ANALISA FAKTOR PENGARUH PEMBENTUKAN KELEMBAGAAN *COMPUTER EMERGENCY RESPONSE TEAM* (CERT) NASIONAL DENGAN MENGGUNAKAN ANALISIS PROSPEKTIF [33]

Ahmad Budi Setiawan
Peneliti Bidang Teknologi Informatika di Puslitbang Aptika & IKP
Balitbang SDM Kominfo

ABSTRACT

Along with the increasing volume of information security attacks in Indonesia, it takes the Information Security Response Team to deal with the threats. Related matter, Carnegie Mellon University established the Computer Emergency Response Team (CERT), which is currently spread throughout the world. Currently in Indonesia have had two information security incident response team, which is ID-SIRTII and CERT ID. Both teams did not have a coordinated response and a efektip command line. Thus the required institutional Information Security Response Team effective in Indonesia. In this research examined the factors that influence the institutional formation of the Information Security Response Team. This study was carried out qualitative and analytical methods are discussed in perspective analysis. Results from this study are the factors that influence the institutional of Information Security Response Team.

Keywords: *information security, the National Information Security Response Team, perspective analysis..*

ABSTRAK

Seiring dengan meningkatnya jumlah insiden serangan keamanan informasi di Indonesia, dibutuhkan adanya Tim Respon Keamanan Informasi untukmenghadapi ancaman tersebut. Terkait hal tersebut, Carnegie Mellon University telah mendirikan Computer Emergency Response Team (CERT) yang saat ini telah tersebar diseluruh dunia. Saat ini di Indonesia telah memiliki dua tim respon insiden keamanan informasi, yaitu ID-SIRTII dan ID CERT. Kedua tim respon tersebut tidak memiliki koordinasi dan garis komando yang efektip. Dengan demikian dibutuhkan kelembagaan Tim Respon Keamanan Informasi di Indonesia yang efektif. Dalam penelitian ini dikaji faktor-faktor yang mempengaruhi pembentukan kelembagaan Tim Respon Keamanan Informasi.

[33] Naskah yang dimuat dalam Jurnal MTI ini merupakan Kajian Akademik, yang di lakukan oleh Tim Peneliti di Balitbang SDM Kominfo tahun,anggaran 2011. Atas kesepakatan Tim ringkasan kajian Akademik tersebut di publikasikan di Jurnal MTI, oleh Ahmad Budi Setiawan atas nama Tim Peneliti.

Kajian ini dilakukan secara kualitatif dan dibahas dengan metode analisa perspektif. Hasil dari kajian ini adalah faktor-faktor yang mempengaruhi kelembagaan Tim Respon Keamanan Informasi tersebut.
Kata kunci: keamanan informasi, Tim Respon Keamanan Informasi Nasional, analisis perspektif

PENDAHULUAN

Latar Belakang

Keberadaan internet telah menciptakan suatu revolusi tersendiri di berbagai sektor, seperti; pemerintahan, industri swasta, komunitas akademik, dan aspek-aspek kehidupan lainnya. Pengguna internet semakin lama semakin meningkat jumlahnya. Diperkirakan bahwa di masa yang akan datang, internet akan menjadi kebutuhan pokok sebagaimana peran telekomunikasi dalam kehidupan sehari-hari. Mengingat adanya potensi tersebut, maka salah satu isu utama yang mengemuka adalah permasalahan keamanan atau *security* – baik dalam hal keamanan informasi (konten), infrastruktur, dan interaksi. Dalam konteks arsitektur internet yang demokratis, faktor resiko terbesar adalah terjadinya *incident* keamanan yang tidak diinginkan – baik yang dilakukan secara sengaja maupun tidak disengaja.

Masalah keamanan seringkali kurang mendapatkan perhatian dari para perancang dan pengelola sistem informasi. Bahkan kadang berada di urutan kedua, ketiga, atau diurutan terakhir dalam daftar hal-hal yang dianggap penting. Jika tidak menggangu perforam system, maka masalah keamanan seringkali tidak begitu diperdulikan, bahkan ditiadakan. Sehingga diperlukan suatu keamanan multimedia yang dapat membantu para perancang dan pengelola system informasi berbasis multimedia untuk mengamankan sistemnya. Ada begitu banyak peristiwa pertukaran informasi setiap detik di internet. Pertukaran informasi tersebut tentu tak lepas dari terjadinya pencurian informasi oleh pihak yang tidak bertanggung jawab. Beberapa ancaman keamanan terhadap informasi, antara lain[34]:

1. *Interruption* yakni suatu ancaman terhadap ketersediaan informasi; data yang berada dalam system computer dirusak atau dihapus, sehingga saat diperlukan, data atau informasi tersebut sudah tidak ada lagi.
2. *Interception* yakni ancaman terhadap kerahasiaan (*secrecy*). Informorasi yang ada disadap atau orang yang tidak berhak bisa mengakses computer tempat informasi tersebut disimpan.
3. *Modification*, merupakan ancaman terhadap integritas. Orang yang tidak berhak berhasil menyadap lalu lintas pengiriman informasi, lalu mengubahnya sesuai keinginan orang tersebut.

[34] Ariyus, D. (2009). *Keamanan Multimedia.* Yogyakarta: Andi Yogyakarta

4. *Fabrication*, merupakan ancaman terhadap integritas. Orang yang tidak berhak berhasil meniru (memalsukan) suatu informasi yang ada sehingga orang yang menerima informasi tersebut menyangka informasi tersebut berasal dari orang yang dikehendaki oleh si penerima informasi tersebut.

Pada sebuah masyarakat berbasis informasi saat ini, informasi menjadi asset yang sangat berharga bagi suatu organisasi, baik pemerintah maupun swasta. Oleh karena itu, informasi menjadi sangat penting untuk dilindungi dari hal-hal yang tidak diinginkan. Perlindungan atas informasi tersebut akan, secara langsung maupun tidak, menentukan kesuksesan suatu organisasi. Dengan kata lain manipulasi informasi, pencurian informasi, dan serangan terhadap informasi akan berpengaruh terhadap prestasi dan kinerja organisasi. Sehingga sangat diperlukan suatu manajemen dalam keamanan informasi yang bertugas merencanakan keamanan informasi, mengaplikasikannya, memonitor, dan melakukan evaluasi.

Karena disini pengamanan informasi adalah melindungi informamsi dari segala kemungkinanan ancaman yang akan berpengaruh terhadap kinerja dan prestasi organisasi dengan cara meminimalisisr kerugian yang bisa ditimbulkan serta memaksimalkan keuntungan dari investasi dan peluang organisasi tersebut. Dalam menghadapi serangan terhadap keamanan sistem informasi tersebut, Carnegie Mellon Software Engineering Institute melakukan inisiatif dengan membentuk sebuah lembaga nirlaba yaitu *Computer Emergency Response Team* (CERT). Organisasi CERT dapat merupakan sebuah organisasi, seperti organisasi formal atau adhoc lainnya, yang bertanggung jawab atas penerimaan, pemantauan dan penanganan laporan dan aktivitas insiden keamanan komputer. Tujuan diberntuknya lembaga ini untuk secara bersama menganalisis dan merespon ancaman keamanan sistem informasi serta memberikan layanan penanganan insiden keamanan komputer untuk meminimalisasi kerusakan dan memungkinkan pemulihan yang efisien dari insiden keamanan komputer[35].

Tim CERT akan bertanggung jawab penuh untuk memonitor dan mengelola berbagai isu-isu terkait dengan keamanan internet untuk menjaga aset informasi dan komunikasi dari seluruh unit-unit aktifitas organisasi. Dengan adanya CERT ini diharapkan ancaman terhadap kemanan sistem informasi dapat segera ditanggulangi. CERT Internasional milik Carnegie Mellon University sendiri memiliki anggota yang tersebar pada 5 benua di masing-masing negara. Jika terdapat insiden keamanan sistem informasi pada satu negara pada malam hari, di negara lain yang memiliki zona siang dapat dengan segera melakukan analisis dan tanggapan terhadap ancaman yang ada. Idealnya pada masing-masing Negara memiliki kontak poin (*point of contact*) dengan CERT Internasional dan komunitas CERT Negara lainnya.

---

[35] CERT, —CSIRT FAQ,□ Carnegie Mellon University, http://www.cert.org/csirts/csirt_faq.html

Lembaga CERT memberikan informasi dan membantu *stakeholder* dalam pelaksanaan langkah proaktif untuk mengurangi risiko insiden keamanan komputer, dan dalam investigasi, penanganan dan meminimalkan kerusakan akibat dari insiden. CSIRT juga menentukan dan merekomendasikan langkah-langkah lebih lanjut. Dua lapisan dalam CSIRT terdiri dari tim operasional yang bertugas untuk identifikasi awal, penanganan, *triage* dan penentuan kebutuhan eskalasi, dan tim manajemen yang bertugas untuk memelopori penanganan nasional terhadap insiden penting. Dalam hal tanggungjawab dan upaya yang dilakukan sebuah organisasi CERT, terdapat tiga domain usaha[36]. Domain pertama terkait dengan usaha yang bersifat reaktif, terkait dengan langkah-langkah yang harus dilakukan ketika terjadinya insiden keamanan informasi. Domain kedua terkait dengan strategi pencegahan. Pada domain ini terkandung beraneka ragam hal seperti: memberikan wawasan dan pendidikan kepada khalayak luas mengenai isu-isu seputar keamanan internet, melakukan audit terhadap teknologi informasi yang dipergunakan organisasi, menjalankan prosedur tes penetrasi kepada sistem yang dimiliki untuk mengidentifikasikan potensi kerawanan yang ada, mempelajari trend teknologi informasi dan internet ke depan terutama terkait dengan isu keamanan perangkat lunak dan peralatan-peralatan baru, dan lain sebagainya. Domain ketiga, adalah suatu usaha untuk meningkatkan level atau mutu kualitas organisasi yang saat ini telah dimiliki, agar semakin baik dalam aspek pengamanan informasi yang dimaksud.

Permasalahan Penelitian

Pada satu sisi, keamanan sistem informasi merupakan prioritas dalam terselenggaranya TIK, namun pada sisi lain, koordinasi antar lembaga, garis komando dan sinergi antar lembaga publik masih belum baik. Hal ini dapat dilihat dari adanya ID-SIRTII maupun ID-CERT yang tugas dan fungsinya sama, sehingga dalam hal penangan insiden sistem keamanan informasi Indonesia masih terlihat sporadis dalam hal kelembagaan. Di sisi lain, keamanan informasi masih merupakan isu pada masing-masing lembaga publik. Dengan demikian, saat ini di Indonesia belum ada bentuk kelembagaan CERT yang berfungsi sebagai pusat koordinasi antar CERT sektoral tingkat nasional sekaligus diakui menjadi kontak poin bagi komunitas CERT Internasional. Sebelum membentuk model kelembagaan CC-CERT Nasional yang ideal untuk diimplementasikan di Indonesia, perlu dilihat factor-faktor yang berpengaruh dalam pembentukan kelembagaan CC-CERT Nasional. Untuk menjawab permasalahan tersebut, dilakukan penelitian yang mengkaji faktor-faktor penentu dalam kelembagaan CC-CERT Nasional yang ideal dengan menggunakan *perspective analysis*.

---

[36] Prof. Ricahrdus Eko Indrajit; CERT, CSIRT, ID-SIRTII. Tim Pengawas Keamanan Internet

Kerangka Konsep

Focus Group Discussion (FGD) merupakan suatu metode pengumpulan data semi-terstruktur dimana sekumpulan partisipan yang terpilih berkumpul untuk mendiskusikan isu-isu dan hal-hal lain berdasarkan daftar topik yang disusun oleh peneliti/fasilitator (Kumar, 1987). FGD juga sekaligus dapat digunakan sebagai kerangka teori awal sebuah penelitian kualitatif. Pendekatan penelitian kualitatif ini pada awalnya dikembangkan untuk memberikan pemahaman yang lebih baik bagi para peneliti pemasaran yang diperoleh dari data survey kuantitatif konsumen. Sebagai suatu instrumen yang tidak terpisahkan dari peneliti pemasaran (Krueger 1988), focus group discussion menjadi populer karena menyediakan cara cepat untuk mempelajari peserta target (Debus 1988; US Department of Health and Human Services 1980). FGD terdiri dari 3 tahapan pelaksanaan, yaitu:

a. Persiapan diskusi
b. Fasilitasi diskusi
c. Mengidentifikasi dan menyusun masukan

Analisis Prospektif

Analisis prospektif digunakan dalam mengkuantifikasi data kualitatif. Analisis prospektif biasa digunakan dalam menyimpulkan hasil Focus Group Discussion sehingga bisa dilihat dalam bentuk matriks dan mampu menarik kesimpulan dari hasil diskusi. Analsisi prospektif digunakan bertujuan untuk menghasilkan klasifikasi faktor-faktor yang berkaitan dengan suatu masalah. Faktor-faktor tersebut, dipetakan keadalam 4 kuadran yaitu faktor penetu (INPUT) faktor berpengaruh (STAKE), faktor terikat (output) dan faktor bebas (UNUSED). Dalam prosesnya, teknik prospektif, secara umum terdiri dari 6 tahapan, yaitu:

Gambar 1 : Tahapan Pada Analisis Prospektif

Tahap 1: membuat Long-List

Tahap ini dapat dilakukan dengan melakukan diskusi atau memberikan kuesioner kepada para informan untuk menyebutkan apa saja dibenak para informan faktor-faktor yang mempengaruhi objek yang diteliti. Dari semua kuesioner yang diberikan kepada para informan, kemudian dituliskan untuk kemudian di diskusikan.

Tahap 2: membuat Short-List

Tahap ini yaitu untuk menghilangkan atau menggabungkan beberapa faktor yang sekiranya memiliki beberapa kesamaan. Beberapa faktor yang telah diungkapkan pada tahap sebelumnya, selanjutnya dimintakan lagi kepada Informan untuk mengeliminasi faktor-faktor yang tidak terlalu penting untuk dikaji.

Tahap 3: menentukan faktor kunci

Pada tahap ini informan diminta untuk menentukan nilai keterkaitan antar faktor tersebut dengan skala: Nilai 0 = apabila tidak berpengaruh; Nilai 1 = ada pengaruh tapi lemah; Nilai 2 = cukup berpengaruh; dan Nilai 3 = sangat berpengaruh. Setelah itu, hasil yang diperoleh dari penentuan nilai tersebut dimasukkan ke dalam matriks *Influences/Dependences* (I/D). Susunan matriks I/D dapat dilihat pada Tabel 2 di bawah ini dan membentuk matriks bujur sangkar. Untuk menentukan nilai I/D dipakai standar normatif (umum).

Sebaiknya saat penentuan penilaian, diselesaikan dulu perbaris horisontal atau Faktor A Berpengaruh Terhadap B, Faktor A Berpengaruh Terhadap C, dst. Kemudian Faktor B Berpengaruh pada A, Faktor B Berpengaruh Terhadap C, dst. Setelah semua baris selesai, kemudian dikoreksi dengan mengaitkan ketergantungan faktor dalam satu baris vertikal. Misalnya, Faktor A tergantung pada Faktor B, Faktor A tergantung pada C, dst. Bila menurut peserta terdapat perbedaan nilai antara nilai pengaruh dan ketergantungan, sebaiknya diambil nilai yang terkecil.

Tabel 1. Penilaian Keterkaitan Antar Faktor yang Berpengaruh

Influences (Pengaruh) → / Depedences (Ketergantungan) ↓	**A**	**B**	**C**	**D**	**E**	**F**	**Total Score**
A							
B							
C							
D							
E							
F							
Total Score							

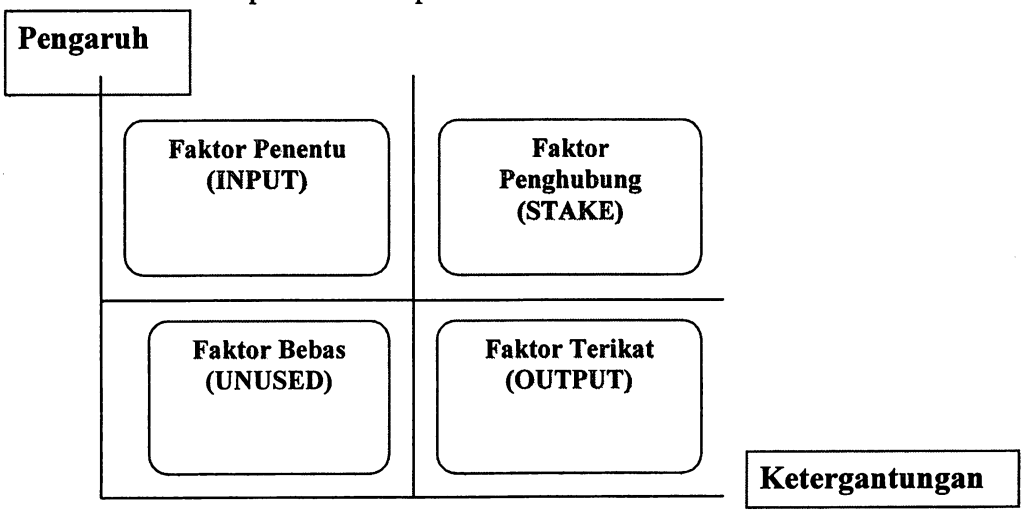
Berdasarkan *scoring* yang telah ada pada Tabel 4.2, maka disusun faktor-faktor tersebut ke dalam tabel yang memperlihatkan besarnya nilai masing-masing faktor, pada sisi pengaruh dan ketergantungan. Adapun hasil penyusunan yang dilakukan seperti terlihat pada Tabel 4.3 berikut

Tabel 2. Perhitungan Pengaruh dan Ketergantungan antarfaktor yang Berpengaruh

Faktor	**Faktor Berpengaruh**	**Ketergantungan Faktor**
A	Total *score* A pada satu baris	Total *score* A pada satu kolom
B	Sama dengan A	Sama dengan A
C		
Dst		

Berdasarkan Tabel 4.3, selanjutnya dipilih beberapa faktor dominan yang didasarkan pada hasil pemetaan grafik (*scatter diagram*).

Faktor-faktor yang berada di wilayah/kuadran *Faktor penentu,* dijadikan sebagai faktor dominan seperti terlihat pada Grafik 1.



Keterangan:

1. *Faktor Penentu* adalah faktor yang mempunyai nilai Pengaruh >1 dan nilai ketergantungannya <1. Artinya, keberadaan faktor tersebut sangat berpengaruh dan ketergantungan terhadap faktor lain sangat kecil.
2. *Faktor Penghubung* adalah faktor yang mempunyai nilai Pengaruh >1 dan nilai ketergantungannya >1. Artinya, keberadaan faktor tersebut dominan untuk mempengaruhi dan juga dominan dipengaruhi/ tergantung faktor lain

3. *Faktor Terikat* adalah faktor yang mempunyai nilai Pengaruh <1 dan nilai ketergantungannya >1. Artinya, keberadaan faktor tersebut sangat tergantung pada faktor lain
4. *Faktor Bebas* adalah faktor yang mempunyai nilai Pengaruh <1 dan nilai ketergantungannya <1. Artinya, keberadaan faktor tersebut dapat diabaikan

Tahap 4: menentukan tujuan strategis
Hasil analisis terhadap beberapa faktor yang menjadi penentu, maka mulai membangun skenario dan analisis dampak terhadap faktor penentu tersebut.
Tahap 5: mengidentifikasi evolusi
Pada tahap ini dengan menentukan skenario yang ada. Cara ini juga untuk menentukan skenario yang dilakukan terhadap faktor-faktor yang ada.

Tahap 6: menentukan strategi dan rekomendasi,
Tahap ini bertujuan untuk menghasilkan rekomendasi dengan melakukan rangkuman atau diskusi penutup.

Metode Penelitian

Penelitian kualitatif ini menggunakan teknik *Focus Group Discussion* (FGD) untuk pengumpulan data. Kemudian mengkuantitatifkan data atau informasi penelitian dilakukan dengan menggunakan metoda analisis prospektif. FGD yang dilkaukan melibatkan para narasumber yang memiliki latar belakang sebagai pakar dan praktisi di bidang keamanan sistem informasi. Selain itu adapula narasumber yang memiliki keterkaiatan dengan tim respon insiden keamanan informasi di Indonesia baik sebagai pengambil keputusan ataupun sebagai eksekutor langsung atau terlibat dalam menangani tim respon insiden keamanan informasi di Indonesia.

Para narasumber tersebut antara lain; Zainal Hasibuan, PhD (DeTIKNas), Ahmad Alkazimy (ID-CERT), Muhammad Salehuddin Manggalany (ID-SIRTII), Zainal Arifin (Praktisi IT dan Keamanan Informasi dari PT Inov8 Software), Iwan Sumantri (Praktisi IT dan Keamanan Informasi dari PT Telkom Bandung), Andika Triwidada (ID-CERT, Bandung). Terkait dengan metode analisis prospektif, maka FGD dilakukan sebanyak dua kali. FGD yang pertama dilakukan untuk melakukan tahap satu sampai dengan tahap tiga, yaitu; membuat *long-list*, membuat *short-list*, menentukan faktor kunci. Sedangkan FGD yang kedua bertujuan untuk menganalisa lebih dalam informasi yang didapat pada FGD sebelumnya. FGD kedua juga bertujuan untuk memenuhi tahapan penentuan tujuan strategis, identifikasi evolusi dan penentuan strategi serta rekomendasi.

Secara garis besar, pada FGD pertama digali faktor-faktor penentu dalam kelembagaan CERT Nasional. Pada FGD tersebut melibatkan beberapa narasumber, yaitu; Zainal Arifin (Praktisi IT dan Keamanan Informasi dari PT

Inov8 Software), Iwan Sumantri (Praktisi IT dan Keamanan Informasi dari PT Telkom Bandung), Andika Triwidada (ID-CERT, Bandung). Pada tahap ini, narasumber diminta untuk menyebutkan apa saja dibenak mereka tentang faktor-faktor yang mempengaruhi kelembagaan CERT Nasional.

Kemudian para narasumber diminta untuk menentukan nilai keterkaitan antar faktor tersebut dengan skala: Nilai 0 = apabila tidak berpengaruh; Nilai 1 = ada pengaruh tapi lemah; Nilai 2 = cukup berpengaruh; dan Nilai 3 = sangat berpengaruh. Setelah itu, hasil yang diperoleh dari penentuan nilai tersebut dimasukkan ke dalam matriks *Influences/Dependences* (I/D). Faktor-faktor kunci yang telah dihasilkan pada FGD pertama, kemudian dianalisa lebih mendalam pada FGD kedua dengan melibatkan narasumber pakar dalam bidang respon insiden keamanan informasi dan merupakan stakeholder dalam permasalahan tersebut. Narasumber yang terlibat, antara lain; Zainal Hasibuan, PhD (DeTIKNas), Ahmad Alkazimy (ID-CERT), dan Muhammad Salehuddin Manggalany (ID-SIRTII). Pada tahap ini dilakukan analisis terhadap beberapa faktor yang menjadi penentu, maka mulai membangun skenario dan analisis dampak terhadap faktor penentu tersebut.

GAMBARAN UMUM

Seiring dengan munculnya berbagai masalah dibidang keamanan informasi di berbagai belahan dunia, maka dibentuklah CERT yang diprakarsai oleh *Carnegie Mellon Software Engineering Institute* dan diberbagai belahan dunia juga mulai tumbuh sejumlah CERT yang dikelola oleh swasta secara mandiri[37]. Oleh karena itu, setiap lembaga CERT/CSIRT memiliki konstituennya masing-masing, karena perbedaan misi yang diembannya. Saat ini di Indonesia terdapat dua tim respon insiden keamanan informasi, yaitu ID-SIRTII dan ID-CERT.

A.ID-SIRTII

Indonesian Security Incident Response Team on Internet Infrastructure (ID-SIRTII) merupakan salah satu dari dua tim insiden keamanan internet yang dimiliki Indonesia saat ini dan dibentuk oleh pemerintah Republik Indonesia melalui Direktorat Jenderal Pos dan Telekomunikasi, Departemen Komunikasi dan Informatika. ID-SIRTII dibentuk Tanggal 4 Mei 2007 melalui Peraturan Menteri Nomor 26/PER/M.KOMINFO/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet. Menteri Komunikasi dan Informatika dalam hal ini menunjuk ID-SIRTII yang bertugas melakukan pengawasan keamanan jaringan telekomunikasi berbasis protokol internet. ID-SIRTII di Indonesia memiliki tugas pokok melakukan sosialisasi dengan pihak terkait tentang IT security (keamanan sistem informasi), melakukan pemantauan

[37] Prof. Ricahrdus Eko Indrajit; CERT, CSIRT, ID-SIRTII. Tim Pengawas Keamanan Internet

dini, pendeteksian dini, peringatan dini terhadap ancaman terhadap jaringan telekomunikasi dari dalam maupun luar negeri khususnya dalam tindakan pengamanan pemanfaatan jaringan, membuat/menjalankan/ mengembangkan dan database log file serta statistik keamanan Internet di Indonesia. Selain itu, ID-SIRTII memberikan bantuan asistensi/pendampingan untuk meningkatkan sistem pengamanan dan keamanan di instansi/lembaga strategis (critical infrastructure) di Indonesia. ID-SIRTII juga menyelenggarakan penelitian dan pengembangan di bidang pengamanan teknologi informasi/sistem informasi. Saat ini fasilitas laboratorium yang telah dimiliki antara lain: pusat pelatihan, laboratorium simulasi pengamanan, digital forensic, malware analysis, data mining dan menyelenggarakan proyek content filtering, anti spam dll. Rentannya pengamanan sistem informasi dapat menimbulkan ancaman, gangguan dan serangan. Bukan tidak mungkin kegiatan tersebut bisa menimbulkan kerugian ekonomis hingga berhentinya layanan bagi pengguna. Sebagai contoh: hilangnya sumber daya internet di Indonesia hanya karena terjadinya penumpukan paket informasi sampah akibat serangan yang dikirimkan oleh pihak yang tidak bertanggung jawab.

ID-SIRTII juga memiliki peran pendukung dalam penegakan hukum khususnya terhadap kejahatan yang memanfaatkan teknologi informasi. Terutama dalam penyajian alat bukti elektronik, ID-SIRTII memiliki fasilitas, keahlian dan prosedur untuk melakukan analisa sehingga dapat menjadikan material alat bukti tersebut bernilai secara hukum. Dalam suatu penyidikan, ID-SIRTII memiliki peran sentral dalam memberikan informasi seputar statistik dan pola serangan (insiden) di dalam lalu lintas internet Indonesia.

Gagasan untuk pendirian ID-SIRTII telah disampaikan oleh beberapa kalangan, yakni praktisi, industri, akademisi, komunitas teknologi informasi dan Pemerintah sejak tahun 2005. Para pendiri ini pada awalnya, antara lain: Direktorat Jenderal Pos dan Telekomunikasi, Kepolisian Republik Indonesia, Kejaksaan Agung Republik Indonesia, Bank Indonesia, Asosiasi Penyelenggara Jasa Internet Indonesia, Asosiasi Warung Internet Indonesia, Asosiasi Kartu Kredit Indonesia, Dan Masyarakat Telematika Indonesia.

Dasar hukum ID-SIRTII:

1. Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi
2. (Lembaran Negara Republik Indonesia tahun 1999 Nomor 154 dan Tambahan Lembaran Negara Nomor 3881).
3. Aspek pengamanan infrastruktur.
4. Peraturan Pemerintah Nomor 52 tahun 2000 tentang Penyelenggaraan Telekomunikasi
5. (Lembaran Negara Republik Indonesia tahun 2000 Nomor 107 dan Tambahan Lembaran Negara Nomor 3980).

6. Peraturan Menteri Komunikasi dan Informatika Nomor 27/PER/M. KOMINFO/9/2006.
7. Tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet (IP-Based)
8. Peraturan Menteri Komunikasi dan Informatika Nomor 26/PER/M. KOMINFO/5/2007.
9. Tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet.

ID-SIRTII memiliki tugas pokok yakni melakukan sosialisasi dengan pihak terkait untuk melakukan pemantauan dini, pendeteksian dini, peringatan dini terhadap ancaman terhadap jaringan telekomunikasi dari dalam maupun luar negeri khususnya dalam tindakan pengamanan pemanfaatan jaringan, membuat / menjalankan / mengembangkan dan database. Rentannya sistim pengamanan dalam suatu sistim informasi dapat menimbulkan beragam ganggu/ serangan/ ancaman terhadap sistim informasi. Bukan tidak mungkin, kegiatan tersebut menimbulkan kerugian ekonomis dikalangan pengguna teknologi informasi. Misalkan saja, hilangnya sumber daya internet di Indonesia hanya disebabkan oleh menumpuknya paket informasi yang dikirimkan oleh yang tidak bertanggung-jawab. Dalam melaksanakan tugas pokok dan fungsinya, ID-SIRTII memiliki struktur organisasi sebagai berikut:

1. Tim Pelaksana (Executive Board)
   Fungsi, tugas dan wewenangnya melakukan kegiatan pengawasan lalu lintas internet sebagaimana tertuang di dalam Peraturan Menteri Komunikasi dan Informatika Nomor 27/PER/M.KOMINFO/9/2006 Tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet juncto Peraturan Menteri Komunikasi dan Informatika Nomor 26/PER/M.KOMINFO/ 5/2007 Tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet.
2. Tim Pengawas (Inspection Board)
   Bertugas mengawasi pelaksanaan fungsi, tugas dan wewenang dari Tim Pelaksana dan bertanggung jawab kepada Menteri Komunikasi dan Informatika Republik Indonesia melalui Direktorat Jenderal Pos dan Telekomunikasi.
3. Tim Penasehat (Advisory Board)
   Bertugas memberikan saran dan rekomendasi bagi Tim Pelaksana di dalam menjalankan fungsi, tugas dan wewenangnya dan bertanggung jawab kepada Menteri Komunikasi dan Informatika Republik Indonesia melalui Direktorat Jenderal Pos dan Telekomunikasi.

Peran ID-SIRTII sebagai infrastruktur pendukung dalam penegakan hukum di Indonesia khususnya terhadap kejahatan yang memanfaatkan teknologi informasi menjadi begitu strategis. Terutama dalam penyajian alat bukti elektronik menjadi

bernilai secara hukum. Dalam suatu penyidikan, ID-SIRTII memilki peran sentral dalam memberikan informasi seputar lalu lintas internet di Indonesia.

B. ID-CERT

Indonesia-Computer Emergency Respons Team (ID CERT) merupakan sebuah forum CERT pertama yang berdiri di Indonesia pada 1998. ID-CERT merupakan sebuah forum koordinasi berbasis komunitas dan untuk komunitas yang bersifat independen. ID-CERT memiliki tujuan untuk melakukan koordinasi penanganan insiden yang melibatkan pihak Indonesia dan luar negeri. Organisasi/ kelembagaan ID CERT adalah bersifat voluntir. Kegiatan ID CERT sebagai respon terhadap kebutuhan pelaporan masalah security yang terkait dengan internet Indonesia sudah dimulai sejak tahun 1998 selain itu, ID CERT juga memasyarakatkan pentingnya keamanan internet di Indonesia serta melakukan berbagai penelitian dibidang keamanan internet yang dibutuhkan oleh komunitas internet Indonesia. ID-CERT bukanlah lembaga/instansi pemerintah, akan tetapi dibangun oleh komunitas dan hasilnya akan kembali kepada komunitas. Dengan demikian, ID-CERT tidak memiliki otoritas secara operasional terhadap konstituensinya baik di Indonesia maupun luar negeri, melainkan hanya menginformasikan berbagai keluhan atas insiden jaringan, serta bergantung sepenuhnya pada kerjasama dengan para-pihak yang terlibat dalam insiden jaringan terkait. Dalam aktivitasnya, ID CERT juga melakaukan koordinasi dengan organisasi CERT regional, seperti My CERT, JP CERT, Aus CERT dan lain sebagainya.
Adapun aktifitas ID CERT, antara lain;

1. Respon "reaktif", berdasarkan laporan yang diterima dari komunitas internet;
2. Riset Internet *Abuse* Indonesia, yang dimulai sejak 2010;
3. Membuat statistik tahunan;
4. Koordinasi dengan tim CERT regional, (seperti: Malaysia CERT, Australian CERT, Japan CERT, dsb);
5. Membangun kesadaran publik tentang pentingnya IT Security melalui Gathering dan Seminar publik.

Program ID CERT lainnya adalah Security Drill, yaitu sebuah simulasi penanganan insiden keamanan informasi dengan berbagai skenario, termasuk namun tidak terbatas pada:

1. Serangan Deface secara masif dan massal;
2. Serangan DDoS yang mengakibatkan lumpuhnya DNS;
3. Serangan Malware yang mengakibatkan kelumpuhan pada jaringan internet;

Kegiatan Security Drill dilakukan sekurang-kurangnya satu kali dalam setahun dari lokasi kerja masing-masing konstituen ID CERT pada waktu yang telah disepakati. Adapun tujuan program ini adalah untuk melatih kesiapsiagaan konstituen bila terjadi keadaan darurat internet. Disamping itu, ID CERT juga melakukan Program riset Statistik Internet *Abuse* yang telah dilaksanakan pada

tahun 2010 dan pada awal tahun 2011. Untuk menunjang aktivitasnya, ID CERT dilengkapi dengan fasilitas Laboratorium Malware.

Fungsi laboratorium ini antara lain: Melakukan Survey Malware; Memparsing data survey Malware ke satu server tertentu/Honeypots; Mencatat nama Malware yang berkembang di Indonesia; Membuat statistik bulanan, Top 10 Malware, Virus, Worm khas Indonesia. Secara finansial, ID CERT mendapatkan dukungan dari Asosiasi Penyedia Jasa Internet Indonesia (APJII) untuk melakukan penelitian dan aktifitas rutin. Disamping itu APJII juga memberikan dukungan data statistik untuk Penelitian ID-CERT serta Dukungan Perangkat yang dibutuhkan.

HASIL DAN PEMBAHASAN

A. Hasil Penelitian

Analisis Prospektif : berdasarkan hasil riset dengan menggunakan metode Focus Group Discussion yang melibatkan beberapa pakar/praktisi IT Security dan juga stake holder dalam hal tim respon insiden keamanan informasi; Zainal Arifin (Praktisi IT, Keamanan Informasi dari PT Inov8 Software), Iwan Sumantri (Praktisi IT, Keamanan Informasi dari PT Telkom Bandung), Andika Triwidada (ID-CERT), Zainal Hasibuan, PhD (DeTIKNas), Ahmad Alkazimy (ID-CERT), dan Muhammad Salehuddin Manggalany (ID-SIRTII). didapatkan hasil sebagai berikut;

a. Semua bentuk insiden keamanan informasi pada dasarnya harus harus ditangani oleh CERT, akan tetapi intensitasnya berbeda-beda, bergantung pada kapabilitas dan beban yang sedang dimiliki termasuk seperti apakah CERT CC akan melakukan tindak lanjut dari permasalahan yang ada;
b. CERT CC tidak menghandle insiden secara langsung, akan tetapi diteruskan kepada sektor yang ada. CERT CC lebih kepada mengklasifikasikan, menerima laporan dan mendiseminasikan informasi yang ada kepada masyarakat. CERT CC bersikap lebih menjadi koordinator.
c. Terdapat CERT Sektoral & CERT Regional menyangkut luas wilayah Indonesia dengan jumlah penduduk yang sangat banyak. CERT tidak hanya CERT CC tapi CERT Sektoral / Regional. Insiden yang perlu ditangani;
   - klasifikasi insiden -> Klasifikasi keamanan informasi.
   - Isu-isu nasional, seperti E-KTP / Pemilu.
   - International Cyberwar
   - Gov CERT (Pemerintah)
   - CERT CC tidak perlu melakukan penanganan langsung dari isu-isu yang muncul.
   - Untuk isu-isu nasional penanganan dapat dilakukan oleh CERT CC. Gov CERT bisa memiliki sub-sub seperti Gov CERT, dll.
d. Pada intinya diharapkan CERT CC merupakan lembaga yang siap berjalan terus dan berkesinambungan. Perlu dikaji lagi tentang bentuk kelembagaan CERT CC yang ideal dan menjamin keberlangsungan CERT CC
e. Diharapkan terbentuknya CERT CC dengan lebih mementingkan faktor kompetensi dalam SDMnya, tidak berdasarkan subjektifitas. Hal ini dikarenakan konsep CC yang

lebih dengan koordinasi sehingga diperlukan faktor komunikasi yang baik, komunikasi yang berdasarkan berdasarkan relasi dan kepercayaan.

Dari hasil pertanyaan Pra-Kuesioner di Bandung, di dapat bahwa terdapat 7 faktor yang mempengaruhi kelembagaan CERT di Indonesia kedepannya yaitu:

Faktor	Alasan
Regulasi	1. Regulasi akan menjadi payung hukum keberadaan dan operasional CERT. 2. Menentukan posisi dan kewenangan CERT 3. Menunjukkan tingkat awareness pemerintah dalam keamanan informasi.
Batasan Kewenangan	1. Dengan adanya batasan kewenangan dalam lingkup operasional CERT, maka akan semakin jelas Tugas pokok dan fungsinya, sehingga memungkinkan pembentukan lembaga insiden respon sejenis lainnya, baik secara horisontal (seperti : Gov-CERT, IIC-CERT dan EDU-CERT) maupun vertikal (seperti : Gov-CERT dengan Jabar-CERT. 2. Kewenangan CERT semakin jelas, yang akan membedakannya dengan lembaga atau bidang lain yang menangani keamanan informasi, seperti : Forensik Insiden Keamanan Informasi, Tata Kelola Keamanan Informasi, Audit Keamanan Informasi, dll.
Kelembagaan	1. Dengan kondisi Indonesia (Kepulauan), luas wilayah dan penduduknya (230 juta lebih), maka penanganan CERT semakin komplek, diperlukan model kelembagaan yang spesifik (CERT/CC, Gov-CERT, IIC-CERT dan EDU-CERT). 2. Koordinasi dan kerjasama antar lembaga dan tim menjadi penentu bagi tingkat keberhasilan CERT dalam penanganan keamanan informasi.
Respon komunitas	Komunitas menjadi kekuatan utama dalam pembentukan CERT, melalui dukungan komunitas inilah CERT dapat menjalankan peranannya dan menjadi lebih "mature" dalam penanganan keamanan informasi.
Koordinator CERT	Pembentukan CERT CC yang mengkoordinir CERT yang sudah ada

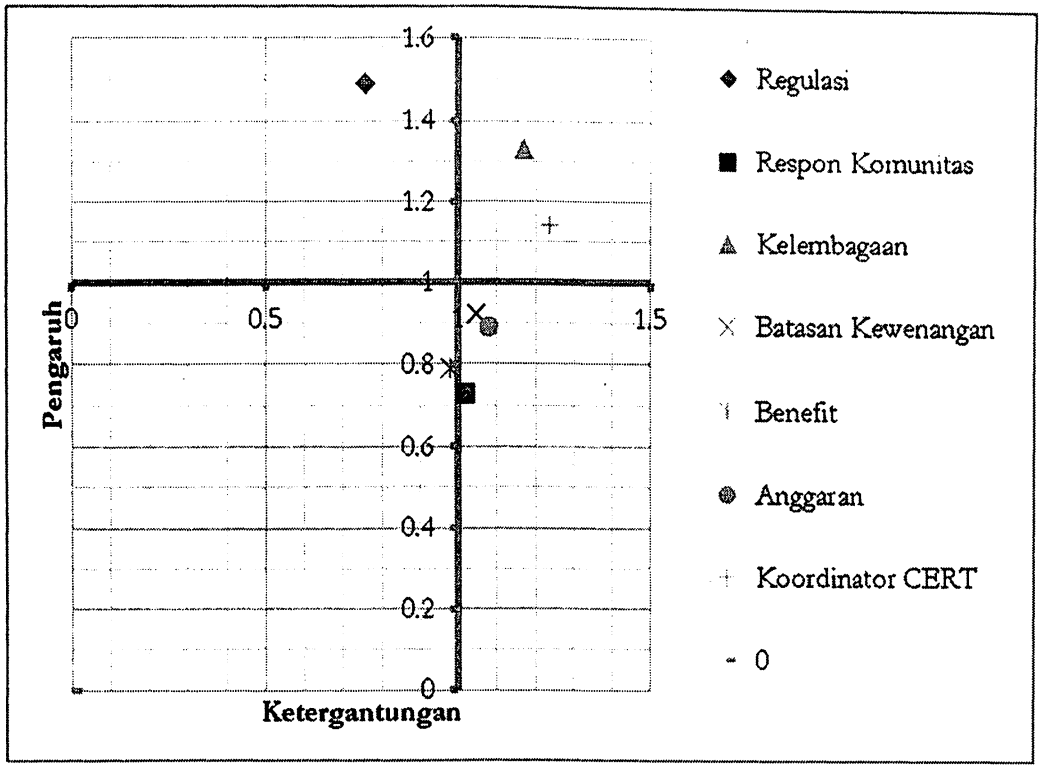
Dari ke tujuh faktor tersebut, masing-masing narasumber diminta untuk melakukan scoring terhadap faktor mana yang berpengaruh dan faktor mana yang

tergantung. Dari ketujuh faktor tersebut hasil yang didapatkan nilai scooring sebagai berikut:

Influences (Pengaruh) / *Dependences* (Ketergantungan)	Regulasi	Respon Komunitas	Kelembagaan	Batasan Kewenangan	Benefit	Anggaran	Koordinator CERT	TOTAL SCORE
Regulasi		2.67	2.67	3	1.67	3	2.67	15.67
Respon Komunitas	1.67		1.33	1	1.33	0.67	1.67	7.67
Kelembagaan	1.67	1.67		3	2.33	3	2.33	14
Batasan Kewenangan	1	1.67	2.33		1.33	1	2.33	9.67
Benefit	1.33	2	1	1		1.33	1.67	8.33
Anggaran	1	0.33	3	1.33	1.33		2.33	9.33
Koordinator CERT	1.33	2.33	2	1.67	2.33	2.33		12
TOTAL SCORE	8	10.67	12.33	11	10.33	11.33	13	76.67

Dari hasil faktor diatas, didapat bahwa faktor-faktor tersebut dapat dipetakan Influence (pengaruh) dan Dependencies (ketergantungan) sebagaimana yang dilihat pada tabel berikut.

Faktor	Pengaruh	Ketergantungan	Influence (I)	Dependences (D)	Koordinat (I ; D)	Klasifikasi Faktor
Regulasi	15.66666667	8	1.49	0.76	(1.49 ; 0.76)	Faktor Penentu
Respon Komunitas	7.666666667	10.66666667	0.73	1.02	(0.73 ; 1.02)	Fakor Terikat
Kelembagaan	14	12.33333333	1.33	1.17	(1.33 ; 1.17)	Faktor penghubung
Batasan Kewenangan	9.666666667	11	0.92	1.05	(0.92 ; 1.05)	Fakor Terikat
Benefit	8.333333333	10.33333333	0.79	0.98	(0.79 ; 0.98)	Faktor Bebas
Anggaran	9.333333333	11.33333333	0.89	1.08	(0.89 ; 1.08)	Fakor Terikat
Koordinator CERT	12	13	1.14	1.24	(1.14 ; 1.24)	Faktor penghubung



Berdasarkan hasil tersebut, dapat dilihat bahwa:

1. Faktor Penentu, adalah faktor utama yang menentukan pembentukan CERT kedepannya, dalam hal ini yakni regulasi. Narasumber berpendapat bahwa hal utama yang wajib dipenuhi untuk pembentukan CERT adalah regulasi ideal yang akan menjadi payung hukum keberadaan dan operasional CERT. Sementara itu, regulasi juga berfungsi untuk menentukan posisi dan kewenangan CERT serta dengan adanya regulasi menunjukkan tingkat awareness pemerintah dalam keamanan informasi.
2. Faktor Penghubung: yaitu faktor yang dinilai dominan, namun juga masih terkait dengan faktor lain, dalam hal ini faktor kelembagaan dan faktor koordinator CERT. Kedua faktor ini dinilai faktor yang penting, namun posisinya dipengaruhi oleh kuatnya regulasi yang akan dibentuk.
3. Faktor Terikat: adalah faktor yang dipengaruhi faktor lain dan tergantung dari kesuksesasn diterapkannya faktor lain, dalam hal ini faktor Batasan Kewenangan, Anggaran dan respon komunitas yang dipengaruhi oleh faktor regulasi serta kelembagaan dan suksesnya implementasi koordinator CERT.
4. Faktor Bebas: dalah faktor yang dianggap bisa diabaikan yakni benefit, atau keuntungan yang diperoleh oleh masyarakat

Analisis Faktor Kunci

Pada hasil analisis Prospektif, terdapat dua faktor yang sangat berpengaruh dalam kelembagaan CERT, yaitu; Faktor Penentu dan Faktor Penghubung. Faktor Penentu adalah faktor utama yang menentukan pembentukan Kelembagaan CERT kedepan. Semantara itu, Faktor Penghubung yaitu faktor yang dinilai dominan, namun juga masih terkait dengan faktor lain. Adapun factor terkait dan faktor bebas tidak memiliki pengaruh yang signifikan dalam pembentukan kelembagaan CERT Nasional. Dalam hal ini, didapatkan bahwa faktor penentu yang paling banyak dipilih oleh mayoritas narasumber yakni regulasi. Mayoritas narasumber berpendapat bahwa hal utama yang wajib dipenuhi untuk pembentukan Kelembagaan CERT adalah regulasi yang ideal yang akan menjadi payung hukum keberadaan dan operasional CERT. Sementara itu, regulasi juga berfungsi untuk menentukan posisi dan kewenangan CERT serta dengan adanya regulasi menunjukkan tingkat awareness pemerintah dalam keamanan informasi. Disamping itu, Regulasi diperlukan untuk hubungan antar CERT dan/atau untuk CERT Nasional (CC CERT).

Regulasi dapat memberikan arah dan kebijakan yang jelas terhadap CERT Nasional. Faktor kelembagaan dan faktor koordinator CERT merupakan Faktor Penghubung yang paling banyak dipilih oleh mayoritas narasumber. Kedua faktor ini dinilai faktor yang penting, namun posisinya dipengaruhi oleh kekuatan regulasi yang akan dibentuk. Kelembagaan yang kuat dan memiliki power sangat diperlukan karena cakupan kerja dan kompleksitas system yang ditangani sangat luas. Disamping itu, dengan adanya kordinator CERT diharapkan dapat membentuk suatu forum diskusi sehingga dapat menghasilkan pendapat dan berbagai macam argumentasi yang lebih rasional dan ilmiah karena mengakomodasi seluruh pendapat untuk tujuan penyatuan, Dengan demikian, dalam kelembagaan CERT sangat dibutuhkan adanya regulasi yang melandasi pembentukannya. Regulasi akan mempengaruhi kelembagaan dan wewenang serta model koordinasi kelembagaan CERT tersebut.

B. Pembahasan

Regulasi : berdasarkan hasil peneltian ini, maka didapatkan bahwa bentuk kelembagaan CC CERT Nasional harus dilandasi dengan adanya regulasi. Penyusun regulasi perlu memperhatikan beberapa hal, seperti dasar pemikiran kebijakan, sumber daya yang tersedia, arah kebijakan, kebutuhan hukum dan anggaran, serta hasil yang diharapkan. Regulasi kelembagaan CC CERT Nasional harus mencakup strategi keamanan informasi, hubungan resmi, organisasi keamanan informasi, teknologi keamanan informasi, dan hubungan antar mereka. Dengan demikian, penyusun regulasi tersebut perlu mempertimbangkan aspek sumber daya manusia dan organisasi keamanan informasi. Regulasi CC CERT Nasional juga perlu melibatkan kalangan swasta, akademisi dan komunitas dalam bidang yang terkait dengan keamanan informasi. Mereka perlu mengetahui organisasi yang terlibat dalam bidang keamanan informasi dan memahami lingkup kerja, peran dan tanggung jawab mereka. Hal ini perlu diterapkan agar tidak terjadi duplikasi struktur dalam keamanan informasi.

Untuk menjamin keberlangsungan lembagaan CC CERT Nasional yang akan dibentuk, maka regulasi yang melandasi kelembagaan CC CERT Nasional tersebut harus dibuat dengan regulasi negara dengan tingkatan yang tertinggi. Regulasi tertinggi dalam sebuah negara adalah regulasi setingkat Undang-Undang. Dengan landasan Undang-Undang, CC CERT Nasional secara struktural berada dibawah garis komando Kepresidenan. Meskipun kedudukan Kelembagaan CC CERT Nasional berada setingkat menteri, namun CERT Nasional bukanlah dipimpin oleh seorang menteri. CC CERT Nasional berkoordinasi dengan instansi-instansi pemerintah baik pusat maupun daerah dan instansi lainnya, seperti; penyedia jasa internet, akademisi, instansi swasta serta komunitas yang memiliki kepentingan dalam hal keamanan informasi.

Kelembagaan dan Koordinator CERT

Sebagai negara kepulauan dengan wilayah yang sangat luas, maka penanganan masalah keamanan infroasi menjadi semakin komplek, diperlukan model kelembagaan yang spesifik (CERT/CC, Gov-CERT, IIC-CERT dan EDU-CERT). Untuk memudahkan pelaksanaan tugas CC CERT Nasional, maka perlu adanya koordinasi dan kerjasama antar lembaga dan tim menjadi penentu bagi tingkat keberhasilan CERT dalam penanganan keamanan informasi. Kelembagaan dapat memperkuat CERT secara institusi. Kelembagaan CERT Nasional yang efektif dan memiliki kekuatan hukum yang kuat sangat diperlukan karena cakupan kerja dan kompleksitas system yang ditangani sangat luas

Setiap Kementerian/Lembaga memiliki sebuah CERT, yaitu Kementerian CERT (Departement CERT) yang berada dibawah koordiansi Government CERT. Kelembagaan Government CERT merupakan sebuah CERT Sektoral dibawah koordinasi CC CERT Nasional. Hal ini dimaksudkan agar Kelembagaan CERT Nasional dapat mengampu kepentingan setiap Kementerian/Lembaga yang memiliki kaitan tugas pokok dan fungsi terkait dengan Keamanan Sistem Informasi dan Transaksi Elektronik atau memiliki *critical infrastructure* agar tidak terjadi tabrakan kepentingan. Kelembagaan CC CERT Nasional sebagai Lembaga yang dibentuk dengan landasan sebuah Undang-Undang dan berada langsung dibawah Presiden dengan koordinasi Kementerian Kominfo serta Kementerian lain yang memiliki kepentingan dengan keamanan informasi.

PENUTUP

Kesimpulan

Faktor utama penentu Lembaga CERT di Indonesia adalah regulasi, sehingga CERT diharapkan menjadi lembaga yang mampu menciptakan iklim kondusif terhadap keamanan komunikasi dan informasi yang bersifat proaktif, reaktif dan berkolaborasi secara efektif dengan melibatkan institusi-institusi yang relevan

dalam struktur kelembagaan. Sementara itu, regulasi juga berfungsi untuk menentukan posisi dan kewenangan CERT serta dengan adanya regulasi menunjukkan tingkat awareness pemerintah dalam keamanan informasi. Alasan perlunya regulasi dalam kelembagaan CERT;

1. Regulasi akan menjadi payung hukum keberadaan dan operasional CERT.
2. Menentukan posisi dan kewenangan CERT
3. Menunjukkan tingkat awareness pemerintah dalam keamanan informasi.

Keberadaan regulasi sebagai landasan dalam pembentukan CC CERT dapat menjamin keberlangsungan kelembagaan CC CERT yang akan dibentuk. Keberadaan regulasi sebagai landasan dalam pembentukan CC CERT Nasional dapat menjamin keberlangsungan kelembagaan CC CERT Nasional yang akan dibentuk. Semakin tinggi landasan hukum yang mendasari pembentukan CC CERT Nasional semakin kuat posisi dan kewenangan CC CERT Nasional T tersebut. Persyaratan kelembagaan sebuah CC CERT Nasional harus permanen dan dapat mengatur koordinasi CERT sektoral dibawahnya.Disamping itu, wewenang sebuah CC CERT Nasional harus dapat bekerja secara lintas sektoral.

Kelembagaan CC CERT Nasional yang kuat dan memiliki power (kekuatan-wewenang) sangat diperlukan karena cakupan kerja dan kompleksitas system yang ditangani sangat luas. Kewenangan yang di buat buat berdasarkan UU merupakan sebuah landasan hukum tertinggi diatas PP atau Peraturan Menteri (PERMEN) dan dapat berlaku untuk lintas sektoral. Dengan demikian, dapat disimpulkan harus ada regulasi tertinggi, yaitu peraturan Per-Undang-Undangan yang melandasi kelembagaan CC CERT Nasional. Hal ini disebabkan semakin tinggi regulasi yang menaungi pembentukan kelembagaan CC CERT Nasional, maka semakin luas wewenang CC CERT Nasional tersebut dan semakin tinggi posisi kelembagaannya. Dengan demikian kelembagaan CC CERT Nasional dapat bersifat sustainable.

Rekomendasi

Berdasarkan hasil riset Kelembagaan CERT Nasional ini perlu dilandasi dengan adanya regulasi tertinggi setingkat Undang-Undang. Mengingat pembuatan regulasi adalah suatu proses yang panjang dan harus dapat menaungi semua pihak dan segala kepentingan, maka dalam hasil penelitian ini direkomendasikan untuk memasukkan regulasi CERT ini kedalam Undang-Undang No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik pada Bab IV: Penyelenggaraan Sertifikasi Elektronik dan Sistem Elektronik, Bagian Kedua: Penyelenggaraan Sistem Elektronik, yaitu dengan penambahan pasal yang mengatur tentang kelembagaan CERT Nasional di Indonesia. Dismping itu, mengingat saat ini masih dalam masa harmonisasi bagi Undang-Undang No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, maka dapat

direkomendasikan untuk menambahkan regulasi tentang CERT Nasional dalam klausa Undang-Undang tersebut sebagaimana telah diusulkan.

Daftar Pustaka

Ariyus, D. (2009). *Keamanan Multimedia.* Yogyakarta: Andi Yogyakarta

Bourgeois, R. &. (2004). *Participatory Prospective Analysis: Exploring And Anticipating Challenges With Stakeholders.* UNESCAP-CAPSA.

Carnegie Mellon University. (2011, Juni 22). *National Computer Security Incident Response Teams.* Dipetik Agustus 16, 2011, dari CERT: http://www.cert.org/csirts/national/contact.html

Korea Information Security Agency . (2009). *Keamanan Jaringan dan Keamanan Informasi dan Privasi.* Akademi Esensi TIK untuk Pimpinan Pemerintah. UNESCAP/APCICT.

http://pdf.usaid.gov/pdf_docs/PNADQ392.pdf. Panduan Pelatihan "Citizen Report Card, Panduan Monitoring Pelayanan Publik Berbasis Masyarakat". USAID dan LGSP. Diakses pada 15 agustus 2011.

http://ricehoppers.net/wp-content/uploads/2009/10/focus-group-discussion.pdf. Focus Group Discussion. M. Escalada and K.L. Heong. Diakses pada 12 Agustus 2011.