SISTEM MANAJEMEN KEAMANAN JARINGAN KOMPUTER

PADA LABORATURIUM MENGGUNAKAN CISCO

Ni Komang Tri Lestari
Jurusan Sistem Komputer Universitas Sriwijaya

E-mail. nikomangtrilestari@gmail.com

Abstrak

The System is a centralized, computer-network Security manage ment tool capable of handling many different kinds of equipment in a Standardized format despite differences in the computer Security features among the diverse range of computer equipment in the computer network. The inven tion uses a layered Software architecture, including a tech nology Specific layer and a technology independent layer. The technology Specific layer Serves to extract and maintain Security data on target platforms and for converting data to and from a common data model used by the technology independent layer. The technology independent layer handles the main functionality of the System Such as locating and removing certain present and former employees from computer access lists, auditing System user data, monitoring Security events (e.g. failed login attempts), automatically initiating corrective action, interfacing with the System users, reporting, querying and Storing of collected data.

Keywords: Computer networks, network management, and network security

1. Pendahuluan

Sistem manajemen keamanan jaringan komputer terpusat yang mampu menangani berbagai jenis peralatan dalam format standar meskipun terdapat perbedaan dalam fitur Keamanan komputer di antara kisaran yang beragam. peralatan komputer di jaringan komputer. Dengan peningkatan ketergantungan saat ini pada informasi Sistem untuk melakukan bisnis risiko penyalahgunaan atau Sabotase Sistem telah tumbuh menjadi sangat nyata. Membuat masalah lebih nyata adalah berita harian tentang peretas membobol komputer, dan komputer terinfeksi virus. Menambah risiko adalah meningkatnya jumlah merger dan akuisisi, yang telah menghasilkan sejumlah besar pengguna Sistem baru dan pekerja yang berpotensi tidak puas. Untuk mengurangi risiko, Berbagai Solusi teknis telah dikembangkan, misalnya persyaratan untuk memasukkan kata sandi sebelum masuk ke Sistem. Selain itu, Solusi non teknis telah dikembangkan, misalnya dalam bentuk kebijakan perusahaan yang mengamanatkan penonaktifan akun logon yang tidak digunakan selama 90 hari atau lebih. Solusi ini telah

membantu meringankan masalah tetapi juga membuka yang baru. Solusi teknis telah membawa kepada mereka kebutuhan untuk administrasi Keamanan, dan dengan itu kadang-kadang datang administrasi tidak lengkap atau tidak kompeten. Ada kebutuhan untuk audit konstan Sistem Keamanan untuk memastikan kepatuhan. Banyaknya pengguna dan Sistem membuat audit manual menjadi tidak praktis. Perusahaan yang lebih besar cenderung memiliki masalah tambahan yang timbul dari penggunaan jaringan komputer besar yang berisi berbagai jenis peralatan, masing-masing dengan versi sendiri fitur dan protokol penanganan Keamanan. Protokol yang tidak kompatibel ini dan masalah tambahan lingkungan teknis yang berubah dengan cepat di jaringan World Wide telah memperburuk dan menghambat Pencarian untuk Solusi yang Memuaskan. Saat ini, banyak perusahaan besar dibebani dengan Skema Keamanan informasi besar dan rumit yang mengandung lubang loop dan yang tidak dapat diawasi dan diaudit secara efektif. Ini telah meningkatkan kerentanan mereka terhadap penggunaan tidak sah atas Sistem informasi dan basis data rahasia mereka untuk spionase industri atau bahkan ke Sabotase.

2. Metode Penelitian

2.1. Computer Security

Menurut Garfinkel dalam Sofana (2010:307) keamanan komputer mencakup empat aspek yaitu, privacy, integrity, authentication, dan avaibility.

a. Privacy atau confidentiality. Privacy mencakup kerahasian informasi. Inti aspek privacy adalah bagaimana menjaga informasi agar tidak dilihat atau diakses oleh orang yang tidak berhak. Sebagai contoh, e-mail seorang pemakai tidak boleh dibaca orang lain bahkan administrator. Salah satu usaha yang dapat dilakukan yaitu penggunaan enkripsi. Kita dapat menggunakan enkripsi untuk setiap dokumen atau informasi lainnya yang dianggap rahasia dan hanya kita sendiri yang dapat membukanya menggunakan kunci yang tepat.
b. Integrity. Integrity atau integritas mencakup keutuhan informasi. Inti aspek integrity ini adalah bagaimana menjaga informasia agar tetap utuh. Informasi tidak boleh diubah, baik ditambah atau pun dikurangi, kecuali jika mendapat izin dari pemilik informasi. Virus, Trojan horse, atau pemakai lain yang mengubah informasi tanpa izin pemiliknya merupakan contoh masalah yang mengganggu aspek ini. Penggunaan anti virus, enkripsi , dan digital signature, merupakan contoh usaha untuk mengatasi masalah ini.
c. Authentication. Authentication atau otentikasi berkaitan dengan keabsahan pemilik informasi. Harus ada cara untuk mengetahui bahwa informasi benar – benar asli, kemudian yang mengakses informasi adalah orang-orang yang berhak, dan hanya yang berhak saja yang boleh memberikan informasi tersebut kepada orang lain. Penggunaan acess control seperti login dan password merupakan usaha yang dilakukan untuk memenuhi aspek ini. Digital signature dan watermarking juga merupakan salah satu usaha untuk melindungi intellectual property yang sesuai dengan aspek authentication.
d. Avaibility. Aspek ini berhubungan dengan ketersediaan informasi. Informasi harus tersedia manakala dibutuhkan. Contoh serangan terhadap aspek ini yaitu ”Denial of Service attack“ atau DoS attack. Misalkan

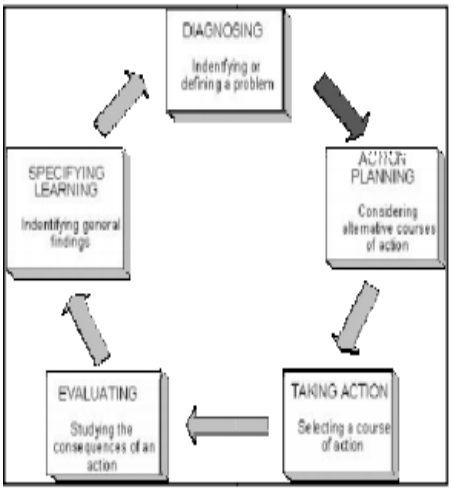
server dikirim request palsu sacara bertubitubi sehingga tidak dapat melayani permintaan.

Menurut Howard dalam Sofana (2010:306) dalam buku yang berjudul CISCO CCNA & Jaringan Komputer mengemukakan tentang computer security. " Computer security is preventing attackers from achieving objectives through unauthorized access or unauthorized use of computers and networks."(Jhon D. Howard, "An Analysis Of Security Incidents On The Internet 1989 – 1995)".

2.2. Metode Action Reserch

Metodologi adalah ilmu yang digunakan untuk memperoleh kebenaran mengggunakan penelusuran dengan tatacara tertentu dalam menemukan kebenaran, tergantung dari realitas yang sedang dikaji. Dalam penelitian ini metode yang digunakan adalah penelitian tindakan atau action research, dalam penelitian tindakan mendeskripsikan, mengiterpretasi dan menjelaskan suatu situasi pada waktu yang bersamaan dengan melakukan perubahan atau intervensi dengan tujuan perbaikan atau partisipasi Menurut Halilintar dalam Davison, Martinson & Kock (2004), menyebutkan penelitian tindakan sebagai metode penelitian, didirikan atas asumsi bahwa teori dan praktek dapat secara tertutup diintegrasikan dengan pembelajaran dari hasil intervensi yang direncanakan setelah diagnosis yang rinci terhadap konteks masalahnya. 5 tahapan yang merupakan siklus dari action research:

1) Melakukan diagnose (Diagnosing). Melakukan identifikasi masalah – masalah pokok yang ada guna menjadi dasar kelompok atau organisasi sehingga terjadi perubahan.
2) Membuat rencana tindakan (Action Planning). Penelitian dan partisipan bersama-sama memahami pokok masalah yang ada kemudian dilanjutkan dengan menyusun rencana tindakan yang tepat untuk menyelesaikan masalah yang ada.
3) Melakukan tindakan (Action Taking). Peneliti dan partisipan bersama-sama mengimplementasikan rencana tindakan dengan harapan dapat menyelesaikan masalah
4) Melakukan evaluasi (Evaluating). Setelah masa implementasi (action taking) dianggap cukup kemudian peneliti bersama partisipan.
5) Pembelajaran (Learning). Tahap ini merupakan bagian akhir siklus yang telah dilalui dengan melaksanakan review tahap pertahap yang telah barakhir kemudian penelitian ini dapat berakhir.



Gambar 1 Action Research Mode

2.3. Keamanan Informasi

Keamanan Informasi adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis (business continuity), meminimasi risiko bisnis (reduce business risk) dan memaksimalkan atau mempercepat pengembalian investasi dan peluang bisnis (ISO 27001 dalam Sarno dan Iffano, 2009, 27). Menurut Syafrizal, M, (2007) Keamanan informasi terdiri dari perlindungan terhadap aspek-aspek berikut: (1) Confidentiality (kerahasiaan) aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.; (2) Integrity (integritas) aspek yang menjamin bahwa data tidak dirubah tanpa ada ijin fihak yang berwenang (authorized), menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integrity ini.; (3) Availability (ketersediaan) aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait (aset yang berhubungan bilamana diperlukan).

Target network security adalah bagaimana mencegah dan menghentikan berbagai threats (potensi serangan) agar tidak memasuki dan menyebar pada suatu network (Sofana 2010:310). Pada dasarnya banyak threats (potensi serangan) yang mengancam network security, seperti yang telah dipaparkan oleh Sofana dalam bukunya yang berjudul Cisco CCNA & Jaringan Komputer (2010: 310) berbagai threats yang mengancam network security dapat digolongkan menjadi beberapa golongan, diantaranya adalah : (1) Viruses, Worms, and Trojan horses; (2) Spyware and adware; (3) Zero-day attacks (zero-hour) attacks; (4) Hacker attacks; (5) Denial of service attacks (DoS); (6) Data interception and theft; (7) Identity theft.

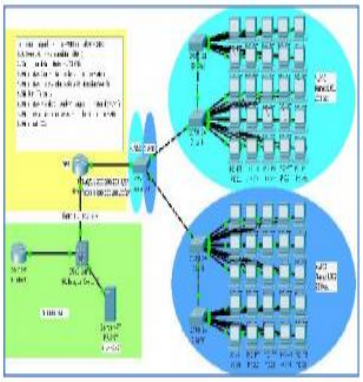
2.4. Gambar Rancangan Managemen Network Security pada Laboratorium Cisco

Analisis yang dilakukan terhadap peta jaringan laboratorium CISCO menghasilkan beberapa rancangan pengembangan. Salah satu rancangan pengembangan yang akan di implementasikan adalah pengembangan management network security laboratorium CISCO. Rancangan pengembangan ini bertujuan untuk meningkatkan keamanan network pada laboratorium tersebut, sehingga nantinya diharapkan dapat membantu kinerja firewall yang telah diimplementasi pada unit pelayanan teknis (UPT). Disamping itu implementasi ini diharapkan memberikan efek yang baik untuk peningkatan proses belajar mengajar pada laboratorium CISCO. Pengembangan yang akan dilakukan antara lain adalah:

a. Pengembangan network topologi dengan menggunakan Cisco Router 2600 series dan Switch catalyst 2950.
b. Implementasi Access Control pada seluruh komputer client yang ada di laboratorium CISCO Universitas Bina Darma.
c. Implementasi dan konfigurasi Network Address Translation (NAT) pada Router Cisco 2600 series.
d. Implementasi dan konfigurasi Virtual Local Area Network (VLAN) pada Router Cisco 2600

series dan implementasi Metode Variabel Length Subnet Mask (VLSM) untuk penghematan host.

e. Implementasi dan konfigurasi sistem keamanan pada Router Cisco 2600 series dan Switch Cisco Catalyst 2960



3. Kesimpulan

Semakin besar skala suatu jaringan maka semakin kompleks administrasi dari jaringan itu, oleh karena itu diperlukan suatu mekanisme keamanan dan metode untuk dapat mengoptimalkan sumber daya jaringan tersebut.

REFERENCES

[1] E. Negara, "Implementasi Management Network Security," *J. Ilm. Matrik*, no. April 2019, pp. 11–20, 2019.

[2] Anonymous,(http://pandawa.ipb.ac.id/ilmukomp uter.org/2018/09/27/monitor-danmemblok-trafik virus-pada-ciscorouter/index.html).http://www.web.net/~r obrien/papers/arfinal.html.

[3] *Sofana. 2017. CISCO CCNA & Jaringan Komputer. Bandung: Informatika Bandung.*

[4] Sarno, R. dan Iffano, I. 2017. Sistem Manajemen Keamanan Informasi. Surabaya: *ITS Press.*

[5] Syafrizal, M, 2019. *Information Security Management System (ISMS) Menggunakan Standar Iso/Iec 27001:2016* .