BAB III
LANDASAN TEORI

3.1 Penanganan Insiden

Penanganan insiden merupakan seperangkat prosedur yang dilakukan untuk mengatasi berbagai jenis insiden serangan yang disebabkan oleh berbagai kerentanan. Banyaknya insiden serangan yang terjadi baik disengaja maupun tidak disengaja oleh orang yang tidak bertanggung jawab dalam memanfaatkan teknologi. Membuat instansi yang mengalami insiden serangan membentuk tim khusus yang bertujuan untuk menangani insiden serangan tersebut. Tim tersebut dibentuk untuk membantu menangani insiden seperti: mendeteksi, memantau, dan memberikan peringatan sebelum insiden serangan terjadi.

Berdasarkan tujuan seorang yang melakukan Penanganan Insiden (*Incident Handling*), berikut adalah beberapa tujuannya:

1. Memastikan apakah insiden serangan tersebut benar-benar terjadi.
2. Melakukan pengumpulan informasi dari berbagai sumber terpercaya.
3. Melakukan pengambilan bukti-bukti yang dapat memperkuat insiden serangan yang terjadi.
4. Meminimalisir insiden serangan yang terjadi, agar insiden serangan tidak meluas.
5. Membuat laporan pasca terjadi insiden serangan, agar jika terdapat insiden serangan yang sama dapat di atasi dengan baik dan cepat.

3.2 Pencegahan Insiden

Pencegahan Insiden adalah tindakan yang dilakukan secara sengaja untuk mencegah terjadinya kerusakan, dan gangguan kerusakan sebelum insiden serangan terjadi. Menurut Kamus Besar Bahasa Indonesia (2007), pencegahan adalah suatu proses, cara, tindakan mencegah atau tindakan menahan agar sesuatu tidak terjadi. Yunita (dalam L.Abate, 1990:10) definisi pencegahan (*prevention*) adalah pencegahan yang terdiri dari berbagai pendekatan, prosedur dan metode

yang dibuat untuk meningkatkan kompetensi interpersonal seseorang dan fungsinya sebagai individu, pasangan, dan sebagai orang tua.

3.3 Serangan Siber

Serangan siber atau yang biasa disebut *cyber crime* merupakan kejahatan yang dilakukan oleh seorang atau pun kelompok yang mampu menggunakan teknologi informasi yang terkoneksi dengan internet sebagai alat kejahatan. Menurut Murti (2005) *cyber crime* adalah sebuah istilah yang digunakan secara luas untuk menggambarkan tindakan kejahatan dengan menggunakan media komputer ataupun internet. Gregory (2015) menggemukan *cyber crime* adalah bentuk kejahatan virtual dengan memanfaatkan media komputer yang terhubung melalui internet, dan dapat mengekspolitasi komputer lain yang terhubung dengan internet.

Keamanan sistem yang memiliki banyak celah dapat menyebabkan seorang *hacker* memanfaatkan celah keamanan untuk masuk ke dalam sistem, merusak serta mengambil data-data yang tidak seharusnya diketahui olah pihak luar. *Hacker* merupakan istilah yang digunakan untuk menggambarkan seorang yang mempelajari, memodifikasi, menerobos masuk ke dalam komputer baik untuk kepentingan sendiri maupun kelompok. Berdasarkan beberapa pengertian tentang *cyber crime* diatas, dapat disimpulkan bahwa *cyber crime* adalah perbuatan melawan hukum yang dilakukan dengan menggunakan internet. Berdasarkan tindakan dan motif yang dilakukan oleh seorang yang melakukan *cyber crime*, menurut Hius, et al. (2014) permasalahan terbagi menjadi lima bagian yaitu :

1. ***Cyber crime* sebagai tindakan kejahatan murni**

   Tindakan kejahatan yang dilakukan secara disengaja, dimana orang tersebut secara sengaja dan terencana untuk melakukan pengrusakkan, pencurian, tindakan anarkis, terhadap suatu sistem informasi atau sistem komputer.

2. ***Cyber crime* sebagai tindakan kejahatan abu-abu**

   Tindakan kejahatan ini tidak jelas antara kejahatan kriminal atau bukan karena dia melakukan pembobolan tetapi tidak merusak, mencuri atau

melakukan perbuatan anarkis terhadap sistem informasi atau sistem komputer tersebut.

3. *Cyber crime* yang menyerang individu

Kejahatan yang dilakukan terhadap orang lain dengan motif dendam atau iseng yang bertujuan untuk merusak nama baik, mencoba ataupun mempermainkan seseorang untuk mendapatkan kepuasan pribadi. Contoh dari tindakan tersebut adalah: *Pornografi*, *cyberstalking*, dan lain-lain.

4. *Cyber crime* yang menyerang hak cipta (hak milik)

Kejahatan yang dilakukan terhadap hasil karya seseorang dengan motif menggandakan, memasarkan, mengubah yang bertujuan untuk kepentingan pribadi atau umum ataupun demi materi atau non materi.

5. *Cyber crime* yang menyerang pemerintah

Kejahatan yang dilakukan terhadap pemerintah sebagai objek dengan motif melakukan teror, membajak ataupun merusak keamanan suatu pemerintahan yang bertujuan untuk mengacaukan sistem pemerintahan, atau menghancurkan suatu Negara.

3.3.1Modus Kejahatan *Cyber Crime*

Kejahatan *cyber crime* yang berhubungan dengan penggunaan teknologi berbasis komputer dan jaringan telekomunikasi terbagi kedalam beberapa kelompok. Menurut Golose (2006) modus kejahatan *cyber crime* dibagi ke dalam beberapa bentuk berdasarkan bentuk sesuai modus operasinya seperti berikut:

1. *Unauthorized Access to Computer System and Service*

Merupakan kejahatan yang dilakukan dengan memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Insiden serangan yang terjadi biasanya dilakukan dengan cara mencuri untuk mendapatkan sebuah informasi penting dan rahasia. Selain itu, ada juga yang melakukan insiden serangan hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem.

2. *Illegal Contents*

Illegal Contents adalah kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Kejahatan yang biasanya terjadi pada *Illegas Contents* seperti pembuatan suatu berita bohong atau fitnah, dimana berita bohong tersebut dapat menghancurkan martabat atau harga diri pihak lain, hal-hal yang berhubungan dengan pornografi atau pemuatan suatu informasi yang merupakan rahasia negara, agitasi dan propaganda untuk melawan pemerintahan yang sah, dan sebagainya.

3. *Data Forgery*

Data Forgery adalah kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen *e-commerce* dengan membuat seolah-olah terjadi "salah ketik" yang pada akhirnya akan menguntungkan pelaku.

2. Cyber Espionage

Cyber Espionage adalah kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network sistem*) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu sistem yang terkomputerisasi.

5. *Cyber Sabotage and Extortion*

Merupakan kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu *logic bomb*, virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh

pelaku. Contoh kejahatan biasanya dengan menyebarkan Virus komputer saat korban melakukan browsing di internet.

6. *Offense against Intellectual Property*

Merupakan kejahatan yang ditujukan terhadap Hak atas Kekayaan Intelektual yang dimiliki pihak lain di internet. Sebagai contoh adalah peniruan tampilan pada web page suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.

7. *Infringements of Privacy*

Merupakan kejahatan yang ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara *computerized*, yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materil maupun immateril, seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.

8. *Cracking*

Cracking merupakan kejahatan dengan menggunakan teknologi komputer yang dilakukan untuk merusak sistem keamaanan suatu sistem komputer dan biasanya melakukan pencurian, tindakan anarkis begitu merekan mendapatkan akses. Biasanya kita sering salah menafsirkan antara seorang *hacker* dan *cracker* dimana *hacker* sendiri identetik dengan perbuatan negatif, padahal hacker adalah orang yang senang memprogram dan percaya bahwa informasi adalah sesuatu hal yang sangat berharga dan ada yang bersifat dapat dipublikasikan dan rahasia.

9. *Carding*

Carding merupakan kejahatan dengan menggunakan teknologi komputer untuk melakukan transaksi dengan menggunakan *card credit* orang lain sehingga dapat merugikan orang tersebut baik materil maupun non materil.

3.3.2Penyebab Terjadinya *Cyber Crime*

Kejahatan yang terjadi [ada computer (*cyber crime*) terus bertambah dan membuat resah.Terdapat beberapa hal yang menyebabkan makin maraknya kejahatan komputer atau *cyber crime*, menurut Hius, et al. (2014) seperti berikut:

1. Akses internet yang tidak terbatas.
2. Kelalaian pengguna komputer.
3. Mudah dilakukan dan sullit untuk melacaknya.
4. Para pelaku umumnya orang yang mempunyai kecerdasan tinggi dan rasa ingin tahu yang besar.

3.3.3Penanganan dan Pencegahan *Cyber Crime*

Insiden serangan yang terjadi dikarenakan *cyber crime* membuat banyak korban menjadi kesulitan terutama dari sisi keamanan dan juga sisi finansial. Berdasarkan banyaknya insiden serangan yang disebabkan oleh *cyber crime*, menurut Arifah (2011) penanganan dan pencegahan dapat di lakukan dengan berbagai cara seperti:

1. *Educate User*

   Educate User merupakan penanganan yang dilakukan dengan cara memberikan pengetahuan baru terhadap cyber crime dan dunia internet, bahwa tindakan yang dilakukan oleh pelaku adalah melanggar hukum.

2. *Use Hacker's Perspective*

   Use Hacker's Perspective merupakan penanganan yang dilakukan dengan cara menggunakan pemikiran dari sisi *hacker* untuk melindungi sistem anda.

3. *Patch System*

   Patch System merupakan penanganan yang dilakukan dengan cara menutup semua lubang kelemahan yang terdapat pada sistem.

4. *Policy*

   Policy menentukan kebijakan dan aturan yang melindungi sistem anda dari orang-orang yang tidak bertanggung jawab.

5. *Firewall*

Firewall merupakan sistem keamanan jaringan komputer yang digunakan untuk melindungi komputer dari berbagai jenis serangan dari komputer luar.

6. Anti Virus

Anti Virus merupakan sebuah perangkat lunak yang digunakan untuk mendeteksi, mengamankan, dan menghapus virus kompur seperti: *worm*, *trojan*, *spyware* dan lain-lain dari sistem komputer.

Beberapa langkah penting yang harus dilakukan dalam pencegahan serangan cyber crime, menurut Arifah (2011) seperti berikut :

a. Melakukan modernisasi hukum pidana nasional beserta hukum acaranya, yang diselaraskan dengan konvensi internasional yang terkait dengan kejahatan tersebut.
b. Meningkatkan sistem pengamanan jaringan komputer nasional sesuai standar internasional.
c. Meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi dan penuntutan perkara yang berhubungan dengan *Cyber crime*.
d. Meningkatkan kesadaran warga negara mengenai masalah *cyber crime* serta pentingnya mencegah kejahatan tersebut terjadi.
e. Meningkatkan kerjasama antar negara, baik bilateral, regional maupun multilateral, dalam upaya penanganan *cyber crime*, antara lain melalui perjanjian ekstradisi dan mutual *assistance treaties*.

Selain pencegahan serangan *cyber crime* yang dapat dilakukan seperti atas, juga terdapat pencegahan lain, menurut Arifah (2011) seperti berikut:

1. IDCERT (*Indonesia Computer Emergency Response Team*)

Melaporkan tindakan terkait dengan kasus keamanan di internet kepada tim IDCERT bahwa adanya insiden serangan.

2. Membantu negara terhindar dari pelaku kejahatan, seperti teroris, kejahatan terorganisasir, dan operasi penipuan.

3. Membantu negara terhindar dari tempat yang nyaman untuk menyimpan aplikasi atau data hasil kejahatan *cyber crime*.

4. Meningkatkan kepercayaan pasar karena adanya kepastian hukum yang mampu melindungi kepentingan dalam berusaha.

5. Memberikan perlindungan terhadap data yang tergolong khusus (*classified*), rahasia, informasi yang bersifat pribadi, data pengadilan kriminal, dan data publik yang dianggap perlu untuk dilindungi.

6. Melindungi konsumen, membantu penegakan hukum, dan aktivitas intelligen.

7. Meningkatkan keamanan nasional dan mengurangi kerentanan dari serangan dan aksi oleh teroris dan mereka yang berniat jahat.

8. Melindungi dunia usaha dari resiko bisnis seperti kehilangan pangsa pasar, rusaknya reputasi, penipuan, tuntutan hukum dari publik, dan kasus perdata maupun pidana.

9. Sebagai sarana untuk menghukum pelaku kejahatan di bidang teknologi informasi.

10. Meningkatkan peluang bagi diakuinya catatan elektronik sebagai alat bukti yang sah di pengadilan dalam kasus kejahatan seperti pencurian, penipuan, pembunuhan, penculikan dan lain – lain, atau kejahatan komputer yang dilakukan menggunakan internet.

3.3.4Tindak Hukum Bagi Pelaku *Cyber Crime*

Tindakan yang dilakukan oleh *cyber crime* berpotensi menimbulkan dampak kerugian pada berbagai bidang seperti: politik, ekonomi, dan sosial budaya. Dampak yang disebabkan oleh *cyber crime* dapat merugikan, maka diperlukan sebuh peraturan hukum yang dapat digunakan oleh aparat penegak hukum untuk menghukum para pelaku *cyber crime*. Menurut Handayani (2005) hukum yang dapat dijadikan oleh aparat penegak hukum untuk menjaring *cyber crime* diantaranya adalah:

1. Undang-Undang Hukum Pidana (KUHP)

Terdapat beberapa ketentuan dalam KUHP yang digunakan oleh aparat penegak hukum dalam menjerat kejahatan *cyber crime* yaitu pada pasal-pasal yang berkaitan antara lain:

a. Pasal 406 KUHP ayat (1) berkaitan dengan tindakan pengrusakan yang menyebutkan bahwa: "barangsiapa dengan sengaja dan dengan melawan hukum menghancurkan, mengrusakkan, membuat tak dapat dipakai atau menghilangkan barang sesuatu seluruhnya atau sebagian adalah kepunyaan orang lain, diancam dengan pidana penjara paling lama dua tahun delapan bulan atau denda paling banyak tiga ratus rupiah". Ketentuan tersebut ditujukan (diancamkan) misalnya kepada *hacker*, karena aktivitas *hacker* ini dinilai telah menimbulkan kerusakan atau kerugian yang luar biasa kepada usaha seseorang, kepentingan institusi atau negara. Aparat menilai kalau yang dilakukan oleh *hacker* jelas-jelas mengakibatkan kerugian pada orang lain, salah satunya berupa kerusakan atau menjadikan tidak berfungsinya barang lain. Jika barang ini termasuk *website*, maka *website* inilah yang mengalami kerusakan.

b. Pasal 282 KUHP

Pasal ini adalah untuk mencegah menjalarnya penggunaan jaringan internet secara melawan hukum, sebagai dasar hukum yang digunakan oleh aparat penegak hukum, yaitu sebagai berikut :

1) Barangsiapa menyiarkan, mempertontonkan, atau menempelkan dengan terang terangan suatu tulisan yang diketahui isinya, gambar atau barang yang dikenalnya melanggar perasaan kesopanan, maupun membuat, membawa masuk, mengirimkan langsung, membawa keluar atau menyediakan tulisan, gambar atau barang itu untuk disiarkan, dipertontonkan atau ditempelkan sehingga kelihatan oleh orang banyak, ataupun terang-terangan diminta atau menunjukkan bahwa tulisan, atau gambar atau barang itu boleh didapat, dihukum penjara selama-lamanya satu tahun empat bulan atau denda sebanyak-banyaknya Rp.45.000,-.

2) Barangsiapa menyiarkan, mempertontonkan atau menempelkan dengan terang-terangan suatu tulisan, gambar atau barang yang melanggar perasaan kesopanan, maupun membawa masuk, mengirimkan terus, membawa keluar atau menyediakan surat, gambar atau barang itu disiarkan, dipertontonkan atau ditempelkan, sehingga kelihatan oleh orang banyak ataupun dengan terang-terangan atau dengan menyiarkan sesuatu tulisan menawarkan dengan tidak diminta atau menunjukkan, bahwa tulisan, gambar atau barang itu tidak boleh didapat, dihukum penjara selama-lamanya sembilan bulan atau denda sebanyak-banyaknya Rp.45.000,-. Jika ada alasan yang sesungguh-sungguhnya untuk menduga, bahwa tulisan, gambar atau barang itu melanggar kesopanan.

3) Jika melakukan kejahatan yang diterangkan dalam ayat pertama dijadikan suatu pencaharian atau kebiasaan, oleh tersangka, dapat dijatuhkan hukuman penjara selama-lamanya dua tahun delapan bulan atau denda sebanyak-banyaknya Rp.75.000,-.

2. Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) Pengaturan *cyber crime* dengan hukum pidana saat ini sudah tertuang dalam UU ITE yang berkaitan dengan masalah kriminalisasi. Ketentuan pidana mengenai kejahatan yang menggunakan transaksi elektronik ada terdapat pada BAB XI mengenai ketentuan pidana yang tertuang mulai dari pasal 45 sampai pasal 52. Pasal 53 menyatakan bahwa:

a. Pasal 27 Ayat (1) jo 45 Ayat (1) UU ITE

Pasal 27 Ayat (1): *Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya ITE dan/ atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan*.

b. Ayat (2): *Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian*.

c. Ayat (3): *Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik*.

d. Ayat (4): *Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman*.

e. Pasal 45 Ayat (1): *Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 Ayat (1), Ayat (2) Ayat (3) atau Ayat (4) dipidana dengan pidana penjara paling lama 6 tahun dan/atau dengan paling banyak Rp 1.000.000.000,00*.

Pada saat berlakunya Undang-Undang ini, semua Peraturan Perundang-undangan dan kelembagaan yang berhubungan dengan pemanfaatan Teknologi Informasi yang tidak bertentangan dengan Undang-Undang ini dinyatakan tetap berlaku.

3.4 Website

Website adalah beberapa kumpulan halaman web yang dimana informasi dalam bentuk teks, gambar, suara dan lain-lain dipresentasikan dalam bentuk *hypertext* dan dapat diakses oleh perangkat lunak yang disebut dengan browser. *Website* memiliki sebuah informasi yang pada umumnya di tulis dalam format HTLM. Informasi yang disajikan pada *website* juga terdiri dari berbagai bentuk mulai dari, grafis (dalam format GIF,JPG,PNG) , suara (dalam format AU,WAV), dan objek multimedia (seperti MIDI,3D World).

Menurut Mandala (2015), *website* merupakan sekumpulan halaman informasi yang disediakan melalui jalur internet sehingga bisa diakses di seluruh dunia selama terkoneksi dengan jaringan internet. *Website* merupakan sekumpulan komponen yang terdiri dari teks, gambar, suara animasi sehingga menjadi media informasi yang menarik untuk dikunjungi oleh orang lain. Bisa dipahami bahwa definisi *website* secara sederhana adalah informasi apa saja yang

bisa diakses dengan menggunakan koneksi jaringan internet. Hartono (2014) *website* merupakan sebuah kumpulan halaman-halaman web beserta file-file pendukungnya, seperti file gambar, video, dan file digital lainnya yang disimpan pada sebuah web server yang umumnya dapat diakses melalui internet. Atau dengan kata lain, *website* adalah sekumpulan folder dan file yang mengandung banyak perintah dan fungsi fungsi tertentu, seperti fungsi tampilan, fungsi menangani penyimpanan data dan sebagainya.

Sebuah *website* biasanya ditempatkan setidaknya pada sebuah web yang dapat diakses melalui jaringan seperti internet, ataupun *Local Area Network* (LAN) melalui alamat internet yang dikenal sebagai URL (*Uniform Resource Locator*). Gabungan atas semua situs yang dapat diakses publik di internet disebut sebagai *world wide web* atau biasa lebih dikenal dengan singkatan WWW. Secara umum, website digolongkan menjadi tiga jenis yaitu :

a. *Website* Statis

Website Statis merupakan *website* yang memiliki isi yang tidak diperbaharui secara berkala, sehingga pengaturan isi atas situs web tersebut dilakukan secara manual. *Website* statis adalah *website* yang tidak memiliki halaman yang tidak berubah. Artinya adalah untuk melakukan perubahan pada suatu halaman dilakukan secara manual dari situs web tersebut.

b. *Website* Dinamis

Website Dinamis merupakan *website* yang secara spesifik didesain agar isi yang terdapat dalam situs tersebut dapat diperbaharui secara berkala dengan mudah. *Website* ini secara struktur diperuntukkan untuk bisa melakukan perubahan sesering mungkin. Contoh umum mengenai *website* dinamis adalah web berita atau web portal yang di dalamnya terdapat fasilitas berita, polling dan sebagainya.

c. *Website* Interaktif

Website Interaktif merupakan *website* yang saat ini memang sedang banyak digemari. Salah satu contoh *website* interaktif ini adalah blog dan forum. Di *website* ini user bisa berinteraksi dan beradu argumen mengenai apa yang menjadi pemikiran mereka. Biasanya *website* seperti ini memiliki moderator

untuk mengatur supaya topik yang diperbincangkan tidak melenceng dari alur pembicaraan.

3.4.1Serangan pada website

Perkembangan *website* yang semakin pesat membuat pengguna *website* terus bertambah, beberapa *website* yang sering akses oleh pengguna diantaranya seperti : *e-commerce, social networking, forum, portal* berita dan lain-lain. Kemudahan layananan yang dimiliki oleh sebuah *website* membuat *website* menjadi sasaran bagi seorang *hacker* untuk membobol sistem keamanan yang dimiliki oleh sebuah *website*. Jenis-jenis teknik serangan yang digunakan untuk menembus keamanan pada *website* juga bermacam-macam. Berikut akan dijelaskan beberapa jenis teknik serangan yang biasa digunakan untuk menyerang *website*, antara lain:

1. **Definisi *Sql Injection***

   Sql Injection (*Structured Query Language*) merupakan teknik serangan yang dilakukan dengan cara mengekspoitasi web aplikasi yang didalamnya menggunakan database untuk menyimpan data. Menurut Herlambang (2010) *Sql Injection* merupakan cara mengeksploitasi celah keamanan yang muncul pada level atau "layer" database dan aplikasi. *Sql Injection* mampu mempengaruhi apa yang akan diteruskan ke database, penyerang dapat memanfaatkan sintaks dan kemampuan dari SQL, serta kekuatan dan fleksibilitas untuk mendukung fungsi operasi database dan fungsionalitas sistem yang tersedia ke database. *Sql Injection* terjadi ketika seorang penyerang dapat memasukkan serangkaian pernyataan Sql ke *query* dengan memanipulasi data input ke aplikasi (Anley, 2002). Berdasarkan definisi tersebut dapat disimpulkan bahwa *Sql Injection* merupakan salah satu jenis serangan yang berbahaya, karena penyerang yang telah berhasil memasuki *database* sistem dapat melakukan manipulasi data yang ada pada *database* sistem.

2. Definisi DDoS

DDoS (*distributed denial of service*) merupakan serangan terdistribusi atau upaya jahat untuk mengganggu lalu lintas normal dari server, layanan, atau jaringan yang ditargetkan dengan membanjiri target atau infrastruktur di sekitarnya dengan membanjiri lalu lintas Internet. Serangan DDoS mencapai efektivitas dengan memanfaatkan beberapa sistem komputer yang dikompromikan sebagai sumber lalu lintas serangan. Mesin yang dieksploitasi dapat mencakup komputer dan sumber daya jaringan lainnya seperti perangkat IoT. Menurut Dharma (2005), DDoS adalah serangan yang bertujuan untuk mematikan pelayanan dari komputer atau jaringan yang diserang. Serangan DDoS ini dapat menghambat bahkan mematikan pelayanan pada sebuah sistem, sehingga pengguna yang memiliki hak dan kepentingan tidak dapat menerima atau mendapatkan pelayanan yang seharusnya.

3. Definisi *Web Deface*

Web Deface merupakan jenis teknik serangan yang dilakukan oleh seorang *hacker* dengan mengubah halaman web tanpa diketahui oleh pemilik sah dari web tersebut. Perubahan tampilan web dapat berupa berubahnya gambar atau teks maupun *link* terhadap halaman web lain. Menurut CSIRT (2014), situs web yang dirusak umumnya memanfaatkan kerentanan yang terdapat pada web server untuk mendapatkan *shell root*, kemudian menyuntikkan kode berbahaya ke halaman web target yang berada pada server.

Serangan seperti *Sql Injection, Ddos, dan Web deface* merupakan serangan siber yang bersifat teknis. Selain itu juga terdapat serangan yang bersifat non teknis seperti tsunami, letusan gunung berapi, kebakaran dan gempa bumi. Fenomena alam digolongkan sebagai serangan non teknis karena manusia dan sistem tidak bisa mengantisipasi kapan adanya bencana alam yang dapat merusak sistem.

3.5 NIST

NIST (*National Institute of Standards and Tecknologi*) merupakan organisasi pemerintahan di Amerika Serikat yang dikembangkan oleh *US Department of Commerce*. NIST adalah kerangka kerja yang bersifat umum yang terdiri dari standar, pedoman, dan praktik terbaik untuk mengelola risiko yang terkait dengan *cybersecurity*. NIST juga membantu mempromosikan perlindungan yang fleksibel dalam ketahanan infrastruktur ekonomi dan keamanan nasional. Menurut Hernandez (2018) NIST merupakan kerangka kerja yang sering digunakan, dikarenakan kerangka kerja NIST mengatur standar pedoman, dan praktek terbaik dalam mengelola resiko terkait segala bentuk yang berkaitan dengan sains, teknologi informasi, teknologi teknik, dan teknologi skala nano. NIST memiliki banyak jenis-jenis standar podoman dengan masing-masing seri nomor yang berbeda-beda, dimana setiap seri nomor pada Nist memiliki fungsi khusus seperti NIST 800-61. NIST 800-61 adalah dokumen standar khusus yang dikembangkan oleh *National Institute of Standards and Teknologi* (NIST) yang mana merupakan dokumen yang berfocus membahas atau menyelesaikan masalah tentang penanganan insiden (*incident handling*). Menurut Cichonski et, al (2012) tahap penanganan insiden (*insiden handling*) terbagi beberapa tahap, Tahapan tersebut dibagi menjadi empat bagian yang di gambarkan melalui bagan dibawah ini :

Gambar 3.1. Tahap *incident handling* berdasarkan NIST 800-61 (Cichonski et, al., 2012).

Berikut adalah penjelasan mengenai tahap *incident handling* berdasarkan NIST 800-61 (Cichonski et, al., 2012) :

1. Tahap Persiapan (*Preparation*)

Tahap persiapan menjadi tahap yang penting dalam sebuah penanganan insiden. Sebuah instansi harus melakukan persiapan dengan membentuk tim yang tidak hanya bertugas untuk menangani insiden serangan, namun juga mempersiapkan kemampuan setiap individu dalam tim untuk mencegah suatu insiden. Dalam proses penanganan sebuah insiden, tahap persiapan terbagi menjadi dua bagian yaitu tahap persiapan penanganan insiden dan pencegahan insiden.

a. Tahap Persiapan Penanganan Insiden

Pada tahap persiapan penanganan insiden, hal yang penting untuk diperhatikan adalah perangkat dan sumber daya. Perangkat komunikasi dan fasilitas untuk melakukan penanganan insiden harus dipersiapkan oleh sebuah instansi. Dalam tahap persiapan penanganan sebuah insiden terdapat beberapa hal penting yang harus dilakukan sebuah instansi yaitu membentuk tim penanganan insiden, mempersiapkan dokumen, menentukan pihak yang bertanggung jawab ketika terjadi insiden (koordinasi), mekanisme pelaporan insiden, mempersiapkan perangkat, *tools* untuk melakukan analisis insiden, dan melakukan *backup* data untuk pemulihan sistem.

b. Tahap Pencegahan Insiden

Tahap pencegahan insiden dapat dilakukan oleh tim penanganan insiden dengan melakukan berbagai hal antara lain: Melakukan *risk assessments* secara berkala untuk mengetahui bahaya yang dapat menyerang sistem dan keamanan informasi sebuah instansi, meningkatkan keamanan komputer dan jaringan sebuah instansi, dan mencegah *malware* dengan memberikan pemahaman kepada semua pihak yang berhubungan dengan sistem instansi tersebut.

2. Tahap Deteksi dan Analisis (*Dectection & Analysis*)

Tahap ini berkaitan dengan pendeteksian sebuah insiden dan penentuan insiden dapat berdasarkan anomali dari keadaan normal yang ditemukan pada sebuah sistem. Tim penanganan insiden sebuah instansi sering mengalami berbagai kesulitan antara lain sulit mendeteksi kemungkianan adanya suatu insiden, sulit mendeteksi apakah insiden benar-benar terjadi, dan ketika suatu insiden benar terjadi maka tim harus dengan jelas menentukan dampak dari insiden tersebut.

Tahap deteksi dapat dilakukan dengan menggunakan indikator-indikator yang berasal dari *Intrusion Detection and Prevention System* (IDPS), *Security Information and Event Management* (SIEM), *antivirus*, *antispam*, perangkat lunak pendeteksi integritas data, jasa monitoring, log dari sistem operasi, servis, aplikasi, perangkat jaringan yang beroperasi, informasi dari pihak lain terkait kerentanan terkini dari sistem yang digunakan, dan laporan yang berasal dari dalam maupun dari luar.

Setelah proses deteksi dilakukan langkah selanjutnya adalah proses analisis lanjut untuk menentukan langkah yang harus dilakukan selanjutnya. Ada beberapa cara yang dapat dilakukan dalam tahap analisis yaitu :

a. Memahami sifat dan ruang lingkup kejadian.
b. Mengumpulkan informasi
c. Melakukan filter data yang dianggap mencurigakan, dan lainya.
d. Menganalisis dampak yang disebabkan oleh insiden.

Jika pada tahap deteksi dan analisis diperoleh lebih dari satu insiden, maka perlu dibuat skala prioritas dari suatu insiden. Insiden yang memiliki prioritas lebih tinggi harus ditangani lebih dahulu dan setelah insiden tersebut ditangani maka insiden yang memiliki prioritas lebih rendah baru bisa ditangani. Dalam memberikan skala prioritas terhadap sebuah insiden terdapat tiga hal yang perlu dipertimbangkan, yaitu :

a. Dampak fungsional dari insiden, seberapa besar dampak yang dihasilkan oleh insiden terhadap fungsionalitas dari kelangsungan fungsi bisnis saat ini dan kemudian hari jika tidak ditangani.

b. Dampak informasi dari insiden, seberapa besar pengaruh insiden terhadap terhadap *confidentiality, integrity, dan availability* dari informasi yang ada dalam sebuah instansi.

c. Kemampuan pemulihan dari sebuah insiden, seberapa besar insiden dan dampak apa yang ditimbulkan dari insiden tersebut sehingga tim yang menangani insiden dapat memperkirakan waktu dan sumber daya yang dibutuhkan untuk menangani insiden tersebut.

3. Tahap Penanganan, Pembersihan, dan Pemulihan (*Containment, Eradiction & Recovery*)

Tahap penanganan insiden (*Countainment*) dilakukan untuk meminimalisir dampak yang ditimbulkan insiden terhadap sistem yang diserang. Bukti-bukti sepeti informasi identitas (IP komputer, MAC), waktu dan tanggal kejadian, pihak yang telibat dalam insiden yang dibutuhkan untuk menyelesaikan insiden harus dicari dan disimpan dengan baik. Semua bentuk bukti yang dibutuhkan untuk menangani insiden harus disimpan dilokasi yang aman.

Tahap pembersihan insiden (Eradiction) dilakukan terhadap sistem yang terkena serangan untuk memastikan bahwa sistem telah bersih sebelum ditempatkan kembali *production environment.* Selain melakukan pembersihan terhadap sistem, dalam tahap ini juga dilakukan improvisasi terhadap keamanan sistem dan melakukan analisis kerentanan (*vulnerability analysis*) untuk memastikan insiden yang sama tidak terulang kembali.

Tahap pemulihan insiden (*Recovery*) dilakukan untuk mengembalikan sistem yang terkena serangan ke *production environment* agar dapat digunakan kembali. Tahap ini harus dilakukan dengan hati-hati agar tidak terjadi kesalahan yang menyebabkan insiden lainnya. Sangat penting untuk melakukan pengujian keamanan dan memastikan sistem telah bersih, monitoring aktifitas sistem agar tetap berjalan normal dan membuktikan sistem sudah berfungsi dengan baik sebelum sistem digunakan kembali.

4. Tahap Pasca Insiden (*Lesson Learned*)

Tahapan terakhir dalam proses penanganan yang sering diabaikan adalah *learning* dan *improving* yaitu pembelajaran yang dapat diambil dari insiden tersebut dan peningkatan yang harus diterapkan terhadap sistem. Hal penting yang harus diperhatikan adalah membuat dokumentasi pada saat menangani insiden dan mempersiapkan dokumentasi tambahan untuk membantu menangani insiden lain. Dokumentasi yang dibuat digunakan untuk meningkatkan pengukuran keamanan informasi pada sebuah instansi dan proses penanganan insiden itu sendiri. Tahap ini bisa dilakukan dengan mengadakan rapat dan memberikan informasi kepada seluruh pihak yang terlibat setelah insiden berakhir.

3.6 Definisi SOP

SOP (*Standard Operating Procedure*) merupakan sebuah petunjuk buku yang sifatnya tertulis dan pedoman yang berisi prosedur-prosedur operasional yang terdapat pada suatu organisasi, yang digunakan untuk memastikan bahwa semua keputusan dan tindakan serta pengunaan fasilitas-fasilitas proses yang dilakukan oleh orang-orang di dalam organisasi berjalan secara efektif, konsisten, *standard*, dan sistematis.

Insani & Istyadi (2010) mengemukakan SOP atau *Standard Operating Procedure* adalah dokumen yang berisi serangkaian instruksi tertulis yang dibakukan mengenai berbagai proses penyelenggaraan administrator perkantoran yang berisi cara melakukan pekerjaan, waktu pelaksanaan, tempat penyelenggaraan dan aktor yang berperan dalam kegiatan.

Menurut Rachmi et al., (2014) SOP (*Standard Operating Procedure*) merupakan serangkaian panduan yang terdokumentasi secara jelas, lengkap, dan rinci mengenai proses, tugas, dan peran setiap individu atau kelompok yang dilakukan sehari-hari di dalam suatu organisasi. Fungsinya SOP membentuk sistem kerja dan aliran kerja yang teratur, sistematis, serta dapat dipertanggungjawabkan dan mengambarkan kebijakan peraturan yang berlaku.

SOP (*Standard Operating Procedure*) menurut Atmoko (2001) secara umum merupakan gambaran langkah-langkah kerja (sistem, mekanisme dan tata kerja internal) yang diperlukan dalam pelaksanaan suatu tugas untuk mencapai tujuan instansi. SOP sebagai suatu dokumen atau instrumen memuat tentang proses dan prosedur suatu kegiatan yang bersifat efektif dan efesien berdasarkan suatu standar yang sudah baik. Pengembangan instrumen manejemen tersebut dimaksudkan unuk memastikan bahwa proses pelayanan diseluruh unit kerja dapat terkendali dan dapat berjalan sesuai dengan ketentuan yang berlaku.

Setiap perusahaan pasti membutuhkan sebuah panduan untuk menjalankan tugas dan fungsi setiap elemen atau unit yang ada pada sebuah perusahaan. SOP (*Standar Operating Procedure*) adalah sistem yang dibuat untuk memudahkan, merapikan, dan menertibkan pekerjaan dalam sebuah perusahaan. Penerapan SOP yang baik, akan menunjukan konsistensi hasil kerja, dan proses pelayanan yang semuanya mengacu pada kemudahaan dan kepuasan pelanggan serta kualitas yang dimiliki sebuah perusahaan.

3.6.1Tujuan SOP

Tujuan SOP (*Standard Operating Procedure*) menurut Agil (2018) adalah sebagai berikut:

1. Untuk menjaga konsistensi tingkat penampilan kinerja atau kondisi tertentu dan kemana petugas dan lingkungan dalam melaksanakan sesuatu tugas atau pekerjaan tertentu.
2. Sebagai acuan dalam pelaksanaan kegiatan tertentu bagi sesama pekerja dan supervisor.
3. Untuk menghindari kegagalan atau kesalahan (dengan demikian menghindari dan mengurangi konflik), keraguan, duplikasi serta pemborosan dalam proses pelaksanaan kegiatan.
4. Untuk menjelaskan alur tugas, wewenang dan tanggung jawab dari petugas yang terkait.
5. Sebagai dokumen yang digunakan untuk pelatihan.
6. Memperlancar tugas petugas, pegawai, tim dan unit kerja.

Berdasarkan tujuan SOP diatas, peneliti menetapkan tujuan pembuatan SOP dalam penelitian ini sebagai berikut:

1. Sebagai acuan dalam melakukan penanganan dan pencegahan insiden serangan siber yang terjadi pada *website*.
2. Sebagai panduan dalam melakukan pencegahan insiden serangan siber sehingga dapat meminimalisir kesalahan saat proses penanganan insiden.
3. Sebagai referensi pembelanjaran dan pelatihan bagi tim penanganan insiden.
4. Membantu tim penanganan insiden dalam melaksanakan tugas.

3.6.2Manfaat SOP

Manfaat SOP (*Standard Operating Procedure*) menurut Agil (2018) adalah sebagai berikut:

1. Sebagai standarisasi cara yang dilakukan pegawai dalam menyelsaikan pekerjaan khusus, mengurangi kesalahan dan kelalaian.
2. SOP membantu staf menjadi lebih mandiri dan tidak tergantung pada intervensi manajemen. Sehingga akan mengurangi keterlibatan pemimpin dalam pelaksanan proses sehari-hari.
3. Meningkatkan akuntabilitas dengan mendokumentasikan tanggung jawab khusus dalam melaksanakan tugas.
4. Menciptakan bahan-bahan training yang dapat membantu pegawai baru untuk cepat melakukan tugasnya.
5. Membantu penelusuran terhadap kesalahan-kesalahan prosedural dalam memberikan pelayanan dan menjamin proses pelayanan tetap bejalan dalam berbagai situasi.

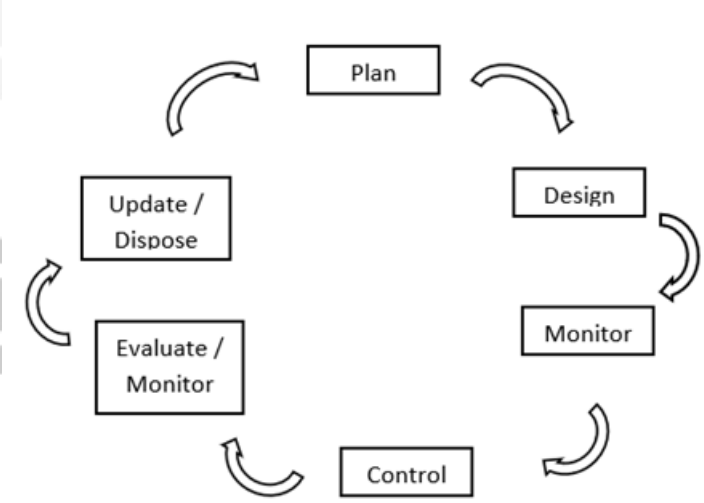
Berdasarkan manfaat SOP diatas, peneliti menetapkan manfaat pembuatan SOP dalam penelitian ini sebagai berikut:

1. Sebagai standarisasi tim penanganan insiden dalam melakukan penanganan dan pencegahan insiden serangan.

2. Sebagai panduan untuk membantu tim penanganan insiden yang baru, agar mengerti tugas dan langka yang harus dilakukan pada saat terjadi insiden serangan.
3. Membantu tim penanganan insiden dalam melakukan penanganan dan pencegah, guna meminimalisir kesalahan pada saat terjadi insiden serangan.

3.7 Perbedaan NIST 800-61 dan Cobit V5

Cobit V5 lebih memposisikan dirinya sebagai alat untuk tata kelola dan manajemen keamanan informasi (*ITGI, Control Objectives for Information and Related Technologies* (COBIT), 2000). Karena itu Cobit V5 tidak cocok digunakan untuk proses penanganan insiden, Sedangkan NIST 800-61 merupakan kerangka kerja khusus yang dimiliki oleh NIST yang dibuat khusus untuk melakukan penanganan insiden serangan. Berikut dapat dilihat perbedaan siklus hidup respon insiden NIST 800-61 dan Cobit V5 pada gambar dibawah ini:

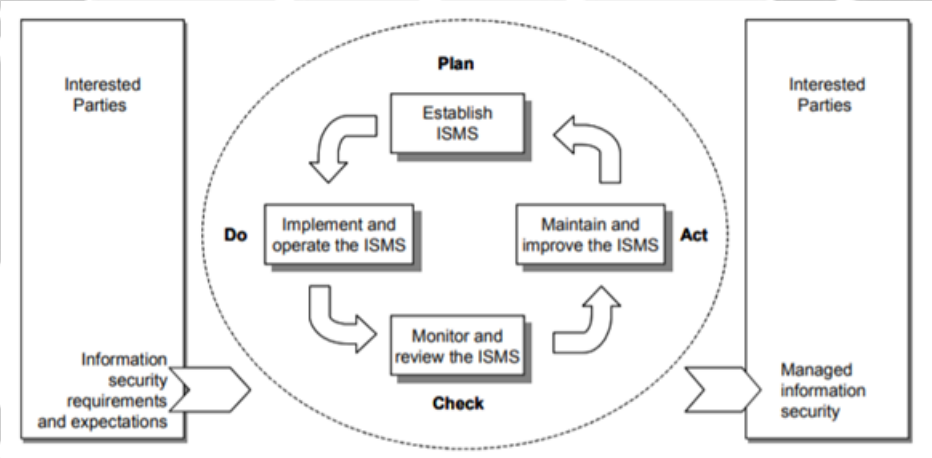


Gambar 3.2. siklus hidup respon insiden Cobit v5 (Cobit, 2012)

Gambar 3.3. siklus hidup respon insiden NIST 800-61 (NIST, 2014)

3.8 Perbedaan NIST 800-61 dan ISO 27001

ISO 27001:2005 merupakan kerangka kerja yang lebih memposisikan dirinya sebagai alat untuk sistem manajemen keamanan informasi (SMKI) atau *information security managemen system* (ISMS) yang memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh sebuah organisasi atau *enterprise* dalam usaha rangka mengimplementasikan konsep-konsep keamanan informasi. Karena itu ISO 27001 tidak cocok digunakan untuk proses penanganan insiden, Sedangkan NIST 800-61 merupakan kerangka kerja khusus yang dimiliki oleh NIST yang dibuat khusus untuk melakukan penanganan insiden serangan. Berikut dapat dilihat perbedaan siklus hidup respon insiden NIST 800-61 dari gambar 3.3 dan ISO 27001 pada gambar di bawah ini:



Gambar3.4. siklus hidup respon insiden ISO 27001 (ISO 27001, 2005)

3.9 Perbedaan NIST 800-61 dan ITIL V3

Gambar 3.5. siklus hidup respon insiden ITIL v3 (ITIL V3, 2007)

ITIL V3 merupakan kerangka kerja yang lebih memposisikan dirinya sebagai alat untuk *best practice* dalam penerapan manajemen layanan teknologi informasi (TI). Karena itu ITIL v3 tidak cocok digunakan untuk proses penanganan insiden, Sedangkan NIST 800-61 merupakan kerangka kerja khusus yang dimiliki oleh NIST yang dibuat khusus untuk melakukan penanganan insiden serangan. Berikut dapat dilihat perbedaan siklus hidup respon insiden NIST 800-61 dari gambar 3.3 dan ITIL v3 pada gambar dibawah ini: