PENGEMBANGAN SISTEM MANAJEMEN TANGGAPAN INSIDEN KEAMANAN KOMPUTER (CSIRMS) STUDI KASUS KANTOR AKUNTAN PUBLIK.

Hadi Syahrial

Program Studi Magister Ilmu Komputer
Program Pascasarjana Teknologi Informasi, Universitas Budi Luhur

hadisyahrial@gmail.com

ABSTRAK

Penelitian ini bertujuan untuk mengembangkan sebuah sistem yang diberi nama Sistem Manajemen Tanggapan Insiden Keamanan Komputer (CSIRMS) yang berbasis Lotus Notes dan yang disesuaikan dengan kebutuhan Kantor Akuntan Publik. Sistem ini nantinya dapat digunakan oleh semua staf Kantor Akuntan Publik untuk melaporkan jika terjadi suatu insiden keamanan informasi. Sistem ini juga dapat digunakan oleh Information Security Officer untuk menganalisa insiden keamanan informasi. Sistem ini dikembangkan dengan menggunakan pendekatan prototyping.

.

Kata Kunci *: **Sistem Manajemen Tanggapan Insiden Keamanan Komputer, CSIRMS, Manajemen keamanan informasi, vulnerability, threats, ancaman keamanan informasi, CSIRT, prototype, 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.

Kenyataan ini mengharuskan pengguna teknologi informasi untuk siap menghadapi berbagai ancaman keamanan informasi ini. Bagaimana jika terjadi insiden terhadap keamanan informasi, siapa yang bertanggung jawab menangani atau merespons, bagaimana prosedur untuk melaporkan jika terjadi insiden, kepada siapa insiden harus dilaporkan, apa yang harus dilakukan untuk menindak lanjuti insiden ini dan apa yang harus dilakukan agar insiden ini tidak terulang kembali di masa depan?

Pertanyaan yang menjadi rumusan masalah penelitian ini adalah bagaimana mengembangkan sebuah Computer Security Incident Response Management System (CSIRMS) yang dapat membantu melindungi kerahasian dan keutuhan informasi dan juga menjaga ketersediaan informasi pada saat informasi dibutuhkan dan menjawab pertanyaan-pertanyaan di atas.

2. Landasan Teori

Informasi adalah salah satu aset institusi bisnis dan non bisnis yang sangat berharga. Kehilangan informasi rahasia dapat menyebabkan rusaknya reputasi dan kerugian finansial yang besar. Oleh karena itu saat ini keamanan informasi merupakan kebutuhan bisnis perusahaan dari sekedar untuk memberikan jaminan atas terkelolanya risiko bisnis sampai dengan penciptaan keunggulan bersaing bagi perusahaan.

Menurut Alan Calder ([CAL2005], 11) dalam bukunya A Business Guide to

Information Security disebutkan *"Information Security is, according to the internationally recoqnized code of information security best practices, ISO 17799:2005, the preservation of the confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also can be involved"*.

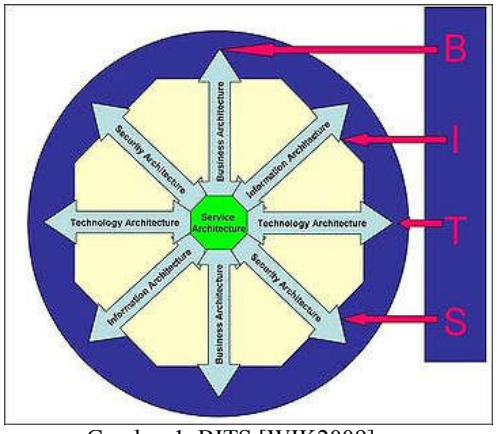
Keamanan informasi adalah, menurut praktek-praktek terbaik dalam bidang keamanan informasi yang sudah dikenal secara internasional yaitu ISO 17799:2005, perlindungan terhadap kerahasiaan, keutuhan dan ketersediaan informasi, hal lain yang dapat ditambahkan seperti keaslian, pertanggung jawaban, tidak dapat disangkal dan kepercayaan.

Aspek kepatuhan terhadap regulasi dan perundang-undangan *(regulatory compliance)* juga merupakan pendorong bagi perusahaan khususnya perusahaan-perusahaan terbuka untuk dapat memastikan kepada para pemilik saham bahwa seluruh transaksi dan informasi bisnis terjamin kerahasiaannya.

Oleh sebab itu pendekatan pengelolaan keamanan informasi harus terintegrasi dan sejalan dengan manajemen dan tujuan institusi. Pendekatan arsitektural dalam mengelola keamanan informasi yang terintegrasi dalam *Enterprise Architecture* (EA) merupakan metoda untuk memastikan terpenuhinya tujuan institusi.

EA adalah satu gambaran dari struktur dan perilaku dari proses, sistem informasi, personel, dan unit-unit dalam satu organisasi, yang diselaraskan dengan tujuan dan arah strategis dari organisasi tersebut.

Arsitektur Keamanan Informasi (AKI) atau sering disebut juga sebagai *Enterprise Information Security Architecture* (EISA) menurut wikipedia [WIK2009] saat ini sudah merupakan bagian dari EA. Menurut wikipedia, secara formal *Enterprise Information Security Architecture* pertama kali diposisikan sebagai bagian dari EA oleh Gartner dengan menerbitkan whitepaper yang berjudul *"Integrating Security into the Enterprise Architecture Framework"* pada 25 Januari 2006.



Gambar 1. BITS [WIK2009]

Dengan diintegrasikannya *Security Architecture* ke dalam EA *framework* maka EA yang umumnya terdiri dari *Business Architecture, Information Architecture,* dan *Technology Architecture* atau disingkat BIT, sekarang menjadi BITS.

Arsitektur-arsitektur lain yang dapat diintegrasikan ke dalam EA *framework* adalah *Application Architecture*, *Integration Architecture*, *Governance Architecture*, *Organisation Architecture* dan lain-lain.

Menurut Jann Killmeyer ([KIL2006], xiv) komponen dari Arsitektur Keamanan Informasi adalah sebagai berikut:

1. Pengorganisasian keamanan/infrastruktur.
2. Kebijakan, standar, prosedur keamanan.
3. Baselines keamanan/penilaian risiko.
4. Program pelatihan dan kesadaran keamanan.
5. Kepatuhan (compliance).
6. Pendeteksian dan monitoring.
7. Tanggapan emergensi dan insiden computer.
8. Rencana kelanjutan bisnis/pemulihan bencana.

Delapan komponen arsitektur keamanan informasi menurut Jann Killmeyer di atas dapat dijadikan acuan dalam mengelola keamanan informasi di suatu institusi. Masih banyak acuan lain yang dapat digunakan dalam mengelola keamanan informasi, diantaranya adalah ISO 27001 *(Information Security Management System)*, ISO 27002, ISO 15408 *(Common Criteria),* COBIT, NIST, *Sherwood Applied Business Security Architecture* (SABSA) dan lain-lain.

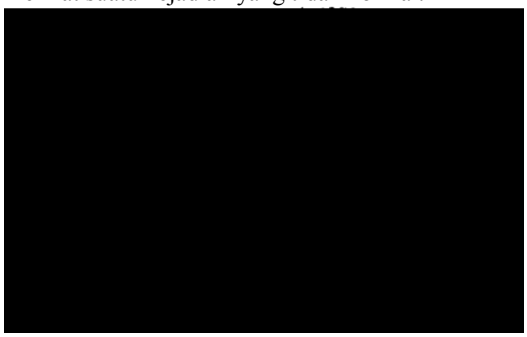
Untuk mengurangi dampak yang disebabkan oleh insiden keamanan informasi, institusi perlu memiliki kemampuan mengelola insiden keamanan informasi secara cepat dan efektif.

Yang dimaksud dengan insiden menurut Van Wyk ([WYK2001], 7) *"An incident is a situation in which an entity's information is at risk, whether the situation is real or simply perceived"*. Sebuah insiden adalah situasi dimana suatu informasi dalam risiko, baik situasinya nyata atau cuma dirasakan. Menurut Douglas Schweitzer ([SCH2003], xx) insiden adalah *"In information technology, incident refers to an adverse event in an information system and/or network or the threat of the occurrence of such an event"*. Dalam teknologi informasi, insiden berhubungan dengan suatu kejadian yang merugikan dalam sistem informasi dan atau jaringan atau ancaman yang menjadi suatu kejadian.

Yang dimaksudkan dengan manajemen insiden menurut Chris Alberts ([ALB2004], 3) *"The term 'incident management' expands the scope of this work to include the other services and functions that may be performed by CSIRTs, including vulnerability handling, artifact handling, security awareness training, and the other services outlined in the CSIRT Services list. The definition of this term to include behavior when they see this expanded set of services is important because incident management is not just responding to an incident when it hap-pens. It also includes proactive activities that help prevent incidents by providing guidance against potential risks and threats, for example, identifying vulnerabilities in software that can be addressed before they are exploited. These proactive actions include training end users to understand the importance of computer security in their daily operations and to define what constitutes abnormal or malicious behavior, so that end users can identify and report this it."*

Selain penanganan insiden, layanan (*service*) lain yang bisa diberikan oleh CSIRT seperti penanganan kelemahan (*vulnerability*), penanganan artifak (*artifact*), pelatihan kesadaran informasi dan layanan lain yang ada dalam daftar CSIRT (lihat tabel I.1) termasuk dalam manajemen insiden.

Manajemen insiden tidak hanya merespon jika terjadi insiden tapi juga melakukan tindakan-tindakan proaktif untuk mencegah terjadinya insiden seperti menemukenali kelemahan-kelemahan pada perangkat lunak dan segera memperbaikinya sebelum kelemahan-kelemahan itu di eksploitasi. Yang juga termasuk tindakan proaktif adalah memberikan pelatihan kepada pengguna teknologi informasi agar mereka mampu menemukenali dan melaporkan jika melihat suatu kejadian yang tidak normal.



Gambar 2. Hubungan manajemen insiden, penanganan insiden dan tanggap insiden ([ALB2004], 3).

Gambar 2 di atas menjelaskan hubungan antara manajemen insiden (*incident management*), penanganan insiden (*incident handling*) dan tanggap insiden (*incident response*). Tanggap insiden merupakan salah satu fungsi dari penanganan insiden dan penanganan insiden merupakan salah satu layanan dari manajemen insiden.

Untuk melakukan manajemen insiden di sebuah institusi atau organisasi perlu dibentuk suatu tim atau organisasi. Menurut Georgia Killcrece ([KIL2003], 1) tim ini secara umum disebut Computer Security Incident Response Team (CSIRT).

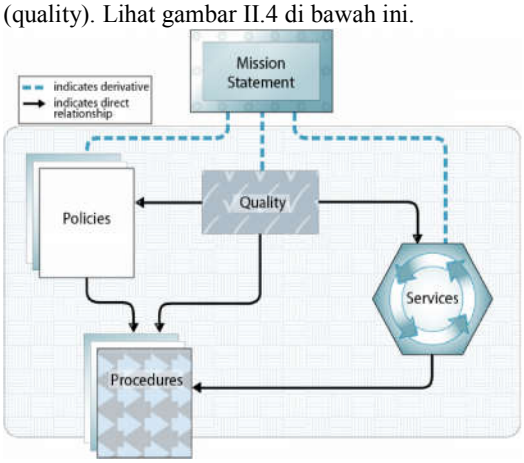
Menurut Georgia Killcrece ([KIL2003], 1) *"A CSIRT provides a single point of contact for reporting computer security incidents and problems. This enables the team to serve as a repository for incident information, a center for incident analysis, and a coordinator of incident response across an organization"*.

CSIRT menyediakan seseorang yang bisa dihubungi (single point of contact) untuk melaporkan jika terjadi insiden-insiden keamanan komputer dan masalah-masalah. Ini memungkinkan tim memberikan layanan sebagai tempat penyimpanan informasi, pusat analisa insiden dan koordinator tanggap insiden dalam organisasi.

Dalam mengimplementasi CSIRT, memiliki misi dan menentukan jenis layanan yang akan diberikan seperti layanan reaktif, proaktif atau manajemen kualitas keamanan (lihat tabel I.1) adalah sangat penting. Menurut Georgia Killcrece ([KIL2003], 13)

"The CSIRT mission should provide a brief, unambiguous description of the basic purpose and function of the CSIRT". Misi CSIRT sebaiknya dibuat singkat dan jelas menggambarkan fungsi dan tujuan dibentuknya CSIRT.

Menurut Moira J.West-Brown ([WES2003], 25) pernyataan misi (mission statement) memiliki tiga turunan (derivative) yaitu pelayanan (services), kebijakan (policy) dan kualitas (quality). Lihat gambar II.4 di bawah ini.

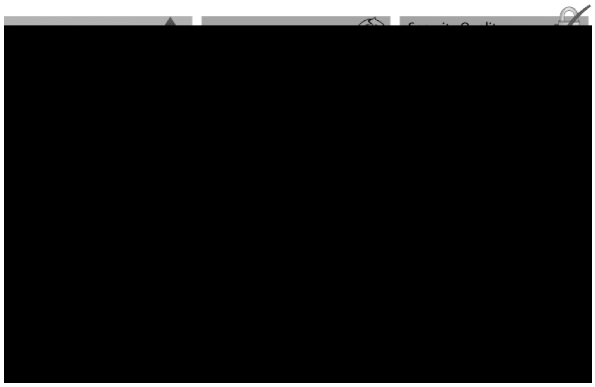


Gambar 3. Kualitas, kebijakan dan layanan-layanan diturunkan dari pernyataan misi ([WES2003], 25).

Layanan atau jasa yang dapat diberikan oleh CSIRT menurut Moira J. West-Brown ([WES2003], 25) dapat dikategorikan menjadi tiga kelompok, yaitu:

- Layanan-layanan reaktif (Reactive Services).
- Layanan-layanan proaktif (Proactive Service).
- Layanan-layanan manajemen kualitas keamanan (Security Quality Management Services).

Untuk lebih jelasnya pengelompokan tersebut di atas bisa lihat pada tabel di bawah ini:



Tabel 1. Daftar layanan-layanan CSIRT ([ALB2004], 4)

Yang dimaksud layanan reaktif menurut Georgia Killcrece ([KIL2003], 14) *"These services are triggered by an event or request, such as a report of a compromised host, wide-spreading malicious code, software vulnerability, or something that was identified by an intrusion detection or logging system. Reactive services are the core component of CSIRT work"*.

Layanan-layanan ini dipicu oleh kejadian atau permintaan seperti laporan tentang server yang sudah di*hack*, penyebaran program yang membahayakan, kelemahan perangkat lunak atau sesuatu yang ditemukenali oleh sistem logging dan alat pendeteksian penyusupan (intrusion detection).

Layanan reaktif terdiri dari tanda siaga dan peringatan (alerts and warnings), penanganan insiden (incident handling), penanganan kelemahan (vulnerability handling) dan penanganan artifak (artifact handling).

Menurut Georgia Killcrece ([KIL2003], 16) *"This service involves disseminating information that describes an intruder attack, security vulnerability, intrusion alert, computer virus, or hoax, and providing any short-term recommended course of action for dealing with the resulting problem. The alert, warning, or advisory is sent as a reaction to the current problem to notify constituents of the activity and to provide guidance for protecting their systems or recovering any systems that were affected. Information may be created by the CSIRT or may be redistributed from vendors, other CSIRTs or security experts, or other parts of the constituency"*.

Layanan Tanda Siaga dan Peringatan adalah layanan yang berfungsi untuk menyebarkan informasi jika terjadi serangan penyusup (intruder attack), kelemahan keamanan (security vulnerability), tanda siaga penyusupan (intrusion alert), virus komputer atau *hoax* dan memberikan rekomendasi jangka pendek untuk hal-hal yang perlu dilakukan dalam menghadapi suatu masalah yang muncul. Tanda siaga, peringatan atau laporan dikirim kepada konstituen tim yang melakukan aktivitas sebagai sebuah reaksi terhadap suatu masalah dalam rangka untuk memberikan petunjuk bagaimana melindungi sistem mereka dan untuk memulihkan sistem yang sudah terkena insiden.

Menurut Georgia Killcrece ([KIL2003], 16) "*Incident handling involves receiving, triaging, and responding to requests and reports, and analyzing incidents and events. Particular response activities can include:*

a. *taking action to protect systems and networks affected or threatened by intruder activity*
b. *providing solutions and mitigation strategies from relevant advisories or alerts*
c. *looking for intruder activity on other parts of the network*
d. *filtering network traffic*
e. *rebuilding systems*
f. *patching or repairing systems*
g. *developing other response or workaround strategies"*

Penanganan insiden melibatkan penerimaan (receiving), *triaging* dan penanggapan (responding) terhadap permintaan dan laporan, dan penganalisaan insiden dan kejadian (analyzing incidents and events). Secara khusus, aktivitas tanggapan (response) diantaranya adalah:

a. bertindak untuk melindungi sistem dan jaringan (network) yang terkena insiden dan dari ancaman kegiatan-kegiatan penyusup.
b. memberikan solusi dan strategi mitigasi dari nasehat-nasehat (advisories) atau tanda siaga (alerts).
c. mencari aktivitas penyusup pada bagian lain dari jaringan.
d. menyaring (filtering) lalulintas jaringan.
e. membangun kembali sistem-sistem.
f. menginstall patch (patching) atau memperbaiki sistem.
g. membangun tanggapan lain atau strategi *workaround.*

Menurut Georgia Killcrece ([KIL2003], 18) *"Vulnerability handling involves receiving information and reports about hardware and soft-ware vulnerabilities, analyzing the nature, mechanics, and effects of the vulnerabilities, and developing response strategies for detecting and repairing the vulnerabilities".*

Penanganan kelemahan melibatkan penerimaan informasi dan laporan-laporan tentang kelemahan-kelemahan pada perangkat keras dan lunak, menganalisa efek-efek, mekanik dan sifat dari kelemahan-kelemahan tersebut dan mengembangkan strategi tanggapan untuk mendeteksi dan memperbaiki kelemahan-kelemahan tersebut.

Menurut Georgia Killcrece ([KIL2003], 16) *"An artifact is any file or object found on a system that might be involved in probing or attacking systems and networks or that is being used to defeat security measures. Artifacts can include but are not limited to computer viruses, Trojan horse programs, worms, exploit scripts, and toolkits. Artifact handling involves receiving information about and copies of artifacts that are used in intruder attacks, reconnaissance, and other unauthorized or disruptive activities. Once received, the artifact is reviewed. This includes analyzing the nature, mechanics, version, and use of the artifacts; and developing (or suggesting) response strategies for detecting, removing, and defending against these artifacts".*

Sebuah artifak adalah obyek atau file pada sebuah sistem yang mungkin terlibat dalam penyerangan sistem dan jaringan atau sedang digunakan untuk mengalahkan pertahanan keamanan. Artifak bisa berupa virus*, Trojan horses, worms, exploit scripts,* dan alat-alat bantu (toolkits). Penanganan artifak melibatkan penerimaan informasi tentang atau salinan-salinan artifak yang digunakan dalam penyerangan oleh penyusup, pengintaian dan aktivitas-aktivitas tidak sah (unauthorized) yang merusak. Setelah informasi diterima selanjutnya artifak di periksa dengan menganalisa sifat-sifat, versi, mekanik dan penggunaannya dan mengembangkan strategi untuk mendeteksi, membersihkan dan menangkal artifak-artifak.

Yang dimaksud layanan proaktif menurut Georgia Killcrece ([KIL2003], 14) *"These services provide assistance and information to help prepare, protect, and*

secure constituent systems in anticipation of attacks, problems, or events. Performance of these services will directly reduce the number of incidents in the future".

Layanan-layanan ini menyediakan bantuan dan informasi untuk membantu mempersiapkan, melindungi dan mengamankan sistem-sistem konstituen dalam rangka mengantisipasi serangan-serangan, masalah-masalah atau kejadian-kejadian. Unjuk kerja layanan ini akan dilihat secara langsung dari berkurangnya jumlah insiden-insiden di masa datang.

Yang dimaksud layanan manajemen kualitas keamanan informasi menurut Georgia Killcrece ([KIL2003], 19) *"These services augment existing and well-established services that are independent of incident handling and traditionally performed by other areas of an organization such as the IT, audit, or training departments. If the CSIRT performs or assists with these services, the CSIRT's point of view and expertise can provide insight to help improve the overall security of the organization and identify risks, threats, and system weaknesses. These services are generally proactive but contribute indirectly to reducing the number of incidents"*.

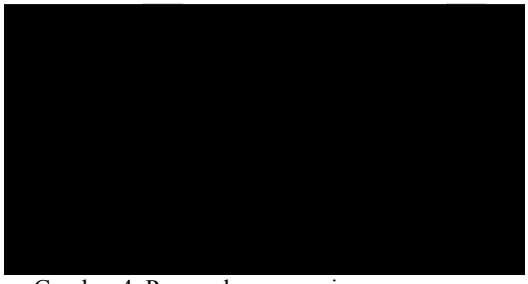
Layanan ini memperluas layanan-layanan yang sudah ada saat ini dan layanan-layanan yang sudah berjalan dengan baik dan sudah independen dalam penanganan insiden, yang secara tradisional dilakukan oleh departemen lain dalam suatu organisasi seperti teknologi informasi, audit atau departemen pelatihan.

Jika CSIRT melakukan layanan ini, keahlian yang dimiliki CSIRT dapat membantu meningkatkan keamanan organisasi secara keseluruhan dan dalam hal menemukenali risiko-risiko, ancaman-ancaman dan kelemahan-kelemahan sistem. Layanan-layanan ini secara umum bersifat proaktif, tetapi secara tidak langsung berkontribusi dalam mengurangi insiden.

Menurut Chris Alberts ([ALB2004], 10), manajeman insiden memiliki lima proses dasar yaitu:

a. Persiapan.
b. Melindungi infrastruktur.
c. Mendeteksi kejadian-kejadian.
d. Triage kejadian-kejadian.
e. Tanggapan

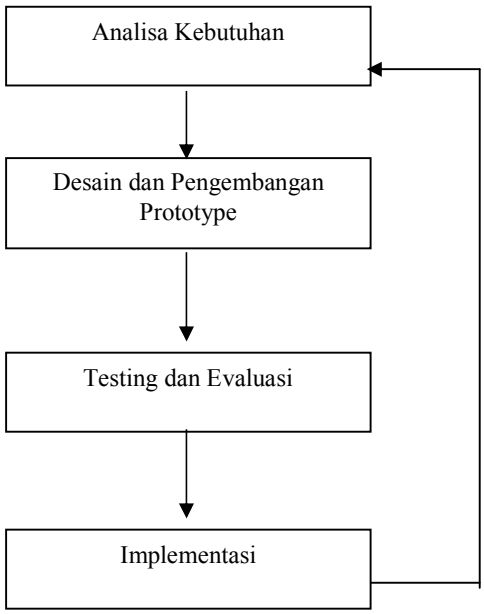
Gambar berikut ini mengilustrasikan proses manajemen insiden tersebut di atas.



Gambar 4. Proses dasar manajemen insiden ([ALB2004], 18)

3. Metodologi

Metodologi penelitian yang digunakan adalah metodologi eksperimental yaitu dengan menggunakan model prototype dengan tahapan-tahapan sebagai berikut yaitu: tahap analisa, tahap desain, tahap testing, tahap implementasi dan evaluasi.



Gambar 5. Tahapan penelitian

Tahapan-tahapan pengembangan CSIRMS adalah:

1. Analisa Kebutuhan
2. Desain dan Pengembangan Prototype
3. Testing dan Evaluasi
4. Implementasi

3.1 Tahapan Analisa Kebutuhan

Pada saat ini CSIRMS belum belum pernah dikembangkan di Kantor Akuntan Publik. Setiap terjadi insiden keamanan, langsung ditangani oleh bagian help desk.

Sebagai tahap awal untuk memulai pengembangan CSIRMS, akan dilakukan analisa yaitu analisa kebutuhan sistem. Tujuan dari analisa ini adalah untuk mengetahui kebutuhan CSIRMS yang diinginkan agar dapat diaplikasikan dalam bentuk sebuah sistem.

Metodologi pengumpulan data dilakukan studi lapangan dengan mempelajari, mengamati, mendalami kebutuhan CSIRMS yang akan dikembangkan dengan tidak mengabaikan kepatuhan (compliance) terhadap kebijakan-kebijakan dan kerangka yang berkaitan dengan manajemen keamanan informasi yang telah dibuat oleh Kantor Akuntan Publik .

3.2. Tahapan Desain dan Pengembangan Prototipe

Tujuan dari desain prototipe CSIRMS adalah untuk mendapat gambaran tentang CSIRMS 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.

3.3 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 Kantor Akuntan Publik.

3.4 Tahapan Implementasi

Setelah sistem diuji dan dievaluasi, maka sistem sudah siap untuk diimplementasi. Untuk mengimplementasi CSIRMS beberapa hal yang perlu diperhatikan adalah kebutuhan perangkat keras, perangkat lunak dan jaringan Kantor Akuntan Publik.

4. Hasil Penelitian

4.1 Kebutuhan Prototype

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

a. Kebijakan manajemen insiden
b. Kerangka Manajemen Insiden Keamanan Informasi
c. Keamanan sistem
d. Perangkat keras
e. Perangkat lunak
f. Jaringan Kantor Akuntan Publik

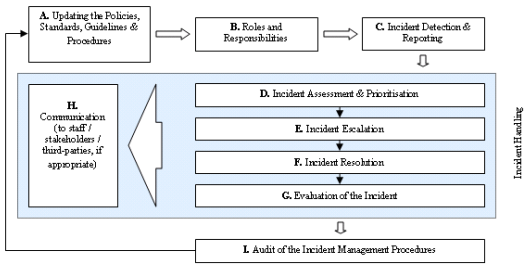
4.1.1 Kebijakan manajemen insiden

Beberapa kebijakan Kantor Akuntan Publik yang berhubungan dengan manajemen insiden keamanan informasi adalah sebagai berikut:

- Setiap Kantor Akuntan Publik harus mengembangkan dan menerapkan prosedur manajemen insiden keamanan.
- Semua staf dan partner harus dibuat sadar bagaimana caranya menemu kenali 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 Kantor Akuntan Publik yang lain, grup keamanan informasi global Kantor Akuntan Publik harus segera diinformasikan.

4.1.2 Kerangka Manajemen Insiden Keamanan Informasi

Grup keamanan informasi global Kantor Akuntan Publik telah mengembangkan suatu kerangka manajemen insiden keamanan informasi sebagai berikut:



Gambar 6. 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.*

4.1.3 Kebutuhan Perangkat Keras dan Perangkat Lunak Sistem

Hampir semua aplikasi yang dikembangkan di Kantor Akuntan Publik 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.

4.1.4 Kebutuhan Keamanan dan Jaringan

CSIRMS yang dikembangkan harus memenuhi beberapa kebutuhan keamanan sebagai berikut:

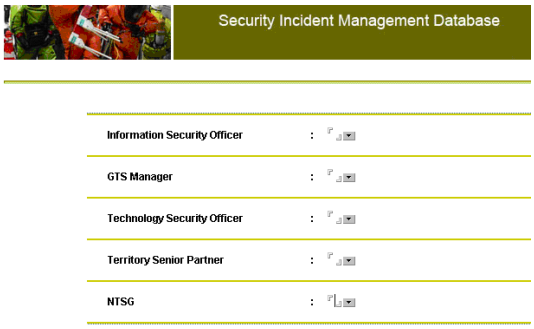
- Password minimal delapan karakter terdiri dari alphanumeric.
- Password hanya berlaku 90 hari.
- Kontrol akses diberikan sesuai dengan peran dan tanggung jawab pengguna sistem.
- Sistem harus bisa diakses secara *remote.*

4.2 Desain Prototype CSIRMS

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

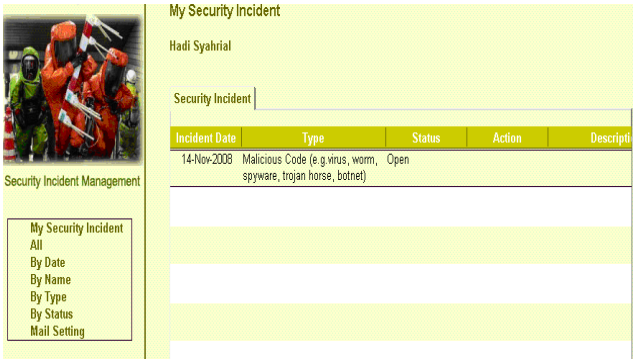
Gambar 7. Lotus Notes Designer

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



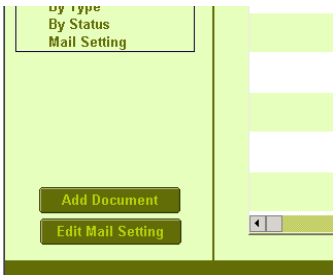
Gambar 8. Formulir Lotus Notes

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



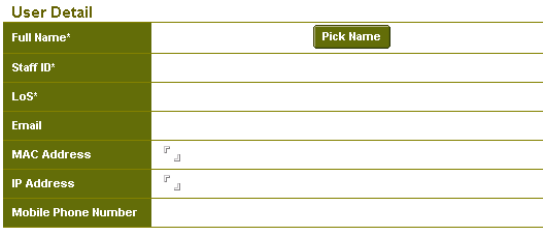
Gambar 9. Tampilan CSIRMS

Untuk membuat sebuah laporan insiden, telah dibuatkan sebuah tombol “add document” seperti gambar di bawah ini:



Gambar 10. Tombol “add document”

Jika tombol “add document” diklik maka akan muncul tampilan berupa formulir tentang identitas pelapor.

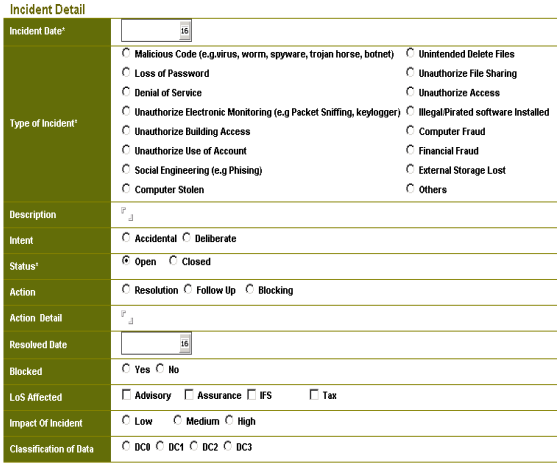


Gambar 11. Identitas pelapor

Identitas pelapor harus diisi, terutama di bagian “Full Name”, “Staff ID”, dan “LoS”. Jika field ini tidak diisi maka laporan tidak bisa disimpan. Setelah mengisi identitas, pelapor juga bisa melanjutkan untuk mengisi:

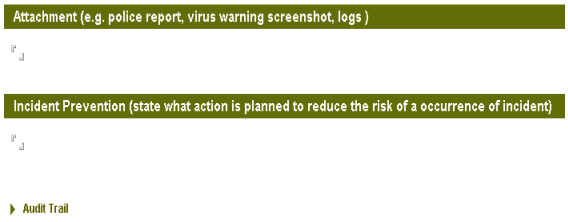
- Jenis insiden.
- Tanggal terjadinya insiden.
- Status insiden.
- Apakah sistem yang terkena dampak insiden sudah di block?
- LoS yang terkena dampak insiden.
- Tingkat dampak yang ditimbulkan.
- Klasifikasi data yang terkena dampak.

Untuk lebih jelasnya bisa dilihat tampilan di bawah ini:



Gambar 12. Jenis insiden

Sistem juga menyediakan field untuk meletakkan attachment dan pernyataan rencana untuk mencegak agar insiden tidak terulang kembali.



Gambar 13. *Field* untuk lampiran dan pencegahan insiden

4.3 Testing dan Evaluasi Prototype

4.3.1 Hasil Testing

Testing terhadap sistem dilakukan berdasarkan fungsi-fungsi yang terdapat pada sistem. Hasil testing prototipe CSIRMS adalah sebagai berikut:

Fungsi	Hasil Testing (Berfungsi dengan baik atau tidak)
Fied identitas pelapor	Berfungsi dengan baik
Field tipe dan deskripsi insiden	Berfungsi dengan baik
Field status Insiden	Berfungsi dengan baik
Field tanggal penyelesaian insiden	Berfungsi dengan baik
Field action dan *action details*	Berfungsi dengan baik
Field LoS Affected	Berfungsi dengan baik
Field Impact of Incident	Berfungsi dengan baik
Field Classification of Data	Berfungsi dengan baik
Mail Notification	Berfungsi dengan baik
Field untuk lampiran dan pencegahan insiden	Berfungsi dengan baik

Tabel 1. Hasil Testing

4.3.2 Hasil Evaluasi

Dari hasil evaluasi dapat disimpulkan bahwa kualitas CSIRMS adalah sebagai berikut:

No	Kualitas CSIRMS	Tidak Memenuhi Kebutuhan 1	Kurang Memenuhi Kebutuhan 2	Sangat Memenuhi Kebutuhan 3
	Persiapan			
1	Sistem mendukung perencanaan dan penerapan kapabilitas CSIRT.		X	
2	Sistem dapat menjaga kapabilitas CSIRT			X
3	Sistem mendukung proses peningkatan infrastruktur.			X
4	Sistem mendukung untuk melakukan review *postmortem*.			X
	Perlindungan			
5	Sistem mendukung untuk membantu menghentikan potensi eksploitasi kelemahan-kelemahan pada perangkat keras dan lunak.			X
6	Sistem memiliki kemampuan mendukung pemonitoran jaringan.	X		
7	Sistem mendukung untuk evaluasi risiko keamanan.			X
8	Sistem mendukung untuk menemukan kelemahan-kelemahan pada perangkat keras dan lunak	X		
	Pendeteksian			
9	Sistem memiliki kemampuan untuk pencatatan dan pelaporan kejadian-kejadian.			X
10	Sistem memiliki kemampuan untuk menerima laporan.			X
11	Sistem memiliki kemampuan sebagai *technology watch*.	X		
12	Sistem memiliki kemampuan untuk meneruskan insiden ke proses *triage*.		X	
	Triage			
13	Sistem memiliki kemampuan untuk pengkategorian insiden.			X
14	Sistem memiliki kemampuan untuk pemprioritasan insiden.			X
15	Sistem memiliki kemampuan untuk penetapan insiden.			X
16	Sistem memiliki kemampuan untuk mengakhiri proses insiden untuk tidak diteruskan ke proses tanggapan.		X	

Tabel 2. Kualitas CSIRMS

4.4 Implementasi CSIRMS

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

4.4.1 Dukungan Perangkat Keras dan Lunak

Untuk implementasi CSRMS 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:

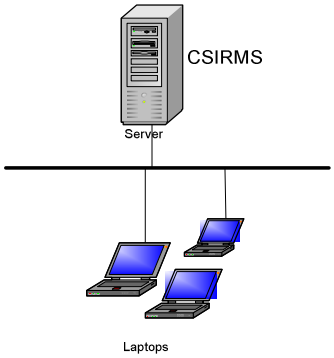
- Memori 2 GB
- Hard disk 40 GB
- Processor Pentium 1,6 GHz

Spesifikasi perangkat lunak

- Sistem Operasi Windows XP
- Lotus Notes Client 7.0.2

4.4.2 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 karyawan Kantor Akuntan Publik melalui *laptop*.



Gambar 14. Instalasi CSIRMS

4.5 Implikasi Penelitian

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

4.5.1 Implikasi manajerial

Implikasi manajerial pengembangan CSIRMS pada Kantor Akuntan Publik adalah pertama jika terjadi suatu insiden keamanan informasi dapat ditangani lebih cepat sehingga dapat memperkecil dampak insiden pada kelangsungan bisnis.

Kedua adalah dengan CSIRMS sebagai basis data yang mencatat semua insiden-insiden keamanan informasi maka dapat diketahui insiden-insiden keamanan apa saja yang sering terjadi sehingga dapat dilakukan tindakan-tindakan pencegahan agar insiden yang sama tidak terulang kembali di kemudian hari.

Yang ketiga adalah untuk mengembangkan CSIRMS perlu mempertimbangkan kebijakan-kebijakan yang dikembangkan oleh departemen-departemen lain di luar departemen teknologi informasi yang terkait dengan keamanan informasi Kantor Akuntan Publik seperti departemen sumber daya manusia, keuangan dan lain-lain.

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

4.5.2 Implikasi sistem

Sistem Manajemen Tanggapan Insiden Kemanan Komputer yang dikembangkan di Kantor Akutan Publik 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 CSIRM 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.

4.5.3 Implikasi lanjutan

Karena manajemen tanggapan insiden keamanan informasi merupakan suatu proses, maka untuk kelanjutan pengembangan CSIRMS di Kantor Akuntan Publik perlu menerapkan sistem flow yang sesuai dengan proses manajemen tanggapan insiden kemananan informasi yaitu:

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

4.5.4 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 CSIRMS merupakan salah satu alat bantu yang dapat mendukung agar manajemen insiden keamanan dapat dikelola dengan lebih proaktif sehingga insiden keamanan dapat dicegah.

5. Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan hasil penelitian dapat disusun kesimpulan sebagai berikut:

1. Dengan menggunakan model pendekatan perangkat lunak prototyping, pengembangan CSIRMS berbasiskan Lotus Notes telah dapat digunakan oleh

seluruh staf dan partner Kantor Akuntan Publik.
2. CSIRMS sangat membantu dalam mencegah terjadinya insiden yang sama terulang kembali.

5.1 Saran-Saran

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

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

Gambar 15. Proses dasar manajemen insiden ([ALB2004], 18)

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

6. 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] Schweitzer, 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