Security Management for Cloud Computing

Abstrak - Salah satu manajemen jaringan dan layanan masalah adalah keamanan, baik dalam mencegah serangan dan menggunakan mekanisme komputasi untuk melindungi data dan sistem atau dalam masalah
administrasi, yang melibatkan tidak hanya apa yang perlu dilindungi, tetapi juga tingkat layanan keamanan apa yang akan diberikan. Makalah ini mengeksplorasi Perjanjian Tingkat Layanan untuk Keamanan atau hanya Sec-SLA. Dicoba untuk memberikan gambaran tentang subjek, kesulitan yang dihadapi selama proses definisi metric keamanan dan pemantauan Sec-SLA, serta analisis tentang peran Sec-SLA dalam paradigma baru seperti komputasi awan.

I. PENDAHULUAN

Untuk memahami apa itu cloud computing, pertama-tama kita perlu memperoleh ide tentang evolusinya. Menurut Toffler, ia membahas tiga gelombang utama peradaban: era pertanian, industri, dan informasi. Era informasi memiliki beberapa sub gelombang dan kami bergerak ke arah komputasi awan. Ini mengacu pada memberikan layanan melalui internet atau berdasarkan pada infrastruktur cloud. Cloud computing akan membawabeberapa keuntungan bagi pasar dan tiga yang paling penting adalah:
efektivitas biaya, keamanan dan skalabilitas. Perhatian utama kami adalah untuk membahas beberapa protokol IAM keamanan yang digunakan untuk melindungi pengguna cloud dan untuk menyimpulkan protokol mana yang terbaik untuk organisasi yang bergerak ke arah mengonsumsi Layanan cloud.

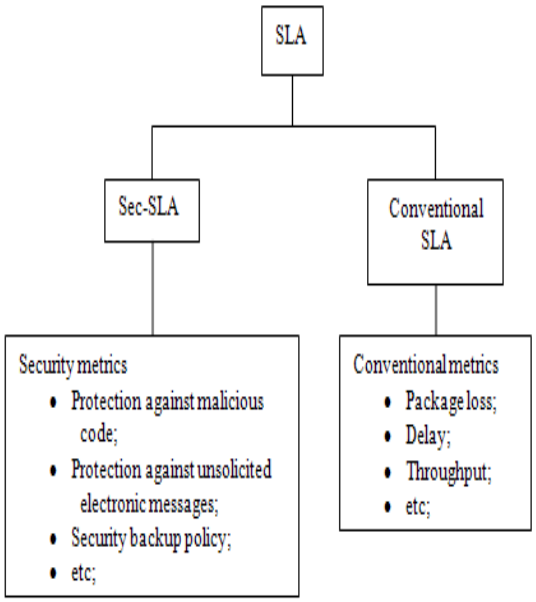
Sistem kontrol dan keamanan data penting dalam sistem komputer mana pun. Permintaan ini dapat dicakup dengan membuat perangkat atau teknik baru dan dengan membuat beberapa penyesuaian dengan cara tradisional untuk menyimpan dan mengendalikan sistem dan data. Dalam pengertian ini, makalah ini mempelajari Perjanjian Tingkat Layanan Keamanan atau hanya Sec-SLA bukan sebagai teknik baru, tetapi sebagai desain baru untuk Perjanjian Tingkat Layanan tradisional atau SLA. Alih-alih mempertimbangkan tradisional tingkat layanan seperti throughput atau penundaan jaringan, misalnya, hanya mempertimbangkan tingkat layanan yang terkait dengan keamanan.

Makalah ini mengeksplorasi Sec-SLA dan membahas beberapa aspek mendefinisikan metrik keamanan. Meskipun subjek sudah banyak dipelajari, paradigma baru seperti komputasi awan membawa pandangan baru tentang hal itu, baik dalam bidang manajemen layanan, seperti dalam pembentukan apa yang merupakan aspek keamanan utama yang akan dibahas. Dalam hal ini, proses empat langkah disajikan untuk digunakan ketika menentukan Sec-SLA untuk komputasi awan dan juga disajikan beberapa metrik keamanan yang cocok untuk lingkungan komputasi awan.

II. APA ITU SLA?

SLA seperti yang biasa dikenal, biasanya didefinisikan sebagai dalam “perjanjian negosiasi resmi antara dua pihak. Ini adalah kontrak yang ada antara Penyedia Layanan (SP) dan Pelanggan. Ini dirancang
untuk menciptakan pemahaman bersama tentang kualitas layanan, prioritas, tanggung jawab, dll. ”
Menurut definisi tingkat layanan di atas adalah konsep utama. Tetapi apakah layanan dalam konteks SLA? Dalam hal ini, jawabannya adalah: itu tergantung pada SLA. Dalam, ditunjukkan bahwa " meskipun kontrak-kontrak ini biasanya mencakup layanan yang disediakan oleh operator telekomunikasi kepada pelanggan korporat, mereka juga dapat menyertakan layanan yang disediakan departemen TI
(Teknologi Informatika) untuk unit bisnis lain dalam organisasi. ”Dalam konsep layanan digunakan seperti dalam ITIL satu atau lebih sistem TI yang memungkinkan proses bisnis. Para penulis dalam menekankan bahwa kita harus memperhitungkan bahwa sistem TI adalah kombinasi dari perangkat keras,
perangkat lunak, keterampilan, proses dan orang-orang. Dalam tulisan ini, kami menggunakan konsep layanan yang sama.Mempertimbangkan pentingnya keamanan sistem komputer, karakteristiknya yang rumit dan meningkatnya

skenario outsourcing, termasuk outsourcing layanan keamanan, tingkat layanan keamanan harus disepakati dalam Perjanjian Tingkat Layanan terpisah. Dengan demikian, SLA-SLA adalah SLA spesifik yang menangani metrik yang terkait dengan keamanan alih-alih metrik telekomunikasi tradisional seperti throughput, delay, packet loss, dan metrik serupa lainnya. Persyaratan atau tuntutan keamanan tingkat layanan, seperti ditunjukkan, kemudian dikonversi dalam seperangkat mekanisme, termasuk kriptografi, penyaringan paket data, redundansi perangkat keras dan perangkat lunak, dll.



Dalam Gambar 1, perbedaan antara Sec-SLA dan SLA konvensional

dirangkum. Di bagian selanjutnya kita membahas konsep metrik keamanan

dan kesulitan yang dihadapi selama definisi mereka.

III. DEFINISI SECURITY METRICS

Definisi istilah metrik kurang dimengerti, terutama ketika merujuk ke bidang IT. Ketidakjelasan ini, seperti yang dikatakan dalam disebabkan oleh fakta bahwa istilah tersebut digunakan dalam beberapa situasi, terkait dengan berbagai properti, bervariasi dari kinerja layanan hingga kematangan proses.

Kemudian ditunjukkan bahwa ketidakjelasan ini menantang ketika merancang metric keamanan yang tepat. Beberapa penulis setuju bahwa menjadi terukur dan terukur adalah atribut metrik yang penting Saat merancang metrik keamanan, tantangan ini juga menjadi perhatian utama.Definisi keamanan yang dapat dikuantifikasi dan dapat dinyatakan dalam tingkat layanan adalah rintangan yang harus diatasi. Kekhawatiran ini, ditunjukkan dalam poin lain dari makalah ini, adalah salah satu pertanyaan utama dalam. Banyak penelitian sedang dilakukan untuk memfasilitasi proses merancang metrik tersebut.

Langkah lebih lanjut diberikan, menyelaraskan metrik keamanan yang diperoleh untuk memenuhi standar informasi keamanan internasional, seperti ISO / IEC 17799: 2005 (sekarang dikenal sebagai ISO / IEC

27002). Perhatian dengan standar internasional sangat penting jika kami menganggap bahwa banyak organisasi yang dapat mengimplementasikan Sec-SLA juga dapat dalam beberapa proses sertifikasi.

Dalam Tabel I adalah transkrip untuk memberikan gambaran yang lebih baik tentang kemungkinan metrik keamanan.

IV. SEC-SLAS DALAM CLOUD

Perubahan yang terjadi dalam paradigma komputasi terdistribusi tradisional mengarah pada kebutuhan penegakan dalam SLA tradisional. Yang lebih baru adalah gagasan "komputasi di awan". Istilah populer untuk model komputasi baru ini adalah komputasi awan. Tidak ada konsensus yang jelas tentang apa sebenarnya komputasi awan itu, tetapi beberapa penulis menguraikan fakta bahwa itu adalah komputasi terdistribusi dan paradigma bisnis baru, yang menyediakan daya komputasi, perangkat lunak, dan penyimpanan dan bahkan infrastruktur pusat data terdistribusi sesuai permintaan, dikirim melalui Internet. Kata-kata kunci dalam definisi sebelumnya adalah sesuai permintaan. Layanan yang diberikan dalam kondisi seperti itu menuntut upaya yang cukup besar dalam proses penentuan tingkat layanan keamanan.

Definisi metrik keamanan, serta pemantauannya, harus dilakukan sesuai permintaan juga. Negosiasi dari SLA harus gesit, agar tidak mempengaruhi perekrutan layanan, karena salah satu daya tarik terbesar dari komputasi awan adalah untuk memungkinkan tuntutan tak terduga dipenuhi lebih cepat. Masalah keamanan dalam komputasi awan menimbulkan banyak pertanyaan, terutama dari pelanggan, yang perlu memahami risiko yang terkait saat melakukan migrasi layanan ke cloud, serta mengetahui apa saja cara yang tersedia untuk memastikan bahwa' keamanan data tersebut akan dipertahankan. Beberapa pekerjaan terbaru dalam komputasi awan mengutip pentingnya negosiasi SLA. Misalnya, The Cloud Security Alliance, yang debut resminya dibuat di RSA Conference 2009 merilis buku putih berjudul Panduan Keamanan untuk Bidang-Bidang Fokus Penting dalam Komputasi Awan, menunjukkan fakta bahwa lebih banyak pertimbangan harus diberikan pada konten SLA, mengingat 'kemampuan auditnya'
Ditunjukkan bahwa untuk menjadi alternatif yang layak untuk perusahaan, infrastruktur komputasi awan perlu memberikan tingkat layanan yang stabil untuk proses bisnis. Juga ditunjukkan bahwa "dalam lingkungan komputasi awan, SLA biasanya disediakan untuk layanan platform dasar (mis. Uptime sistem,
throughput jaringan)." Karakteristik yang sama sudah ditunjukkan dalam topic sebelumnya dalam makalah ini dan merupakan motivasi untuk memiliki tingkat layanan keamanan diperlakukan dalam SLA terpisah, yang kami sebut Sec-SLA. Karena sifatnya, komputasi awan memiliki beberapa jenis kegunaan, yaitu, seseorang mungkin melakukan komputasi di cloud saat membuat lembar data di Google Documents, serta ketika menyewa server di pusat data untuk tujuan perusahaan apa pun. Beberapa kategorisasi cloud computing dilakukan, mencoba untuk membedakan kemungkinan penggunaan ini, sesuai dengan tujuan utama penggunaan. Kategori yang lebih ditunjukkan dalam pekerjaan terkait komputasi awan adalah tiga berikut, direproduksi dalam bagian ini seperti definisi yang diberikan.

A. Infrastruktur sebagai Layanan (IaaS)

Produk dalam hal ini “menghadirkan infrastruktur komputer lengkap melalui
Internet

B. Platform sebagai Layanan (PaaS)

Dalam hal ini, ditawarkan "lingkungan pengembangan aplikasi penuh atau sebagian yang pengguna dapat mengakses dan memanfaatkan online, bahkan dalam kolaborasi dengan yang lain."

C. Perangkat Lunak sebagai Layanan (SaaS).

Dalam hal ini, disediakan "aplikasi turnkey yang lengkap — termasuk program kompleks seperti CRM atau manajemen sumber daya perusahaan melalui Internet."

Langkah-langkah yang diusulkan cocok sebagai pendekatan untuk menurunkan tingkat layanan keamanan untuk layanan yang dimigrasi ke cloud. Bahkan mempertimbangkan fakta bahwa generasi Sec-SLA dan negosiasi harus dinamis, seperti yang disebutkan sebelumnya dalam makalah ini, dalam skenario di mana organisasi bermaksud untuk memindahkan layanan atau proses ke cloud, analisis pertama yang bertujuan untuk menemukan kebutuhan keamanan organisasi terkait untuk layanan atau proses ini harus dilakukan. Jika organisasi sudah memiliki persyaratan keamanan ini yang diketahui dan didokumentasikan, analisis dapat melompat ke penyempurnaan, mengingat kekhasan kategori komputasi awan yang akan digunakan. Di bawah ini dijelaskan langkah-langkah ini, dengan mempertimbangkan skenario layanan atau proses yang dimigrasi ke penyedia cloud.

A. Analisis Kebijakan

Pada fase ini, akan dianalisis dokumentasi yang tersedia di organisasi dan mungkin di bidang tempat organisasi memiliki aktivitasnya, seperti kontrak pelanggan, peraturan nasional, kebijakan internal, dan sebagainya.

Hasil yang diinginkan:
Daftar awal kategori layanan keamanan untuk Sec-SLA. Langkah ini harus dilakukan oleh organisasi, karena ini adalah survei khusus, yaitu, meskipun beberapa generalisasi dimungkinkan,

masing-masing organisasi memiliki kekhususannya terkait dengan kebutuhan keamanan.

B. Analisis Arsitektur

Mempertimbangkan bahwa cloud computing memiliki banyak kategori penggunaan dan masing-masing kategori memiliki kekhasan sendiri, organisasi harus tahu, setidaknya pada saat pertama, tipe mana yang dimaksudkan. Definisi kategori apa yang lebih cocok untuk kebutuhan organisasi dilakukan pada fase lain dan tidak pada lingkup pekerjaan saat ini. Dengan kategori layanan keamanan awal dikumpulkan dalam langkah analisis kebijakan, pada fase analisis arsitektur akan dianalisis kategori mana yang dapat langsung dipetakan ke kategori cloud computing yang dimaksud. Mungkin juga untuk menganalisis mekanisme keamanan yang dimiliki oleh organisasi yang dapat dimigrasikan ke cloud juga (manajemen identitas, misalnya).

Dokumen yang dapat membantu dalam fase ini adalah diagram yang
tersedia seperti peta jaringan, diagram arsitektur perangkat lunak, diagram proses, dll. Hasil yang dimaksudkan: daftar kategori keamanan yang disempurnakan untuk Sec-SLA, serta pertanyaan yang akan dibuat dalam fase wawancara.

C. Wawancara

Dalam fase ini, wawancara dengan orang-orang yang terkait dengan layanan yang akan dimigrasi ke cloud akan dilakukan. Pertanyaan akan diarahkan ke pertanyaan spesifik tentang topik SLA yang akan dihasilkan. Banyak pertanyaan sudah dirumuskan pada langkah sebelumnya, analisis arsitektur, yang bertujuan untuk mengumpulkan lebih banyak rincian tentang topik-topik tertentu.

D. Negosiasi

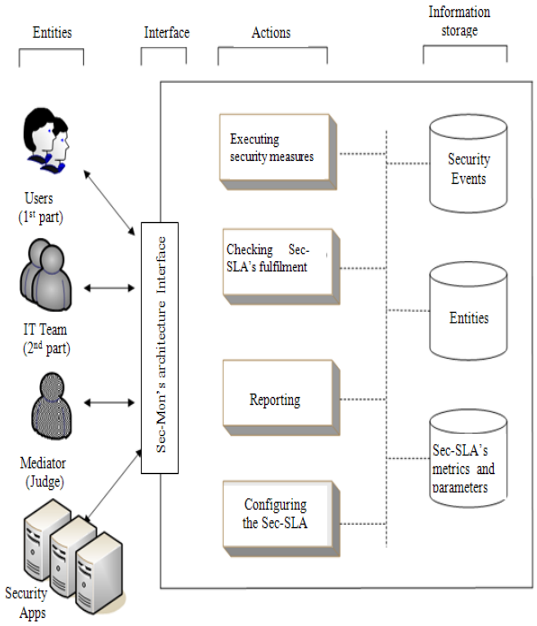
Jika ada negosiasi dengan beberapa penyedia komputasi awan, pada fase ini tingkat layanan keamanan akan dinegosiasikan. Jika tidak ada, akan perlu untuk memeriksa dengan penyedia yang mungkin yang mana dari mereka menawarkan dukungan untuk menegosiasikan tingkat layanan keamanan. Jika daftar tingkat layanan keamanan yang dibangun pada langkah-langkah sebelumnya adalah wajib, penyedia yang tidak menawarkan negosiasi tingkat layanan keamanan akan dihilangkan, banyak penyedia cloud memasukkan perjanjian tingkat layanan dalam kontrak online mereka, sudah menentukan bagaimana layanan akan diberikan, apa yang membuatnya berpotensi tidak dapat dinegosiasikan.

Dalam penelitian yang kami lakukan sebelumnya, daftar masalah keamanan pelanggan utama dikumpulkan.

V. MONITORING THE SEC-SLA

Setelah pelanggan mencapai kesepakatan dengan penyedia cloud, melalui Sec-SLA, ada langkah penting lainnya: memantau apakah metric keamanan terpenuhi.

Pada Gambar 2, ditunjukkan gambaran umum arsitektur yang diusulkan untuk memantau dan mengendalikan Sec-SLA, yang disebut Sec-Mon.



A. Sec-Mon architecture security aspects

Arsitektur seperti Sec-Mon mewakili kontribusi dalam mencari cara untuk memantau dan mengendalikan Sec-SLA. Namun, perlu untuk mengamankan arsitektur itu sendiri, karena bahkan ketika digunakan dalam lingkungan perusahaan, itu bisa menjadi titik lemah dalam proses pemantauan Sec-SLA.

Ketika digunakan, arsitektur tidak hanya akan melibatkan perangkat lunak dan perangkat keras, tetapi juga orang-orang dan proses,

semuanya gagal dan rawan penyalahgunaan (disengaja atau tidak). Dengan demikian, arsitektur ini harus dianalisis terhadap beberapa prinsip keamanan, seperti misalnya, integritas, privasi, ketersediaan, keaslian dan non-penolakan.

VI. KESIMPULAN

Sec-SLA adalah dokumen dinegosiasikan resmi yang mendefinisikan, khususnya,secara kuantitatif tingkat layanan apa yang akan diberikan dari penyedia ke pelanggan. Dengan kata lain, Sec-SLA berkaitan dengan "apa", bukan "bagaimana". Namun, dengan mendefinisikan metrik keamanan yang baik (dalam istilah yang didefinisikan dalam bagian IV), "bagaimana" bisa divisualisasikan dengan lebih baik. Biasanya tim IT menghadapi banyak pilihan dalam solusi teknologi dan memiliki pemahaman yang jelas dan terdokumentasi tentang apa saja persyaratan keamanan yang tentunya akan membantu. Salah satu keuntungan utama Sec-SLA, di luar yang legal, adalah kemungkinan pemahaman yang lebih baik tentang bagaimana keamanan sedang dicapai.

Itu juga mungkin untuk memperhatikan bahwa banyak penelitian sedang dilakukan berfokus pada subjek metrik keamanan. Untungnya, metrik keamanan menjadi perhatian besar di lebih banyak bidang daripada manajemen jaringan dan layanan dan banyak upaya yang dilakukan untukmeningkatkan definisi dan keterukurnya berguna dalam konteks Sec-SLA. Arsitektur yang diusulkan seperti Sec-Mon mewakili subsidi penting dalam mencari cara untuk memantau dan mengendalikan Sec-SLA. Gambaran umum
yang ditunjukkan pada Gambar 2 adalah konseptual, yaitu, arsitektur Sec-Mon tidak tergantung pada teknologi tertentu dan bahkan pada saat pembangunannya tidak dianggap sebagai paradigma komputasi awan, ia dapat dengan mudah disesuaikan untuk menyediakan sarana untuk menjadi
dikerahkan di lingkungan cloud.

Finalisasi, sebuah penelitian untuk pra-desain metrik keamanan sesuai dengan kategori komputasi awan, yang bertujuan untuk membantu kebutuhan negosiasi dinamik Sec-SLA di cloud sudah ada. Ini adalah tantangan besar karena paradigma masih berkembang, serta pemahaman tentang apa saja tantangan keamanan yang ditimbulkannya.

REFERENSI