, perubahan infrastruktur TI, perubahan tingkat informasi kritis (penting), dan perubahan penting lainnya harus segera tergambarkan dalam kebijakan keamanan informasi nasional.

Latihan

Identifikasi lembaga pemerintah dan organisasi swasta di negara Anda yang perlu bekerja sama dalam penerapan kebijakan keamanan informasi nasional. Identifikasi juga organisasi yang perlu diajak bekerja sama.

Peserta pelatihan dari negara yang sama dapat melakukan kegiatan ini bersama.

Referensi

(ISC)². (2020). *Cybersecurity Certification: CISSP - Certified Information Systems Security Professional: (ISC)²*. Cybersecurity Certification| CISSP - Certified Information Systems Security Professional | (ISC)². http://www.isc2.org/cissp.

Asia Pacific Computer Emergency Response Team. *Background*. Background: About APCERT. http://www.apcert.org/about/background/index.html.

Carnegie Mellon University. (2017, January 18). CSIRT Frequently Asked Questions (FAQ). https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=485652.

Carnegie Mellon University. *Software Engineering Institute*. The CERT Division. https://www.sei.cmu.edu/about/divisions/cert/index.cfm.

CERT. (2002). *CSIRT Services*. Software Engineering Institute. Retrieved from https://resources.sei.cmu.edu/asset_files/WhitePaper/2002_019_001_53048.pdf

Commission of the European Communities, A European Programme for Critical Infrastructure Protection (2006). Brussels, Belgium. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF.

Commission of the European Communities, A strategy for a Secure Information Society – “Dialogue, partnership and empowerment” (2006). Brussels, Belgium. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0251&qid=1612332935197&from=EN.

Commission of the European Communities, Critical Information Infrastructure Protection: "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" (2009). Brussels, Belgium. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52009DC0149&qid=1612333230526&from=EN.

Commitment to a Free,Fair and Secure Cyberspace. NISC. (2018). https://www.nisc.go.jp/eng/.

Common Criteria. (2009). (publication). *Common Criteria for Information Technology Security Evaluation*. Retrieved from https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.pdf

Common Criteria. Common Criteria: New CC Portal. http://www.commoncriteriaportal.org/.

Council of Europe action against Cybercrime. Council of Europe. https://www.coe.int/en/web/portal/coe-action-against-cybercrime.

Council of the European Union, Council Conclusions on the Digital Agenda for Europe (2010). Brussels, Belgium. https://data.consilium.europa.eu/doc/document/ST-10130-2010-INIT/en/pdf.

Council of the European Union, Council Resolution of 18 December 2009 on a collaborative European approach to Network and Information Security (2009). Belgium, Brussels. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:321:0001:0004:EN:PDF.

Cross, D. (2017, January 10). *World's Most Recent & Biggest Hacking Incidents*. Web Hosting Media. https://webhostingmedia.net/recent-biggest-hacking-incidents.

Denning, D. E., Arquilla, J., & Ronfeldt, D. (2001). Activism, Hacktivism, And Cyberterrorism: The Internet As A Tool For Influencing Foreign Policy. In *Networks and Netwars. The Future of Terror, Crime, and Militancy* (pp. 239–288). essay, RAND Corporation.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. (1995). *Official Journal of the European Communities*, *38*(281), 31–50. https://doi.org/https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN

EGC Group. *EGC group*. European Government CERTs (EGC) group. http://www.egc-group.org/.

Egede, I. (2018, July 31). *Threat Hunting for File Hashes as an IOC*. Infosec Resources. https://resources.infosecinstitute.com/topic/threat-hunting-for-file-hashes-as-an-ioc.

ENISA. (2021, January 15). *About ENISA - The European Union Agency for Cybersecurity*. ENISA. http://www.enisa.europa.eu/about-enisa.

EUR-Lex, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504.

European Commission, A Digital Agenda for Europe (2010). Brussels, Belgium. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0245&qid=1612333676302&from=EN.

European Commission, Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision (2010). Brussels, Belgium. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010PC0517&qid=1612334410667&from=EN.

European Commission, Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 460/2004 establishing the European Network and

Information Security Agency as regards its duration (2010). Brussels, Belgium. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010PC0520&qid=1612335155929&from=EN.

European Commission, Proposal For A Regulation Of The European Parliament And Of The Council Concerning The European Network And Information Security Agency (ENISA) (2010). Brussels, Belgium. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010PC0521&qid=1612334562226&from=EN.

European Council, Conclusions of the European Council (25/26 March 2010) (2010). Brussels, Belgium. https://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/en/ec/113591.pdf.

Forum of Incident Response and Security Teams, Inc. (2020). *About FIRST*. FIRST. http://www.first.org/about.

Gillis, A. S. (2020, February 12). *What is an Intrusion Prevention System (IPS)?* SearchSecurity. https://searchsecurity.techtarget.com/definition/intrusion-prevention.

HM Government. (2016). (rep.). *National Cyber Security Strategy 2016-2021*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Information and Privacy Commissioner of Ontario, Planning for Success: Privacy Impact Assessment Guide (2015). https://www.ipc.on.ca/wp-content/uploads/2015/05/planning-for-success-pia-guide.pdf.

International Telecommunication Union. ICT Security Standards Roadmap. http://www.itu.int/ITU-T/studygroups/com17/ict/index.html.

International Telecommunications Union. (2006). World Summit on the Information Society: About WSIS. http://www.itu.int/wsis/basic/about.html.

International Telecommunications Union. (2021). ITU Cybersecurity Activities. http://www.itu.int/en/action/cybersecurity/Pages/default.aspx.

International Telecommunications Union. (2021). *ITU-D Cybersecurity*. ITU-D. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx.

International Telecommunications Union. *SG17 - Study Group Structure (Study Period 2017-2020)*. ITU. http://www.itu.int/net4/ITU-T/lists/sgstructure.aspx?Group=17&Period=16.

International Telecommunications Union. Study Group 17 at a glance. http://www.itu.int/net/ITU-T/info/sg17.aspx.

Internet Governance Forum. (2021). http://www.intgovforum.org/.

ISMS Accreditation Centre. *Overview of the ISMS conformity assessment scheme*. ISMS-AC. https://isms.jp/english/isms/about.html.

ITU-D ICT Applications and Cybersecurity Division. (2009). ITU National Cybersecurity/CIIP Self-Assessment Tool. http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html.

Killcrece, G. (2004). *Steps for Creating National CSIRTs*. Software Engineering Institute. Retrieved from https://resources.sei.cmu.edu/asset_files/WhitePaper/2004_019_001_53064.pdf

Killcrece, G., Kossakowski, K.-P., Ruefle, R., & Zajicek, M. (2003). *Organizational Models for Computer Security Incident Response Teams (CSIRTs)*. Software Engineering Institute. Retrieved from 10.1184/R1/6575921.v1

Korolov, M. (2019, June 27). *What is a botnet? When armies of infected IoT devices attack*. CSO Online. https://www.csoonline.com/article/3240364/what-is-a-botnet.html.

Kotadia, M. (2005, April 5). *E-mail worm graduates to IM*. ZDNet. https://www.zdnet.com/article/e-mail-worm-graduates-to-im/.

OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 9–17 (2013). Paris, France. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

OECD, OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (2002). Paris, France. https://www.oecd.org/digital/ieconomy/15582260.pdf.

OECD. (2006, May). OECD Working Party on Information Security and Privacy WPISP. Paris.

https://www.gpdp.it/documents/10160/10704/Working+Party+on+Information+Security+and+Privacy.pdf/586b9ff2-0ae8-4cb1-873a-2025fb6f5a15?version=1.1

Organisation for Economic Co-operation and Development. *Privacy Online: OECD Guidance on Policy and Practice*. OECD. https://www.oecd.org/digital/ieconomy/privacyonlineoecdguidanceonpolicyandpractice.htm.

Permanent Stakeholders' Group. (P. Dorey & S. Perry, Eds.), The PSG Vision for ENISA (2006). https://www.enisa.europa. eu/about-enisa/structure-organization/psg/files/psg-vision.

Ramasubramanian, S., & Shaw, R. (2007, September). ITU Botnet Mitigation Project: Background & Approach. International Telecommunication Union. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-botnet-mitigation-toolkit.pdf

Ramasubramanian, S., Ansari, S., & Purcell, F. (2005). Governing Internet Use: Spam, Cybercrime and e-Commerce. In D. Butt (Ed.), *Internet governance: Asia-Pacific*

Perspectives (pp. 89–104). essay, APDIP. https://www.unapcict.org/sites/default/files/2019-01/Internet%20Governance%20-%20Asia-Pacific%20perspectives.pdf.

Rosencrance, L. (2020, August 27). *What is advanced persistent threat?* SearchSecurity. https://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT.

SecureAuth. (2017, July 14). secureauth_ciam_infographic_170714.pdf. Irvine.

Shimeall, T. J., & Williams, P. (2002). Models of information security trend analysis. *Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Defense and Law Enforcement*. https://doi.org/10.1117/12.479291

Sinclair Community College. *Information Security Organization – Roles and Responsibilities*. Information Security Policy. https://it.sinclair.edu/index.cfm/services/student-and-guests-services/policies-and-security-information/information-security-policy/.

Stack, B. (2017, December 6). *Here's How Much Your Personal Information Is Selling for on the Dark Web*. Experian. https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

Tan, D. R. (1999). Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United Stats and European Union. *Loyola of Los Angeles International and Comparative Law Review*, *21*(4). https://digitalcommons.lmu.edu/ilr/vol21/iss4/5.

Telecommunications and Information. Asia-Pacific Economic Cooperation. (2020, April). https://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information.

U.S. Government Printing Office. (2014). *An Act to Provide for an Ongoing, Voluntary Public-Private Partnership to Improve Cybersecurity, and to Strengthen Cybersecurity Research and Development, Workforce Development and Education, and Public Awareness and Preparedness, and for Other Purposes*.

UN General Assembly, Guidelines for the Regulation of Computerized Personal Data Files (1990). https://www.refworld.org/docid/3ddcafaac.html.

Adopted by General Assembly resolution 45/95 of 14 December 1990. Contain procedures for implementing regulations concerning computerized personal data files.

The White House. (2003). (rep.). *The National Strategy to Secure Cyberspace*. Retrieved from https://www.hsdl.org/?view&did=1040

The White House. (2018). (rep.). *National Cyber Strategy of the United States of America*. Retrieved from https://www.defense.gov/Explore/News/Article/Article/1641969/white-house-releases-first-national-cyber-strategy-in-15-years/

Wikimedia Foundation. (2020, December 31). *Zero-day (computing)*. Wikipedia. https://en.wikipedia.org/wiki/Zero-day_(computing).

Wikimedia Foundation. (2021, February 1). *Antivirus software*. Wikipedia. http://en.wikipedia.org/wiki/Antivirus_software.

WSIS, WSIS: Plan of Action (2003). International Telecommunications Union. https://www.itu.int/net/wsis/docs/geneva/official/poa.html.

APCICT/ESCAP

Pusat Pelatihan untuk Teknologi Informasi dan Komunikasi untuk Pembangunan Asia dan Pasifik atau Asian and Pacific Training Centre for Information and Communication Technology for Development (APCICT) merupakan lembaga regional Komisi Ekonomi dan Sosial untuk Asia dan Pasifik atau Economic and Social Commission for Asia and the Pacific (ESCAP). APCICT bertujuan memperkuat upaya negara-negara anggota ESCAP untuk pemanfaatan TIK dalam rangka pembangunan sosial ekonomi mereka melalui peningkatan kapasitas manusia dan kelembagaan. Tugas APCICT difokuskan pada tiga pilar: pelatihan, berbagi pengetahuan, serta dialog dan kemitraan multi pemangku kepentingan. Mereka bersama-sama membentuk pendekatan terintegrasi untuk pengembangan kapasitas manusia TIK.

APCICT berlokasi di Incheon, Republik Korea.

http://www.unapcict.org

ESCAP

Komisi Ekonomi dan Sosial untuk Asia dan Pasifik atau Economic and Social Commission for Asia and the Pacific (ESCAP) merupakan platform antar pemerintah paling inklusif di kawasan Asia-Pasifik. Komisi tersebut mendorong kerja sama di antara 53 negara anggotanya dan 9 anggota asosiasi dalam mencari solusi untuk tantangan pembangunan berkelanjutan. ESCAP adalah salah satu dari lima komisi regional Perserikatan Bangsa-Bangsa.

Sekretariat ESCAP mendukung pembangunan yang inklusif, tangguh dan berkelanjutan di kawasan tersebut dengan menghasilkan pengetahuan yang berorientasi pada tindakan, dan dengan memberikan bantuan teknis dan layanan pengembangan kapasitas untuk mendukung tujuan pembangunan nasional, kesepakatan regional, dan pelaksanaan Agenda 2030 untuk Pembangunan Berkelanjutan.

https://www.unescap.org

UNITED NATIONS ESCAP
Economic and Social Commission for Asia and the Pacific
/ APCICT

Asian and Pacific Training Centre for Information and
Communication Technology for Development
5th Floor, G-Tower, 175 Art Center Daero, Yeonsu-gu,
Incheon, Republic of Korea

www.unapcict.org