j

STRATEGI DAN PENINGKATAN KEAMANAN PADA KOMPUTASI AWAN

Novianti Indah Putri[1] , Dadad Zainal Musadad[2], Zen Munawar[3], Rita Komalasari[4]

1. Teknik Informatika, Fakultas Teknologi Informasi Universitas Bale Bandung
2. Manajemen Informatika, Politeknik LP3I Bandung
3. Manajemen Informatika, Politeknik LP3I Bandung
4. Teknik Informatika, Politeknik LP3I Bandung

ABSTRACT

Today the computing world has changed from distributed systems and cloud computing. With cloud computing, the location of the data and the process of differences in the field of computing. An individual can have full control over the data and processes on his computer, but on the other hand, have cloud computing where services and data maintenance are provided by multiple vendors which keep the client from knowing where processes are running or where data is stored. The principle is logistical, the client has no control over it. Cloud computing uses the internet as a communication medium. Data security in cloud computing, as a vendor, must provide some assurance in the service level agreement and the customer regarding security issues. Cloud computing is still in the web, cloud computing, utilities, and platforms. All system services are individual, even though these systems are in full integration. One of the most important threats to cloud computing itself comes from HTTP Denial of Service or XML-Based Denial of Service attacks. This type of attack is simple and easy for attackers to implement, but for security experts, it is twice as difficult to carry out. The research analyzes current attacks by attackers as HTTP and XML. The results provide a solution for tracing back through Cloud TraceBack to find the source of the attack and introduce the use of a backpropagation network, called Cloud Protector, which detects and filters the attack traffic. The results show that it can detect and filter most of the attack messages and can detect frequently attacked sources in a short time.

Key Word: cloud computing, cloud computing security, network security

ABSTRAK

Saat ini dunia komputasi telah berubah dari terpusat ke sistem terdistribusi lalu ke komputasi awan. Dengan komputasi awan maka lokasi data dan proses terdapat perbedaan dalam bidang komputasi. Seorang individu dapat memiliki kendali penuh atas data dan proses di komputernya tetapi di sisi lain memiliki komputasi awan di mana, layanan dan pemeliharaan data disediakan oleh beberapa vendor yang membuat klien tidak mengetahui di mana proses sedang berjalan atau di mana data disimpan. Prinsipnya secara logis, klien tidak memiliki kendali atasnya. Komputasi awan menggunakan internet sebagai media komunikasi. Keamanan data dalam komputasi awan, sebagai vendor harus memberikan beberapa jaminan dalam perjanjian tingkat layanan dan meyakinkan pelanggan tentang masalah keamanan.. Komputasi awan masih dalam layanan web, komputasi utilitas, dan platform sebagai layanan. Semua layanan sistem individual, meskipun sistem ini sedang dalam integrasi penuh. Salah satu ancaman paling serius terhadap komputasi awan itu sendiri berasal dari serangan HTTP *Denial of Service* atau XML-Based Denial of Service. Jenis serangan ini sederhana dan mudah diterapkan oleh penyerang, tetapi bagi pakar keamanan, serangan ini dua kali lebih sulit untuk dilakukan. Penelitian menganalisis serangan saat ini oleh penyerang sebagai HTTP dan XML. Hasil penelitian memberikan solusi untuk melacak kembali melalui *Cloud TraceBack* untuk menemukan sumber dari serangan, dan memperkenalkan penggunaan jaringan netral *backpropagation*, yang disebut *Cloud Protector*, yang dilatih untuk mendeteksi dan memfilter lalu lintas serangan tersebut. Hasil penelitian menunjukkan dapat mendeteksi dan memfilter sebagian besar pesan serangan dan dapat mengidentifikasi sumber yang sering diserang dalam waktu singkat.

Kata Kunci: komputasi awan, keamanan komputasi awan, keamanan jaringan

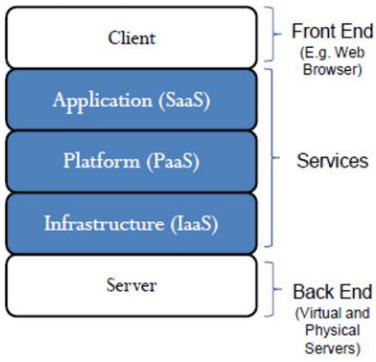
1. PENDAHULUAN

Cloud Computing telah berkembang melalui sejumlah: implementasi yang mencakup layanan aplikasi penyediaan (ASP), komputasi grid dan utilitas, dan Perangkat Lunak sebagai Layanan (SaaS). Tapi konsep menyeluruh dari memberikan sumber daya komputasi melalui jaringan global berakar pada tahun enam puluhan. Gagasan tentang "intergalaksi" jaringan komputer" diperkenalkan pada tahun enam puluhan oleh J.C.R. Licklider, yang bertanggung jawab untuk mengaktifkan pengembangan ARPANET (Proyek Penelitian Lanjutan Agency Network) pada tahun 1969. Visinya adalah untuk semua orang di dunia untuk saling berhubungan dan mengakses program dan data di situs mana pun, dari mana pun. Awan memiliki arsitektur yang berbeda berdasarkan layanan yang mereka berikan. Data disimpan ke terpusat lokasi yang disebut pusat data yang memiliki ukuran data yang besar penyimpanan. Data serta pemrosesan ada di suatu tempat server. Jadi, klien harus mempercayai penyedia pada ketersediaan serta keamanan data. SLA adalah satu-satunya perjanjian hukum antara penyedia layanan dan klien. Satu-satunya cara penyedia bisa mendapatkan kepercayaan dari klien adalah melalui SLA, sehingga harus distandardisasi. Dalam penelitian ini, bagian dua menjelaskan perjanjian tingkat layanan, bagian tiga menjelaskan SLA komputasi awan saat ini, dan bagian empat membahas bagaimana standarisasi SLA diikuti oleh masalah keamanan data yang diusulkan.. Teknologi informasi dan komunikasi bukan hanya sebatas bagaimana mengoperasikan komputer saja, namun bagaimana menggunakan teknologi untuk berkolaborasi dan berkomunikasi [1]. Industri teknologi informasi pernah fenomenal dengan penemuan revolusioner sejak adanya komputer generasi pertama [2]. Penggunaan program aplikasi dapat mempermudah dalam pencatatan, perbaikan, serta penghapusan data [3].. Dalam pengendalian aplikasi, fitnes terkait dengan ukuran kinerja dari pengendali proses [4]. Di satu sisi, manajemen hubungan pemasok dapat dilihat sebagai cerminan dari manajemen hubungan pelanggaan. Seperti halnya perusahaan perlu mengembangkan hubungan dengan pelanggannya, perusahaan juga perlu membina hubungan dengan pemasoknya. Hasil yang diinginkan adalah hubungan yang saling menguntungkan di mana kedua belah pihak saling menguntungkan.

Platform perangkat yang ada dan digunakan heterogen karena bergantung pada jaringan dan platform perangkat keras yang berbedadan sangat efektif dalam memberikan keamanan data dan informasi [5].

2. PERJANJIAN TINGKAT LAYANAN

Perjanjian tingkat layanan adalah dokumen yang mendefinisikan hubungan antara dua pihak: penyedia dan penerima. Ini jelas merupakan item dokumentasi yang sangat penting bagi kedua belah pihak. Jika digunakan dengan benar seharusnya: Identifikasi dan tentukan kebutuhan pelanggan. Menyediakan kerangka kerja untuk pemahaman. Menyederhanakan masalah yang kompleks. Mengurangi area konflik. Mendorong dialog jika terjadi perselisihan. Hilangkan ekspektasi yang tidak realistis.



Gambar 1. Tumpukan layanan cloud [6]

Seperti yang ditunjukkan pada Gambar. 1, layanan *Cloud* ditawarkan dalam bentuk Infrastructure-as-aservice (IaaS), *Platform-as-a-service (PaaS),* dan *Software-as-a-service* (SaaS). Ini mengikuti pendekatan bottom-up dimana pada tingkat infrastruktur; tenaga mesin dikirimkan dalam hal konsumsi CPU untuk alokasi memori [6]. Di atasnya, terletak lapisan yang memberikan lingkungan dalam hal kerangka kerja untuk pengembangan aplikasi, disebut sebagai PaaS. Di tingkat atas terdapat lapisan aplikasi, memberikan perangkat lunak yang dialihdayakan melalui Internet, menghilangkan kebutuhan untuk pemeliharaan perangkat lunak canggih di rumah. Pada lapisan aplikasi, pengguna akhir dapat memanfaatkan perangkat lunak yang berjalan di situs jarak jauh oleh Penyedia Layanan Aplikasi. Di sini, pelanggan tidak perlu membeli dan menginstal perangkat lunak yang mahal. Mereka dapat membayar untuk penggunaan dan kekhawatiran mereka untuk pemeliharaan dihilangkan.

Secara khusus itu harus mencakup berbagai

isu. Di antaranya biasanya sebagai berikut: Layanan yang akan diberikan Kinerja, Pelacakan dan Pelaporan Manajemen Masalah Kepatuhan Hukum dan Penyelesaian Sengketa Tugas dan Tanggung Jawab Pelanggan Keamanan HKI dan Pemutusan Informasi Rahasia.

2.1 Isi Perjanjian Tingkat Layanan Umum:

Ini adalah bagian paling penting dari Perjanjian karena menggambarkan layanan dan cara di mana mereka layanan harus disampaikan. Layanan standar sering dipisahkan dari layanan yang disesuaikan tetapi perbedaan ini adalah tidak kritis. Informasi tentang layanan harus akurat dan berisi spesifikasi rinci persis apa yang sedang disampaikan. Manajemen Kinerja : Bagian penting dari Perjanjian Tingkat Layanan berkaitan dengan pemantauan dan pengukuran kinerja tingkat layanan. Pada dasarnya, setiap layanan harus mampu diukur dan hasilnya dianalisis dan dilaporkan. Tolok ukur, target, dan metrik yang akan digunakan harus ditentukan dalam perjanjian itu sendiri. Tingkat kinerja layanan harus ditinjau secara berkala oleh kedua belah pihak. Manajemen Masalah : Tujuan dari manajemen masalah adalah untuk meminimalkan dampak buruk dari insiden dan masalah. Ini biasanya menentukan bahwa harus ada proses yang memadai untuk menangani dan menyelesaikan insiden yang tidak direncanakan dan harus ada juga kegiatan pencegahan untuk mengurangi terjadinya insiden kecelakaan yang tidak direncanakan. Tugas dan Tanggung Jawab Pelanggan : Penting bagi pelanggan untuk memahami bahwa ia juga memiliki tanggung jawab untuk mendukung proses penyampaian layanan. SLA mendefinisikan hubungan yang tentu saja merupakan entitas dua arah. Biasanya, pelanggan harus mengatur akses, fasilitas, dan sumber daya untuk karyawan pemasok yang perlu bekerja di lokasi. Jaminan dan Perbaikan : Bagian SLA ini biasanya mencakup hal-hal berikut: topik utama:

Kualitas layanan Ganti Rugi Klaim bagian ketiga Remedies untuk pelanggaran Pengecualian Force majeure. Keamanan adalah fitur yang sangat penting dari setiap SLA. Pelanggan harus menyediakan akses fisik dan logis yang terkontrol ke tempat dan informasinya. Sama halnya, pemasok harus menghormati dan mematuhi kebijakan dan prosedur keamanan Klien. Pemulihan bencana dan kelangsungan bisnis dapat menjadi sangat penting. Fakta ini harus tercermin dalam SLA-nya. Topiknya adalah pemulihan bencana biasanya dianut dalam bagian keamanan. Namun, itu juga sering dimasukkan dalam area

Manajemen Masalah. Pada tingkat tertinggi, kedua bidang ini biasanya menyatakan bahwa harus ada ketentuan yang memadai untuk pemulihan bencana dan perencanaan kesinambungan bisnis untuk melindungi kelangsungannya dari layanan yang disampaikan. Pengakhiran : Bagian dari perjanjian SLA ini biasanya mencakup topik utama berikut: Pengakhiran di akhir masa berlaku awal, pengakhiran untuk kenyamanan, pengakhiran karena alasan, pembayaran pada pengakhiran.

Sistem rekomendasi diperlukan karena sebelumnya terdapat kelemahan pada sistem berbasis konten [7]. Proses pengujian dilakukan untuk memastikan apakah sistem berjalan sesuai rencana awal yang telah dibuat atau tidak dan untuk mengetahui letak kesalahan yang ada pada sistem [8]. Sub sistem mempunyai kemampuan mengelola basis model dengan fungsi manajemen yang analog dan manajemen basis data [9].

Analisis dilakukan dengan cara evaluasi offline untuk memahami konsekuensi perbedaan topik pada metrik akurasi, dan analisis online untuk menyelidiki bagaimana metode inimemengaruhi kepuasan pengguna yang sebenarnya [10]. Dalam merancang tampilan antarmuka pengguna perlu memperhatikan kebutuhan pengguna [11]. Sistem Informasi yang popular saat ini adalah e-commerce. Secara komersial, e-commerce dapat disebut sebagai kegiatan yang berusaha menciptakan transaksi yang panjang antara perusahaan dan individu [12]. Kedewasaan secara umum dapat didefinisikan sebagai Keadaan menjadi lengkap, sempurna atau siap . Sistem Informasi harus mempunyai keamanan data yang pada sistem tersebut. Keamanan merupakan jaminan integritas, keaslian, dan kerahasiaan informasi [3].

2.2 Kebutuhan akan keamanan dan privasi dalam komputasi Cloud

Komputasi awan adalah penggabungan beberapa teknologi yang dikenal termasuk komputasi grid dan terdistribusi, memanfaatkan Internet sebagai jaringan pengiriman layanan. Lingkungan Cloud publik sangat kompleks jika dibandingkan dengan lingkungan pusat data tradisional [13]. Di bawah paradigma komputasi awan, sebuah organisasi menyerahkan kendali langsung atas aspek-aspek utama keamanan, memberikan tingkat kepercayaan yang substansial kepada penyedia awan. Sebuah survei terbaru mengenai penggunaan layanan awan yang

dilakukan oleh IDC menyoroti bahwa keamanan adalah tantangan terbesar untuk adopsi awan [14].

Lingkungan virtual digunakan di Cloud untuk mencapai multi-tenancy. Kerentanan dalam mesin virtual [15] menimbulkan ancaman langsung terhadap privasi dan keamanan layanan awan. Faktor-faktor yang melumpuhkan penggunaan layanan awan adalah migrasi langsung data melalui Internet, mempercayakan penyedia keamanan dan privasi data, kerentanan pada API browser, kerentanan dalam jaringan, dan peraturan ekspor untuk enkripsi.

Sumber daya bersama dan terdistribusi dalam sistem awan mempersulit pengembangan model keamanan untuk memastikan keamanan dan privasi data. Karena masalah transparansi, tidak ada penyedia awan yang mengizinkan pelanggannya untuk menerapkan deteksi intrusi atau sistem pemantauan keamanan yang meluas ke lapisan layanan manajemen di belakang instans awantervirtualisasi. Pelanggan mungkin tidak mengetahui detail insiden keamanan, kerentanan, atau laporan malware. Misalnya, melalui saluran belakang, penyerang mungkin dapat mengakses konten instance awan dan memperbaiki rootkit tingkat kernel [16]. Serangan pada "tingkat fisik" seperti membaca memori akses acak dari host tervirtualisasi atau menumbangkan lapisan virtualisasi [47] diketahui masyarakat. Bahkan sistem host yang menyediakan data tidak lagi dapat dipercaya sepenuhnya karena penyedia Cloud memiliki sumber daya fisik. Penyedia layanan cloud sering kali membuat perjanjian tingkat layanan untuk menyoroti keamanan dan privasi layanan terkait. Sampai batas tertentu, ada kekurangan metodologi standar Penyedia cloud seperti Amazon, Google, dan Salesforce sama-sama mengandalkan SLA terperinci untuk menjamin keamanan dan parameter lain kepada pelanggan mereka, misalnya, EC2 Amazon menyediakan abstraksi perangkat keras virtual kepada penggunanya, mencakup semua jenis kegagalan termasuk kegagalan simpul operator dan simpul perangkat lunak kegagalan [17]. Di masa mendatang, Google App Engine berbasis perjanjian tingkat layanan kemungkinan akan mengelola semua penyebab kegagalan.

3. HADIRKAN TINGKAT LAYANAN UMUM

Perjanjian Tingkat Layanan (SLA) dimasukkan ke dalam Perjanjian Layanan Utama dan berlaku untuk semua layanan yang dikirimkan langsung ke Pelanggan penyedia layanan cloud. SLA tidak berlaku untuk pihak ketiga yang tidak terkait atau pihak ketiga yang tidak memiliki privasi kontrak dengan penyedia layanan cloud tersebut. Jaminan uptime dan kredit perjanjian tingkat layanan yang dihasilkan diterapkan secara bulanan kecuali ditentukan lain. Semua jaminan dan informasi perjanjian tingkat layanan yang tercantum di bawah ini: Klaim Kredit perjanjian tingkat layanan: Untuk mengklaim kredit perjanjian tingkat layanan yang jatuh tempo dengan benar, pengguna pelanggan harus membuka tiket Penjualan dengan mengirimkan email ke Penjualan dalam waktu tujuh hari sejak penghentian yang dimaksud. Pelanggan harus menyertakan jenis layanan, Alamat IP, informasi kontak, dan deskripsi lengkap tentang gangguan layanan termasuk log jika berlaku. Kredit perjanjian tingkat layanan dikeluarkan sebagai kredit layanan pada siklus penagihan mendatang. Kesalahan Klaim perjanjian tingkat layanan: Pelanggan yang membuat klaim palsu atau berulang akan dikenakan biaya satu kali per insiden untuk klaim tersebut. Klaim palsu atau berulang juga pelanggaran terhadap Persyaratan Layanan dan dapat dikenakan penangguhan layanan. Pelanggan yang berpartisipasi dalam aktivitas internet yang berbahaya atau agresif sehingga menyebabkan serangan atau serangan balik tidak memenuhi syarat untuk klaim perjanjian tingkat layanan dan akan melanggar Kebijakan Penggunaan yang Dapat Diterima. Jaringan Publik: Penyedia layanan cloud (mis., Server Intellect) menjamin 99,9% waktu aktif di semua layanan jaringan publik kepada Pelanggan yang berada di pusat data mitra mereka. Semua layanan jaringan publik mencakup koneksi backbone internet kelas operator yang redundan, sistem deteksi intrusi tingkat lanjut, mitigasi penolakan layanan, analisis lalu lintas, dan grafik bandwidth terperinci. Jaringan Pribadi: Penyedia layanan cloud menjamin 99,9% uptime pada layanan jaringan layanan untuk Pelanggan yang berlokasi di pusat data mitra. Semua layanan jaringan pribadi termasuk akses ke koneksi VPN yang aman, bandwidth tak terbatas antar server, unggahan/unduh tak terbatas ke server, akses ke layanan yang dikontrak, analisis lalu lintas, dan grafik bandwidth terperinci. Infrastruktur Redundan: : Penyedia layanan cloud menjamin 99,9% uptime pada daya dan layanan HVAC kepada Pelanggan yang berlokasi di pusat data mitra kami. Semua peralatan komputer dan layanan terkait dilayani oleh unit daya UPS redundan dengan generator diesel cadangan di lokasi. Jaminan khusus dengan informasi SLA,

Jaringan Publik, Jaringan Pribadi, dan SLA Infrastruktur tercantum di bawah ini:

Prosedur pencarian otomatis diperlukan untuk pengendali parameter [18]. Certainty factor adalah metode untuk mengelola ketidakpastian dalam sistem berbasis aturan [19].

Peningkatan Perangkat Keras: Penyedia layanan cloud menjamin peningkatan perangkat keras akan dimulai dan diselesaikan dalam waktu empat jam dari jendela pemeliharaan peningkatan perangkat keras yang dijadwalkan. Upgrade perangkat keras harus dijadwalkan dan dikonfirmasi sebelumnya melalui sistem tiket online. Kegagalan memasang perangkat keras dalam waktu empat jam akan mengakibatkan pengabaian biaya pemasangan satu kali.

Pengolahan informasi dasar terjadi di banyak elemen sederhana [20]. Sistem Pengukuran Model, yang membedakan empat dimensi untuk mengevaluasi suatu sistem [21]:

Setelah implementasi dilakukan pengujian untuk mengetahui kinerja aplikasi dengan membandingkan dengan aplikasi yang sudah ada [22]. Dataset dunia nyata digunakan untuk memvalidasi modul yang diusulkan dan dicocokkan dengan model dasar yang berbeda [23].

Penyelesaian berbagai persoalan yang terdapat dalam domain ini tidak mudah dihitung dengan menggunakan berbagai model analisis yang ada [24].

4. BAGAIMANA MENSTANDARISASI SLA

4.1 SLA harus mendiskusikan bagaimana risiko keamanan berikut ditangani:

SLA yang lalu menyatakan pengabaian jika janji tidak dipenuhi tetapi melakukan ini benar-benar membantu pelanggan dalam memenuhi kerugian mereka. SLA juga harus membahas tentang bagaimana keamanan dipertahankan, metode apa yang digunakan dalam menjaga keamanan dan bagaimana penanganan keluhan pelanggan? Berikut ini adalah masalah keamanan yang harus didiskusikan SLA: Akses pengguna yang diistimewakan. Data sensitif yang diproses di luar perusahaan membawa serta tingkat risiko yang melekat, karena layanan yang dialihdayakan melewati "kontrol fisik, logis, dan personel" yang diberikan toko TI atas program internal. Dapatkan informasi sebanyak-banyaknya tentang orang-orang yang mengelola data kita. Minta penyedia untuk memberikan informasi spesifik tentang perekrutan dan pengawasan administrator yang memiliki hak istimewa, dan kontrol atas akses mereka. Kepatuhan terhadap peraturan. Pelanggan pada akhirnya bertanggung jawab atas keamanan dan integritas data mereka sendiri, meskipun data tersebut dipegang oleh penyedia layanan. Penyedia layanan tradisional tunduk pada audit eksternal dan sertifikasi keamanan. Penyedia komputasi awan yang menolak untuk menjalani ini

pengawasan menandakan bahwa pelanggan hanya dapat menggunakannya untuk fungsi yang paling sepele. Lokasi data. Saat menggunakan cloud, kita mungkin tidak akan tahu persis di mana data kita di-host. Bahkan, kita mungkin tidak tahu di negara mana ia akan disimpan. Tanyakan kepada penyedia apakah mereka akan berkomitmen untuk menyimpan dan memproses data di yurisdiksi tertentu, dan apakah mereka akan membuat komitmen kontraktual untuk mematuhi persyaratan privasi lokal atas nama pelanggan mereka. Pemisahan data.

Data di cloud biasanya berada di lingkungan bersama bersama data dari pelanggan lain. Enkripsi efektif tetapi bukan obat untuk semua. Penyedia cloud harus memberikan bukti bahwa skema enkripsi dirancang dan diuji oleh spesialis berpengalaman. Pemulihan. Bahkan jika kami tidak tahu di mana data Anda berada, penyedia cloud harus memberi tahu kami apa yang akan terjadi pada data dan layanan kami jika terjadi bencana. Setiap penawaran yang tidak mereplikasi data dan infrastruktur aplikasi di seluruh

beberapa situs rentan terhadap kegagalan total. Dukungan investigasi. Investigasi aktivitas yang tidak pantas atau ilegal mungkin tidak mungkin dilakukan dalam komputasi awan. Layanan cloud sangat sulit untuk diselidiki, karena logging dan data untuk banyak pelanggan mungkin berada di lokasi yang sama dan mungkin juga tersebar di kumpulan host dan server yang selalu berubah.

Pusat Data. Jika kami tidak dapat memperoleh komitmen kontraktual untuk mendukung bentuk investigasi tertentu, bersama dengan bukti bahwa vendor telah berhasil mendukung aktivitas tersebut, maka asumsi kami yang aman adalah bahwa permintaan investigasi dan penemuan akan menjadi mungkin. Kelangsungan hidup jangka panjang. Idealnya, penyedia komputasi awan tidak akan pernah bangkrut atau diakuisisi dan ditelan oleh perusahaan yang lebih besar. Tapi harus yakin tentang data akan tetap tersedia bahkan setelah kejadian seperti itu.

Penelitian sebelumnya sudah menyelidiki apakah ada efek signifikan dalam keakuratan

model prediktif [25].

4.2 Kuesioner yang harus dijawab oleh SLA

- Bagaimana tagihan dihasilkan? Apa saja mode pembayarannya? Bagaimana pengaruh layanan jika pelanggan menunda pembayaran tagihan? Ini harus berisi masa tenggang dan bagaimana pelanggan bisa mendapatkan layanan kembali setelah pembayaran ketika layanan dihentikan?

-Apa yang terjadi jika SLA tidak terpenuhi? Bagaimana penanganan data saat kontrak layanan berakhir, jenis data yang dikembalikan ke perusahaan?

-Apa yang terjadi jika kontrak layanan ditarik? Bagaimana data akan ditangani dan dikembalikan ke perusahaan? - Bagaimana layanan menggunakan log peristiwa dan siapa yang sebenarnya memiliki akses ke data di backend?

-Siapa yang akan memeriksa keamanan penyedia cloud? - Manakah dari karyawan SaaS yang memiliki akses root dan database, dan apakah ada yang mencegah mereka mendapatkan akses ke data perusahaan Anda? Kontrol apa yang ada? -Apakah data yang disimpan dipisahkan antara klien atau semuanya disimpan pada satu database besar di luar sana? Bagaimana data dipisahkan? Bagaimana pertanyaan hukum tentang e-discovery akan ditangani jika muncul sebagai masalah bisnis? - Dalam hal ketersediaan layanan, bisakah Anda meminta vendor Anda untuk menandatangani perjanjian tingkat layanan? -Pengaturan Keamanan apa yang Anda miliki dengan penyedia layanan cloud yang Anda andalkan untuk memberikan layanan Anda? Apa yang Anda lakukan untuk membangun "kepercayaan mendalam" di cloud? -Banyak tantangan utama pada komputasi awan muncul di perbatasan antara infrastruktur Anda dan awan. - Bagaimana Anda memindahkan sumber daya dari satu sisi ke sisi lain? Apakah aplikasi cloud bergantung pada penyimpanan yang berada di sisi perbatasan Anda? -Apa dampaknya terhadap kebutuhan bandwidth? Dan bagaimana Anda dengan mulus memindahkan mesin virtual antara cloud dan pusat data Anda saat permintaan tumbuh dan menyusut? -Ini semua adalah pertanyaan yang valid dan menarik. Tetapi pertanyaan yang lebih besar yang membayangi seperti awan gelap di cakrawala adalah tentang yurisdiksi dan status hukum. Apakah barang-barang di cloud memiliki pijakan hukum yang sama dengan barang-barang di pusat data Anda? - Bagaimana peralihan terjadi pada cloud publik ketika infrastruktur cloud pribadi tercampur? Atau apakah Anda akan menggunakan cloud publik hanya untuk menjalankan layanan Anda? - Seberapa aman Skema enkripsi • Seberapa aman data dari bencana alam?

• Apakah mungkin semua data saya dienkripsi sepenuhnya? • Algoritma apa yang digunakan? Siapa yang memegang, memelihara, dan mengeluarkan kunci?

-Bagaimana cara memastikan Pengguna bahwa Data dan Kode aman? 4.2.1. Keamanan di Berbagai Tingkat Kami membutuhkan keamanan di tingkat berikut:

- Keamanan akses server - Keamanan akses Internet - Keamanan akses database - Keamanan privasi data - Keamanan akses program - Pertanyaan

- Apa itu Keamanan Data di Lapisan Fisik? Apa itu Keamanan Data di Lapisan Jaringan? Bagaimana dengan Dukungan investigasi? Seberapa aman data dari bencana alam? Seberapa tepercaya skema Enkripsi Penyedia Layanan?

5. KESIMPULAN

Tingkat layanan umum ini hanya membahas tentang layanan yang diberikan dan keringanan yang diberikan jika layanan tidak memenuhi kesepakatan, tetapi keringanan ini tidak terlalu membantu pelanggan memenuhi kerugian mereka. Pengabaian harus dilakukan sesuai dengan jenis usaha yang dilakukan oleh pelanggan. Selain pengabaian, Tingkat layanan umum harus membahas banyak masalah lain seperti kebijakan keamanan, metode, dan implementasinya. Juga harus dibicarakan tindakan hukum apa yang diambil jika layanan disalahgunakan oleh pelanggan.

DAFTAR PUSTAKA

[1] Z. Munawar and D. Z. Musadad, “Penggunaan TIK untuk Bidang Pendidikan,” in *Munuju Masyarakat Madani*, 2015, pp. 555–563.

[2] Z. Munawar, “Pertimbangan Umum Keamanan Pada Mobile Computing,” *Temat. - J. Teknol. Inf. dan Komun.*, vol. 2, no. 1, pp. 72–84, Jun. 2015.

[3] Z. Munawar, “Mekanisme keselamatan, keamanan dan keberlanjutan untuk sistem siber fisik,” *J. Teknol. Inf. Dan Komun.*, vol. 7, no. 1, pp. 58–87, 2020.

[4] N. Ramsari and Z. Munawar, “Pengambilan Keputusan Dengan Teknik Soft Computing,” *J. Ilm. Teknol. Inf. Terap.*, vol. 2, no. 3, pp.

244–253, 2016.

[5] Novianti Indah Putri, Rita Komalasari, and Zen Munawar, "Pentingnya Keamanan Data Dalam Intelijen Bisnis," *J-SIKA|Jurnal Sist. Inf. Karya Anak Bangsa*, vol. 2, no. 2, pp. 41–48, 2021.

[6] W. Web, "Software as a service," *Wikipedia - The Free Encylopedia*, 2021. [Online]. Available: http://en.wikipedia.org/wiki/Software_as_a_service. [Accessed: 01-Apr-2021].

[7] Z. Munawar, N. Suryana, Z. B. Sa'aya, and Y. Herdiana, "Framework With An Approach To The User As An Evaluation For The Recommender Systems," in *2020 Fifth International Conference on Informatics and Computing (ICIC)*, 2020, pp. 1–5.

[8] Z. Munawar, "Aplikasi Registrasi Seminar Berbasis Web Menggunakan QR Code pada Universitas XYZ," *Temat. J. Teknol. Inf. Dan Komun.*, vol. 6, no. 2, pp. 68–77, 2019.

[9] Z. Munawar, "Penerapan Metode Analytical Hierarchy Process Dan Technique For Order Preference By Similarity To Order Solution Dalam Seleksi Penerimaan Mahasiswa Baru Jalur Bidik Misi," *Temat. - J. Teknol. Inf. dan Komun.*, vol. 4, no. 1, pp. 34–53, Jun. 2017.

[10] Zen Munawar, Novianti Indah Putri, and Dadad Zainal Musadad, "Meningkatkan Rekomendasi Menggunakan Algoritma Perbedaan Topik," *J-SIKA|Jurnal Sist. Inf. Karya Anak Bangsa*, vol. 2, no. 02 SE-, pp. 17–26, 2021.

[11] Z. Munawar, "Perancangan Interface Aplikasi Pencatatan Persediaan Barang Di Kios Buku Palasari Bandung Dengan Metode User Centered Design Menggunakan Balsamiq Mockups," *Comput. | J. Inform.*, vol. 6, no. 2 SE-, pp. 10–20, Dec. 2019.

[12] Z. Munawar, "Keamanan Pada E-Commerce Usaha Kecil dan Menengah," *Temat. - J. Teknol. Inf. dan Komun.*, vol. 5, no. 1, pp. 1–16, Jun. 2018.

[13] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," in *Recommendations of the National Institute of Standards and Technology*, Gaithersburg: NIST Special Publication 800-145 U.S. Department of Commerce, 2011, pp. 269–274.

[14] F. Gens, "New idc it cloud services survey: top benefits and challenges," 2009. [Online]. Available: http://blogs.idc.com/%0Aie/?p=730. [Accessed: 01-Apr-2021].

[15] NIST, "National vulnerability database version 2.2," 2021. [Online]. Available: http://web.nvd.nist.gov/view/vuln/search-results?query=virtual&search%25_type=all&cves=on. [Accessed: 01-Apr-2021].

[16] D. Durkee, "Why cloud computing will never be free," *Commun. ACM*, vol. 53, no. 5, pp. 62–69, 2010.

[17] K. Sripanidkulchai, S. Sahu, Y. Ruan, A. Shaikh, and C. Dorai, "Are clouds ready for large distributed applications," *SIGOPS Oper Syst Rev*, vol. 44, no. 2, pp. 18–23, 2010.

[18] Z. Munawar, "Penerapan Metode Soft Computing Dalam Menyelesaikan Permasalahan di Bidang Teknik," *Temat. - J. Teknol. Inf. dan Komun.*, vol. 3, no. 2, pp. 1–13, Dec. 2016.

[19] N. I. Putri, "Sistem pakar diagnosa tingkat kecanduan gadget pada remaja menggunakan metode Certainty Factor." UIN Sunan Gunung Djati Bandung, 2018.

[20] Z. Munawar, "Perkembangan Riset di Bidang Neurocomputing," *Temat. - J. Teknol. Inf. dan Komun.*, vol. 2, no. 2, pp. 17–31, Dec. 2015.

[21] Y. Saleh and M. Alshawi, "An alternative model formeasuring the success of ISprojects: the GPIS model," *J. Enterp. Inf. Manag.*, vol. 18, no. 1, pp. 47–63, 2005.

[22] Z. Munawar, "Penggunaan Metode Multi Threads untuk Pengelolaan Proses Download di Internet," *Temat. - J. Teknol. Inf. dan Komun.*, vol. 1, no. 1, pp. 47–58, Jun. 2014.

[23] N. I. Putri, Rustiyana, Y. Herdiana, and Z. Munawar, "Sistem Rekomendasi Hibrid Pemilihan Mobil Berdasarkan Profil Pengguna dan Profil Barang," *Temat. - J. Teknol. Inf. dan Komun.*, vol. 8, no. 1 SE-Articles, pp. 56–68, Jun. 2021.

[24] Z. Munawar, "Research developments in the field neurocomputing," in *2016 4th International Conference on Cyber and IT Service Management*, 2016, pp. 1–6.

[25] Z. Munawar, "Penggunaan Profil Media Sosial Untuk Memprediksi Kepribadian," *Temat. - J. Teknol. Inf. dan Komun.*, vol. 4, no. 2 SE-Articles, pp. 18–37, Dec. 2017.