ISBN: 978-602-60280-1-3

Analisis Kebijakan Keamanan Hotel Java Heritage mengacu pada Kerangka Kerja Octave-S

[1st]Ranggi Praharaningtyas Aji
Sistem Informasi
STMIK Amikom Purwokerto
Purwokerto,Banyumas, Indonesia
ranggi.p.aji@amikompurwokerto.ac.id

[2nd]Muhammad Aziz Alkautsar
Magister Teknik Informatika
UNIVERSITAS AMIKOM Yogyakarta
Yogyakarta, Indonesia
muhammad.alkautsar@students.amikom.ac.id

[3rd]Ito setiawan
Sistem Informasi
STMIK Amikom Purwokerto
Purwokerto,Banyumas, Indonesia
itosetiawan@amikompurwokerto.ac.id

***Abstrak*—Pentingnya menjaga keamanan sebuah sistem terlihat dari kebijakan keamanan yang diterapkan oleh sebuah organisasi. Pada hotel Java Heritage terdapat kasus seperti penyalahgunaan komputer, akses informasi yang tidak sah (*unauthorized*), dan masih ada pula masalah teknis yang terjadi. Untuk menyelesaikan masalah tersebut dibutuhkan analisis kebijakan keamanan sehingga pemilik kepentingan mampu fokus dalam membuat mitigasi risiko. Octave-S dapat memberikan pandangan mengenai kebijakan keamanan sistem hotel Java Heritage secara lebih mudah dan membantu hotel Java Heritage mengetahui apakah kebijakan keamanan yang mereka terapkan sudah dilakukan secara maksimal. Hasil penelitian ini adalah penilaian atas kebijakan keamanan Pada hotel Java Heritage yang dapat dijadikan acuan dalam melakukan mitigasi atas kelemahan keamanan sistem yang ada pada hotel Java Heritage.**

Kata kunci—Octave-S, Kebijakan keamanan, Keamanan sistem.

I. PENDAHULUAN

Masalah keamanan sistem informasi sering kali kurang mendapatkan perhatian serta pertimbangan dari para *stakeholder* dan pengelola sistem informasi. Sering kali, permasalahan keamanan sistem informasi mendapatkan perhatian dari para *stakeholder* dan pengelola sistem informasi ketika sudah terjadi sebuah ancaman yang menimbulkan kerugian pada perusahaan. Hal ini menjadikan kerugian yang dialami oleh perusahaan nyata dan berdampak kepada organisasi/perusahaan. Ketika sebuah ancaman sudah menimbulkan kerugian pada perusahaan, stakeholder dan pengelola sistem mulai melakukan berbagai tindakan pencegahan dan perbaikan atas keamanan sistem informasi.

Pada hotel Java Heritage terdapat kasus seperti penyalah gunaan komputer, akses informasi yang tidak sah (*unauthorized*). Sedangkan dari segi teknis kendala yang ditemui ganguan listrik yang sering terjadi dan *human error* seperti: karyawan meninggalkan komputer dalam keadaan menyala, berbagi *password* kepada karyawan lain, kesalahan menginputkan data. Kasus tersebut dapat menyebabkan kerugian bagi hotel Java Heritage jika tidak segera diselesaikan. Namun sebelum kita dapat menyelesaikan masalah tersebut perlu dilakukan analisis bagaimana kebijakan keamanan hotel Java Heritage dikerjakan. Dengan diketahuinya kebijakan keamanan apa saja yang sudah dan belum dilaksanakan maka pihak hotel Java Heritage mampu fokus dalam melakukan mitigasi risiko yang mungkin akan dihadapi.

Cara yang bisa dilakukan adalah dengan menggunakan penilaian yang mengacu pada kerangka kerja Octave-S. Octave-S merupakan salah satu teknik dan metode yang digunakan untuk strategi dan perencanaan risiko keamanan informasi. Terdapat perbedaan antara metode analisa risiko lain dengan metode Octave-S yaitu Octave-S lebih fokus pada praktek keamanan, isu-isu strategis, dan evaluasi organisasi dan Keuntungan lain metode Octave-S adalah *self-directed, flexible, evolved* [1]. pada Octave-S Standar kebijakan keamanan berfokus pada langkah 3a, 3b, dan 4 Octave-S. Pada langkah 3a ditentukan sejauh mana setiap praktik Keamanan digunakan oleh organisasi. Pada langkah 3b menentukan sudah atau belum praktek keamanan tersebut dilakukan oleh organisasi. Dan langkah 4 memberikan status berupa tanda (merah, hijau, kuning) untuk masing-masing area praktik kebijakan keamanan. Status tersebut harus mencerminkan seberapa baik organisasi telah memenuhi setiap area keamanan yang ada [1]. .

II. TINJAUAN PUSTAKA

A. Kebijakan Keamanan

"Kebijakaan Keamanan" atau "*Security Policies*" merupakan sebuah infrastruktur keamanan yang harus dimiliki oleh sebuah organisasi atau perusahaan yang ingin melindungi aset informasi terpentingnya[2]. Funsi utama dari *security policy* untuk perusahaan atau organisasi diantaranya [3]:

1. Untuk melindungi suatu perusahaan secara keseluruhan, baik Sumber Daya Manusia, informasi maupun sistemnya.
2. Memberikan panduan tentang apa yang harus dilakukan untuk melindungi informasi yang disimpan pada komputer atau sistem
3. Sebagai perlindungan dari orang-orang yang mecoba melakukan tindakan yang merugikan perusahaan

B. OCTAVE-S

OCTAVE-S adalah sebuah variasi dari pendekatan OCTAVE yang dikembangkan untuk menemukan kebutuhan-kebutuhan kecil dari organisasi-organisasi yang tidak memiliki hierarki. OCTAVE-S berdasar pada 3 tahap yang dideskripsikan dalam kriteria OCTAVE, meskipun nomor dan urutan kegiatan berbeda dari metode OCTAVE yang digunakan. Bagian ini memberikan tinjauan singkat atas tahapan, proses, dan kegiatan OCTAVE-S [1]

Berdasarkan Octave-S *implementation guide version* 1.0, Proses-proses metode OCTAVE-S terdiri dari 3 fase :

a. Fase I (*Build Asset-Based Threat Profiles*)

Pada proses pada fase ini terdiri atas Fase I proses I *Identify Organizational Information* dan Fase I proses II *Create Threat Profiles*. Sedangkan untuk aktifitas yang dilakukan pada proses 1 terdiri atas *Activity* 1 *Establish Impact Evaluation Criteria*, *Activity* 2 *Identify Organizational Assets*, *Activity* 3 *Evaluate Organizational Security Practices*. Dan pada proses 2 terdiri atas *Activity* 1 *Select Critical Assets*, *Activity* 2 *Identify Security Requirements for Critical Assets*, dan *Activity* 3 *Identify Threats to Critical Assets*.

b. Fase II (*Identify Infrastructure Vulnerability*)

Fase kedua dalam OCTAVE-S adalah *Identify Infrastructure Vulnerabilities*. Fase ini melihat kerawanan risiko secara teknis yang terjadi pada aset kritis dan komponen

ISBN: 978-602-60280-1-3

infrastruktur kunci yang mendukung aset tersebut. Terdapat 1 proses yaitu Fase II proses III *Examine Computing Infrastructure in Relation to Critical Assets*. Dengan 2 aktivitas yang dilakukan yaitu *Activity* 1 *Examine Access Paths* dan *Activity* 2 *Analyze Technology-Related Processes.*

c. Fase III (*Develop Security Strategy and Plans*)

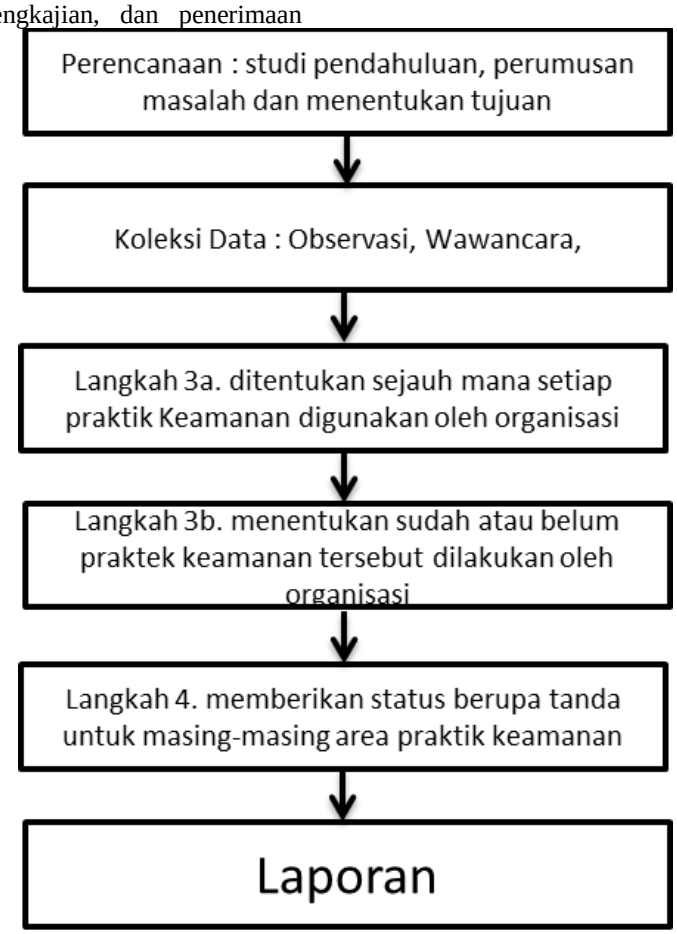
Fase ketiga dalam OCTAVE-S adalah *Develop Security Strategy and Plans*. Pada fase ini didefinisikan risiko terkait dengan aset kritis, membuat rencana mitigasi untuk risiko tersebut, dan membuat strategi perlindungan bagi perusahaan. Rencana dan strategi dikaji dan diterima oleh manajer senior. Terdapat dua proses dalam fase ketiga yang akan dibahas berikutnya. Terdapat 2 proses yang dijalankan pertama Fase III proses IV *Identify and Analyze Risks* dengan 3 aktifitas yang dijalankan berupa *Activity* 1 *Evaluate Impacts of Threats, Activity* 2 *Establish Probability Evaluation Criteria*, dan *Activity* 3 *Evaluate Probabilities of Threats*.

Selanjutnya ada proses 5 yaitu Fase III proses V (*Develop Protection Strategy and Mitigation Plans*) Proses 5 melibatkan pengembangan, pengkajian, dan penerimaan strategi proteksi organisasi secara menyeluruh, rencana mitigasi untuk risiko terhadap aset kritis. Aktifitas proses ini terdiri dari 5 tahap. *Activity* 1 *Describe Current Protection Strategy*, *Activity* 2 Select Mitigation Approaches, Activity 3 *Develop Risk Mitigation Plans*, *Activity* 4 *Identify Changes to Protection Strategy*, dan *Activity* 5 *Identify Next Steps*.

Selama mengevaluasi OCTAVE-S, tim analisis melihat keamanan dari beberapa prespektif, memastikan bahwa rekomendasi yang dicapai sesuai dengan keseimbangan berdasarkan kebutuhan organisasi [1].

III. METODE PENELITIAN

Sifat penelitian ini adalah penelitian deskriptif. Penelitian deskriptif bertujuan untuk menggambarkan tentang ciri-ciri tertentu menggunakan sebuah prosedur penelitian dengan ketentuan-ketentuan yang baku [4]. Penelitian ini mendeskripsikan langkah-langkah keamanan yang diambil oleh bagian Unit Pelaksana Teknis Teknologi Informasi dan bagian Unit Pelaksana Teknis.



Gambar 1. Alur penelitian

Gambar 1 menjelaskan Alur dalam penelitain ini. Langkah awal yang dilakukan adalah perencanaan yaitu melakukan studi pendahuluan, perumusan masalah dan menentukan tujuan penelitian. Selanjutnya pengumpulan data dengan menggunakan metode *observasi* dan wawancara. Dari hasil wawancara dan *observasi* ditentukan sejauh mana setiap praktik Keamanan digunakan oleh organisasi. Serta menentukan sudah atau belum praktek keamanan tersebut dilakukan oleh organisasi. Dan memberikan status berupa tanda (merah, hijau, kuning) untuk masing-masing area praktik keamanan. Terakhir membuat laporan yang berupa formulir kebijakan keamanan pada hotel Java Heritage.

IV. PEMBAHASAN

Dari hasil observasi dan wawancara kepada pihak hotel Java Heritage didapati beberapa hal kebijakan keamanan yang belum dikerjakan. Tabel 1 merupakan pelaksanaan dari langkah 3a. Peneliti menanyakan praktek kebijakan keamanan yang ada pada hotel Java Heritage.

ISBN: 978-602-60280-1-3

Tebel 1 formulir penilaian pemenuhan kebijakan keamana (langkah 3a)

P.4 Kebijakan Keamanan dan Peraturan	
Organisasi memiliki kumpulan dokumentasi yang menyeluruh dan kebijakan terkini yang secara periodik ditinjau serta diperbarui.	**Agak Sesuai**
Ada proses terdokumentasi untuk manajemen dari kebijakan keamanan, yang meliputi pembuatan kebijakan, administrasi (termasuk *review* dan pembaruan periodik), dan komunikasi	**Sesuai**
Organisasi memiliki proses terdokumentasi untuk mengevaluasi dan memastikan informasi sesuai dengan kebijakan keamanan, hukum dan aturan yang berlaku, dan jaminan yang dibutuhkan	**Agak Sesuai**
Organisasi secara seragam menegakkan kebijakan keamanannya.	**Agak Sesuai**
P.5 Manajemen Keamanan Kolaboratif	
Organisasi memiliki kebijakan dan prosedur untuk melindungi informasi ketika bekerja sama dengan organisasi lain	**Tidak Sesuai**
Terdapat dokumen yang menginformasikan keamanan yang dibutuhkan dan secara tegas dikomunikasikan dengan pihak ketiga	**Tidak Sesuai**
Terdapat mekanisme resmi untuk verifikasi ke semua pihak organisasi, *outsource* layanan keamanan, mekanisme dan teknologi, agar seusai dengan kebutuhan dan persyaratan.	**Agak Sesuai**
Terdapat prosedur dan kebijakan untuk berkolaborasi dengan organisasi lain seperti, Memberikan layanan *training* dan kesadaran keamanan, Membangun kebijakan keamanan untuk organisasi., dan Membangun perencanaan terpadu untuk organisasi	**Tidak Sesuai**

Tabel 2 memuat area yang kurangan dalam pemenuhan kebijakan keamanan pada hotel Java Heritage. Hasil tersebut didapatkan dari pelaksanaan langkah 3a.

Tabel 2 Kekurangan dalam pemenuhan Kebijakan Keamanan Octave-S (langkah 3b)

Area	**Apa kekurangan perusahaan di dalam area ini?**
4. Kebijakan Keamanan dan Peraturan	Belum ada peraturan tertulis mengenai peraturan untuk keamanan.
5. Manajemen Keamanan Kolaboratif	Tidak adanya prosedur dan peraturan baku dalam perlindungan informasi dan untuk melakukan kerjasama dengan pihak lain.
6. Perencanaan *Contingency*	Belum dilakukannya dokumentasi atas terjadinya bencana, kesadaran dan pemahaman lain akan rencana kemungkinan pemulihan belum cukup baik.
7. Pengendalian Akses Fisik	Masih bayak orang yg tidak berkepentingan masuk ke area terlarang, dan belum maksimalnya pengamanan area terlarang.
8. Pemantauan dan Audit Keamanan Fisik	Belum melakukan sepenuhnya dalam mencatat audit dan pemantauan secara rutin diperiksa terhadap kesalahan.
15. Manajemen Insiden	Tidak adanya kebijakan dan prosedur yang didokumentasikan untuk bekerja dengan lembaga penegak hukum. Belum juga adanya kerjasama dengan pihak ketiga sehingga tidak adanya verifikasi secara resmi

Dari kekurangan yang telah dijabarkan pada tabel 2 selanjutnya penulis melakukan pemberian tanda berupa spotlight merah(*red*), kuning(*yellow*) dan hijau(*green*). Pemberian tanda berupa spotlight didasarkan atas hasil penilaian yang dilakukan pada langkah 3a. Adapun keterangan dari tanda yang diberikan pertama merah menandakan area praktek Kebijakan keamanan belum dilakukan dan atau memiliki banyak kekurangan, kuning menandakan praktek Kebijakan keamanan sudah dilakukan namun masih ada kekurangan dalam pelaksanaan. Dan hijau menunjukan bahwa praktek Kebijakan keamanan sudah dijalankan secara maksimal.

Tabel 3 Stoplight Praktek Kebijakan Keamanan (langkah 4)

Area	***Red***	***Yellow***	***Green***
4. Kebijakan Keamanan dan Peraturan	X		
5. Manajemen Keamanan Kolaboratif	X		
6. Perencanaan *Contingency*	X		
7. Pengendalian Akses Fisik	X		
8. Pemantauan dan Audit Keamanan Fisik	X		
15. Manajemen Insiden	X		

Tabel 3 menjelaskan mengenai area kebijakana keamanan yang mendapatkan tanda stoplight merah yang menjadikan area kebijakan keamanan tersebut perlu mendapatkan perhatian khusus dikarenakan tidak atau belum dikerjakan secara maksimal. Pada area Kebijakan Keamanan dan Peraturan mendapatkan stoplight merah karena belum ada peraturan tertulis mengenai peraturan untuk keamanan. Sehingga dimungkinkan akan berdampak kepada ketidak tahuan karyawan hotel Java Heritage dalam mengamankan aset-aset hotel Java Heritage.

Pada area Manajemen Keamanan Kolaboratif dikarenakan tidak adanya prosedur dan dokumen yang baku atas kerjasama pihak hotel Java Heritage dengan pihak ke-3. Pada area Perencanaan Contingency, hotel Java Heritage belum memiliki dokumentasi atas bencana atau bahkan data

ISBN: 978-602-60280-1-3

pemulihan atas bencana yang selama ini telah terjadi pada hotel Java Heritage. Ini dapat menyebabkan hotel Java Heritage tidak efektif mengatasi bencana atau masalah yang sama saat terjadi kembali dikemudian hari.

Selain itu hotel Java Heritage juga lemah dalam pengendalia akses fisik, hal ini tercermin dari masih ada orang yang masuk kearea terlarang tanpa ada himbauan atau teguran dari pihak berwenang. Dan permasalahan ini juga diperkuat dengan tidak adanya Pemantauan dan Audit Keamanan Fisik.

Terakhir adalah Manajemen Insiden dimana pihak hotel Java Heritage tidak melakukan kerjasama khusus dengan pihak penegak hokum yang ada sehingga dikawatirkan akan menyebabkan kurangnya perhatian penegak hokum atas insiden yang mungkin terjadi pada hotel Java Heritage dikemudian hari.

V. KESIMPULAN DAN SARAN

1. Simpulan

Dari penelitian ini dapat disimpulkan:

a. Kerangka kerja Octave-s mampu menjabarkan dengan baik area kebijakan keamanan apa saja yang perlu diperhatiakan dalam melakukan pengamanan system.

b. Ditemukan area yang kurang dalam pemenuhan kebijakan keamanannya yaitu area Kebijakan Keamanan dan Peraturan, area Manajemen Keamanan Kolaboratif, area Perencanaan Contingency, area Pengendalian Akses Fisik,. Area Pemantauan dan Audit Keamanan Fisik, serta area. Dan area Manajemen Insiden

2. Saran

Saran untuk penelitian selanjutnya adalah melakukan mitigasi pada area yang kurang dalam melakukan kebijakan keamanan. Serta melakukan penilaian risiko secara menyeluruh sehingga dapat meninimalisir kerugian atas risiko yang mungkin muncul

DAFTAR PUSTAKA

[1] Alberts, C., Dorofee, A., Stecens, J.,Woody, C., (2005), OCTAVE-S Implementation Guide Version 1.0., Caenegie Mellon University, USA.

[2] https://id.scribd.com/document/51590534/kebijakan-keamanan , diakses 5 juli 2018

[3] https://netsec.id/security-policy/ diakses 5 juli 2018

[4] Sukandarrumidi. (2012). Metodologi Penelitian. Yogyakarta: UGM Press.