PERANCANGAN PENGAMANAN JARINGAN PADA PERGURUAN TINGGI XYZ

Fandi Aditya Putra[1)], Joko Purwanto[2)]
Manajemen Persandian, Sekolah Tinggi Sandi Negara
E-mail : fandi.available@gmail.com[1)], joko77sm@gmail.com[2)]

Abstrak

Berkembangnya teknologi informasi menyebabkan tindak kejahatan terus berkembang. Contoh kasusnya seperti yang terjadi pada akun Yale University. Yale University diretas oleh hacker yang mendapatkan 1200 akun yang berisi data mahasiswa dan staf karyawan. Semakin banyak tindak kejahatan, setiap organisasi haruslah mengembangkan keamanan infrastruktur TI yang dimilikinya. Perancangan pengamanan jaringan pada paper ini menerapkan strategi keamanan jaringan TI dengan sebuah arsitektur LAN Hardening. LAN Hardening ini memiliki 3 bagian, yakni client/server hardening, hardware hardening, dan topology hardening. Penanaman arsitektur pada LAN hardening bertujuan untuk mengokohkan pengamanan jaringan terhadap unauthorized user. Keamanan infrastruktur TI yang diberikan bukan hanya berdasarkan pada arsitekturnya saja, namun dari segi access control user juga dianggap sebagai hal yang utama. Adanya remote access user terhadap sistem menyebabkan VPN diperlukan. Perancangan ini tidak hanya mampu menjamin keamanan sistem jaringannya saja tetapi juga diharapkan menjamin keamanan informasi yang dimilikinya.

Kata kunci: *Pengamanan jaringan, LAN hardening, arsitektur, perguruan tinggi.*

Abstract

The development of information technology causes criminalities to keep developing. For example, the case that happened to the accounts of Yale University. The Yale University had been hacked by a hacker which got 1200 accounts containing data of students and employees. With the increasing number of criminalities, every organization must develops its IT security infrastructure. The network security design on this paper applied the stategy of IT network security with an architecture of LAN Hardening. This LAN Hardening has 3 part, those are client/server hardening, hardware hardening, and topology hardening. Planting this architecture on the LAN hardening is aiming to strengthen the network security to the unauthorized user. IT infrastructure security which given is not only based on its architecture, but also from the side of access control is considered as the main case. Enabling the remote access user to the system causes VPN to be needed. This design is not only can guaranteed its network security system but also it is hoped to guarantee its information security.

Keywords: *Network security, LAN hardening, architecture, university.*

1. PENDAHULUAN

Organisasi memiliki kekuatan dalam menjalankan tugas dan fungsinya. Keberlangsungan suatu organisasi didasari oleh kebutuhan yang ada saat ini. Namun, setiap organisasi pastinya memiliki risiko keamanan baik dari segi ancaman (*threats*) maupun celah yang mudah diserang lawan (*vulnerabilities*). Ancaman tersebut dapat berupa ancaman terhadap sistem operasi, personil, dan teknologi. Perkembangan Teknologi Informasi (TI) sekarang ini menimbulkan berbagai tindak kejahatan di dunia *cyber*. Kejahatan yang terjadi menyebabkan kerugian bagi sebagian pihak seperti hilangnya aset berharga pada organisasi, rusaknya sistem informasi, dan berbagai ancaman lainnya. Salah satu contoh kasus yang terjadi pada tahun 2012, *Yale University* mengalami peretasan pada sistem informasinya. Dari peretasan sistem informasi tersebut, *hacker* mendapatkan *database* yang bersi 1200 akun data mahasiswa dan anggota staf karyawan. *Hacker* menunjukkan *username*, *password*, dan alamat *email* yang digunakan pada sistem. *Hacker* tersebut menyerang sistem *database* melalui pencurian jaringan LAN. Hal tersebut terjadi karena infrastruktur sistem keamanan yang lemah. Dalam mengatasi infrastruktur sistem keamanan yang kurang baik, haruslah diiringi dengan pengamanan dari risiko yang ada. Salah satunya adalah pengamanan pada jaringannya, pada pengamanan ini harus diperhatikan masalah arsitekturnya. Pada perancangan arsitektur keamanan jaringan ini, arsitekturnya harus disesuaikan dengan aset

yang akan diamankan pada organisasi tersebut.Sedangkan dalam pengamanan aset, hal yang diutamakan adalah pengamanan teknologi informasinya agar aman dan terhindar dari segala bentuk ancaman.

Organisasi yang dapat menerapkan pengamanan jaringan ini, salah satunya adalah Perguruan Tinggi XYZ. Perguruan tinggi ini membutuhkan pengamanan aset yang dimilikinya, diantaranya adalah sistem informasi, hasil riset yang dikembangkan, data mahasiswa, data karyawan, dan data dosen, serta transfer data yang dilakukan antar bagian atau unit. Bukan hanya pada jaringannya saja, namun personil yang mengendalikan sistem tersebut perlu memiliki wawasan yang luas dalam mengatasi kondisi dari universitas tersebut. Rancangan pengamanan ini, tidak hanya dilihat dari unsur keamananya saja, namun sistem operasi pintar yang juga mudah digunakan oleh pengguna (*smart reusable service*). Oleh karena itu, perlu adanya suatu pengembangan rancangan keamanan jaringan yang digunakan pada perguruan tinggi. Dengan adanya perancangan pengamanan jaringan ini, diharapkan mampu memperkuat infrastruktur keamanan TI yang digunakan oleh perguruan tinggi tanpa mempersulit pengguna.

2. TINJAUAN PUSTAKA

2.1 Keamanan Informasi di Dunia *Cyber*

Dunia *Cyber* merupakan dunia maya dimana para individu maupun kelompok-kelompok masyarakat saling berinteraksi, bertukar pikiran, dan berkolaborasi untuk melakukan sejumlah aktivitas kehidupan. Dalam dunia *Cyber* banyak tindak kejahatan keamanan informasi, salah satunya adalah *Cyber Threat*. *Cyber Threat* merupakan ancaman yang dilakukan oleh pihak yang ingin mengambil beraneka ragam harta atau barang berharga yang ditransaksikan maupun dipertukarkan di dunia maya. Contoh tersebut merupakan upaya ancaman yang dilakukan di dunia *cyber* yang berhubungan dengan penyerangan *database* maupun penyerangan pada jaringan LAN dengan pencurian informasi melalui jalur transfer data [3]. Keamanan informasi berbeda dengan keamanan teknologi informasi atau IT *security*, karena keamanan informasi fokusnya pada data dan informasi milik suatu organisasi, untuk dilindungi agar data-data tersebut dapat digunakan dan tidak disalahgunakan atau bahkan dibocorkan ke pihak-pihak yang tidak berkepentingan. Sedangkan IT *security* fokusnya pada segala upaya untuk mengamankan infrastruktur teknologi informasi dari segala gangguan atau ancaman [6].

2.2 Sistem Pengamanan Jaringan

Sistem pengamanan jaringan adalah sebuah sistem rekayasa baru yang berfokus pada pendekatan untuk mengatasi segala ancaman, dengan menggunakan sebuah formulasi arsitektur keamanan jaringan yang dapat memberikan layanan yang dapat digunakan kembali (*reusable*) [10]. Sistem ini dapat diterapkan di sebuah instansi termasuk perguruan tinggi. Dalam menerapkan sistem ini, proses yang terjadi pada pengiriman dan penerimaan informasi yang dilakukan pada perguruan tinggi melalui jaringan dapat terjamin keamanannya. Dalam membentuk sistem pengamanan jaringan, terlebih dahulu mengetahui kerangka logika terstruktur bagaimana proses komunikasi data berinteraksi melalui jaringan. Kerangka ini disebut sebagai model OSI yang memiliki 7 *layer*. Tujuh *layer* tersebut diantaranya adalah *application, presentation, session, transport, network, data link,* dan *physical* [9].

2.3 Kriptografi pada VPN

VPN merupakan teknik pengamanan jaringan yang bekerja dengan cara membuat suatu *tunnel* sehingga jaringan yang terpercaya dapat terhubung dengan jaringan yang ada di luar melalui internet [7]. VPN membutuhkan sebuah *server* yang berfungsi sebagai penghubung antar komputer berupa *router*. Salah satu jenis dari VPN adalah *remote access*, yaitu *client* dapat mengakses ke *server* melalui VPN yang aksesnya dilakukan oleh para *user* yang bersifat berpindah/tidak menetap [14].

2.4 Strategi *Defense-In-Depth*

Pengamanan sumber daya sistem TI pada *layer* (*layered* protections) dapat disebut sebagai *defense in depth*. Risiko Keamanan pada *defense in depth* timbul dari 3 aspek yang meliputi sistem operasi, personil, dan teknologi. Aspek tersebut dikembangkan menjadi kondisi-kondisi seperti lingkungan fisik, *perimeter defense*, kebijakan dan prosedur, pelatihan dan kesadaran keamanan personil, arsitektur keamanan TI, dan kemudahan mendapatkan produk. Kontrol dalam strategi *Defense in depth* meliputi 3 tipe kontrol yaitu *administrative control, logical control,*dan *physical control*. Kontrol tersebut didasari dari jenis-jenis serangan yang muncul pada sistem seperti serangan menggunakan protokol biasa, serangan ke dalam sistem kontrrol, serangan *database* dan *SQL injection*, dan serangan *man-in-the*-middle [4].

3. Perancangan Pengamanan Jaringan pada Universitas XYZ

3.1 Strategi Keamanan Sumber Daya Sistem TI

Dalam menerapkan strategi sistem keamanan jaringan, acuan pokok prinsip keamanan sistem TI perlu diaplikasikan. Acuan tersebut meliputi *least previlage* (hak akses sesuai dengan kebutuhan *user*), *Defense-In-Depth* (lapisan pertahanan keamanan), *choke point* (keluar masuk *user* hanya satu gerbang), *weakest link*, dan *diversity of defence (*menggunakan beberapa jenis sistem pertahanan yang berbeda). Pada intinya, semua aktivitas yang menyangkut dengan sistem diatur dari hak akses sampai jenis sistem pertahanan yang dipakai sistem agar dapat berlangsung secara aman dan dapat diatur dengan baik. Hal ini merupakan strategi kebijakan yang diterapkan suatu Perguruan Tinggi atau instansi lainnya yang membutuhkan keamanan yang baik. Tentunya *user* dan administrator merupakan orang yang sama dan juga berbeda sehingga setiap *user* memiliki kewenangan terhadap sistem yang berbeda pula sesuai dengan hak akses pada masing-masing *user*.

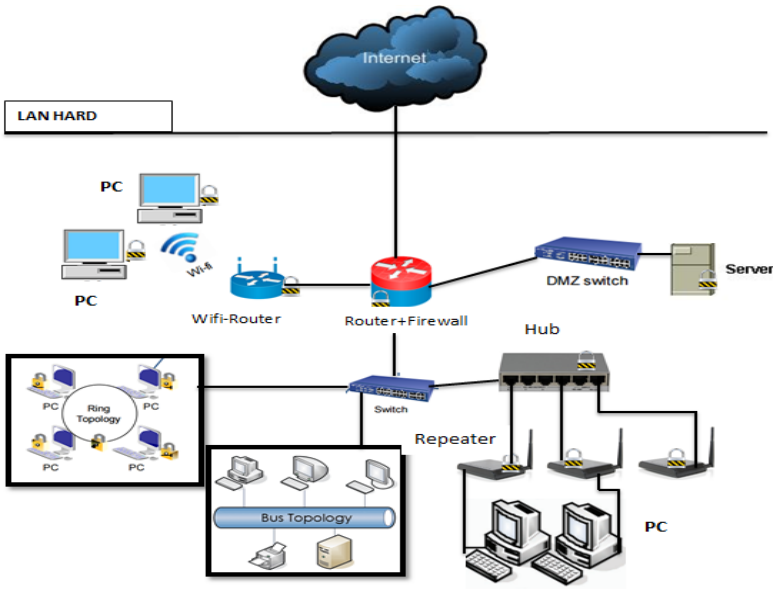
3.2 Lapisan Keamanan Jaringan *Defense-In-Depth*

Menurut jurnal *IT Security Review*, pengamanan pada *layer defense* pada *Defense in Depth* meliputi *Security Risk*, *Host Layer*, *Network Layer*, *Operational Layer*. Lapisan ini dibentuk menjadi satu kesatuan dalam mencegah lawan mengetahui celah yang mudah diserang. Pembangun strategi *defense in depth* salah satunya adalah *logical control*, meliputi *software* dan data sebagai monitor dan akses kontrol terhadap informasi dan sistem komputasi. Hal yang diangkat disini adalah hanya *user* yang dapat bertindak sebagai *access conrol* pada sistem. Sistem ini dibangun dengan TI yang berfungsi sebagai pertahanan terhadap ancaman yang dilakukan musuh. TI disini memiliki elemen utama dalam keamanan jaringan pada Perguruan Tinggi XYZ.

3.3 Arsitektur Pengamanan Jaringan Sistem Perguruan Tinggi

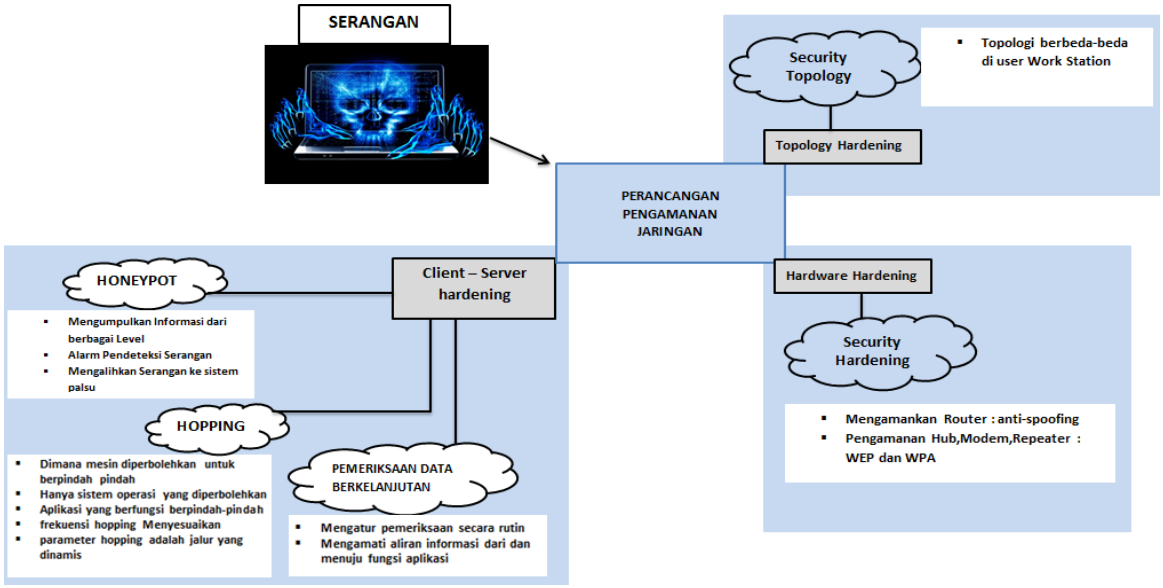
Dalam mengamankan sistem pada Perguruan Tinggi ini, administrator tentunya harus mengetahui serangan dan celah yang akan diserang oleh musuh terhadap sistem. Administrator diwajibkan dapat mengendalikan sistem dengan baik. Dengan bantuan arsitektur yang aman, diharapkan arsitektur tersebut dapat dimanfaatkan oleh administrator dalam menjalankan fungsi dari sistem tersebut. Menurut jurnal *System-Aware Cyber Security*, terdapat arsitektur pengamanan jaringan pada *System-Aware* yaitu honeypot, konfigurasi *hopping*, dan pemeriksaan data berkelanjutan. Namun, arsitektur tersebut bekerja yakni pada jaringan LAN. Penerapan arsitektur keamanan tersebut berada pada zona aman (*security zone*). Dalam menentukan zona aman dari sistem, perlu adanya pemisah antara jaringan publik dengan jaringan LAN. Dari perbedaan fungsi jaringan tersebut, tentunya ada suatu arsitektur yang mengamankan jaringan LAN terhadap jaringan publik.

Menurut jurnal *Security Enhanching of a LAN Network*, jaringan komputer hanya dapat mengakses informasi dan pelayanan dengan kontrol dan pengorganisasian yang baik. *Hardening* membuat sistem *hard* yang memproteksi sistem dari *unauthorized user*. *Unauthorized user* bertindak sebagai *user* yang tidak dikenal yang diduga melakukan ancaman keamanan sistem. LAN *hardening* dibagi menjadi tiga bagian, yakni *client/server hardening*, *hardware hardening*, dan *topology hardening* [17].



Gambar 1. Arsitektur LAN Hardening pada Perguruan Tinggi XYZ

Honeypot adalah sumber sistem informasi yang biasanya didesain bertujuan untuk mendeteksi, menejebak dalam usaha percobaan penetrasi kedalam sistem [12]. Pada LAN *hardening*, terdapat *client hardening* yaitu perlindungan terhadap OS dari serangan musuh yang menyebabkan risiko keamanan. Pada umumnya, *server hardening* pun sama fungsinya seperti *client hardening*. *Hardening* penting ditujukkan kepada pengacau, sehingga sistem dapat diakses *user* dengan aman dari *unauthorized user*. Jika *unauthorized user* terdeteksi saat memasuki sistem pada arsitektur sistem keamanan yang dibentuk, sistem mengalihkan *user* tersebut ke dalam jebakan honeypot (teknik *masking*). Honeypot yang akan berperan secara optimal dalam rancangan ini bekerja pada DMZ (*demilitary zone*). Honeypot ini bagaikan sebuah jebakan dengan mesin virtualnya yang menyebabkan seakan-akan musuh memasuki sistem, namun sebenernya *user* tersebut dipantau oleh administrator sistem. DMZ akan mengalihkan kepada honeypot apabila tindakan-tindakan mencurigakan terdeteksi. Apabila tindakan tersebut dianggap aman dan sah maka akan dihubungkan kepada *web server* yang akan diteruskan kepada jaringan LAN.
Fungsi dari *firewall* yang bekerjasama dengan honeypot yaitu apabila penyerang sudah terdeteksi sebagai ancaman aktif, maka honeypot dapat menjadi alarm pendeteksi serangan dari ancaman tersebut. Ancaman tersebut dapat diperoleh dari berbagai aspek dari mulai *interuders,virus*, dan sebagainya. Maka dari itu, dalam *security zone* dibagi menjadi daerah DMZ, *Database Zone*, dan LAN *zone* dengan perlindungan *firewall* terhadap *server* yang ada. *Database Zone* hanya dapat diakses oleh *user* yang memiliki kewenangan mengakses *database* contohnya *database* mahasiswa, maupun administrator sebagai pengendali sistem.



Gambar 2. Elemen Arsitektur Pengamanan Jaringan Perguruan Tinggi XYZ

Menurut jurnal *Defense-in-Depth*, setiap keamanan jaringan selalu diikuti dengan penerapan *firewall*. Tentunya setiap sistem aman memiliki fungsi *firewall* dalam jaringannya. *Firewall* bertujuan untuk mengamankan berbagai ancaman dan celah yang dapat diserang oleh lawan. Aplikasi *firewall* ini tentunya dibutuhkan karena *firewall* yang digunakan adalah *double-firewall*. *Firewall* pada rancangan ini memuat *firewall* dalam dan *firewall* luar dan diantara kedua *firewall* tersebut adalah DMZ yang kemudian di dalamnya terdapat honeypot. *Firewall* ini berada pada sebuah *router* yang menghubungkan antara *client* dan *server* sehingga dapat diperlihatkan bahwa disinilah awal *user* memasuki jaringan LAN dari jaringan publik.

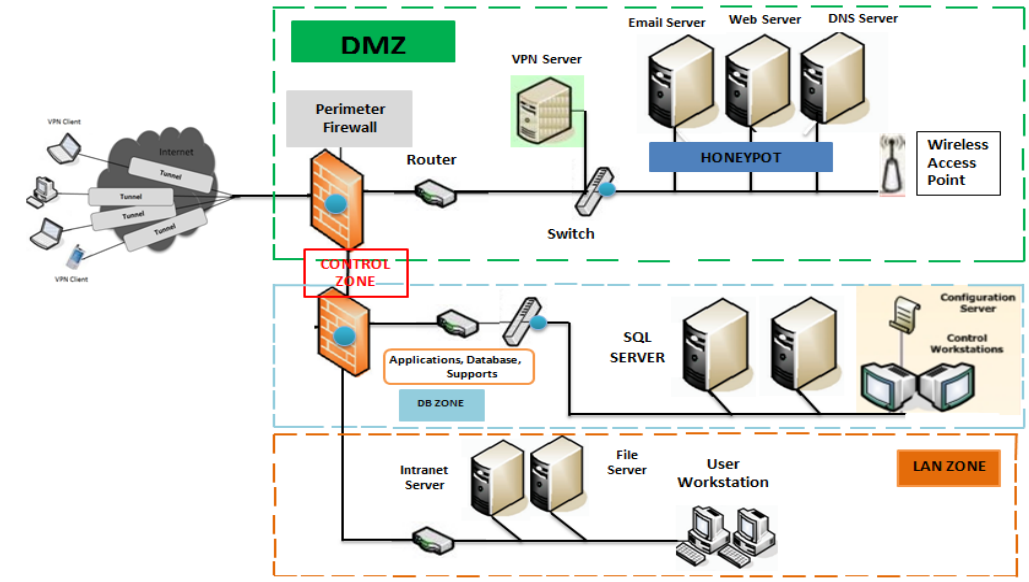
Arsitektur kedua dari *System-Aware Cyber Security*, arsitektur rancangan ini adalah konfigurasi *hopping* yang merupakan sebuah layanan keamanan yang dalam penebaran sinyal informasinya menyesuaikan frekuensi yang dinamis (selalu berpindah pindah menyesuaikan kondisi). Penyesuaian kondisi sesuai frekuensi tersebut dialiri pada jaringan LAN. Dengan adanya konfigurasi *Hopping*, aliran pengiriman informasi dari satu unit ke unit lainnya menjadi dinamis karena frekuensi yang dihasilkannya berbeda-beda. Jaringan yang dilewati berpindah-pindah sesuai frekuensi ini membuat ancaman dan celah keamanan yang didapatkan sistem menjadi lebih kecil terhadap data yang dialiri pada jaringan pengiriman antar unit di Perguruan Tinggi. Hal ini didasari karena adanya teknik ancaman "*Island Hopping Attack*". Teknik ini bekerja untuk *unauthorized user* dalam melemahkan area keamanan sistem, tentunya hal ini tidak menguntungkan bagi organisasi. Pemanfaatan teknik ini pun menggunakan penetrasi yang baik dan juga sebagai sumber daya yang bernilai pada sistem TI.

Arsitektur *system-aware* ketiga yaitu pemeriksaan data berkelanjutan. Arsitektur ini dianggap penting, karena data yang dimiliki tentunya harus selalu dicek secara berkala oleh administrator. Kondisi *server* dan data yang ada di dalamnya selalu dicek secara berkala untuk mengamati aliran informasi sebagai fungsi aplikasi. Pemeriksaan tersebut melalui *user* yang bertindak sebagai *access control* pada sistem sehingga ancaman yang timbul bisa dideteksi sedini mungkin. *User* tersebut dapat pula dianggap sebagai administrator. *User* ini dirancang untuk mengetahui peringatan atau deteksi ancaman melalui sebuah aplikasi, contohnya seperti *SMS Alert*. *SMS Alert* ini berfungsi sebagai *monitoring* sistem yang dilakukan oleh *user* melalui *handphone*. Aplikasi seperti ini bertujuan untuk kenyamanan dari *user*. Dengan kombinasi tersebut, pengelolaan sistem dengan peringatan otomatis membuat data akan terpantau secara berkala.

Secara umum, arsitektur yang bekerja pada *secure zone* tersebut dilihat dari sisi *client/server hardening*. Namun bukan hanya sebatas itu saja, *hardware hardening* juga dianggap penting untuk diamankan. *Hardware hardening* mengamankan komponen *hardware* jaringan seperti *bridge*, *router*, *switch*, *repeater*, *hub*, maupun *modem*. Semua komponen ini memungkinkan ada pada elemen perancang sistem Perguruan Tinggi. Dalam rancangan ini, ditunjukkan bahwa *router* yang berperan sehingga dibentuklah peraturan *anti-spoofing* dan mematikan HTTP *configuration* maupun IP *source routing*. Penerapan pada *hub*, *modem*, dan *repeater* pun menggunakan teknik *hardening* berupa 2 tipe keamanan seperti WEP (*wireless equivalent policy*) dan WPA (*wireless protected access)* [17]. Topologi yang dibentuk dalam sistem seharusnya dibentuk dengan baik. Dengan topologi yang aman maka jaringan dapat dianggap aman juga. Dalam hal ini penting dibentuk *topology hardening*, yakni dalam mengelola jaringan yang aman tentunya *user* memiliki peran yang penting. Skenario dari *topology hardening* yaitu dengan *user workstation* pada masing-masing unit memiliki topologi yang berbeda-beda (topologi *bus*, *ring*, *star*, dan *tree*).

User sebagai pimpinan harus mendukung aturan dan prosedur tentang hak akses terhadap *resource-resource* yang ada pada sistem. *User* memantau sistem dan memastikan bahwa prosedur dan kebijakan yang dibuat dijalankan dengan baik. Sistem ini juga menggunakan *remote access* yang berasal dari *user*. *User* tersebut adalah *user* yang bertindak sebagai administrator. *Remote Access* ini dirancang agar *user* dapat mengakses sistem. Menurut Jurnal *Network Security Architecure*, pelayanan keamanan *remote access* yang aman untuk *user* adalah penggunaan VPN. Salah satu rekomendasi dari jenis VPN yang dipakai adalah *Secure Socket Layer* (SSL) *Virtual Private Network* (VPN). Menurut NIST, SSL VPN memberikan layanan keamanan akses kontrol pada sumber daya organisasi. SSL VPN menyediakan *remote user* untuk mengakses *web application* dan *client/server application*, serta koneksi jaringan internal [5]. SSL VPN mudah digunakan *user* karena sudah terdapat pada *web browser* sehingga *client* tidak memerlukan konfigurasi SSL VPN dari *user*. Ada 5 fase yang dapat direkomendasi pada Perguruan Tinggi dalam menggunakan SSL VPN yaitu mengidentifikasi syarat-syarat yang bisa masuk untuk *remote access*, membuat solusi desain (segi *access control*, kebijakan kriptografi, arsitektur, metode otentikasi dan *endpoint security*), mengimplementasi dan melakukan tes prototipe pada solusi desain di lab (identifikasi potensi berbagai persoalan), menyebarkan solusi SSL VPN, dan kelola solusi tersebut. Dalam jurnal *administrative acces control*, terdapat 4 point yang memberikan kewenangan kontrol oleh *user*.

3.4 Desain Arsitektur Keamanan Jaringan Perguruan Tinggi XYZ



Gambar 3. Perancangan Pengamanan Jaringan pada Perguruan Tinggi XYZ

Berdasarkan jurnal Perancangan dan Implementasi *Intrusion Detection System* (IDS) pada jaringan Nirkabel Binus *University*, IDS diterapkan sebagai salah satu solusi untuk membantu dalam keamanan jaringan. IDS digunakan karena dapat mengontrol dan menganalisa gangguan-gangguan terhadap keamanan jaringan. IDS ditempatkan pada *router*, sehingga semua paket yang keluar maupun masuk melalui *router* akan dicerminkan ke IDS yang kemudian akan dianalisis.

Pada perguruan tinggi, jaringan dibentuk dengan keamanan pada TI bertujuan untuk membangun keamanan sistem TI dari segala bentuk ancaman. Dengan adanya perancangan pengamaan jaringan ini, sebuah sistem TI pada perguruan tinggi dapat menjadi sebuah sistem yang dapat digunakan kembali (*reusable*). Rancangan ini dapat juga berfungsi sebagai pendistribusi informasi secara menyeluruh ke seluruh bagian yang berhubungan pada perguruan tinggi. Sistem ini pun dapat menjadi layanan keamanan yang aktif dari potensi-potensi ancaman yang ada. Penerapan sistem dengan arsitektur yang ada tersebut tentunya disertai dengan aturan yang telah ditetapkan sehingga bukan hanya arsitektur yang aman tetapi dalam pengaplikasian sistem, dapat tertata dengan baik. Suatu sistem dapat dikatakan baik pula apabila disesuaikan dengan kemampuan sumber daya yang ada dala organisasi.

4. SIMPULAN DAN SARAN

4.1 Simpulan

Dengan adanya penerapan dari perancangan pengamanan jaringan ini, Perguruan Tinggi XYZ dapat menjamin keamanan pada infrastruktur TI yang ada pada sistem. Perancangan pengamanan jaringan ini memberikan sebuah rancangan dalam keamanan jaringan sebagai layanan yang dapat digunakan kembali (*reusable service*). Hal ini penting terkait strategi yang dilakukan Perguruan Tinggi dalam menjalankan tugas dan fungsinya. Rancangan ini diharapkan dapat menjamin sistem pada Perguruan Tinggi XYZ dari serangan atau ancaman aktif dengan teknik LAN *hardening.* LAN *hardening* dibagi menjadi 3 bagian, yakni *client/server hardening, hardware hardening*, dan *topology hardening.* Dengan penggunaan honeypot sebagai pendeteksi ancaman *unauthorized user*, sistem membuat teknik *masking* pada *client/server hardening*. *Firewall* sebagai komponen arsitektur keamanan sistem ini yang berada sebagai penyaring akses *user* terhadap sistem, bukan hanya itu saja namun melindungi dari bentuk ancaman lainnya seperti virus maupun trojan. Arsitektur ini dilengkapi dengan pemeriksaan sistem secara rutin dengan sistem *monitoring* oleh *user* dan konfigurasi *hopping,* sehingga frekuensi pada transaksi informasi terjadi secara dinamis, serta penggunaan SSL VPN yang direkomendasikan untuk mengamankan arus jaringan. Perlindungan keamanan ini menggunakan *hardware hardening* yang mengamankan komponen *hardware* pada sistem. Selain itu, dibentuk pula kombinasi topologi jaringan yang bervariasi sehingga menghasilkan *topology hardening*. LAN *hardening* akan terbentuk dengan baik ketika fungsi *access control* dari *user* sebagai administrator dijalankan dengan baik pula. Dengan kombinasi elemen arsitektur tersebut, keamanan infrastruktur TI dan proses transaksi data pada Perguruan Tinggi XYZ diharapkan dapat berlangsung secara aman dan terhindar dari ancaman penyerang.

4.2 Saran

Dengan berkembangnya teknologi yang mengakibatkan tindak kejahatan, khususnya pada dunia *Cyber*, Perancangan pengamanan jaringan pada sistem ini perlu diuji pada Perguruan Tinggi, serta dapat mengetahui celah kelemahan pada sistem yang mengakibatkan suatu ancaman baru. Penerapan sistem ini bukan hanya dapat diterapkan di Perguruan Tinggi saja namun dapat menjadi bahan rekomendasi pada instansi lain seperti Perusahaan Industri maupun Instansi Pemerintahan.

5. DAFTAR RUJUKAN

[1] Munir, Rinaldi., 2006. *Kriptografi*. 1st ed. Bandung: Informatika.

[2] Dharma Oetomo, Budi Sutedjo, dkk., 2006. *Konsep & Aplikasi Pemrograman Client Server dan Sistem Terdistribusi*. 1st ed. Yogyakarta: Andi.

[3] Eko Indrajit, Richardus., 2014. *Konsep dan Strategi Keamanan Informasi di Dunia Cyber*. 1st ed. Yogyakarta: Graha Ilmu.

[4] Homeland Security. 2009. *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies*. Homeland Security: USA.

[5] Frankel, Sheila dkk. 2008. *Guide to SSL VPNs*. NIST: U.S Departement of Commerce.

[6] Syafrizal, Melwin., 2008. AMIKOM. *Information Security Management System (ISMS) menggunakan Standar ISO/IEC 27001:2005*. 1 (1), pp.92-117.

[7] Hendriana, Yana., 2012. Jurnal Teknologi. *Evaluasi Implementasi Keamanan Jaringan Virtual Private Network (VPN) (Studi Kasus pada CV. Pangestu Jaya)*. 5 (2), pp.132-142.

[8] Stawowski, Mariusz. 2009. ISSA Journal. *Network Security Architecture*. pp.34-38.

[9] Hudson Atwell, Denise J. McManus, and Houston H. Carr. 2013. International Journal of Applied Science and Technology. *The OSI Model and the Seven Chakras of Hinduism: A Comparative Analysis*. 3 (3), pp.1-6.

[10] Jones, Rick A and Barry Horowitz., 2011. System-Aware Cyber Security. In: IEEE (Institute of Electrical and Electronics Engineers), *8th International Conference on Information Technology: New Generations*. Las Vegas, 11-13 April 2011. IEEE: Canada.

[11] Abraham Nethanel Setiawan Junior, Agus Harianto, and Alexander. Jurnal BINUS. *Perancangan dan Implementasi Intrusion Detection System pada Jaringan Nurkabel BINU S University*. pp.1-15.

[12] Bosman Tambunan, Willy Sudiarto Raharjo, and Joko Purwadi., 2013. ULTIMA Computing. *Desain dan Implementasi Honeypot dengan Fwsnort dan PSAD sebagai Instrusion Prevention System*. 5 (1), pp.1-7.

[13] Stawowski, Mariusz. 2007. ISSA Journal. *The Principles of Network Security Design*. pp.29-31.

[14] Toni Firnandes, Sumantri K. Risandriya, and Kamarudin., 2013. Makalah Integrasi Polibatam. *Aplikasi Wireless Sensor Network (WSN) Berbasis Radio Frequency (RF) dan SMS Alert GSM*. 1 (1), pp.1-8.

[15] perantiNET, 2012. *1200 akun Universitas Yale diretas Hacker*. [online] (Update 19 Juli 2012)
Available at: http://www.peranti.net/1200-akun-universitas-yale-diretas-*Hacker*/ [Accessed 25 April 2015]

[16] Sandhu and Pierangela Samarati. 1994. IEEE Comunication Magazine. *Access Control: Principles and Practice*. pp.40-48.

[17] Sakshi Sharma, Gurleen Singh, and Prabhdeep Singh. IJITEE. *Security Enhancing of a LAN Network Using Hardening Technique*. 2(3), pp.174-181.