PENGEMBANGAN SISTEM MANAJEMEN KELEMAHAN KEAMANAN INFORMASI (SMKKI) MENGGUNAKAN LOTUS NOTES

Hadi Syahrial
Jurusan Teknik Informatika STMIK Antar Bangsa
E-mail: hadisyahrial@gmail.com

ABSTRAK

Penelitian ini bertujuan untuk mengembangkan sebuah prototipe sistem yang diberi nama Sistem Manajemen Kelemahan Keamanan Informasi (SMKKI) yang berbasis Lotus Notes dan yang disesuaikan dengan kebutuhan akan manajemen kelemahan keamanan informasi. Sistem ini nantinya dapat digunakan oleh petugas keamanan informasi (Information Security Officer) untuk menganalisa, mencatat dan mengirim notifikasi kepada staf departemen yang terkait dengan keamanan informasi seperti departemen Teknologi Informasi. Sistem ini juga dapat digunakan untuk memonitor status kelemahan keamanan informasi yang terdeteksi oleh alat pemindai kelemahan, sehingga dapat diketahui sudah berapa lama kelemahan-kelemahan tersebut terdapat pada sistem operasi maupun aplikasi. Dengan sistem ini diharapkan manajemen kelemahan keamanan informasi menjadi lebih efisien dan efektif.

Kata Kunci:Sistem Manajemen Kelemahan Keamanan Komputer, SMKKI, Manajemen keamanan informasi, resiko, kelemahan keamanan informasi, ancaman keamanan informasi, *CSIRT*, *CERT*, prototipe, Lotus Notes.

1. PENDAHULUAN

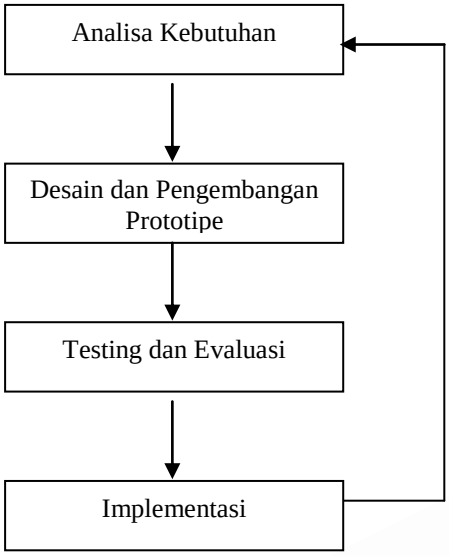
Dengan semakin tergantungnya institusi bisnis maupun nonbisnis terhadap pemanfaatan teknologi informasi, maka ancaman terhadap keamanan informasi juga tidak dapat dihindari, mulai dari ancaman yang paling umum seperti virus sampai ancaman berupa pencurian informasi rahasia dan lain-lain. Ancaman-ancaman ini bisa bersumber dari dalam maupun dari luar institusi. Ancaman-ancaman yang masih bersifat potensial ini setiap saat dapat berubah menjadi serangan dan insiden nyata bagi institusi apabila kelemahan-kelemahan keamanan yang terdapat pada sistem operasi dan aplikasi tidak segera diperbaiki.

Kenyataan ini mengharuskan pengguna teknologi informasi untuk siap menghadapi berbagai ancaman keamanan informasi. Bagaimana jika terdapat kelemahan pada sistem operasi dan aplikasi?, siapa yang bertanggung jawab menangani atau merespons?, bagaimana prosedur untuk melaporkan jika terdeteksi adanya kelemahan pada sistem operasi dan aplikasi?, kepada siapa kelemahan-kelemahan harus dilaporkan?, apa yang harus dilakukan untuk menindak lanjuti kelemahan-kelemahan ini? dan apa yang harus dilakukan agar kelemahan-kelemahan ini bisa diperbaiki segera?.

Pertanyaan yang menjadi rumusan masalah penelitian ini adalah bagaimana mengembangkan sebuah Sistem Manajemen Kelemahan Keamanan Informasi (SMKKI) yang dapat membantu seorang ISO dalam menganalisa, mencatat dan mengirim notifikasi kepada staf departemen yang terkait dengan keamanan informasi. Model yang digunakan dalam pengembangan sistem ini adalah model manajemen insiden keamanan informasi. Terdeteksinya sebuah kelemahan dianggap sebagai insiden keamanan informasi yang harus segera ditangani.

2. METODE PENELITIAN

Metode penelitian yang digunakan adalah metodei eksperimental yaitu dengan menggunakan model prototype dengan tahapan-tahapan sebagai berikut yaitu: tahap analisa kebutuhan, tahap desain dan pengembangan prototipe, tahap testing dan evaluasi, dan tahap implementasi.



Gambar 1 Tahapan penelitian

Tahapan-tahapan pengembangan SMKKI adalah:
1. Analisa Kebutuhan
2. Desain dan Pengembangan Prototype
3. Testing dan Evaluasi
4. Implementasi

2.1 Tahapan Analisa Kebutuhan

Pada saat ini SMKKI belum belum pernah dikembangkan di STMIK Antar Bangsa. Setiap terjadi insiden keamanan, langsung ditangani oleh bagian help desk. Sebagai tahap awal untuk memulai pengembangan SMKKI, akan dilakukan analisa yaitu analisa kebutuhan sistem. Tujuan dari analisa ini adalah untuk mengetahui kebutuhan SMKKI yang diinginkan agar dapat diaplikasikan dalam bentuk sebuah sistem.
Metodologi pengumpulan data dilakukan studi lapangan dengan mempelajari, mengamati, mendalami kebutuhan SMKKI yang akan dikembangkan dengan tidak mengabaikan kepatuhan (compliance) terhadap kebijakan-kebijakan dan kerangka yang berkaitan dengan manajemen keamanan informasi yang telah dibuat oleh pimpinan STMIK Antar Bangsa.

2.2. Tahapan Desain dan Pengembangan Prototipe

Tujuan dari desain prototipe SMKKI adalah untuk mendapat gambaran tentang SMKKI yang akan dikembangkan. Prototipe sistem informasi bukanlah merupakan sesuatu yang lengkap, tetapi sesuatu yang harus dimodifikasi kembali, dikembangkan, ditambahkan atau digabungkan dengan sistem informasi yang lain bila perlu.

2.3 Tahapan Testing dan Evaluasi

Sebelum sistem diimplementasi, perlu dilakukan pengujian dan evaluasi apakah sistem bekerja dengan baik dan sesuai dengan kebutuhan. Untuk menguji sistem, beberapa staf ditugaskan untuk melakukan uji coba terhadap semua fungsi-fungsi yang terdapat pada sistem.

Evaluasi sistem dilakukan untuk mengetahui kualitas sistem, apakah sistem sudah memenuhi kebutuhan sesuai dengan kebijakan dan kerangka manajemen tanggapan insiden keamanan informasi SMKKI.

2.4 Tahapan Implementasi

Setelah sistem diuji dan dievaluasi, maka sistem sudah siap untuk diimplementasi. Untuk mengimplementasi SMKKI beberapa hal yang perlu diperhatikan adalah kebutuhan perangkat keras, perangkat lunak dan jaringan STMIK Antar Bangsa.

3. HASIL PENELITIAN

3.1 Kebutuhan Prototype

Dari hasil analisa kebutuhan prototype, sebuah SMKKI harus memenuhi beberapa kriteria sebagai berikut:

- Kebijakan manajemen insiden
- Kerangka Manajemen Insiden Keamanan Informasi
- Keamanan sistem
- Perangkat keras
- Perangkat lunak
- Arsitektur jaringan STMIK Antar Bangsa

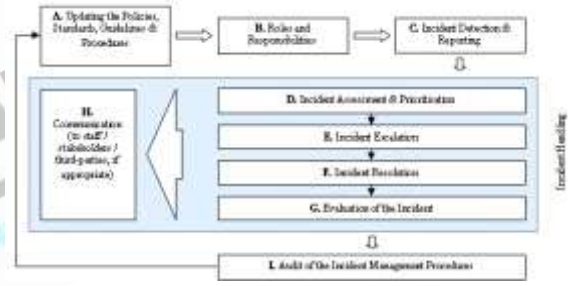
3.1.1 Kebijakan Manajemen Insiden

Beberapa kebijakan STMIK Antar Bangsa yang berhubungan dengan manajemen insiden keamanan informasi adalah sebagai berikut:

- STMIK Antar Bangsa harus mengembangkan dan menerapkan prosedur manajemen insiden keamanan.
- Semua staf harus dibuat sadar bagaimana caranya menemukenali pelanggaran keamanan dan kepada siapa harus melapor.
- Ketika pelanggaran keamanan terjadi, sistem yang terkena dampak harus diisolasi agar tidak memberi dampak pada yang lain. Sistem yang terkena dampak harus dilakukan investigasi.
- Pelanggaran keamanan yang berhubungan dengan keuangan harus dilakukan analisa forensik oleh seorang pakar investigasi forensik.
- Jika terjadi insiden keamanan yang berdampak pada STMIK Antar Bangsa, grup keamanan informasi harus segera diinformasikan.

3.1.2 Kerangka Manajemen Insiden Keamanan Informasi

Grup keamanan informasi STMIK Antar Bangsa telah mengembangkan suatu kerangka manajemen insiden keamanan informasi sebagai berikut:



Gambar 2 Kerangka Manajemen Insiden Keamanan Informasi

Kerangka manajemen insiden keamanan informasi terdiri dari:

A. *Updating the Policies, Standards, Guidelines and Procedures.*
B. *Roles and Responsinbilities*
C. *Incident Detection and Reporting.*
D. *Incident Assessment and Prioritisation.*
E. *Insident Escalation.*
F. *Insident Resolution.*
G. *Evaluation of the Incident.*
H. *Communication (to staff / stakeholders / third-parties, if appropriate).*
I. *Audit of the Incident Management Procedures.*

3.1.3 Kebutuhan Perangkat Keras dan Perangkat Lunak Sistem

SMKKI yang akan dikembangkan di STMIK Antar Bangsa menggunakan Lotus Notes. Lotus Notes adalah sistem aplikasi *groupware* berorientasi dokumen yang terdistribusi. Setiap aplikasi Lotus Notes terdiri dari

paling sedikit satu database. Setiap database Notes mempunyai beberapa komponen dasar, yaitu dokumen, *form* dan *field*, serta *views* dan *folders*. Setiap aplikasi Lotus Notes menggunakan paling sedikit satu database.

3.1.4 Kebutuhan Keamanan dan Jaringan

SMKKI yang dikembangkan harus memenuhi beberapa kebutuhan keamanan sebagai berikut:

- Password minimal delapan karakter terdiri dari alphanumeric.
- Password hanya berlaku 90 hari.
- Kontrol akses diberikan sesuai dengan peran dan tanggung jawab pengguna sistem.
- Sistem harus bisa diakses secara *remote.*

3.2 Desain Prototype SMKKI

Untuk memulai membangun aplikasi menggunakan Lotus Notes digunakan program Lotus Notes Designer.

Gambar 3 Lotus Notes Designer

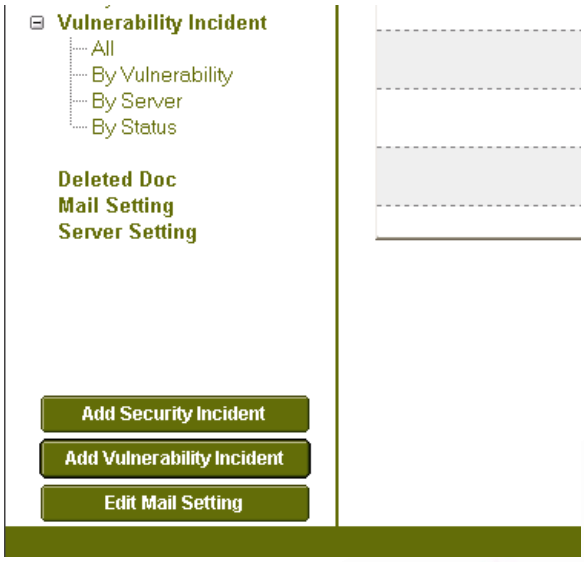
Dari Lotus Notes Designer ini kemudian di buat formulir seperti gambar-gambar di bawah ini:

Gambar 4 Formulir Lotus Notes

Prototipe sistem manajemen tanggapan insiden keamanan komputer yang dikembangkan menggunakan perangkat lunak aplikasi Lotus Notes memiliki tampilan seperti di bawah ini:

Gambar 5 Tampilan SMKKI

Untuk membuat sebuah laporan kelemahan, telah dibuatkan sebuah tombol *"add vulnerability"* seperti gambar di bawah ini:



Gambar 6 Tombol *"add vulnerability"*

Jika tombol *"add vulnerability"* diklik maka akan muncul tampilan berupa formulir tentang deskripsi kelemahan.

Gambar 7 Deskripsi Kelemahan

3.3 Testing dan Evaluasi Prototype

3.3 Hasil Testing dan Evaluasi

Testing terhadap SMKKI dilakukan berdasarkan fungsi-fungsi yang terdapat pada sistem. Dari hasil testing dan evaluasi prototipe SMKKI, semua fungsi yang tersedia dapat berjalan dengan baik dan normal.

3.4 Implementasi SMKKI

Untuk implementasi sistem perlu didukung oleh perangkat keras dan perangkat lunak dengan spesifikasi tertentu dan prosedur untuk menginstalasi sistem agar siap digunakan.

3.4.1 Dukungan Perangkat Keras dan Lunak

Untuk implementasi SMKKI menggunakan server dan client dengan spesifikasi sebagai berikut:

Untuk Server:
Spesifikasi Perangkat keras:
- Memori 4 GB RAM
- Hard disk 500 GB
- Processor Pentium 4 Dual Core 2.8 GHz

Spesifikasi Perangkat Lunak:
- Sistem Operasi Windows Server 2003
- Lotus Notes Domino 7.1

Untuk Client:
Spesifikasi perangkat keras:
- Memori 2 GB
- Hard disk 40 GB
- Processor Pentium 1,6 GHz

Spesifikasi perangkat lunak
- Sistem Operasi Windows XP
- Lotus Notes Client 7.0.2

3.4.2 Instalasi

Instalasi sistem dilakukan dengan mengcopy sistem dari lingkungan testing ke lingkungan produksi dengan terlebih dahulu melakukan review terhadap manajemen perubahan. Setelah selesai dilakukan review terhadap manajemen perubahan, baru kemudian sistem siap untuk dicopy ke server Lotus Notes dan siap diakses oleh staf ISO STMIK Antar Bangsa melalui *laptop*.

3.5 Implikasi Penelitian

Dari hasil penelitian ini terdapat beberapa implikasi yaitu implikasi manajerial, sistem, lanjutan dan regulasi.

3.5.1 Implikasi manajerial

Implikasi manajerial pengembangan SMKKI pada STMIK Antar Bangsa adalah pertama jika terdeteksi suatu kelemahan keamanan informasi dapat ditangani lebih cepat sehingga dapat memperkecil dampak kelemahan tersebut pada kelangsungan bisnis.

Kedua adalah dengan SMKKI sebagai basis data yang mencatat semua kelemahan-kelemahan keamanan informasi maka dapat diketahui sudah berapa lama kelemahan terdapat pada sistem operasi atau aplikasi sehingga dapat dilakukan tindakan-tindakan perbaikan agar tidak terjadi insiden keamanan di kemudian hari.

Yang ketiga adalah untuk mengembangkan SMKKI perlu mempertimbangkan kebijakan-kebijakan yang dikembangkan oleh departemen-departemen lain di luar departemen teknologi informasi yang terkait dengan keamanan informasi STMIK Antar Bangsa seperti departemen sumber daya manusia, keuangan dan lain-lain.

Yang keempat adalah dengan mengembangkan SMKKI penanganan kelemahan keamanan menjadi lebih mudah karena untuk setiap kelemahan dicatat cara penyelesaiannya.

3.5.2 Implikasi sistem

Sistem Manajemen Tanggapan Insiden Kemanan Komputer yang dikembangkan di STMIK Antar Bangsa menggunakan Lotus Notes yaitu sebuah aplikasi *groupware* yang memiliki kemampuan untuk melakukan kolaborasi sesama pengguna. Sehingga beberapa pengguna dapat mengerjakan suatu proyek yang sama secara bersama-sama.

Lotus Notes adalah sejenis aplikasi *client-server* dimana aplikasi-aplikasi yang dikembangkan disimpan di server dan dapat diakses oleh *client* melalui jaringan. Perangkat lunak yang diinstal di server dinamakan Lotus Notes Domino, dan yang diinstal di *client* dinamakan Lotus Notes Client.

Karena SMKKI diakses melalui client menggunakan jaringan, maka jaringan harus selalu dimonitor agar tidak terjadi kemacetan lalu lintas paket data. Disamping itu juga kesehatan server perlu dimonitor seperti kapasitas *hard disk*, penggunaan *processor* dan *Random Access Memory*. Pemonitoran server ini dilakukan untuk mencegah penggunaan *hard disk* dan *memory* yang melampaui kapasitas yang tersedia.

3.5.3 Implikasi lanjutan

Karena manajemen tanggapan insiden keamanan informasi merupakan suatu proses, maka untuk kelanjutan pengembangan SMKKI di STMIK Antar Bangsa perlu menerapkan sistem flow yang sesuai dengan proses manajemen tanggapan insiden kemananan informasi yaitu:

- Persiapan.
- Melindungi infrastruktur.
- Mendeteksi kejadian-kejadian.
- *Triage* kejadian-kejadian.
- Tanggapan

3.5.4 Implikasi Regulasi

Dengan telah diterbitkannya Undang-Undang Informasi dan Transaksi Elektronik (ITE) Republik Indonesia, yang mana setiap penyelenggara sistem elektronik harus menyelenggarakan sistem elektronik secara andal dan aman, maka SMKKI merupakan salah satu alat bantu yang dapat mendukung agar manajemen kelemahan keamanan dapat dikelola dengan lebih proaktif sehingga insiden keamanan dapat dicegah.

4. PENUTUP

4.1 Kesimpulan

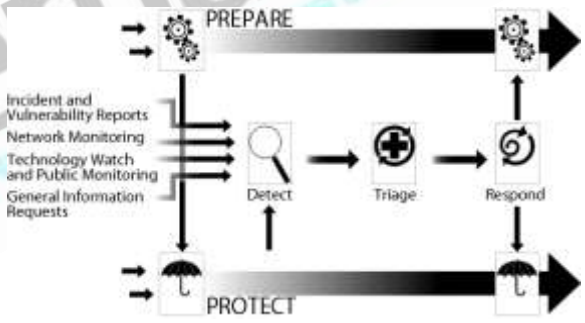
Berdasarkan hasil penelitian dapat disusun kesimpulan sebagai berikut:

1. Dengan menggunakan model pendekatan perangkat lunak prototyping, pengembangan SMKKI berbasiskan Lotus Notes telah dapat digunakan oleh staf ISO di STMIK Antar Bangsa.
2. SMKKI sangat membantu dalam mencegah terjadinya insiden yang sama terulang kembali.

4.2 Saran-Saran

Dari hasil penelitian, penulis dapat memberikan saran-saran untuk pengembangan lebih lanjut SMKKI sebagai berikut:

1. Sistem akan lebih baik kalau menerapkan aliran proses tanggapan insiden keamanan seperti gambar di bawah ini:



Gambar V.1 Proses dasar manajemen insiden ([ALB2004], 18)

2. Evaluasi kualitas sistem akan lebih baik jika menggunakan analisa statistik.

DAFTAR PUSTAKA

[AUN2008] Aunur R. Mulayanto, *Rekayasa Perangkat Lunak JILID 1*, Direktorat Pembinaan Sekolah Menengah Kejuruan, 2008

[ALB2004] Alberts, Chris, et.al., *Defining Incident Management Processes for CSIRTs: A Work in Progress,* CMU/SEI, 2004

[BAC2008] Bacik, Sandi, *Building an Effective Information Security Policy Architecture*, Auerbach Publication, 2008

[CAL2005] Calder, Alan, *A Business Guide to Information Security*, Kogan Page, 2005

[HAR2008] Harris, Shon, *CISSP All-in-One Exam Guide, Fourth Edition*, McGraw-Hill 2008

[ISF2006] Information Security Forum, *Establishing an Information Security Incident Management Capability*, ISF 2006

[KIL2003] Killcrece, Georgia, et.al., *Organizational Models for Computer Security Incident Response Teams (CSIRTs)*, CMU/SEI, 2003

[KIL2006] Killmeyer, Jann, *Information Security Architecture 2nd Edition*, Auerbach Publication, 2006

[PFL2001] Pfleeger, Shari Lawrence, *Software Engineering Theory and Practicing, Second Edition*, Prentice Hall, 2001

[RIT2005] Rittinghouse, John W. and James F. Ransome, *Business Continuity and Disaster Recovery for Infosec Managers*, Elsevier Digital Press, 2005

[SCH2003] chweitzer, Douglas, *Incident Response: Computer Forensics Toolkit*, Wiley Publishing, Inc, 2003

[SOE2008] Soetam Rizky, *Disaster Recovery Planning, Prestasi Pustaka*, 2008

[WES2003] West-Brown, Moira J., et.al., *Handbook for Computer Security Incident Response Teams (CSIRTs) 2nd Edition*, CMU/SEI, 2003

[WIK2009] Wikipedia, *Enterprise Information Security Architecture*, http://en.wikipedia.org/wiki/Enterprise_Information_Security_Architecture, Diakses 23 Maret 2009.

[WYK2001] Wyk, Van and Richard Forno, *Incident Response*, O'Reilly, 2001