TLP : WHITE

COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT)

STARTER KIT v1.0

DAFTAR ISI

PENDAHULUAN

CSIRT dibentuk berdasarkan tujuan dan latar belakang masing-masing organisasi, sehingga CSIRT akan memiliki model/struktur yang berbeda-beda. Hal ini juga akan menyebabkan operasional setiap CSIRT dapat berbeda-beda.

Dokumen ini menjelaskan tahapan-tahapan yang perlu diperhatikan dan dirumuskan dalam pembentukan *Computer Security Incident Response Team* (CSIRT) di Indonesia yang bertujuan sebagai panduan umum untuk membentuk CSIRT. Dokumen ini juga dapat digunakan sebagai referensi ketika mengevaluasi kesesuaian operasional CSIRT dengan organisasi.

Kami berharap dokumen ini dapat digunakan secara efektif dalam proses pembentukan CSIRT, sehingga dengan terbentuk dan beropersionalnya CSIRT dapat meningkatkan keamanan siber di Indonesia.

Depok, Juli 2021

COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT)

Melihat kemajuan besar akhir-akhir ini dalam komputerisasi, sistem informasi memainkan peran yang semakin penting dan informasi yang diproses oleh sistem tersebut sangat penting untuk keberlangsungan proses bisnis organisasi. Atas alasan tersebut, organisasi yang tidak memiliki alat untuk mengidentifikasi penyebab insiden keamanan komputer ("Insiden") atau rencana perbaikan sistem yang tepat dapat mengalami penurunan produktivitas, kehilangan kepercayaan, membayar sejumlah besar kerusakan pada orang luar dalam beberapa kasus, atau menghadapi keadaan yang mengancam keberadaan organisasi karena terjadinya insiden memiliki dampak signifikan pada proses bisnis organisasi.

Kemungkinan tidak ada organisasi yang mampu mengambil segala tindakan keamanan untuk mencegah setiap potensi Insiden. Meskipun sebuah sistem semakin canggih, sangat tidak mungkin menghilangkan potensi terjadinya insiden, tanpa peduli seberapa aman sistem informasi yang dibangun dan dioperasikan.

CSIRT tidak hanya terlibat dalam analisis dan respon terhadap insiden yang terjadi, tetapi dapat terlibat dalam kegiatan seperti edukasi dan monitoring sistem untuk meningkatkan kualitas keamanan. Kegiatan ini dimaksudkan untuk menerapkan insiden respon yang efektif dan untuk mengurangi risiko bisnis.

Membangun CSIRT akan memberikan manfaat sebagai berikut:

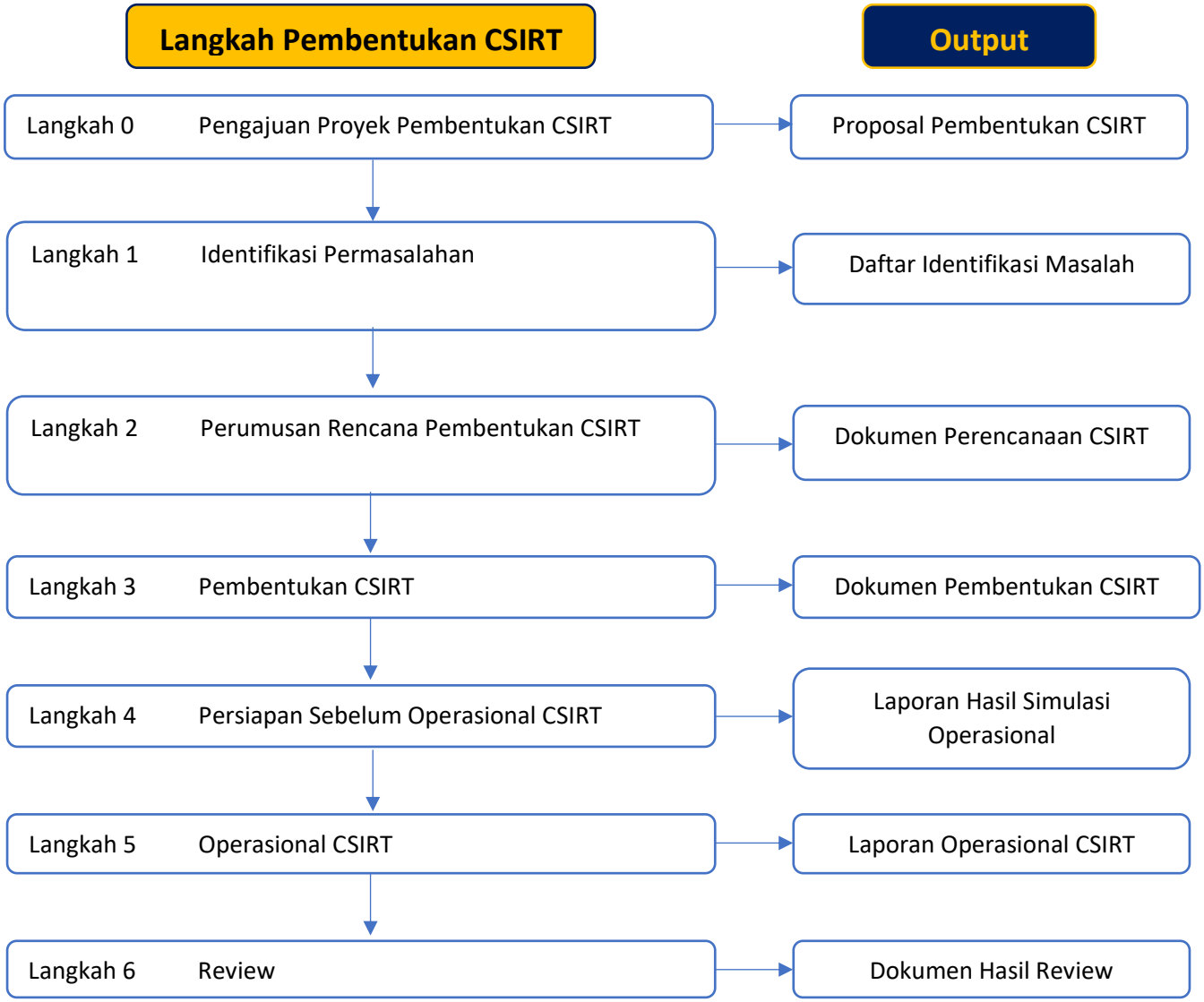
- Mendeteksi Insiden dan *Security Events*[*)] dengan cepat dan secara akurat menyampaikan informasi kepada organisasi;
- Dokumentasi dan berbagi pengetahuan dalam penanganan insiden; dan
- Meningkatkan kualitas keamanan untuk mencegah terulangnya insiden.

Sebagian besar organisasi telah melakukan tindakan untuk merespon insiden. Namun, tidak semua organisasi memiliki kerangka kerja untuk melakukan respon insiden. Oleh karena itu, membentuk CSIRT adalah kebutuhan yang mendesak, dengan tujuan untuk menangani insiden secara tepat dan memanfaatkan sumber daya yang ada secara efektif.

Satu insiden saja dapat mengancam keberadaan suatu organisasi dan karenanya tindakan harus diambil tanpa kegagalan. Ketika sebuah organisasi membentuk CSIRT dan membangun kerangka kerja untuk insiden respon yang tepat, maka produktivitas akan meningkat. Hal ini akan meningkatkan kepercayaan masyarakat dan mendukung pencapaian tujuan bisnis organisasi.

TAHAPAN PEMBENTUKAN CSIRT

Cara membentuk CSIRT bergantung pada lingkungan yang dimiiki organisasi, seperti kebijakan, keahlian anggota organisasi atau anggaran yang dimiliki. Namun, terdapat langkah-langkah dasar yang berlaku bagi seluruh CSIRT. Berikut adalah langkah-langkah dalam membentuk CSIRT:



RINCIAN TAHAPAN PEMBENTUKAN CSIRT

Bagian ini mendeskripsikan secara rinci tahapan yang dijelaskan pada pembahasan "Tahapan Pembentukan CSIRT".

Langkah 0 Pengajuan Proyek Pembentukan CSIRT

Pada Langkah 0, proyek pembentukan CSIRT diajukan kepada manajemen atau pembuat keputusan untuk melakukan kegiatan yang dibutuhkan dalam pembentukan CSIRT. Poin-poin berikut harus diperhitungkan untuk memfasilitasi perkembangan proyek.

1. Tujuan membentuk CSIRT

   Menjelaskan alasan/kebutuhan pembentukan CSIRT
2. Tim Pembentukan CSIRT
   a. Terdiri dari anggota yang dibutuhkan keahliannya maupun tanggung jawabnya saat proyek pembentukan CSIRT ini diajukan. Berikut contoh personel yang dapat menjadi anggota tim:
      1) Personel yang mengelola atau mengoperasikan sistem elektronik;
      2) Personel yang bertanggung jawab pada kontrol internal;
      3) Personel yang bertanggung jawab menangani masalah-masalah hukum;
      4) Personel yang bertanggung jawab untuk berhubungan dengan pers;
      5) Personel yang bertanggung jawab pada pembinaan sumber daya manusia;
      6) Personel yang bertanggung jawab pada perencanaan organisasi;
      7) Personel yang bertanggung jawab pada keamanan fisik organisasi;
      8) Personel yang bertanggung jawab untuk pembuatan peraturan-peraturan di organisasi;
      9) Personel yang bertanggung jawab mengelola perubahan-perubahan di organisasi terutama terkait dengan struktur.
   b. Menjelaskan pentingnya peran anggota tim.
   c. Menentukan sarana komunikasi untuk anggota yang secara fisik posisinya berjauhan dengan yang lain.
   d. Membuat kerangka kerja dimana keahlian atau pendapat apa pun dapat dicari bila perlu.

3. Penjadwalan

   Menentukan batasan waktu kerja tim pembentukan CSIRT

4. Aturan Operasional Proyek
   a. Klarifikasi aturan operasional pembentukan CSIRT
   b. Mengonfirmasi aliran pengambilan keputusan dalam tim
   c. Batasan proyek pembentukan CSIRT

Pada Langkah 0, mendapatkan persetujuan dan komitmen dari manajemen atau pembuat keputusan ketika meluncurkan proyek pembentukan CSIRT merupakan hal yang penting.

Output Langkah 0 Proposal Pembentukan CSIRT

Dokumen Proposal Pembentukan CSIRT minimal terdiri dari:

1. Penjelasan tentang CSIRT
2. Tujuan Pembentukan CSIRT
3. Tim Pembentukan CSIRT
4. Jadwal Proyek Pembentukan CSIRT

Pada tahap ini, tambahan informasi penting lainnya dapat disampaikan pula kepada pimpinan organisasi untuk mendukung pengambilan keputusan dalam proyek pembentukan CSIRT ini.

Langkah 1 Identifikasi Permasalahan

Pada Langkah 1, dimulai dengan memeriksa latar belakang organisasi dimana CSIRT akan dibentuk serta situasi organisasi saat ini. Berdasarkan temuan dari pemeriksaan tersebut, identifikasi hal-hal yang harus dicapai dengan pembentukan CSIRT dan masalah yang mungkin timbul saat pembentukan CSIRT.

Berikut ini adalah contoh informasi yang harus dikumpulkan untuk menunjukkan situasi organisasi saat ini.

Major Item	Minor Item	Tujuan Penggunaan
Pahami Target yang akan dilindungi dan ancamannya	Jaringan Sistem Internal • Administrator yang bertanggung jawab • Sistem yang penting • Aset informasi	Informasi digunakan dalam membuat keputusan tentang Insiden yang akan ditangani oleh CSIRT
	Informasi tentang Insiden yang pernah terjadi • Insiden serius yang terjadi • Insiden yang cenderung berulang	
	Hasil analisis dari risiko yang dimiliki	
Kerangka respon insiden yang dimiliki	Tindakan pencegahan terhadap insiden yang ada • Organisasi yang bertanggung jawab atas operasi atau kerangka kerja kolaborasi atau prosedur lintas departemen	Identifikasi masalah dan poin untuk perbaikan dalam hal fungsi dan kerangka kerja untuk insiden respon yang ada
	Tindakan korektif terhadap Insiden yang ada • Organisasi yang bertanggung jawab atas operasi atau kolaborasi kerangka kerja atau prosedur lintas departemen	
	Upaya meningkatkan keamanan yang ada • Organisasi yang bertanggung jawab atas operasi atau kolaborasi kerangka kerja atau prosedur lintas departemen	
	Organisasi eksternal yang terlibat dalam kegiatan insiden respon	Membangun kerangka kerja kolaborasi eksternal yang efektif untuk insiden respon
	Membangun kerangka kerja kolaborasi eksternal yang efektif untuk insiden respon	

Major Item	Minor Item	Tujuan Penggunaan
Kebijakan keamanan yang dimiliki dan dokumen terkait keamanan	Kebijakan Keamanan	Memahami batasan dalam menangani insiden
	Disaster Recovery Plan atau *Business Continuity Plan*	
	Pembatasan dan regulasi terkait keamanan	
	Batasan yang berkaitan dengan keamanan fisik	
Referensi	Informasi terkait CSIRT lainnya	Referensi untuk membentuk CSIRT

Setelah itu, selesaikan masalah yang ada saat ini berdasarkan informasi yang dikumpulkan dan lakukan pemeriksaan untuk membentuk CSIRT. Berikut ini adalah beberapa permasalahan yang harus dipertimbangkan saat membentuk CSIRT:

→ Apa kebutuhan dasar dalam membangun CSIRT?
→ Jenis layanan apa yang harus diberikan?
→ Dimana CSIRT harus ditempatkan di dalam organisasi?
→ Seberapa besar organisasi CSIRT yang dibutuhkan?
→ Berapa biaya untuk membangun CSIRT?

Output Langkah 1 Daftar Identifikasi Masalah

Daftar Identifikasi Masalah minimal mencakup:

1. Gambaran rinci terkait kondisi Organisasi yang berkaitan dengan pembentukan CSIRT
2. Manfaat dari pembentukan CSIRT disandingkan dengan kondisi organisasi
3. Permasalahan-permasalahan yang mungkin timbul saat pembentukan CSIRT

Berdasarkan hasil pemeriksaan dapat dirumuskan rencana untuk membentuk CSIRT pada Langkah 2 di bawah ini

Langkah 2 Perumusan Rencana Pembentukan CSIRT

1. Menentukan konsep dasar CSIRT
2. Menentukan layanan yang akan diberikan
3. Memeriksa kerangka internal organisasi
4. Memeriksa kolaborasi eksternal
5. Menyusun struktur organisasi CSIRT
6. Menginventarisasi sumber daya yang dibutuhkan
7. Melakukan pemeriksaan komparatif
8. Melakukan identifikasi kebutuhan kebijakan dan prosedur
9. Menentukan jangka waktu pembentukan CSIRT
10. Mempersiapkan bahan untuk pembentukan CSIRT

Pada tahapan ini, dilakukan perumusan rencana pembentukan CSIRT dengan menentukan jenis CSIRT yang harus dibentuk untuk menyelesaikan permasalahan pada Langkah 1. Prosedur untuk mengembangkan rencana pembentukan CSIRT adalah sebagai berikut:

1. Menentukan konsep dasar CSIRT

   Menyusun konsep dasar CSIRT dan mengklarifikasi arah CSIRT yang akan dibentuk, dilakukan untuk mendapatkan pemahaman dasar tentang tujuan yang ingin dicapai. Berikut adalah hal-hal yang dapat dilakukan untuk memeriksa konsep dasar CSIRT:

   a. Menetapkan Konstituen (Penerima Layanan)

      Mendefinisikan konstituen merupakan faktor utama dalam menentukan arah CSIRT yang akan dibentuk. Penentuan konstituen dapat dilakukan dengan mengidentifikasi kelompok dan/atau organisasi yang akan mendapatkan layanan dari CSIRT yang dibentuk. Sebagai rujukan, berikut contoh konstituen:

      > ***Konstituen ABC-CSIRT***
      >
      > *Administrator sistem informasi, personel yang bertanggung jawab atas operasi, pengguna, dan administrator keamanan yang bekerja untuk Organisasi ABC*

   b. Menentukan Jenis CSIRT

      Dengan menentukan jenis CSIRT yang akan dibentuk maka dapat diketahui tugas dan jalur koordinasi antar CSIRT.

Jenis CSIRT terdiri atas:

1) CSIRT Nasional merupakan institusi yang dibentuk dan diselenggarakan oleh BSSN untuk mengelola penanggulangan dan pemulihan insiden keamanan siber secara nasional;

2) CSIRT Sektoral merupakan institusi yang berada di bawah CSIRT nasional yang mengelola penanggulangan dan pemulihan insiden keamanan siber pada sektor tertentu dan berperan mengkoordinasikan CSIRT di sektornya;

3) CSIRT Organisasi merupakan institusi yang dibentuk untuk mengelola penanggulangan dan pemulihan insiden keamanan siber pada instansi penyelenggara negara, badan usaha, kelompok usaha, dan organisasi lainnya;

4) CSIRT Khusus merupakan institusi yang mengelola penanggulangan dan pemulihan insiden keamanan siber untuk memenuhi kebutuhan kewilayahan, komunitas tertentu, pelanggan, atau kegiatan dengan jangka waktu tertentu.

Dalam menentukan jenis CSIRT dapat mempertimbangkan konstituen yang akan dilayani.

c. Menentukan misi

Dalam pembentukan CSIRT perlu ditentukan misi yang harus dicapai. Berikut merupakan hal-hal perlu dicantumkan dalam misi:

- Posisi atau situasi organisasi saat ini
- Sarana yang digunakan untuk mencapai tujuan
- Tujuan yang ingin dicapai

Selain itu, tujuan utama yang harus dicapai oleh CSIRT bervariasi, tergantung pada latar belakang organisasi dimana CSIRT akan dibentuk, tetapi sebagian besar dapat diringkas sebagai berikut:

- Melakukan kegiatan untuk mencegah terjadinya atau terulangnya Insiden
- Mengurangi kerusakan yang disebabkan oleh Insiden dan meminimalkan kerugian dengan menerapkan respon yang tepat dan tindakan yang efektif

Misi yang ditentukan oleh masing-masing organisasi harus jelas dan ringkas dalam hal prosedur khusus untuk pencapaian dan tujuan spesifik yang ingin dicapai. Hal

tersebut juga harus menunjukkan bagaimana CSIRT akan berinteraksi dengan konstituen. Sebagai rujukan, berikut contoh misi:

> ***Misi ABC-CSIRT***
>
> *Misi kami adalah berkontribusi pada peningkatan keamanan di organisasi ABC dan masyarakat jaringan informasi dengan bertindak sebagai inti dari upaya di bidang keamanan pada organisasi ABC. Berfungsi sebagai point of contact (prahubung) untuk memberikan layanan konsultasi keamanan informasi serta bekerja sama dengan organisasi dan ahli di organisasi ABC dengan memberikan asistensi untuk deteksi, penyelesaian insiden, membatasi kerusakan, dan pencegahan insiden keamanan.*

d. Menentukan insiden yang akan ditangani

Berdasarkan hasil identifikasi permasalahan pada Langkah 1, tentukan permasalahan mana yang harus dituntaskan oleh CSIRT dan tentukan insiden yang akan ditangani. Mendefinisikan insiden yang akan ditangani memungkinkan untuk memeriksa layanan dan sumber daya mana yang harus dimiliki oleh CSIRT.

Berikut adalah referensi jenis insiden yang akan ditangani seperti yang ditunjukkan pada Tabel 1. Namun, perlu diketahui bahwa klasifikasi ini diberikan dari perspektif sistem dan kerusakan aktual akan sangat bervariasi tergantung pada sifat sistem informasi.

Tabel 1. Referensi Jenis Insiden

Jenis Insiden	Keterangan
Probing, scanning, atau akses mencurigakan lainnya	▪ Mencari kelemahan (misal, memeriksa versi program server) ▪ Upaya intrusi (upaya yang gagal) ▪ Upaya infeksi *worm* (upaya yang gagal)
Relay program server yang tidak sah	Penggunaan pesan elektronik atau *proxy* server oleh pihak ketiga yang tidak diharapkan oleh administrator
Akses yang mencurigakan	Peniruan pengirim
Intrusi kedalam sistem	▪ Masuk ke sistem, merusak (termasuk menggunakan *root kit* atau alat khusus lainnya) ▪ Mengatur program untuk serangan DDoS
Serangan yang mengarah ke gangguan operasi layanan (DoS)	▪ Gangguan oleh kemacetan jaringan ▪ Menghentikan program server ▪ Menghentikan atau *reboot* OS server

Virus komputer atau infeksi *worm*	
Lainnya	Penerimaan *e-mail* komersial yang tidak diminta (*Unsolicited commercial e-mail*/UCE) yang sering disebut sebagai *spam e-mail*

2. Menentukan layanan yang akan diberikan

"Layanan" berarti detail spesifik dari tanggap Insiden yang akan diberikan oleh CSIRT yang akan dibentuk. Berikut ini menunjukkan garis besar layanan umum CSIRT. Namun, CSIRT tidak harus menyediakan semua layanan ini. Penentuan jenis layanan yang harus disediakan oleh CSIRT tergantung pada konstituen, jenis CSIRT, misi, dan insiden yang akan ditangani.

Layanan CSIRT dapat dibagi menjadi tiga kategori utama, yaitu:

a. Layanan Reaktif (Korektif/Perbaikan)

Layanan ini meliputi kegiatan tanggap Insiden dan peristiwa lain yang berkaitan dengan Insiden guna membatasi kerusakan yang disebabkan oleh Insiden. Layanan ini terdiri dari:

1) Layanan pemberian peringatan dini terkait keamanan siber;
2) Layanan tanggap Insiden Keamanan Siber;
3) Layanan penanganan kerawanan sistem elektronik;
4) Layanan penanganan artefak.

b. Layanan Proaktif (Preventif/Pencegahan)

Layanan ini meliputi kegiatan mendeteksi dan mengurangi potensi Insiden dan *Security Event* lainnya dengan tujuan untuk mencegah terjadinya Insiden. Layanan ini terdiri dari:

1) Pemberitahuan hasil pengamatan terkait dengan ancaman baru yang dapat muncul akibat perkembangan teknologi, politik, ekonomi dan perkembangan lainnya;
2) Dalam hal diperlukan dan tersedianya sumber daya dapat disediakan layanan pendeteksian serangan.

c. Layanan Peningkatan Kapabilitas Kesiapan Penanggulangan dan Pemulihan Insiden Keamanan Siber

Layanan ini ditujukan untuk meningkatkan kualitas keamanan internal. CSIRT memberikan wawasan dari sudut pandang dan keahliannya, sehingga kegiatan

secara efektif dapat dilakukan melalui kolaborasi dengan organisasi internal. CSIRT secara tidak langsung juga dapat mencegah terjadinya insiden.

Layanan ini terdiri dari:

1) Analisis risiko;
2) Konsultasi terkait kesiapan penanggulangan dan pemulihan insiden keamanan siber;
3) Pembangunan kesadaran dan kepedulian terhadap keamanan siber.

Pada Tabel 2. dijelaskan mengenai daftar layanan dasar CSIRT. CSIRT tidak harus melaksanakan seluruh layanan pada Tabel 2., dalam beberapa kasus dapat memberikan layanan lain.

Tabel 2. Garis Besar Layanan CSIRT

<table>
<tr><th>Reaktif</th><th>Proaktif</th><th>Peningkatan Kualitas Keamanan</th></tr>
<tr><td>Penanganan Insiden</td><td rowspan="2">Memberikan Informasi Terkait Keamanan</td><td>Risk Assessment atau Analisis (Penilaian atau analisis risiko)</td></tr>
<tr><td>Koordinasi</td><td rowspan="2">Menyiapkan dan memodifikasi Business Continuity dan Disaster Recovery Plan</td></tr>
<tr><td rowspan="2">Forensik Komputer</td><td rowspan="2">Mendeteksi Insiden atau Security Event</td></tr>
<tr><td>Konsultasi Keamanan</td></tr>
<tr><td rowspan="2">Insiden Respon On-site</td><td>Survei Tren Teknis</td><td rowspan="2">Kegiatan pendidikan atau pelatihan keamanan</td></tr>
<tr><td>Security Auditing atau Assessment</td></tr>
<tr><td>Dukungan Insiden Respon</td><td>Mengelola Security Tools</td><td rowspan="3">Evaluasi Produk atau Sertifikasi</td></tr>
<tr><td>Penanganan Artefak</td><td rowspan="2">Mengembangkan Security Tools</td></tr>
<tr><td>Penanganan Informasi Kerentanan</td></tr>
</table>

Rincian layanan adalah sebagai berikut:

a. Layanan Reaktif

Penanganan insiden merupakan fungsi dasar CSIRT dan harus diterapkan tanpa kegagalan. Penanganan insiden adalah aktivitas menanggapi insiden yang terjadi untuk tujuan membatasi kerusakan dan memulihkan sistem. Dalam hal penanganan insiden, perlu menetapkan prosedur CSIRT secara keseluruhan. Gambar 1 menunjukkan langkah-langkah dalam penanganan Insiden dan memberikan dasar untuk menyiapkan prosedur.

Gambar 1 Langkah-langkah Penanganan Insiden

Berikut ini merupakan penjelasan langkah-langkah di atas:

1) Mendeteksi atau menerima *Security Event*

   Langkah ini melibatkan penerimaan dan pengelolaan laporan *Security Event*.

2) Triase

   Triase melibatkan pilihan apakah *Security Event* adalah Insiden atau tidak, dan memprioritaskan Insiden. Dalam triase, tentukan kriteria dan sebagai CSIRT harus selalu melakukan triase berdasarkan kriteria yang sama. Namun, kriteria tersebut harus ditinjau secara berkala karena unsur-unsur yang membentuk kriteria terus berubah mengingat lingkungan di sekitar keamanan komputer berkembang pesat.

   Pertimbangkan hal-hal berikut dan lakukan triase berdasarkan kriteria yang ditentukan.

→ Verifikasi fakta-fakta dari kasus ini

→ Periksa sejauh mana dampaknya

Dianjurkan untuk menetapkan pengidentifikasi untuk setiap triase insiden untuk memudahkan referensi saat terjadi insiden.

3) Insiden Respon

Insiden respon adalah aktivitas investigasi untuk menentukan penyebab Insiden dan melakukan upaya pemulihan. Triase insiden harus dianalisa dan diidentifikasi sifatnya.

Suatu Insiden dapat ditandai dengan hal berikut:

→ Penyerang

→ Target serangan

→ Tanggal terjadinya Insiden

→ Metode serangan

→ Tingkat dampak

→ Penyebab utama kerusakan

→ Tindakan yang dapat diambil

→ Kemungkinan penyebaran kerusakan

Tentukan dan terapkan tindakan pencegahan berdasarkan elemen-elemen yang tercantum di atas.

Fungsi khusus CSIRT dalam hal insiden respon adalah sebagai berikut:

→ Koordinasi

Terkadang penanganan insiden mungkin diperlukan dalam beberapa organisasi internal atau eksternal di bawah tanggung jawab mereka sendiri. CSIRT diharapkan berperan sebagai koordinator dengan memahami seluruh gambaran insiden untuk memastikan penanganan Insiden yang konsisten dan efektif. Penanganan Insiden yang cepat membutuhkan koordinasi yang segera.

→ Penanganan insiden *on-site*

CSIRT akan secara langsung melakukan pemulihan terhadap sistem atau jaringan tempat insiden terjadi. Penting untuk menetapkan pembagian tanggung jawab antara CSIRT dan penanggung jawab operasi sistem.

→ Dukungan penanganan insiden

CSIRT akan melakukan penanganan Insiden melalui *email* dan/atau telepon serta menyediakan dokumen atau lainnya.

→ Forensik komputer

Melakukan penanganan Insiden dengan menyimpan data dari komputer yang terkena insiden dapat memberikan bukti dan dengan menganalisis misalnya: (1) jenis kerusakan apa yang disebabkan; (2) di mana penyusup masuk; dan (3) siapa penyusup tersebut. CSIRT perlu dikelola oleh anggota yang memiliki keterampilan spesialis dan dilengkapi dengan alat khusus untuk forensik komputer. Selain itu, informasi harus sepenuhnya dikontrol di dalam CSIRT karena banyak informasi rahasia yang ditangani saat forensik komputer.

→ Penanganan artefak

Langkah ini melibatkan layanan untuk menganalisis program mencurigakan yang ditemukan melalui penanganan insiden. Lakukan penyelidikan untuk menentukan apakah program yang mencurigakan telah menyebabkan insiden dengan menganalisis kode sumbernya serta dengan menganalisis perilaku program di lingkungan yang terisolasi. CSIRT perlu dikelola oleh anggota yang memiliki keterampilan spesialis dan dilengkapi dengan fasilitas artefak khusus yang terisolasi dari jaringan lain.

4) Pelaporan

Laporkan hasil penanganan insiden setelah menyelidiki penyebab insiden dan melakukan upaya pemulihan. Hal tersebut dapat digunakan untuk mengumpulkan pengetahuan dalam penanganan insiden yang dilakukan CSIRT dan untuk memberikan laporan kepada pemilik sistem.

5) Memeriksa tindakan pencegahan insiden kembali terjadi

Analisis penyebab insiden yang telah diselesaikan dan mengambil tindakan untuk mencegah terulangnya insiden. Dalam menganalisis Insiden, perlu memilah hal-hal berikut:

→ Detail Insiden

- Penyebab
- Situasi kerusakan
- Pemicu untuk mendeteksi Insiden
- Tindakan awal atau sementara
- Tindakan permanen

→ Organisasi yang terlibat dalam penanganan Insiden

→ Poin baik dan/atau buruk tentang penanganan insiden

Perlu diambil tindakan untuk mencegah terulangnya berdasarkan hasil analisis.

b. Layanan Proaktif

1) Memberikan / mengumumkan informasi terkait keamanan

Layanan ini memberikan informasi keamanan kepada para konstituen. Berikut ini adalah contoh informasi yang disediakan:

- Informasi yang disebarluaskan tentang kegiatan CSIRT atau informasi kontak.
- Kebijakan atau prosedur atau daftar periksa terkait keamanan
- Informasi tentang virus atau *worm* dan metode serangan yang lazim
- Metode khusus insiden respon
- Statistik insiden

2) Penanganan informasi kerentanan

Layanan ini untuk menganalisis informasi tentang kerentanan perangkat lunak dan perangkat keras serta mengkomunikasikannya kepada konstituen. Konstituen harus mengelola *patch* aplikasi untuk memperbaiki kerentanan dan mengimplementasikan solusi. Dalam penanganan informasi kerentanan, CSIRT harus memahami jenis perangkat lunak dan perangkat keras apa yang digunakan oleh konstituen. Dalam hal kerentanan ditemukan pada produk yang dikembangkan oleh CSIRT, penanganan kerentanan tersebut termasuk dalam layanan ini.

3) Mendeteksi insiden atau Security Event

Layanan ini untuk mendeteksi Insiden atau *Security Event*. Metode pendeteksian termasuk memasang *Intrusion Detection Systems* (IDS) atau *honeypot*, menganalisis log dari berbagai server, dan lingkungan khusus untuk mendeteksi kebocoran informasi melalui aplikasi berbagi file *peer-to-peer* (P2P).

4) Survei tren teknis

Layanan ini untuk melakukan survei tren dan memberikan pendapat ahli tentang teknologi keamanan terbaru seperti teknologi peningkatan keamanan, teknologi deteksi insiden, atau teknik intrusi dan memverifikasi kegunaannya bagi konstituen. Menerapkan teknologi yang berguna untuk CSIRT dan menggunakannya untuk memberikan informasi kepada konstituen.

- Audit atau penilaian keamanan

  Layanan audit atau penilaian melalui pemeriksaan dokumen atau pengujian penetrasi.

- Mengembangkan alat keamanan

  Layanan mengembangkan alat untuk digunakan oleh CSIRT atau konstituen. Sebagai contoh, pengembangan alat pendeteksi insiden baru dan *script* untuk

membuat teknologi enkripsi lebih mudah digunakan atau untuk mengotomatisasi distribusi *patch.*

c. Layanan peningkatan kualitas keamanan

1) Penilaian atau analisis risiko

Layanan ini untuk mengidentifikasi berbagai risiko yang dapat mengganggu kerahasiaan, integritas, atau ketersediaan entitas bisnis atau sistem informasi yang menjadi target dan menganalisis dampaknya. Hal ini dimaksudkan untuk mengenali dan mengurangi risiko yang ada.

Secara umum, hal ini termasuk

- Mengidentifikasi aset informasi (prioritisasi)
- Menganalisis risiko pada aset yang diidentifikasi

Risiko dapat dikurangi dengan merefleksikannya dalam kebijakan keamanan, layanan CSIRT, prosedur penanganan insiden dan lain sebagainya berdasarkan analisis risiko.

2) Mempersiapkan dan memodifikasi *business continuity plan* dan *disaster recovery plan*

Layanan ini mencerminkan fungsi insiden respon CSIRT dalam strategi manajemen sebagai *business continuity plan* dan *disaster recovery plan* untuk melindungi organisasi dari hilangnya transaksi pelanggan kepada pesaing, penurunan pangsa pasar, atau penurunan penilaian organisasi dengan tidak membiarkan insiden skala besar mengganggu bisnis penting perubahan atau dengan melanjutkan bisnis sesegera mungkin jika telah terganggu.

3) Konsultasi keamanan

Layanan konsultasi ini mencerminkan pengetahuan CSIRT dalam bisnis para konstituennya. Pengetahuan tersebut dapat digunakan untuk memenuhi persyaratan keamanan dalam bisnis, atau pengetahuan itu sendiri dapat menjadi bisnis. Dengan demikian, bagaimana pengetahuan tersebut digunakan akan bervariasi tergantung pada lini bisnis organisasi.

4) Kegiatan pendidikan atau pelatihan atau pencerahan keamanan

Layanan ini untuk mendidik, melatih, dan mencerahkan konstituen melalui seminar, lokakarya, kursus, materi pendidikan, atau sejenisnya dalam hal pengetahuan CSIRT serta kebijakan atau prosedur dan lain-lain, dimana tercermin pengetahuan tersebut. Layanan ini sering bekerja sama dengan departemen pengembangan sumber daya manusia atau sejenisnya.

5) Evaluasi atau sertifikasi produk

Melalui layanan ini, CSIRT mengevaluasi dan mensertifikasi produk, alat, layanan, dan lain-lain, dengan menentukan apakah konstituen dapat menggunakannya dengan aman atau tidak. CSIRT perlu menetapkan kriteria untuk evaluasi dan sertifikasi yang sesuai untuk organisasi.

Periksa layanan yang akan diberikan serta otoritas yang diperlukan untuk CSIRT memberikan layanan. Jika ada fungsi insiden respon internal, CSIRT harus menggunakan fungsi-fungsi tersebut secara efektif dan memeriksa keterkaitannya dengan CSIRT. Pertimbangkan bagaimana fungsi insiden respon yang ada akan ditransfer ke CSIRT sebagaimana diperlukan.

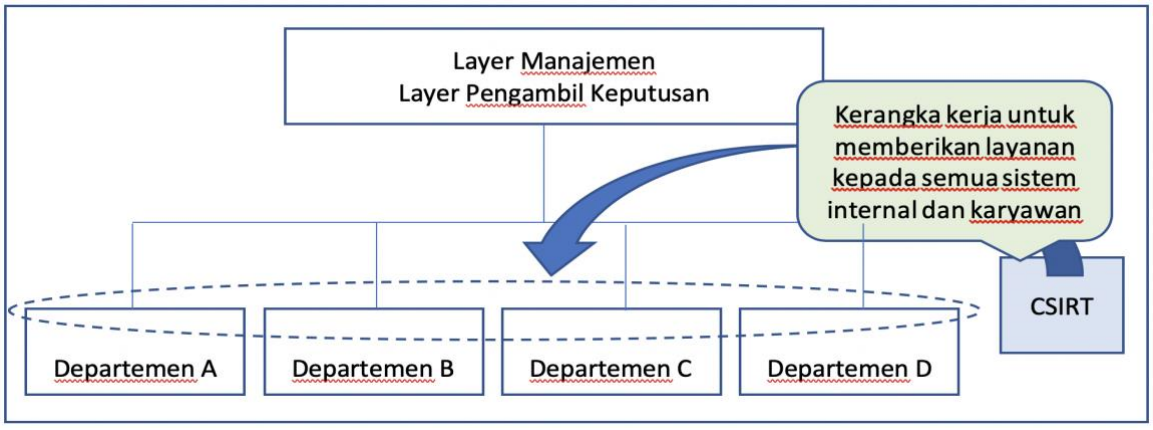
3. Memeriksa Kerangka Internal Organisasi

Memeriksa kerangka internal organisasi bertujuan untuk menentukan bagaimana CSIRT akan berfungsi di organisasi. Berikut contoh daftar Departemen yang terlibat dalam insiden respon:

Level manajemen / level pengambilan keputusan	Mengamankan dana dan sumber daya, mencerminkan tugas dan wewenang yang dibutuhkan oleh CSIRT dalam sistem internal dengan menyetujui pembentukan CSIRT. Level ini adalah penerima pelaporan akhir tentang insiden.
Departemen yang bertanggung jawab mengelola / mengoperasikan sistem informasi	Bagian ini sangat terlibat dalam kegiatan CSIRT karena terkadang dapat diposisikan sebagai penerima layanan dan mungkin memiliki fungsi penanganan Insiden.
Departemen kontrol internal	Mengkoordinasikan respon insiden dengan aktivitas kontrol internal (perlu diingat bahwa aktivitas CSIRT hanya dimaksudkan untuk merespon Insiden, bukan untuk melakukan aktivitas kontrol internal).
Departemen Hukum	Berkaitan dengan masalah hukum dalam hal respons Insiden.
Departemen Hubungan Masyarakat	Berurusan dengan pers dalam hal respons Insiden.

Departemen Sumber Daya Manusia	Menugaskan atau mempekerjakan staf CSIRT. Menerapkan tindakan SDM di unit tempat insiden terjadi (perlu diingat bahwa aktivitas CSIRT hanya dimaksudkan untuk merespon Insiden, bukan untuk memberikan tindakan terhadap personel).
Departemen pengembangan sumber daya manusia	Mendidik dan melatih konstituen melalui seminar, lokakarya, kursus, materi pendidikan, atau sejenisnya dalam hal pengetahuan dan kebijakan keamanan.
Departemen perencanaan organisasi	Mencerminkan *business continuity plan* dan *disaster recovery plan* serta insiden respon.
Help Desk	Titik kontak tingkat pertama untuk penanganan Insiden.
Departemen keamanan fisik	Berkaitan dengan pencurian barang (terutama PC). Tugasnya adalah mengelola dan mengimplementasikan kontrol akses.

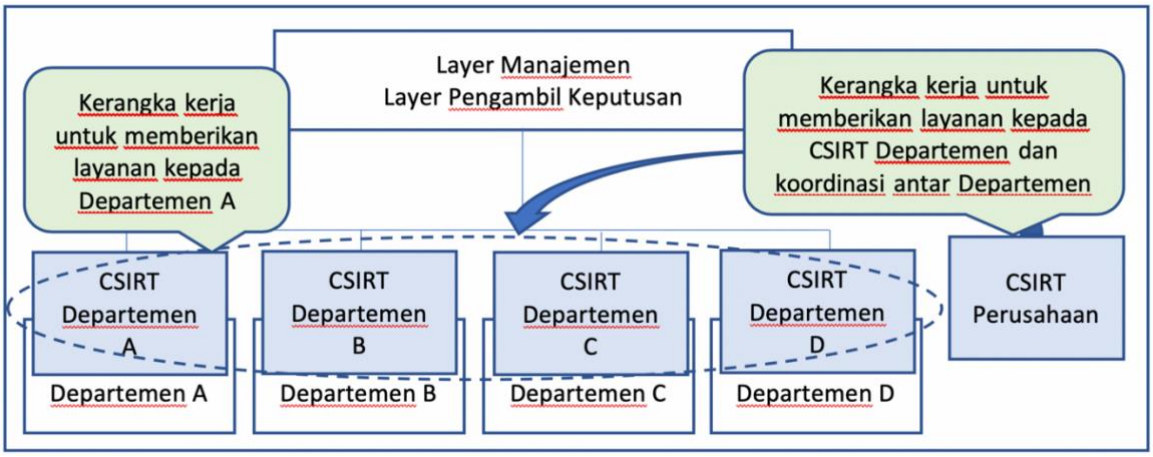
Sebagai contoh, jika semua sistem internal dan karyawan akan menjadi penerima layanan CSIRT, harus ada kerangka kerja internal untuk memungkinkan layanan diberikan kepada konstituen tersebut. Untuk mencapai ini, kerangka kerja seperti yang ditunjukkan pada Gambar 2 dapat bekerja secara efektif.



Gambar 2 Kerangka Kerja untuk Entitas Bisnis dimana Seluruh Sistem Internal dan Karyawan adalah Konstituen

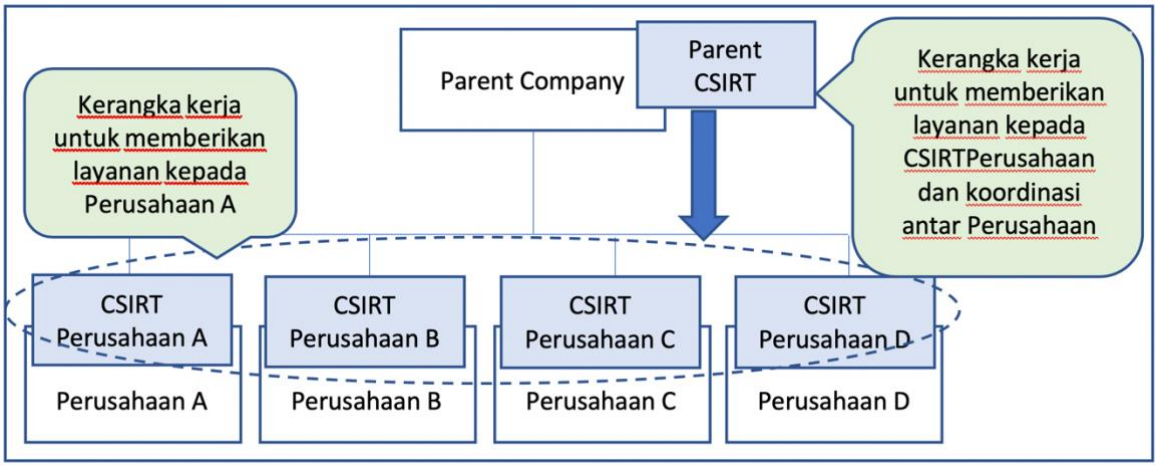
Selain itu, jika sulit bagi CSIRT untuk memberikan layanannya kepada semua sistem internal dan karyawan karena entitas bisnisnya yang besar, kerangka kerja seperti yang ditunjukkan pada Gambar 3 dapat bekerja secara efektif. Dengan kerangka kerja ini,

CSIRT dibentuk untuk setiap departemen serta CSIRT untuk koordinasi seluruh organisasi.



Gambar 3 Kerangka Kerja untuk Entitas Bisnis yang Besar dimana Seluruh Sistem Internal dan Karyawan adalah Konstituen

Kerangka kerja CSIRT hirarki serupa dengan Gambar 3 dapat bekerja secara efektif untuk CSIRT dari entitas bisnis yang memiliki grup organisasi di bawah kendalinya, dimana semua organisasi grup adalah konstituennya. Gambar 4 menunjukkan kerangka kerja untuk kasus tersebut.



Gambar 4 Kerangka Kerja untuk Entitas Bisnis dimana Seluruh Kelompok Organisasi adalah Konstituen

Dalam memeriksa kerangka kerja internal, wewenang yang diperlukan oleh CSIRT serta sistem terkait dan batas pemisah antara CSIRT dan departemen dengan fungsi insiden respon yang ada akan tercermin dalam agenda pemeriksaan tersebut. Selain itu, periksa pula kedudukan CSIRT dalam organisasi.

4. Memeriksa Kolaborasi Eksternal

   Dalam melakukan insiden respon dimungkinkan untuk berkolaborasi dengan pihak luar. Oleh karena itu, perlu dilakukan pemeriksaan terhadap kerangka kerja untuk berkolaborasi dengan organisasi eksternal.

   a. Berkolaborasi dengan CSIRT Eksternal

      Dengan berkolaborasi bersama CSIRT eksternal, organisasi dapat melakukan aktivitas CSIRT secara lebih efektif dalam hal mendeteksi insiden, berbagi pengetahuan tentang insiden respon, menerapkan penanganan insiden lintas organisasi, dan lain sebagainya. Untuk mencapai kolaborasi yang efektif antar CSIRT, organisasi perlu memeriksa jenis CSIRT eksternal yang akan berkolaborasi dan apa yang akan dicapai oleh organisasi.

   b. Kolaborasi dengan Organisasi Eksternal

      CSIRT mungkin perlu merespon dan/atau berkolaborasi dengan lembaga penegak hukum, pers, dan vendor produk dalam melakukan insiden respon. Oleh sebab itu, organisasi harus membuat kebijakan tentang kerjasama dengan organisasi eksternal tersebut.

5. Menyusun Struktur Organisasi CSIRT

   Struktur organisasi CSIRT yang tepat dapat ditentukan berdasarkan struktur organisasi penyelenggara dan konstituen. Hal ini juga tergantung pada aksesibilitas tenaga ahli yang terampil untuk dipekerjakan secara permanen atau secara *ad-hoc*. Berikut susunan organisasi CSIRT yang umum ada :

   a. Ketua

      Bertugas memimpin pelaksanaan tugas dan bertanggung jawab dalam pengalokasian sumber daya yang dibutuhkan untuk mengoperasionalkan layanan CSIRT.

   b. Sekretaris

      Bertugas melaksanakan kegiatan kesekretariatan meliputi administrasi dan dokumentasi pada operasional layanan CSIRT.

   c. Tim Teknis Operasional

      Bertugas memberikan layanan CSIRT.

   d. Konsultan Eksternal

      Dipekerjakan saat dibutuhkan.

Jika sumber daya tidak memungkinkan untuk membentuk struktur umum tersebut, paling minimal sebuah CSIRT memiliki penanggung jawab dan perespon insiden.

6. Menginventarisasi sumber daya yang dibutuhkan

Hal yang perlu dilakukan berikutnya adalah memeriksa sumber daya yang akan dibutuhkan untuk memberikan layanan dan membangun kerangka kerja internal dan eksternal. Pembatasan sumber daya dalam organisasi juga harus diperhitungkan. Berikut ini merupakan garis besar sumber daya yang diperlukan.

a. Sumber daya manusia

Identifikasi kebutuhan anggota staf dengan keterampilan yang dibutuhkan untuk melakukan kegiatan CSIRT dalam kerangka kerja organisasi. Berikut pendekatan perhitungan yang dapat digunakan sebagai acuan awal terkait jumlah personel yang perlu ditugaskan pada CSIRT:

- CSIRT dengan tugas memberikan dua layanan inti, misal layanan reaktif berupa penanganan insiden dan layanan pro-aktif berupa pemberian buletin *security advisory* secara rutin, minimal jumlah personil adalah 4 orang (*full time*).
- CSIRT dengan tugas memberikan tiga layanan secara penuh, misal layanan reaktif berupa penanganan insiden, layanan pro-aktif berupa pemberian buletin *security advisory* secara rutin, dan layanan peningkatan kualitas keamanan siber, minimal jumlah personil adalah 6-8 orang (*full time*).
- CSIRT dengan tugas memberikan layanan 24x7 (terdiri dari 3 shift yang bekerja secara bergantian), minimal jumlah personil adalah 12 orang (*full time*).

Pendekatan perhitungan ini tidak bersifat mutlak. Jika organisasi mendapatkan pendekatan yang lebih tepat diterapkan sesuai kebutuhan, maka organisasi dapat menggunakan pendekatan tersebut untuk menghitung jumlah personil yang perlu ditugaskan pada CSIRT. Dalam hal adanya kendala dalam pemenuhan kebutuhan sumber daya manusia, organisasi diperbolehkan untuk menggunakan jasa/bantuan dari luar organisasi atau kombinasi personil dari dalam dan luar organisasi. Ada beberapa hal yang harus dipersiapkan sebelum merekrut sumber daya manusia dari luar organisasi, diantaranya:

- Membuat dokuman *non-disclosure agreements* (NDA), *service level agreements* (SLA), *memorandum of understanding* (MoU), dan dokumen lainnya yang dibutuhkan;
- Informasi terbaru dari personil (nomor telepon dan alamat tempat tinggal);
- Menentukan prosedur komunikasi yang aman;

Selain jumlah, organisasi juga perlu menentukan peran-peran dalam CSIRT. Berikut adalah peran-peran yang dibutuhkan oleh CSIRT:

- Manajer / pemimpin tim / pemimpin kelompok

  Orang yang mengawasi tim atau kelompok dan membuat keputusan untuk tim atau kelompok tersebut.
- *Hotline Specialist*/*Service Desk*

  Anggota yang bertanggungjawab untuk mencatat setiap laporan/aduan yang dilaporkan, merekomendasikan langkah penanganan awal dan meneruskan kepada tim perespon insiden jika insiden yang dilaporkan adalah insiden baru.
- Staf Triase

  Anggota staf yang bertanggung jawab atas triase. Mereka melakukan triase sesuai dengan kriteria yang ditetapkan dan memprioritaskan insiden yang penangannya akan ditugaskan.
- Perespon insiden

  Anggota staf yang melakukan penanganan insiden dan mendukung tugas utama sebagai anggota CSIRT.
- Analis Media (Pengumpul atau analis bukti digital)

  Anggota yang memiliki kemampuan dan keterampilan untuk merespon insiden-insiden siber dan melakukan pemeriksaan awal terhadap barang bukti elektronik dan digital sebelum dilakukan analisis secara mendalam.
- Staf lain untuk layanan yang akan diberikan.

  Anggota staf yang melakukan aktivitas untuk layanan yang akan diberikan seperti Analis Malware, Analis Ancaman, Analis Kerentanan, Analis Hukum, Hubungan Publik, dan *Technical Writing*.

Setelah menentukan peran-peran pada CSIRT yang akan dibentuk, selanjutnya identifikasi kompetensi yang dibutuhkan untuk setiap peran tersebut. Berikut adalah ringkasan kompetensi utama untuk personil teknis pada CSIRT :

a. Kompetensi personal
   - Kemampuan bekerja/kerjasama dalam tim;
   - Kemampuan analisis atas permasalahan secara mendalam;
   - Kemampuan bekerja dalam situasi krisis atau tekanan;
   - Kemampuan komunikasi dan penulisan laporan secara terstruktur.

b. Kompetensi teknis
   - Pengetahuan tentang jaringan komputer dan protokol internet;
   - Pengetahuan tentang sistem operasi Linux dan Unix;

- Pengetahuan tentang sistem operasi Windows;
- Pengetahuan tentang administrasi sistem pada perangkat-perangkat jaringan (*router*, *switch*, *mail server*, DNS, *proxy*, dsb);
- Pengetahuan tentang aplikasi-aplikasi umum pada internet (HTTP, SMTP, Telnet, SSH, dsb);
- Pengetahuan tentang Bahasa pemrograman;
- Pengetahuan umum tentang ancaman keamanan dan teknik serangan pada protokol internet (DDoS, *phishing*, *defacing*, *sniffing*, dsb);
- Pengetahuan tentang manajemen risiko dan praktek implementasinya;
- Pengetahuan penggunaan menggunakan Pretty Good Privacy (PGP).

c. Kompetensi tambahan (opsional)

- Bersedia bekerja dalam *shift* 24x7 atau berdasarkan panggilan (bergantung pada model layanan yang diberikan);
- Pengalaman minimum dalam bidang keamanan TI atau siber;
- Pendidikan formal di bidang TI.

Selain mengacu pada ringkasan kompetensi tersebut, organisasi dapat mengidentifikasi kompetensi yang dibutuhkan berdasarkan layanan yang akan diberikan oleh CSIRT.

Jika tidak terdapat sumber daya siap kerja yang cukup untuk insiden respon, identifikasi juga pelatihan yang dibutuhkan untuk mengembangkan staf. Dalam kondisi tersebut, selain pengembangan internal, organisasi dapat menggunakan pelatihan komersial untuk mengembangkan staf CSIRT secara efisien. Berikut adalah acuan yang dapat digunakan untuk menentukan kebutuhan pelatihan atau peningkatan kompetensi.

1) Pelatihan Tingkat Dasar.

   Pelatihan ini ditujukan kepada anggota/staf baru, yang bertujuan untuk mempelajari bagaimana CSIRT beroperasi.

2) Pelatihan Tingkat Lanjut

   Pelatihan ini ditujukan kepada anggota/staf Standar Kompetensi Kerja Nasional Indonesia (SKKNI).

3) Pelatihan Tingkat Mahir

   Pelatihan ini ditujukan kepada anggota/staf dengan sertifikasi internasional.

4) Peningkatan Kompetensi dalam bentuk seminar, konferensi, dan Drill Test,

   CSIRT memberikan kesempatan kepada staf nya untuk mengikuti seminar, konferensi, dan Drill Test dalam skala nasional, dan internasional baik yang

bersifat langsung (*offline*) maupun *online*. Khusus untuk Drill Test, perlu ditetapkan intensitas pelaksanaan Drill Test yang akan diselenggakaran oleh CSIRT.

b. Sumber daya fasilitas

CSIRT seringkali menangani informasi sensitif milik organisasi (misal, laporan kejadian insiden siber, laporan kerentanan pada sistem, laporan indikasi adanya anomali pada sistem, *fraud*, dsb), maka atur mekanisme dan fasilitas untuk mencegah pengungkapan informasi yang tidak perlu bahkan di dalam organisasi. Contoh mekanisme dan fasilitas adalah sebagai berikut:

- Gunakan akses kontrol ke fasilitas/tempat kerja CSIRT;
- Terapkan *monitoring*/pengawasan pada tempat-tempat penting (misal, menggunakan kamera CCTV);
- Simpan dokumen dan informasi rahasia pada brankas atau lemari terkunci;
- Terapkan praktek-praktek pemanfaatan perangkat TI yang aman (*cyber hygiene*);
- Gunakan perangkat pengamanan TI untuk pengamanan aset internal CSIRT (misal, antivirus, *firewall*, *intrusion detection system*, dan lain sebagainya);
- Lakukan pembaruan secara periodik setiap perangkat lunak yang digunakan;
- Gunakan fasilitas TI untuk mendukung komunikasi antar personel dalam CSIRT dan CSIRT dengan konstituen (misal, email, intranet website, dan lain sebagainya);
- Gunakan dan sosialisasikan nomor kontak CSIRT yang dapat dihubungi saat keadaan darurat (misal, nomor telepon khusus, SMS, dan lain sebagainya);
- Simpan daftar kontak setiap anggota CSIRT dan pihak-pihak lainnya yang dapat dihubungi saat keadaan darurat (misal, petugas penegak hukum, pengacara, konsultan ahli, dan lain sebagainya);
- Gunakan *incident handling ticketing system* untuk merekam dan memantau status penanganan setiap laporan kejadian insiden;
- Jika diperlukan, gunakan jalur komunikasi cadangan untuk mengantisipasi jika sewaktu-waktu terjadi gangguan pada sistem komunikasi utama (misal, telepon satelit, radio, dan lain sebagainya).

c. Anggaran

Perhitungkan anggaran yang akan diperlukan untuk kegiatan CSIRT berdasarkan jumlah sumber daya manusia dan fasilitas, serta biaya yang diperlukan untuk memelihara dan mengoperasikan atau mengelola sumber daya tersebut, baik biaya awal maupun biaya operasional.

7. Melakukan Pemeriksaan Komparatif

   Dengan membandingkan "situasi saat ini," "CSIRT yang akan dibentuk," dan "insiden respon yang ideal," organisasi dapat mengklarifikasi detail implementasi untuk membentuk CSIRT dan mendapatkan visi untuk mengembangkan CSIRT.

   a. Identifikasi masalah saat membentuk CSIRT dengan membandingkan kondisi saat ini dengan kondisi setelah pembentukan CSIRT

      Dengan membandingkan kondisi saat ini dengan kondisi setelah pembentukan CSIRT, organisasi dapat mengidentifikasi masalah implementasi spesifik selama pembentukan CSIRT dan memprioritaskannya.

      Menyimulasikan insiden respon sesuai dengan skenario insiden yang dibuat berdasarkan insiden aktual di masa lalu akan memungkinkan organisasi mengidentifikasi masalah implementasi spesifik secara efektif dalam kondisi saat ini dan kondisi setelah pembentukan CSIRT. Selain itu, jika simulasi mengungkapkan adanya cacat dalam perencanaan, organisasi dapat pula meninjau kembali rencana tersebut.

   b. Pertimbangkan celah antara kondisi ideal dengan CSIRT yang akan dibentuk

      Jika CSIRT yang dibentuk tidak mencapai kondisi insiden respon yang ideal karena keterbatasan sumber daya atau pembatasan dalam organisasi, penyimpangan tersebut harus ditangani sebagai sebuah masalah. Masalah tersebut akan menjadi titik untuk perbaikan setelah CSIRT mulai beroperasi dan memberi panduan aktivitas jangka menengah dan jangka panjang bagi organisasi untuk semakin mendekati kondisi ideal tersebut.

8. Melakukan Identifikasi Kebutuhan Kebijakan dan Prosedur

   Lakukan identifikasi kebutuhan kebijakan dan prosedur yang dibutuhkan untuk operasional CSIRT. Selain menggambarkan aturan pelaksanaan serta keadaan yang diinginkan dari proses operasional dan administrasi pada CSIRT, kebijakan tersebut juga harus sejalan dengan peraturan perundang-undangan atau hukum nasional, standar yang berlaku dalam industri, serta kebijakan internal organisasi. Beberapa peraturan perundang-undangan dan standar nasional yang perlu menjadi acuan adalah Undang-Undang Nomor 8 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, SNI/ISO 27001:2013 – Sistem Manajemen Keamanan Informasi, dan peraturan lainnya yang dianggap perlu oleh organisasi untuk dijadikan acuan.

Beberapa kebijakan dan prosedur terkait penanganan insiden siber yang perlu disusun oleh organisasi antara lain sebagai berikut :

- Kebijakan tentang pengelolaan atau rencana penanganan insiden siber;
- Kebijakan tentang penyimpanan dan/atau retensi rekam digital (*log management*, *log retention*);
- Prosedur tentang pelaporan insiden siber;
- Prosedur tentang penanganan insiden siber;
- Membuat dan mengelola daftar kontak informasi (nama, nomor telepon, dan alamat email) dari tim IT, jaringan, dan penyedia layanan keamanan.

9. Menentukan Jangka Waktu Pembentukan CSIRT

   Dalam menentukan estimasi waktu yang dibutuhkan untuk pembentukan CSIRT bergantung dengan sumber daya yang tersedia. Jangka waktu pembentukan dari tahap awal hingga operasional CSIRT dapat ditentukan dari Sumber Daya Manusia yang tesedia untuk mendefinisikan misi, tujuan, ruang lingkup, dan lain sebagainya.

10. Mempersiapkan Bahan untuk Pembentukan CSIRT

    Persiapkan bahan yang menjelaskan rencana pembentukan CSIRT untuk menciptakan kesadaran akan perlunya CSIRT di organisasi dengan menunjukkan manfaat dari kegiatan CSIRT. Persiapkan bahan untuk pengambilan keputusan sebagai berikut:

    a. Manajemen dan pengambil keputusan
       → Bahan untuk menyetujui pembuatan CSIRT
    b. Departemen yang terlibat dengan insiden respon
       → Bahan untuk koordinasi internal
    c. Konstituen
       → Materi yang menjelaskan tentang CSIRT
    d. Staf atau anggota CSIRT
       → Bahan untuk mempertahankan organisasi CSIRT internal

Output Langkah 2 Dokumen Perencanaan CSIRT

Dokumen ini dibuat secara rinci untuk mendokumentasikan rencana pembentukan CSIRT. Dokumen Proposal Pembentukan CSIRT minimal terdiri dari:

1. Definisikan Konsep Dasar CSIRT mencakup Tujuan, Jenis, Misi, Layanan, dll
2. Kerangka Internal Organisasi dan Kolaborasi Eksternal
3. Bentuk Struktur Organisasi dan Kebutuhan SDM
4. Gambaran perbandingan keadaan sebelum dan setelah terbentuknya CSIRT
5. Identifikasi kebutuhan Kebijakan dan Prosedur untuk operasional CSIRT
6. Jangka waktu pembentukan dan terget CSIRT dibentuk.

Langkah 3 Pembentukan CSIRT

1. Pastikan Persetujuan dari Level Manajemen atau Level Pengambil Keputusan
2. Pastikan Sumber Daya
3. Melaksanakan Koordinasi Internal
4. Jelaskan pada Konstituen
5. Atur Kerangka Kerja CSIRT
6. Susun Kebijakan dan Prosedur yang Dibutuhkan dalam Operasional CSIRT
7. Siapkan Dokumen yang Diperlukan

Pada Langkah 3, bentuk CSIRT berdasarkan rencana pembentukan CSIRT yang ditentukan di Langkah 2. Lakukan hal-hal sebagai berikut:

1. Pastikan persetujuan dari level manajemen atau level pengambil keputusan

   Dapatkan persetujuan dari level manajemen atau level pengambil keputusan untuk rencana pembentukan CSIRT yang disiapkan pada Langkah 2.
2. Pastikan Sumber Daya

   Pada saat yang sama dengan poin 1, pastikan ketersediaan sumber daya yang dibutuhkan untuk membentuk CSIRT. Khusus untuk sumber daya manusia, komunikasikan dengan bagian yang menangani sumber daya manusia terkait kebutuhan personel untuk operasional CSIRT.
3. Melaksanakan koordinasi internal

   Berkoordinasi dengan berbagai departemen internal yang terlibat dan menyiapkan kerangka kerja di mana CSIRT dapat berfungsi.
4. Jelaskan pada konstituen

   Jelaskan pada konstituen tentang pembentukan CSIRT dan beri mereka pemahaman tentang CSIRT. Selain itu jelaskan pula tentang kebutuhan konstituen dan faktor yang menjadi pemeriksaan, apakah kebutuhan tersebut harus tercermin dalam arah kegiatan dalam membentuk CSIRT.
5. Mempersiapkan kerangka kerja CSIRT

   Siapkan kerangka kerja CSIRT yang akan dibentuk. Peroleh sumber daya dan melatih staf.
6. Menyusun kebijakan dan prosedur yang dibutuhkan dalam operasional CSIRT

   Susun Kebijakan dan prosedur sesuai hasil identifikasi pada Langkah 2. Dimungkinkan dalam proses penyusunan, tim mendapatkan informasi-informasi baru terkait dengan kebijakan maupun prosedur yang harus dibuat namun belum terdapat dalam daftar hasil

identifikasi. Jika terjadi hal tersebut, tim harus menetapkan skala prioritas dibandingkan dengan waktu yang tersedia.

7. Siapkan dokumen yang diperlukan

   Susun dokumen yang menjabarkan tentang CSIRT sesuai RFC 2350. Berikut *template* dokumen sesuai RFC 2350.

1 Document Information

1.1 Date of Last Update

1.2 Distribution List for Notifications

1.3 Locations where this Document May Be Found

2 Contact Information

2.1 Name of the Team

2.2 Address

2.3 Time Zone

2.4 Telephone Number

2.5 Facsimile Number

2.6 Other Telecommunication

2.7 Electronic Mail Address

2.8 Public Keys and Encryption

2.9 Team Members

2.10 Other Information

2.11 Customer Contact Information

3 Charter

3.1 Mission Statement

3.2 Constituency

3.3 Sponsorship and/or Affiliation

3.4 Authority

4 Policies

4.1 Types of Incidents and Level of Support

4.2 Co-operation, Interaction and Disclosure of Information

4.3 Communication and Authentication

5 Services

5.1 Incident Response

5.1.1. Incident Triage

5.1.2. Incident Coordination

5.1.3. Incident Resolution

5.2 Proactive Activities

6 Incident Reporting Forms

7 Disclaimers

Output Langkah 3 Dokumen Pembentukan CSIRT

Dokumen Pembentukan CSIRT minimal terdiri dari:

1. Sumber Daya CSIRT
2. Hasil Sosialisasi Kepada Konstituen dan Masukan dari Konstituen (jika ada)
3. Kerangka kerja CSIRT
4. Kebijakan dan Prosedur yang Telah Disusun
5. Dokumen RFC 2350

Langkah 4 Persiapan Sebelum CSIRT Beroperasi

Jalankan Simulasi

Pada Langkah 4, buat skenario insiden berdasarkan insiden aktual yang pernah terjadi dan buatlah simulasi desktop dari aktivitas yang harus dilakukan oleh CSIRT. Simulasi memungkinkan organisasi untuk memastikan kegunaan CSIRT yang dibentuk dan mengidentifikasi masalah sebelum dimulainya operasi. Masalah yang dapat diidentifikasi termasuk kerangka kerja kolaborasi internal, saluran komunikasi untuk informasi, dan pembagian tanggung jawab. Perwakilan dari organisasi yang terlibat dengan insiden respon harus hadir untuk simulasi sehingga dapat memastikan efektifitas penerapannya.

Pastikan untuk melakukan pemeriksaan agar dapat mengidentifikasi poin perbaikan setelah melakukan simulasi dan mencerminkan hasilnya dalam materi yang disiapkan pada Langkah 3. Jika ditemukan hal-hal yang perlu diperbaiki, maka lakukan perbaikan sebelum CSIRT beroperasi secara penuh.

Output Langkah 4 Laporan Hasil Simulasi Operasional

Laporan Hasil Simulasi Operasional minimal terdiri dari:

1. Tujuan Simulasi
2. Waktu Pelaksanaan Simulasi
3. Peserta Simulasi
4. Skenario Simulasi
5. Hasil dan Kendala Simulasi
6. Rekomendasi

Langkah 5 Mulai Operasional CSIRT

1. Pendaftaran CSIRT
2. Menyebarkan Informasi
3. Memberikan Layanan CSIRT ke Konstituen
4. Menetapkan Kerangka Kerja Kolaborasi Eksternal

Pada Langkah 5, mulai operasional CSIRT setelah mengikuti prosedur pembuatan hingga Langkah 4.

1. Pendaftaran CSIRT

   Lakukan pendaftaran ke National CSIRT/CC sesuai ketentuan yang berlaku. Beberapa dokumen yang diperlukan dalam pendaftaran CSIRT adalah sebagai berikut:

   a. Surat pengajuan pembentukan CSIRT yang ditandatangani oleh ketua CSIRT;
   b. Surat penunjukan *point of contact* (*POC*) / single *point of contact* (SPOC);
   c. Formulir Keanggotaan CSIRT;
   d. Surat dukungan *top level* manajemen dari institusi/organisasi;
   e. Dokumen sesuai RFC 2350 yang mendeskripsikan CSIRT yang di bentuk dan mengirimkannya ke *National* CSIRT/CC melalui email dan/atau kurir;

2. Menyebarkan informasi

   Organisasi harus menginformasikan kepada konstituen dan pihak eksternal mengenai keberadaan CSIRT. Selain itu perlu pula diinformasikan kepada konstituen, pihak CSIRT yang harus dihubungi untuk menjalankan CSIRT.

3. Memberikan layanan CSIRT ke konstituen

   Operasional CSIRT akan benar-benar dimulai ketika layanannya diberikan kepada konstituen. Upayakan untuk mengurangi risiko bisnis melalui insiden respon yang efektif.

4. Menetapkan kerangka kerja kolaborasi eksternal

   Tetapkan kerangka kerja kolaborasi eksternal yang diperiksa dalam Langkah 2. Bangun kolaborasi yang efektif untuk mengurangi risiko bisnis.

Saat operasional CSIRT dimulai, tujuan Proyek Pembentukan CSIRT telah tercapai. Langkah selanjutnya adalah Langkah 6 yang menjelaskan operasional CSIRT.

Output Langkah 5 Laporan Operasional CSIRT

Laporan Operasional CSIRT minimal terdiri dari:

1. Proses Pendaftaran yang dilakukan.
2. Informasi yang disebarkan dan alamat informasi tersebut disebarkan
3. Layanan yang telah diberikan oleh CSIRT kepada Konstituen
4. Kolaborasi eksternal yang sudah dilakukan

Langkah 6 Review

Pada Langkah 6, review fungsi organisasi CSIRT yang mulai beroperasi pada Langkah 5. Review perlu dilakukan secara berkala setelah mulai beroperasinya CSIRT untuk meningkatkan kualitas serta untuk meningkatkan fungsi CSIRT. Review dapat dilakukan berdasarkan hasil analisis kegiatan CSIRT, memahami kebutuhan konstituen, dan simulasi yang telah dilakukan. Selain itu, organisasi perlu mengingat bahwa CSIRT harus beradaptasi sesuai dengan perkembangan keamanan komputer yang terus meningkat, serta perlu berupaya membuat kerangka kerja sama yang bermanfaat dengan pihak luar secara berkelanjutan.

Output Langkah 6 Dokumen Hasil Review

Dokumen Hasil Review minimal terdiri dari:

1. Tim Pelaksana Review
2. Jangka waktu Review
3. Mekanisme review yang digunakan
4. Bagian-bagian yang menjadi objek review
5. Hasil Review
6. Rekomendasi Perbaikan

PENUTUP

Membentuk CSIRT merupakan salah satu cara untuk mengurangi risiko insiden dan menjadi tindakan pencegahan yang efektif bagi organisasi. Oleh karena itu, BSSN berkomitmen untuk mendukung kegiatan pembentukan CSIRT di Indonesia. Jika memiliki pertanyaan atau membutuhkan informasi lainnya terkait dengan pembentukan CSIRT, dapat menghubungi kontak dibawah ini.

Direktorat Penanggulangan dan Pemulihan Infrastruktur Informasi Kritikal Nasional

Deputi Bidang Penanggulangan dan Pemulihan

Badan Siber dan Sandi Negara

Jalan Raya Muchtar No. 70, Bojongsari Lama, Kec. Bojongsari, Kota Depok, Jawa Barat
Telp : (021) 7805814

REFERENSI

[1] CSIRT Starter Kit English Version 1.0; Nippon CSIRT Association.

[2] SO/IEC 27035-2 : Information technology - Security techniques - Information security incident management. Part 2 : Guidelines to plan and prepare for incident response;

[3] Establishing a CSIRT; ThaiCERT.

[4] A Step by Step Approach on How to Set Up a CSIRT; ENISA.

[5] Create a CSIRT; Software Engineering Institute Carnegie Mellon University.