Analisa Kebutuhan Keamanan Sistem Jaringan dan Aplikasi Dengan Metode Square Studi Kasus PT Tawada Healthcare

Fahmi Rusdi Al Islami[1], Selviany Nuri Izatie[2], Indri Destiana[3]
[1,2,3]Magister Ilmu Komputer, Universitas Budi Luhur
Email : alrufahmi@gmail.com[1], nuriselviany@gmail.com[2], destiana.indri@gmail.com[3]

Abstrak- Security in a system that was absolutely needed to maintain the data contained in the system . Security needs to be important when the system can be accessed many and connected to the internet. Integrity, Confidential and availability, be aspect needs to be maintained on those systems, three aspects are in the ERP system application (Enterprise, Resource, Planning) on private companies in general. Security issues in the system ERP of course corresponded to issues the base that must be filled a system security. So badly needed analysis in order to protect the data and do precautionary measures so that data not occurredin use .Hence required security management an appropriate information order to ensure the success of the implementation of a system security ERP. So we emphasises the use of method by using the method SQUARE.

Keyword : Integrity, Confidential, Availability, SQUARE, Network

I. PENDAHULUAN

Kemanan pada sebuah jaringan dan sistem informasi dibutuhkan untuk menjaga kemanan data. Integritas, kerahasiaan dan ketersediaan merupakan aspek-aspek yang harus dipenuhi untuk menjaga data tersebut, dengan melakukan analisis kebutuhan keamanan pada sebuah ERP dan jaringan merupakan upaya dari pencegahan agar data tidak disalah gunakan oleh orang yang tidak berkepentingan. *SQUARE* merupakan salah satu metode analisis kebutuhan kemanan sistem informasi yang dapat digunakan untuk menilai sebuah sistem informasi yang aman.

II. LANDASAN TEORI

A. DoS

DoS adalah serangan yang bertujuan untuk mematikan pelayanan dari *computer* atau jaringan yang diserang.[4]

B. DDoS

Merupakan *Dos* yang dilakukan secara terdistribusi atau berjamaah dalam jumlah besar.[5]

C. SQL Injection

SQL *Injection* merupakan penyerangan yang mengizinkan user tidak sah (penyerang) untuk mengakses database server atau memasukan (injeksi) *commands SQL* kedalam *query SQL* di program.[4]

D. ERP

ERP adalah sebuah sistem informasi perusahaan yang dirancang untuk mengkoordinasikan semua sumberdaya, informasi dan aktifitas yang diperlukan untuk proses bisnis lengkap. Sistem ERP didasarkan pada database pada umumnya dan rancangan perangkat lunak modular. ERP merupakan software yang mengintegrasikan semua departemen dan fungsi suatu perusahaan kedalam satu sistem yang dapat melayani semua kebutuhan perusahaan, baik dari departemen penjualan, HRD, produksi atau keuangan.[2]

E. Key Logger

Key Logger adalah aplikasi yang bisa merekam aktifitas pengguna komputer.[1]

F. Password Attack

Password Attack adalah usaha penerobosan suatu sistem jaringan dengan cara memperoleh password dari jaringan tersebut. Password merupakan sesuatu yang umum jika bicara tentang keamanan. Kadang seorang user tidak peduli dengan nomor pin yang mereka miliki, seperti bertransaksi online di warnet, bahkan online dirumahpun sangat berbahaya jika tidak dilengkapi dengan software security seperti SSL dan PGP.[3]

G. Dread

Dread Model ialah untuk menghitung resiko berdasarkan jenisnya, Tujuan dari DREAD model adalah menggambarkan area resiko bisnis yang di ketahui dengan kelangsungan dari sebuah penyerangan, penyerangan dari model ancaman dapat di katarogrikan sebagai berikut :

1. *Demage Potential* (Potensial kerusakan) : Bagaimana luas kerusakan dari terbukanya sebuah kerentanan apabila menjadi berhasil diekploitasi? Ini membantu untuk menentukan dampak keseluruhan dari penyerangan terhadapa kerentanan yang teridenfikasi jika berhasil diluncurkan.
2. *Reproductability* (Reproduksifitas): seberapa mudah jenis dari serangan untuk di reproduksi ? Ini membantu mengidentifikasi apakah serangan dapat diulang.
3. *Exploitability* (Ekploitas): Seberapa mudah kerentanan dikenal untuk dieksploitas? Faktor ini mambahas masalah pada tingkat keahlian atau sumberdaya yang dibutuhkan untuk mengekploitas sebuah kerentanan yang ditemukan.

4. *Affected User* (Efek Pengguna): Menjawab pertanyaan prediksi dampak pada basis pengguna melalui aset informasi mereka atau lingkungan aplikasi yang dimanfaatkan beberapa pengguna.
5. *Discoverability*: Ini membantu mengidentifikasi seberapa mudah sebuah kerentanan terdeteksi untuk lingkungan aplikasi tertentu. Informasi itu membantu mengidetifikasi seberapa mudah kerentanan dapat ditemukan untuk diekploitasi.

Seperti banyaknya sistem rating resiko yang lainnya, *DREAD* meliputi *HIGH*, *MEDIUM*, *LOW* deskriptor kualitatif resiko bersama dengan nilai resiko kuantitatif 3, 2, 1 yang diterapkan masing masing. Pada basis informasi model ancaman mungkin memiliki pada kedua kerentanan berpotensi dieksploitas dan sumberdaya dari penyerang, analisis yang sama dapat dilakukan untuk mempresentasikan sebuah penyerangan bercabang untuk semua tree model.[9]

III. METODE PENELITIAN

Metode yang digunakan untuk penlitian ini menggunakank pendekatan metode *SQUARE*, yang mana terdiri dari sembilan langkah dikembangkan untuk membantu menganalisis kebutuhan keamanan sistem sebagai berikut:

Gambar 1. Langkah-Langkah Metode *SQUARE*

Langkah 1: Persetujuan Definisi

Mendeskripsikan sistem informasi perusahaan yang akan dibangun dan mendefinisikan istilah-istilah keamanan informasi untuk sistem yang akan dianalisis yang disepakati di dalam perusahaan.

Langkah 2: Identifikasi *Goal*

Menganalisis tujuan dan persyaratan keamanan sistem yang diperlukan oleh perusahaan untuk memastikan keamanan secara keseluruhan sistem dan ketersediaan (availability) setiap saat.

Langkah 3: Pengembangan Artefak

Tahap ini diperlukan apa saja artefak yang mendukung terkait dalam proses perbaikan sistem *ERP* ini. Artefak akan diperoleh dari kondisi yang ada pada sistem saat ini diantaranya: arsitektur sistem terdapat pada perusahaan akan dikembangkan sebagai perbaikan sistem,use case, misusecase dan attack tree yang merupakan skenario dari sistem yang ada, kemudian dikembangkan sebagaiperbaikan sistem.

Langkah 4: Penilaian Resiko

Hal terpenting dalam penilaian resiko ini adalah menyediakan cara yang bermakna dalam mengkategorikan *Likelihood* (kemungkinan-kemungkinan yang terjadi) dan dampak dari ancaman utama dari sistem *ERP* ini.

Langkah 5: Pemilihan Teknik Elisitasi

Tahap ini akan dipilih satu atau lebih teknik elisitasi yang sesuai dengan perbaikan sistem. *SQUARE* memberikan contoh macam-macam teknik elisitasi, Namun proses pemilihan teknik juga disesuaikan terhadap lingkungan perusahaan dan juga dari jenis sistem yang akan dibangun. Sehingga tidak menutup kemungkinan menggunakan teknik elisitasi lain diluar dari contoh teknik yang telah diberikan.

Langkah 6 : Elisitasi Kebutuhan

Tahap Proses elisitasi pada penilitian ini menggunakan teknik yang telah dihasilkan melalui proses pemilihan yang dilakukan pada tahap sebelumnya. Elisitasi kebutuhan akan menyertakan hasil penilaian resiko dan artefak yang dikembangkan, sehingga nantinya stakeholder dapat mengetahui kebutuhan yang sebenarnya dari keamanan data mereka terkait dengan rencana perbaikan sistem ini.

Langkah 7: Pengkatagorian Kebutuhan

Tahap ini mengkategorikan semua kebutuhan sistem ERP dari stakeholder yang dihasilkan melalui proses elisitasi. Hasil elisitasi akan dikategorikan berdasarkan kebutuhan sistem dan kebutuhan pengguna.

Langkah 8: Pengkatagorian Kebutuhan

Tahap ini dilakukan langkah dalam memprioritaskan kebutuhan dari sistem. Pada langkah ini digunakan pendekatan metode Analytic Hierarcy Process (AHP) dalam memprioritaskan kebutuhan dari stakholder dengan membandingkan diantara masing-masing kebutuhan tersebut.

Langkah 9: Inspeksi Kebutuhan

Tahap ini merupakan langkah terakhir dari metodologi *SQUARE* dimana semua kebutuhan untuk ERP akan diperiksa apakah sesuai dengan kebutuhan dari stakeholder. Cheklist kebutuhan ERP akan disusun dan diberikan pada stakeholder untuk diverifikasi. Jika masih terdapat kebutuhan ERP yang tidak sesuai maka akan dilakukan perbaikan terhadap cheklist tersebut.

IV. PERSETUJUAN DEFINISI

Mendefinisikan istilah-istilah yang digunakan dalam menganlisis sistem informasi.

Tabel 1. Definisi

Beberapa definisi serangan pada sistem: a. *Denail of Service (DoS)*, jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber *(resource)* yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut. b. *Distributed DoS (DDoS)*, salah satu jenis serangan Denial of Service yang menggunakan banyak host penyerang (baik itu menggunakan komputer yang didedikasikan untuk melakukan penyerangan atau komputer yang "dipaksa" menjadi zombie) untuk menyerang satu buah host target dalam sebuah jaringan. c. Serangan Injeksi *SQL*, pada serangan ini objek yang diserang adalah halaman web yang menggunakan *Structured Query Language (SQL)* untuk melakukan *query* dan memanipulasi database. d. *Password Attack*, serangan untuk meng-*crack* sebuah *password*. e. *Keylogger*, *software* untuk men-*record* ketikan *keyboard*.

V. IDENTIFIKASI GOAL

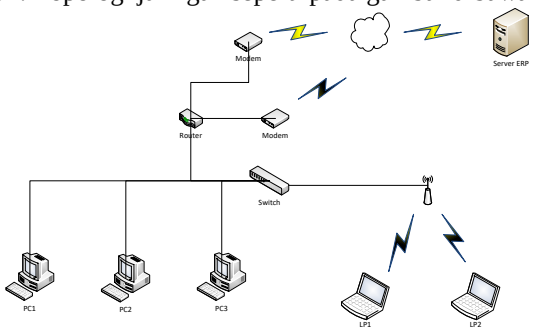
Menganalisatujuankemanandankeselamatan sistem informasi yang ada.

Table 2. Identifikasi Goal

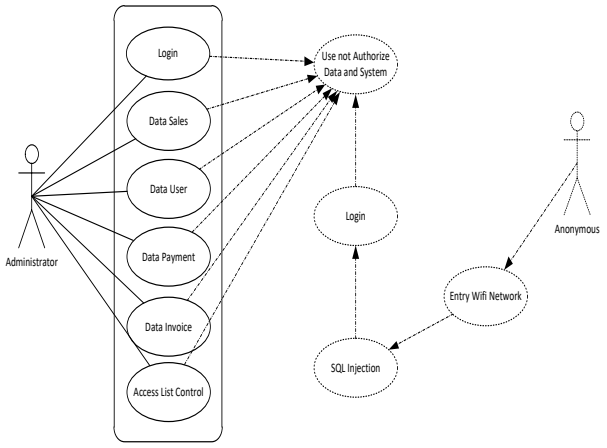
Tujuan:	a. Melakukan *control*konfigurasi sistem dan penggunaan. b. Menjamin Kerahasiaan, akurasi, dan integritas data *system*. c. Menjamin ketersediaan *system* jika diperlukan

VI. PENGEMBANGAN ARTEFAK

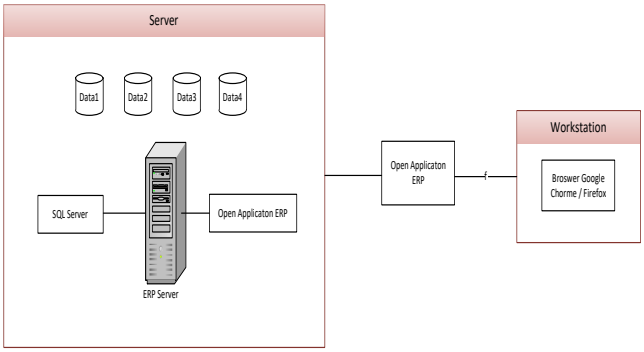
Pengembangan artefak didapatkan dari bagian-bagian sistem yang masih dapatdigunakan untuk perbaikan sistem yang mencakup arsitektur sistem,misusecase dan topologi jaringan. Topologi jaringan seperti pada gambar dibawah



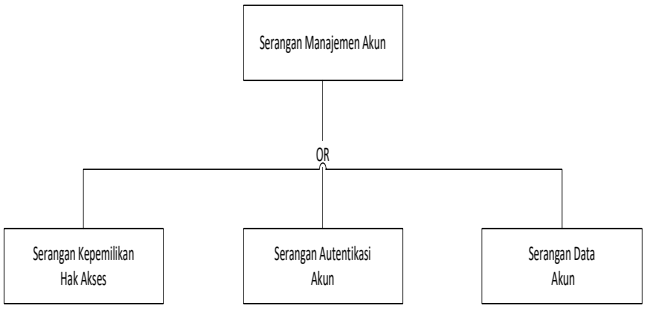
Gambar 2. Topologi Jaringan



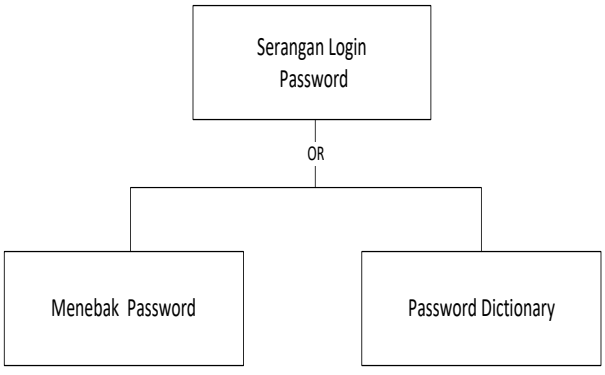
Gambar 3. *Misusecase*



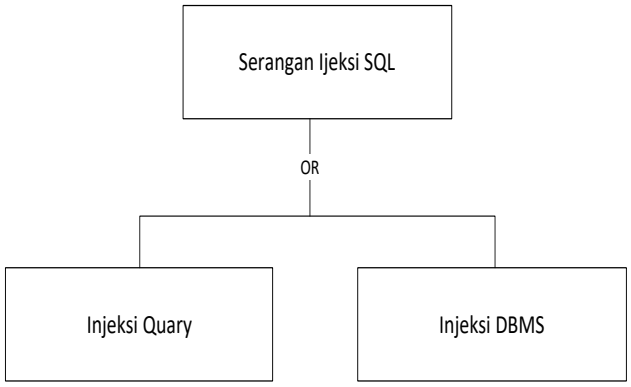
Gambar 4. Arsitektur Sistem



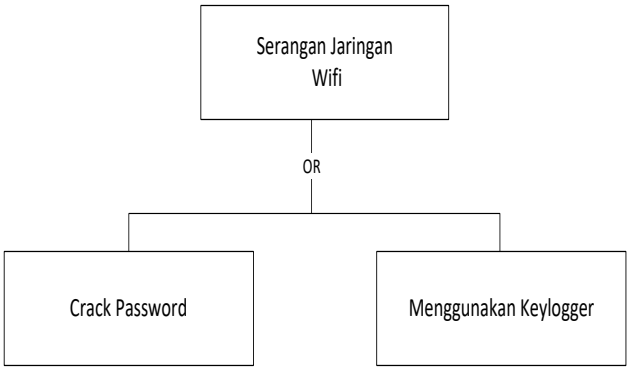
Gambar 6. *Attack Tree* Serangan Manajemen Akun



Gambar 7. *Attack Tree* Serangkan Login Password



Gambar 8. *Attack Tree SQL Ijection*



Gambar 9. *Attack Tree* Serangan Jaringan Wifi

VII. PENILAIAN RESIKO

Langkah-langkah penilaian resiko diantaranya : identifikasi ancaman, identifikasi kerentanan, analisis pengendalian, penentuan *likelihood*, analisis dampak, dan penentuan resiko. Hasil yang didapatkan dari proses penilaian resiko seperti pada

Tabel 3. Penilain Resiko

Kemungkinan	Level
MC-01 Serangan Manajemen Akun	*High*
MC-02 Serangan *Login* Password	*Mid*
MC-03 Serangan *SQL Injection*	*High*
MC-04 Serangan Jaringan*Wifi*	*High*

.

VIII. PEMILIHAN TEKNIK ELISITASI

Pemilihan elisitasi teknik yang dilakukan yaitu dengan melakukan interview, kuesioner dan observasi berkaitan dengan pendapat keamanan pada sistem *ERP*.

IX. ELISITASI KEBUTUHAN

Table 4. Elisitasi Kebutuhan

No	Kebutuhan	Keterangan
1	Rekomendasi Arsitektur (AR)	• Penggunaan *firewall* • Penggunaan *MAC Authentication* • Penggunaan *ACL* • Penggunaan Ekripsi pada *System* Informasi
2	Rekomendasi Kebijakan (PR)	• Penggunaan tanda tangan digital untuk sistem login • Penggunaan *password* yang kuat • Aplikasi harus di patch secara berkala • Penggantian *password* secara berkala

X. PRIORITAS KEBUTUHAN

Prioritas kebutuhan adalah menentukan skala prioritas dari setiap kebutuhan hasil elisitasi. Proses ini menggunakan metode statistikal untuk membandingkan antara kebutuhan yang satu dengan yang lain yaitu degan menggunakan *DREAD Modeling Threat*. Hasil dari langkah ini merupakan kebutuhan yang terprioritaskan seperti table dibawah ini.

Table 4. Prioritas Kebutuhan

Threat *Likelihood*	D	R	E	A	D	Total	*Avarage*	Prioritas
MC 01	3	2	2	3	2	12	2.4	2
MC 02	2	1	2	3	2	10	2	4
MC 03	3	3	3	3	2	14	2.8	1
MC 04	2	2	2	3	3	12	2.4	3

XI. INSPEKSI KEBUTUHAN

Inspeksi kebutuhan merupakan langkah terakhir dalam melakukan proses rekayasa kebutuhan yang menggunakan pendekatan petodologi *SQUARE*. Didalam proses inspeksi kebutuhan, hal terpenting adalah bagaimana hasil elisitasi kebutuhan sistem *ERP* yang telah terprioritaskan ini diperiksa kesesuaiannya terhadap kebutuhan stakeholder.

XII. KESIMPULAN

Kesimpulan dari penelitian ini adalah :

A. Dari hasil analisa rekayasa kebutuhan, perbaikan sistem yang melibatkan stakeholder sudah dapat memenuhi kebutuhan pengguna sehingga dapat digunakan sebagai acuan untuk merancang perbaikan sistem ini nantinya.

B. Melalui metode square ini, dapat diketahui bagian yang memiliki celah keamanan yang dapat dimasuki oleh pengguna berbahaya.

DAFTAR PUSTAKA

[1] https://blog.tibandung.com/apa-itu-keylogger/ (diakses pada 13-12-2015).

[2] https://killuazoldyck10.wordpress.com/2013/08/03/konsep-dasar-erp/ (diakses pada 13-12-2015).

[3] http://igdblogger.blogspot.co.id/2012/11/jenis-jenis-serangan-pada-jaringan.html (diakses pada 13-12-2015).

[4] Andi,2010,*Tutorial 5 hari : Belajar Hacking dari Nol*,Wahana Komputer, Bandung.

[5] Muzammi Sanusi,2010,*The Genius : Hacking untuk membobok Facebook dan email*, PT Elex Media Komputindo, Jakarta.

[6] Hadi Syahrial,2013, SIMANTIK, *Analisa Kebutuhan Keamanan Sistem Dengan Menggunakan Metode SQUARE :Studi Kasus Pengembangan Sistem Informasi Rumah Sakit Berbasis Open Source ERP (Open Sikes)*.

[7] Nauval Munif, Daniel O.Siahaan, Seminar Nasional Manajemen Teknologi XVI,2012,*Rekayasa Kebutuhan Untuk Perbaikan Sistem Disaster Recovery Plan Dengan Pendekatan Metodologi Security Quality Requirements Engineering (Square) (Studi Kasus : Data Enterprise Resource Planning Pada PT. CSA)*.

[8] M.Agreindra Helmiawan,*Keamanan E-Learning Menggunakan Metode SQUARE (Studi Kasus STMIK SUMEDANG)*.

[9] Tony Uceda Velez and Marco M.Morana, *RISK CENTRIC THREAT MODELING*, John Willey & Sons. Inc, 2015, New Jersey.