BAB II
LAYANAN KEAMANAN INTERNET DAN PERENCANAAN STRATEGI BISNIS SECURENET

2.1 Keamanan Internet

Internet merupakan jaringan publik yang dapat menghubungkan setiap komputer diseluruh dunia. Dengan terhubungnya komputer ke internet, maka tiap-tiap komputer tersebut dapat saling bertukar informasi satu dengan yang lainnya. Dengan semakin canggihnya teknologi internet, kita dapat memperoleh informasi dalam berbagai macam bentuk, seperti teks, gambar, suara dan video. Dengan segala kemudahan dalam mengakses informasi yang diberikan oleh internet, terdapat banyak sekali potensi ancaman yang dapat terjadi. Potensi ancaman tersebut dapat terjadi kapan saja, dimana saja dan oleh siapa saja yang terhubung ke internet. Ancaman-ancaman yang berasal dari internet, dapat merugikan si pengguna dari segi finansial maupun sosial, contohnya seperti pencurian informasi rahasia, pengerusakan data atau sumber daya, pemalsuan identitas, pengambil-alihan sumber daya dan lain sebagainya. Oleh sebab itu keamanan dalam mengakses internet sangat diperlukan dalam menjaga terjadinya potensi ancaman dari internet.

2.1.1 Klasifikasi Ancaman Internet

Klasifikasi ancaman internet dibagi berdasarkan keempat atribut keamanan komputer [11], yaitu:

- *Confidentiality*, atribut yang menyangkut kerahasiaan suatu data;
- *Integrity*, atribut yang menyangkut akurasi atau keutuhan dari suatu data;
- *Availability*, atribut yang menyakut tentang ketersediaan suatu layanan;
- *Privacy*, atribut yang menyangkut tentang kemampuan untuk melindungi data rahasia.

Pada Tabel 2.1 di bawah ini dapat dilihat tipe serangan berdasarkan atribut keamanan komputer.

Tabel 2.1 Metode Penyerangan dan Solusi Keamanan Internet [11]

No	Security Atributes	Attacks Method	Internet Security Solution
1	Confidentiality	Eavesdropping, hacking, phishing, DoS and IP Spoofing	IDS, Firewall, Cryptographic Systems, IPsec and SSL
2	Integrity	Malware, eavesdropping, DoS and IP Spoofing	IDS, Firewall, Anti-Malware, IPsec and SSL
3	Privacy	Email bombing, Spamming, Hacking, DoS and Cookies	IDS, Firewall, Anti-Malware, IPsec and SSL
4	Availability	DoS, Email Bombing, Spamming, and System Boot Record Infectors	IDS, Firewall, Anti-Malware

1. *Eavesdropping*, merupakan kegiatan yang bertujuan untuk mendengarkan sesi komunikasi oleh pihak yang tidak berwenang. Terdapat pasif dan aktif *eavesdropping*, pasif bersifat hanya mendengarkan sesi komunikasi, sedangkan aktif *eavesdropping* tidak hanya mendengarkan saja, namun juga memasukkan suatu data ke dalam sesi komunikasi tersebut.
2. *Hacker*, merupakan orang yang memiliki keahlian yang tinggi dalam menggunakan komputer. Ketika mereka menemukan celah pada suatu sistem, mereka akan menggunakan celah tersebut untuk melakukan penyerangan.
3. *Phishing*, merupakan kegiatan yang bertujuan untuk mendapatkan data rahasia perorangan, grup maupun organisasi. Tujuan akhir dari kegiatan tersebut biasanya untuk memperoleh keuntungan finansial.
4. *Denial of Services* (DoS), merupakan suatu kegiatan yang membuat akses atau fungsi suatu sistem terhalang.
5. *IP Spoofing*, merupakan kegiatan yang bertujuan untuk memalsukan identitas jaringan yang menyerupai identitas jaringan yang terpercaya.
6. *Malware*, merupakan suatu program yang secara disengaja dimasukkan ke dalam suatu sistem dengan tujuan untuk melakukan tindakan kejahatan. Adapun beberapa tipe ancaman yang termasuk *malware* yaitu:
   - *Virus*, merupakan program komputer yang memiliki kemampuan mereplikasi diri dan biasanya tersembunyi. Virus berkembang dengan cara melakukan infeksi, misalnya menyalin dirinya ke dalam atau

menjadi bagian dari suatu program. Virus tidak dapat berjalan dengan sendirinya, virus memerlukan aksi dari program lain agar dapat aktif [12].

- *Worm*, merupakan program komputer yang dapat berjalan dengan sendirinya. Worm dapat berpropagasi secara penuh menuju pengguna internet ataupun suatu jaringan, dan juga dapat menggunakan sumber daya sistem secara destruktif [12].
- Trojan merupakan suatu program komputer yang terlihat seperti suatu program yang memiliki fungsi yang berguna, namun memiliki fungsi tersembunyi untuk menghindari mekanisme keamanan. Terkadang trojan mengeksploitasi otorisasi pengguna yang menjalankan programnya [12].
- *Back Door*, merupakan suatu mekanisme perangkat keras atau perangkat lunak yang menyediakan akses ke suatu sistem dan sumber dayanya dengan prosedur yang tidak biasa [13].

2.1.2 Layanan Keamanan Internet

Dalam mengatasi problematika keamanan internet seperti pada Table 2.1 di atas, maka dikembangkan berbagai sistem keamanan oleh berbagai macam komunitas dan vendor. Sistem yang dikembangkan diharapkan dapat memberikan layanan keamanan terhadap ancaman-ancaman internet. Beberapa sistem keamanan tersebut yaitu:

- *Intrusion Detection System* (IDS), dapat berupa perangkat keras atau perangkat lunak yang berfungsi untuk mendeteksi serangan.
- *Anti-Malware*, merupakan suatu perangkat lunak yang dapat mendeteksi program-program jahat seperti virus, backdoor, worm , trojan dan spam.
- *Firewall*, merupakan perangkat keras atau perangkat lunak yang berfungsi sebagai gerbang pengendali trafik.
- *Cryptographic System*, merupakan suatu mekanisme yang bertujuan untuk menjaga informasi rahasia dengan penggunaan enkripsi.

- *Internet Protocol Security* (IPsec), merupaka suatu set protokol yang berfungsi dalam menyediakan mekanisme keamanan komunikasi pada *Internet Protocol* (IP).
- *Secure Socket Layer* (SSL), merupakan protokol yang berfungsi dalam menyediakan mekanisme keamanan komunikasi pada *layer transport*.

Pada umumnya teknologi keamanan di atas masih terpisah satu dengan yang lainnya, sehingga untuk implementasinya memerlukan bermacam perangkat keras ataupun perangkat lunak dalam memberikan perlindungan terhadap ancaman-ancaman di internet. Oleh karena itu diperlukan alokasi dana yang cukup untuk implementasi teknologi tersebut. Pengguna teknologi keamanan di atas selain dituntut untuk memahami karakteristik penggunaan internetnya, juga harus memahami fungsi dan kegunaan dari teknologi keamanan tersebut, agar implementasi teknologi keamanan tersebut lebih efektif dan efisien.

Masih sedikit penyelenggara jasa internet yang menyediakan layanan yang serupa dengan SecureNET, karena memang kebanyakan penyelenggara jasa internet masih terkonsentrasi terhadap pangsa pasar layanan akses internet saja, sehingga memberikan peluang yang tinggi bagi Indonet dalam melakukan pemasaran terhadap layanan tersebut. Namun perlu diperhatikan juga bahwa ancaman tidak hanya datang dari penyelenggara jasa internet saja, namun ancaman dapat datang dari vendor-vendor yang sudah lama berkecimpung lama di bidang keamanan akses internet. Pada Table 2.2 di bawah diperlihatkan beberapa layanan keamanan internet yang diberikan oleh beberapa ISP di Indonesia.

Tabel 2.2 Layanan Keamanan Internet beberapa ISP

No	ISP	Layanan Keamanan Internet	Keterangan
1	IndosatM2	VPN, Mail filtering	
2	Biznet	Mail Filtering	
3	CBN	Mail Filtering, Network Blackhole, iControl	Relatif sama dengan SecureNET
4	Radnet	Mail Filtering	
5	Centrin	Mail Filtering	

2.2 Profil Indonet

Indonet berdiri pada tahun 1994 dan menjadi ISP pertama di Indonesia yang mendapatkan ijin komersial.

Visi: menjadi penyelenggara jasa jaringan yang memberikan kualitas layanan tinggi di Indonesia

Misi: menyediakan informasi dan komunikasi terbaik untuk komunitas di Indonesia

Indonet memiliki berbagai macam layanan akses internet dengan menggunakan media kabel maupun nirkabel. Berikut beberapa macam layanan akses internet yang disediakan oleh Indonet [10]:

- Kabel : Dial UP, ADSL, VDSL dan Serat Optik
- Nirkabel : *Microwave Access* dan VSAT
- *Manage Services* : Server Hosting, Web dan Email hosting
- *Value Added Service* : *Email anti spam* dan *anti virus*

Dari komposisi pengguna layanan akses internet, Indonet memiliki kurang lebih 20.000 pengguna personal dan 367 pengguna korporasi [14]. Dengan daerah distribusi layanan di 33 kota besar di Indonesia, Indonet memiliki potensi tinggi dalam memberikan jasa layanan nilai tambah akses internet.

2.3 Profil Layanan SecureNET

Layanan SecureNET merupakan *value added service* akses internet dalam hal keamanan akses internet. SecureNET memberikan layanan keamanan akses internet cukup lengkap dan terintegrasi menjadi satu kesatuan sistem keamanan. Dengan layanan SecureNET ini maka pelanggan diharapkan dapat meningkatkan efisiensi dan kinerjanya dalam pemanfaatan akses internet. Layanan SecureNET ini sesuai bagi pengguna personal, korporasi, institusi pendidikan, institusi pemerintahan dan sebagainya dimana alokasi dana terbatas serta sumber daya manusia yang minim dibidang teknologi informasi.

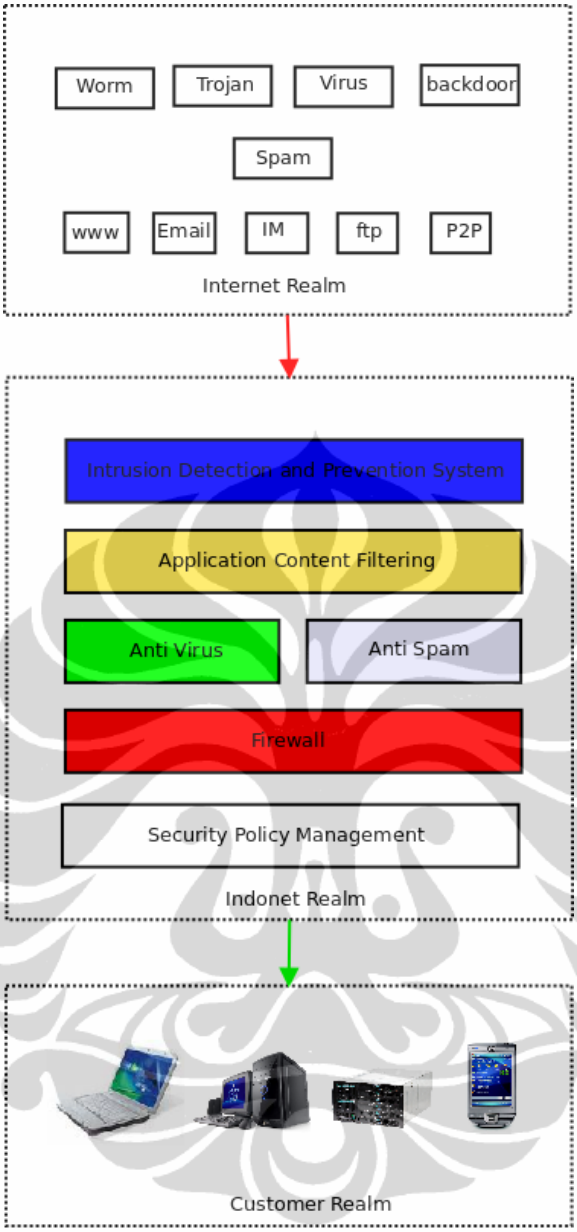
Layanan SecureNET ini terbagi menjadi dua varian yaitu:

1. SecureNET Central

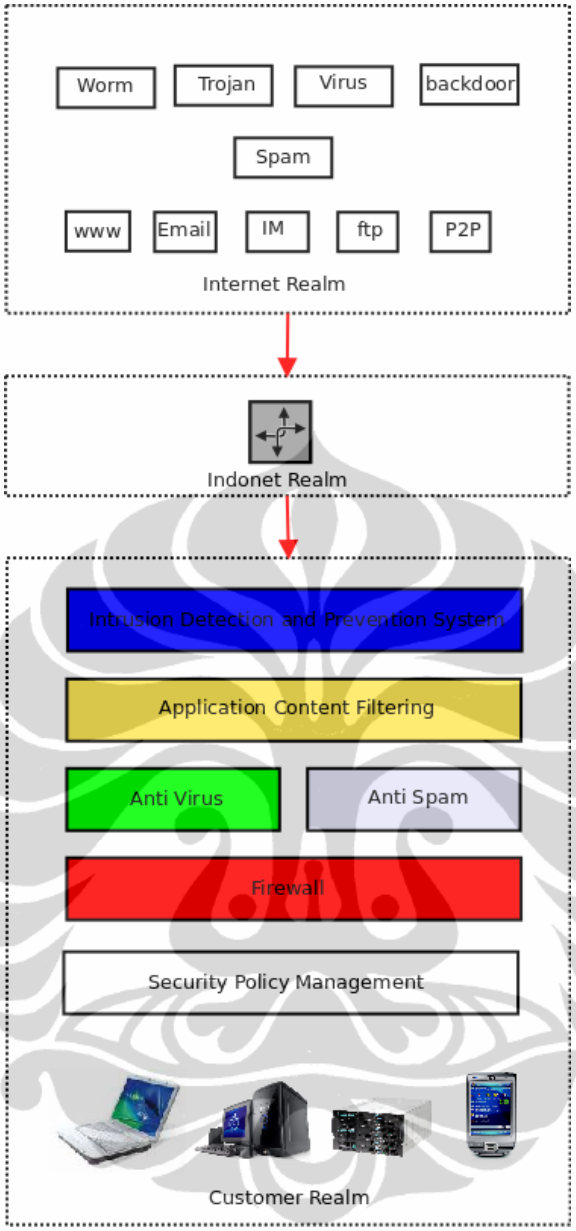
   Merupakan layanan keamanan akses internet dimana segala jenis trafik internet yang menuju pelanggan dilakukan penyaringan terhadap tipe-tipe ancaman terdaftar dalam definisi kebijakan keamanan, sehingga traffik menuju pelanggan terlebih dahulu diminimalisir dari ancaman. Dengan menggunakan layanan ini, efisiensi dan efektifitas penggunaan internet dapat meningkat seiring menurunnya potensi ancaman dari jaringan internet. Layanan ini memiliki keuntungan dimana pengguna tidak perlu mengalokasikan data untuk investasi piranti keamanan tersebut di sisi pelanggan, piranti keamanan tersentralisasi di Indonet. Kekurangan dari layanan ini adalah keterbatasan bagi layanan tersebut dalam mengimplementasikan kebijakan keamanan di internal jaringan pelanggan. Oleh karena itu, untuk memenuhi permintaan layanan keamanan yang memberikan fitur pengaturan sampai ke sisi pelanggan, dibentuklah layanan SecureNET Host. Topologi dari layanan SecureNET Central ini dapat dilihat pada gambar 2.1.

2. SecureNET Host

   Merupakan layanan keamanan akses internet dimana proteksi keamanan dilakukan di internal jaringan pelanggan itu sendiri, sehingga pelanggan bebas melakukan kebijakan-kebijakan akses internet, penggunaan sumber daya teknologi informasi sesuai dengan kebutuhan pelanggan yang diharapkan dapat meningkatkan efisiensi dan efektifitas penggunaan teknologi informasi di ruang lingkup internal pelanggan. Kekurangan dari layanan ini adalah diperlukannya tambahan investasi untuk implementasi piranti keamanan tersebut di sisi pelanggan. Topologi dari layanan SecureNET Host dapat dilihat pada Gambar 2.2.



Gambar 2.1 Topologi SecureNET Central



Gambar 2.2 Topologi SecureNET Host

Dari topologi SecureNET di atas terdapat beberapa sistem yang menjadi kesatuan layanan yang diharapkan dapat meminimalisir ancaman-ancaman pada jaringan komputer. Sistem-sistem tersebut yaitu:

- *Intrusion Detection and Prevention System*, berfungsi sebagai pendeteksi ancaman, ancaman dari internet menuju pelanggan dan dapat melakukan aksi pemblokan terhadap terhadap trafik yang terdeteksi sebagai ancaman tersebut.

- *Application Content Filtering*, berfungsi sebagai gerbang yang melakukan penyaringan terhadap aplikasi-aplikasi internet sesuai dengan kebijakan keamanan yang telah ditentukan sebelumnya
- *Anti Virus* dan *Anti Spam*, berfungsi untuk mendeteksi data yang dikenali sebagai virus dan spam
- *Firewall*, berfungsi sebagai pengatur trafik-trafik apa saja, berasal dari mana dan menuju kemana yang dapat melewatinya.
- *Security Policy Management*, berfungsi sebagai pengatur kebijakan keamanan bagi sistem-sistem lainnya.

2.4 Perencanaan Strategi Bisnis SecureNET

Penelitian ini akan menggunakan metode analisa *Porter's 5 Forces* untuk mengetahui tingkat kompetitif layanan di pasar [15] dan *Strength, Weakness. Opportunity and Threats* (SWOT) untuk menemukan gambaran kecenderungan kondisi organisasi yang aktual pada saat ini dengan tujuan agar dapat menentukan strategi yang tepat [16]. Selain SWOT, akan digunakan juga analisa *Balanced Scorecard* (BSC), dimana BSC menyediakan kerangka pikir yang memandang perusahaan dari empat perspektif yaitu finansial, pelanggan, proses bisnis internal, serta pembelajaran dan pertumbuhan. Keempat perpektif tersebut dinilai mampu mendefinisikan strategi perusahaan secara komprehensif dan detil. Selain itu, BSC juga merupakan metodologi dalam penentuan ukuran kinerja dan target perusahaan, serta rencana aksi yang dapat dilakukan dalam rangka pemenuhan target tersebut [17].