UNIVERSITAS PERTAHANAN

STRATEGI KEAMANAN INFORMASI DALAM MENGHADAPI ANCAMAN SIBER PADA SISTEM PENGADAAN SECARA ELEKTRONIK (STUDI SERANGAN HACKER PADA SPSE PROVINSI LAMPUNG TAHUN 2015)

ADI WIJAYA

NIM: 120170102001

Tesis yang ditulis untuk Memenuhi Sebagian Persyaratan
dalam Mendapatkan Gelar Magister Pertahanan

FAKULTAS STRATEGI PERTAHANAN

PROGRAM STUDI PEPERANGAN ASIMETRIS

BOGOR

FEBRUARI 2019

UNIVERSITAS PERTAHANAN

STRATEGI KEAMANAN INFORMASI DALAM MENGHADAPI ANCAMAN SIBER PADA SISTEM PENGADAAN SECARA ELEKTRONIK (STUDI SERANGAN HACKER PADA SPSE PROVINSI LAMPUNG TAHUN 2015)

ADI WIJAYA

NIM: 120170102001

Tesis yang ditulis untuk Memenuhi Sebagian Persyaratan
dalam Mendapatkan Gelar Magister Pertahanan

FAKULTAS STRATEGI PERTAHANAN

PROGRAM STUDI PEPERANGAN ASIMETRIS

BOGOR

FEBRUARI 2019

LEMBAR PENGESAHAN

Penelitian ini diajukan oleh:

Nama	:	Adi Wijaya
NIM	:	120170102001
Program Studi	:	Peperangan Asimetris
Judul	:	Strategi Keamanan Informasi Dalam Menghadapi Ancaman Siber Pada Sistem Pengadaan Secara Elektronik (Studi Serangan Hacker Pada SPSE Provinsi Lampung Tahun 2015)

Tesis telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai persyaratan yang diperlukan untuk memperoleh gelar Magister dalam Ilmu Pertahanan pada Program Studi Peperangan Asimetris, Fakultas Strategi Pertahanan, Universitas Pertahanan.

DEWAN PENGUJI

Pembimbing I	:	Laksamana Pertama TNI Dr. Suhirwan, S.T., M.MT.	( )
Pembimbing II	:	Kolonel Sus. Dr. Ir. Rudy AG Gultom, M.Sc.	( )
Penguji I	:	Brigjen TNI Dr. Moch. Afifuddin, M.Si (Han).	( )
Penguji II	:	Kolonel Kav. Dr. Yusuf S.Sos., M.M.	( )
Penguji III	:	Letkol Inf. Dr. Triyoga Budi Prasetyo, M.Si	( )

Ditetapkan di : Bogor

Tanggal : 19 Februari 2019

PERNYATAAN ORISINALITAS

Dengan ini saya menyatakan bahwa dalam tesis ini tidak terdapat karya atau bagian dari karya yang pernah diajukan untuk memperoleh gelar kesarjanaan jenjang apapun di suatu Perguruan Tinggi; dan sepanjang sepengetahuan saya juga tidak terdapat istilah, frasa, kalimat, paragraf, subbab atau bab dari karya yang pernah saya tulis atau terbitkan; kecuali yang secara tertulis diajukan dalam naskah ini dan disebutkan dalam daftar referensi.

Apabila dikemudian hari terbukti bahwa terdapat plagiat dalam tesis ini, saya bersedia menerima sanksi sesuai dengan ketentuan peraturan/undang-undang yang berlaku.

Bogor, Februari 2019

Adi Wijaya

PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH
UNTUK KEPENTINGAN AKADEMIS

Tesis ini diajukan oleh :

Nama : Adi Wijaya

NIM : 120170102001

Program Studi : Peperangan Asimetris

Fakultas : Strategi Pertahanan

Jenis Karya : Tesis

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pertahanan Hak Bebas Royalty Noneksekutif (*Non-executive Royalty-Free Right*) atas karya ilmiah saya berjudul :

Strategi Keamanan Informasi Dalam Menghadapi Ancaman Siber Pada Sistem Pengadaan Secara Elektronik (Studi Serangan Hacker Pada Spse Provinsi Lampung Tahun 2015)

Beserta perangkat yang ada jika diperlukan. Dengan hak bebas Royalty Noneksekutif ini Universitas Pertahanan berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (database), merawat dan mempulikasikan Tesis saya selama tetap mencantumkan nama saya sebagai penulis dan sebagai pemilik Hak Cipta/Karya Intelektual dari Tesis ini.

Demikian pernyataan ini saya buat dengan kesadaran penuh tanpa paksaan dari pihak manapun.

Bogor, 19 Februari 2019

Adi Wijaya

KATA PENGANTAR

Alhamdulillah, puji syukur peneliti panjatkan kehadirat Allah SWT., Tuhan Yang Maha Esa, karena berkat rahmat dan karunia-Nya penyusunan tesis dengan judul **"Strategi Keamanan Informasi Dalam Menghadapi Ancaman Siber Pada Sistem Pengadaan Secara Elektronik (Studi Serangan *Hacker* Pada SPSE Provinsi Lampung Tahun 2015)",** dapat diselesaikan.

Penyusunan tesis ini ditujukan sebagai salah satu syarat dalam memperoleh gelar Magister pada Program Studi Peperangan Asimetris Fakultas Strategi Pertahanan Universitas Pertahanan.

Penyusunan tesis ini dapat diselesaikan berkat bantuan dan dukungan dari berbagai pihak baik secara langsung maupun tidak langsung. Untuk itu, pada kesempatan ini peneliti mengucapkan terima kasih kepada:

1. Letjen TNI Dr. Tri Legionosuko, S.IP., M.AP selaku Rektor Universitas Pertahanan;
2. Mayjen TNI Dr. Hipdizah, S.Adm., M.Si., selaku Dekan Fakultas Strategi Pertahanan;
3. Laksamana Pertama TNI Dr. Suhirwan selaku Wakil Dekan Fakultas Strategi Pertahanan sekaligus Pembimbing I;
4. Kolonel Kav. Dr. Yusuf, S.Sos., MM., selaku Sesprodi Peperangan Asimetris;
5. Kolonel Sus. Dr. Ir. Rudy Gultom, M.Sc selaku Pembimbing II;
6. Seluruh dosen pengajar di Universitas Pertahanan khususnya dosen Program Studi Peperangan Asimetris;
7. Para Narasumber yang telah memberikan waktu dan pikirannya dalam membantu memberikan data kepada peneliti;
8. Para penguji baik pada saat ujian pra-proposal, seminar proposal , pra-tesis dan ujian tesis;
9. Rekan-rekan kerja di Bagian Pengadaan Barang dan Jasa Setda Kabupaten Tanggamus yang turut membantu dan mendukung dalam penyusunan tesis ini;
10. Orang tua yang selalu mengiringi perjalanan studi di Universitas Pertahanan dengan doa dan dukungannya; dan
11. Teman-teman Program Studi Peperangan Asimetris Cohort 6 Universitas Pertahanan.

Semoga Allah SWT., Tuhan Yang Maha Esa membalas kebaikan-kebaikan berbagai pihak atas bantuannya.

Peneliti menyadari bahwa tesis ini masih kurang dari sempurna, oleh karena itu dengan kerendahan hati mengharapkan kritik dan saran yang konstruktif demi perbaikan kedepan.

Akhirnya, semoga tesis ini dapat memberikan manfaat terhadap pengembangan ilmu pertahanan dan bermanfaat bagi *stakeholder* terkait strategi Keamanan Informasi Dalam Menghadapi Ancaman Siber Pada Sistem Pengadaan Secara Elektronik.

Bogor, 19 Februari 2019

Adi Wijaya

ABSTRAK

STRATEGI KEAMANAN INFORMASI DALAM MENGHADAPI ANCAMAN SIBER PADA SISTEM PENGADAAN SECARA ELEKTRONIK (STUDI SERANGAN HACKER PADA SPSE PROVINSI LAMPUNG TAHUN 2015)

ADI WIJAYA

Keamanan Informasi di era perkembangan teknologi saat ini telah menjadi kebutuhan yang wajib di penuhi, sebab perkembangan teknologi yang pesat menyebabkan celah kerentanan terhadap sistem informasi. Pemerintah sebagai salah satu pemanfaat teknologi telah melahirkan sistem *elektronik procurement* yang merupakan bentuk dari *elektronik goverment*. Dengan adanya sistem ini proses pengadaan barang dan jasa dilakukan secara elektronik dengan memanfaatkan teknologi informasi. Sistem ini di sebut dengan Sistem Pengadaan Secara Elektronik (SPSE). Beralihnya proses pengadaan barang/jasa ke dalam sistem elektronik, justru menimbulkan kerentanan terhadap keamanan dari sistem informasi tersebut. Hal ini menyebabkan terjadinya beberapa serangan *hacker* pada sistem tersebut. SPSE Provinsi Lampung merupakan salah satu dari sekian banyak SPSE di Indonesia yang menjadi sasaran serangan *hacker*. Dimana pada tahun 2015 SPSE Provinsi Lampung mendapat serangan *hacker* yang mengakibatkan ratusan paket yang sedang proses tander harus tander ulang dan berdampak pada keterlambatan pengadaan barang dan jasa di Pemerintah Provinsi Lampung. Maka, oleh sebab itu dibutuhkan suatu strategi keamanan informasi yang dapat mencegah terjadinya serangan *hacker* maupun ancaman siber lain. Dalam membangun strategi tersebut maka dibutuhkan teori strategi dan model keamanan informasi yang tepat mampu menghadapi berbagai macam ancaman siber. Sehingga pelaksanaan penelitian ini menggunakan model keamanan informasi *defense in depth* untuk membangun strategi tersebut. Penelitian ini akan menggunakan metode penelitian kualitatif dengan berdasarkan studi serangan *hacker* pada SPSE Provinsi Lampung tahun 2015. Penelitian ini juga memuat rekomendasi yang dapat digunakan oleh LPSE Provinsi Lampung untuk peningkatan keamanan informasi pada sistem pengadaan secara elektronik.

Kata Kunci : Keamanan Informasi, Ancaman Siber, Strategi, SPSE Provinsi Lampung

ABSTRACT

INFORMATION SECURITY STRATEGY TO COUNTER CYBER THREATS IN ELECTRONIC PROCUREMENT SYSTEMS (STUDY OF HACKER ATTACKS IN SPSE PROVINSI LAMPUNG 2015)

ADI WIJAYA

Information security in the current era of technological development has become a necessity that must be fulfilled, because rapid technological developments cause vulnerabilities to information systems. The government as one of the technology users has produced a procurement electronic system which is a form of electronic government. With this system the process of procuring goods and services is done electronically by utilizing information technology. This system is called the Sistem Pengadaan Secara Elektronik (SPSE). The shifting of the process of procuring goods / services into an electronic system actually creates vulnerability to the security of the information system. This causes several hacker attacks on the system. SPSE Provinsi Lampung is one of the many SPSE in Indonesia which was the target of hacker attacks. Where in 2015 SPSE Provinsi Lampung got a hacker attack which resulted in hundreds of packages being tandered to have to be reset and resulted in delays in the procurement of goods and services in the Provinsi Lampung Government. Therefore, an information security strategy is needed that can prevent hacker attacks and other cyber threats. In developing this strategy, the right strategy theory and information security model are needed to be able to deal with various cyber threats. So that the implementation of this research uses a defense in depth information security model to develop this strategy. This study will use a qualitative research method based on a hacker attack study at the Provinsi Lampung SPSE in 2015. This study also contains recommendations that can be used by LPSE Provinsi Lampung to improve information security on an electronic procurement system.

Keywords : Information Security, Cyber Threat, Strategy, SPSE Provinsi Lampung

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

BAB I
PENDAHULUAN

1.1. Latar Belakang

Teknologi kini telah menjadi kebutuhan bagi setiap orang, dengan adanya teknologi semua bisa menjadi lebih mudah dan cepat. Perkembangan teknologi saat ini telah memasuki era revolusi industri 4.0, era ini ditandai dengan segala sesuatu yang kini telah berbasis teknologi informasi dan komunikasi dimana internet digunakan sebagai media pertukaran informasi tersebut. Dengan adanya pemanfaatan teknologi informasi dan komunikasi ini segala sesuatu kini bisa diakses dengan mudah melalui internet. Perkembangan teknologi informasi dan komunikasi dengan memanfaatkan teknologi internet kini semakin canggih dan kompleks. Seiring dengan hal tersebut, manusia sebagai pemilik dan pemakai teknologi itu sendiri terus meningkatkan pemanfaat dari teknologi informasi dan komunikasi tersebut agar sesuai dengan apa yang diharapkan. Hasilnya, kini teknologi telah dapat menembus berbagai aspek kehidupan. Pemanfaatan teknologi informasi dan komunikasi sendiri saat ini telah banyak digunakan dalam bidang pendidikan, pertanian, perindustrian, dan juga pemerintahan.

Pemerintah sebagai organisasi yang memiliki kewajiban memberikan pelayanan publik yang merata keseluruh warga negara, harus senantiasa berusaha memperbaiki kualitas pelayanannya. Peningkatan kualitas pelayanan tersebut dapat dilaksanakan dengan menggunakan teknologi informasi yang sesuai dengan kebutuhan organisasi yang mampu mengelola data dengan cepat, efektif dan efisien serta menghasilkan informasi yang tepat, cepat, dan akurat. Di dalam Undang-Undang Republik Indonesia Nomor 14 tahun 2008, menyebutkan bahwa “Untuk mewujudkan pelayanan cepat, tepat, dan sederhana setiap Badan Publik: Menunjuk Pejabat Pengelola Informasi dan Dokumentasi; dan Membuat dan mengembangkan sistem penyediaan layanan informasi

secara cepat, mudah, dan wajar sesuai dengan petunjuk teknis standar layanan Informasi Publik yang berlaku secara nasional."[1] Pada sektor pelayanan publik yang dilakukan oleh pemerintah, perkembangan teknologi informasi dan komunikasi telah melahirkan model pelayanan publik yang dilakukan melalui *e-government*.

Dasar dari pelaksanaan *e-government* adalah instruksi Presiden No 3 tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan e-*government* yang berangkat dari pemikiran tentang pertimbangan pemanfaatan teknologi komunikasi dan informasi dalam proses pemerintahan yang diyakini akan meningkatkan efesiensi, efektifitas, transparansi serta akuntabilitas penyelenggaraan pemerintahaan. Sedangkan tujuan dari pelaksanaan *e-government* adalah mengembangkan penyelenggaraan kepemerintahan yang berbasis (menggunakan) elektronik dalam rangka meningkatkan kualitas layanan publik secara efektif dan efisien. Melalui pengembangan e-government dilakukan penataan sistem manajemen dan proses kerja di lingkungan pemerintah dengan mengoptimasikan pemanfaatan teknologi informasi.[2]

E-government menjadi sangat popular sejalan dengan perkembangan teknologi informasi dan komunikasi. Berbagai Negara dibelahan dunia berlomba mengimplementasikan *e-government* dengan strategi yang disesuaikan dengan kondisi sosial politik serta geografisnya masing-masing, yang tujuan akhirnya diharapkan meningkatkan kualitas kinerja pemerintah terutama dalam lingkup pelayanan masyarakat sehingga dapat bermanfaat bagi segenap warga negaranya. Bahkan di Indonesia khususnya di daerah-daerah yang telah mengimplementasikan *e-government* dengan strategi yang telah direncanakan di daerah tersebut. Dapat dikatakan bahwa *e-government* adalah penyelenggaraan kepemerintahan yang berbasis elektronik. Dengan menerapkan

[1] Undang-Undang Republik Indonesia Nomor 14 tahun 2008, Bab IV Pasal 13 ayat 1 huruf a, b

[2] Instruksi Presiden No 3 tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan E-Government

e-government diharapkan mutu pelayanan kepada publik dapat lebih ditingkatkan, baik dari segi efisiensi dan efektivitas biaya, maupun dari segi implementasinya yang menjadi lebih mudah dan transparan. Salah satu produk dari *e-government* yang sudah banyak diterapkan di intansi pemerintah ialah *e-procurement* atau pengadaan secara elektronik.

E-procurement adalah proses pengadaan barang dan jasa secara online melalui internet, dimana seluruh proses pengumuman, pendaftaran, proses penawaran, *aanwijzing*, hasil evaluasi atas penawaran dilakukan dengan memanfaatkan sarana teknologi informasi.[3] *E-procurement* dapat dilakukan melalui dua cara yang terdiri dari *e-tendering* dan *e-purchasing.*

Sebelum adanya konsep *e-procurement*, Pengadaan barang dan jasa masih menggunakan cara manual yaitu dengan mempertemukan langsung pihak-pihak yang terkait seperti penyedia barang dan jasa dengan panitia pengadaan. Proses yang dilakukan secara manual ini memiliki beberapa kelebihan dan kelemahan. Kelebihan yang didapat yaitu para pengguna dan penyedia barang dan jasa dapat mengetahui proses pengadaan yang berlangsung secara bersama-sama. Tetapi kelemahan dari tahap-tahap pelaksanaan pengadaan barang dan jasa konvesional dirasa kurang efektif pada waktu dan biaya.

Dari sudut pandang tersebut, pemerintah akhirnya menentukan langkah positif dengan menerapkan *e-procurement* untuk seluruh instansi pemerintah. Untuk mendukung aktifitas pengadaan barang dan jasa, beberapa instansi pemerintah mendirikan pusat-pusat Layanan Pengadaan Secara Elektronik (LPSE). Dasar Hukum pembentukan LPSE adalah Peraturan Presiden pasal 111 Nomor 54 tahun 2010 tentang pengadaan barang atau jasa pemerintah yang diubah menjadi Peraturan Presiden Nomor 70 Tahun 2012 tentang pengadaan barang atau jasa pemerintah yang ketentuan teknis operasionalnya diatur oleh Kepala Lembaga Kebijakan Pengadaan Barang Jasa Pemerintah didahului

[3] Mochammad Jasin, *Mencegah Korupsi Melalui E-procurement,* (Jakarta : Komisi Pemberantasan Korupsi, 2007), hlm. 3.

dengan kalimat yang disingkat LKPP Nomor 2 Tahun 2010 tentang Layanan pengadaan Barang atau Jasa secara elektronik. LPSE dalam menyelenggarakan sistem pelayanan Pengadaan barang atau jasa secara elektronik juga wajib memenuhi persyaratan sebagaimana yang ditentukan dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Pusat layanan ini mengelola segala sesuatu yang berkaitan dengan proses elektronik dalam pengadaan barang dan jasa pemerintah. Layanan Pengadaan Secara Elektronik (LPSE) diimplementasikan dalam bentuk pengadaan barang dan jasa secara elektronik yang memfasilitasi proses lelang secara elektronik. Aplikasi Sistem Pengadaan Secara Elektronik (SPSE) merupakan aplikasi e-pengadaan yang dikembangkan oleh Lembaga Kebijakan Pengadaan barang atau jasa Pemerintah (LKPP) untuk digunakan oleh instansi seluruh Indonesia.

E-procurement memberikan cukup banyak manfaat dan kemudahan bagi instansi yang menerapkannya, salah satunya dengan terciptanya efisiensi waktu dan pengurangan biaya administrasi. Adapun *e-procurement* dianggap efisien dan efektif dikarenakan pengadaan barang dan jasa ini diusahakan dengan menggunakan dana dan daya yang terbatas untuk mencapai sasaran yang ditetapkan dalam waktu sesingkat-singkatnya dan dapat dipertanggung jawabkan. Aplikasi ini dapat diakses melalui website dengan situs yang telah ditetapkan oleh LPSE instansi terkait. Dengan diadakannya sistem ini diharapkan menjadi sebuah sistem yang dapat memutus rantai korupsi, mewujudkan transparansi dan menciptakan persaingan usaha yang sehat.

Namun dengan memanfaatkan teknologi infomasi pada sistem pengadaan barang dan jasa, justru menimbulkan kendala tersendiri. Hal ini disebabkan dengan menggunakan sistem pengadaan secara elektronik yang berbasis teknologi informasi menyebabkan kerentanan terhadap keamanan dari sistem informasi itu sendiri. Sehingga pada pelaksanaanya, sistem *e-procurement* ini kerap kali terganggu oleh

berbagai ancaman siber. Salah satu ancaman siber yang kerap kali mengganggu pelaksanaan sistem *e-procurement* ialah serangan *hacker*. Akibat serangan *hacker* tersebut membuat pemenuhan kebutuhan akan layanan publik khususnya pada layanan pengadaan barang/jasa di pemerintah menjadi tidak maksimal. Di Indonesia sendiri banyak sekali terjadi kasus serangan *hacker* yang menyerang sistem pengadaan secara elektronik. Beberapa kasus serangan hacker tersebut dapat dilihat pada tabel di bawah ini :

Tabel 1.1 Data Serang Siber di Indonesia

No	Instansi	Tahun	Serangan	Dampak
1	LPSE Provinsi Lampung	2015	*Hacker*	166 paket tender ulang
2	LPSE Kabupaten Mesuji	2015	*Hacker*	Website tidak bisa di akses
3	LPSE Kementerian PUPR	2016	*Hacker*	Penyedia tidak bisa login
4	LPSE Pemkab Mojokerto	2016	*Hacker*	Tender ulang

(Sumber : Dikelola oleh Peneliti)

Pada tahun 2015, terjadi peretasan pada Sistem Pengadaan Secara Elektronik (SPSE) provinsi Lampung. Pada tanggal 22 April 2015 SPSE Provinsi Lampung mengalami kerusakan server akibat serangan *hacker*. Dampak dari serang tersebut membuat 166 dari 168 paket yang sedang proses lelang harus tender ulang.[4] Peretasan-peretasan yang dilakukan oleh para hacker terhadap Sistem Pengadaan Secara Elektronik ini tentu sangat mengganggu jalannya proses pemerintah sehingga program yang harusnya bisa dikerjakan sesuai jadwal menjadi tertunda akibat serangan *hacker* ini. Di tahun yang sama dengan LPSE Provinsi

[4] Yulianto, Beni. "Awalnya Diserang Hacker, Katanya Sudah Bisa Diakses, Nyatanya Tak Bisa" Dalam http://lampung.tribunnews.com/2015/05/23/awalnya-diserang-hacker-katanya-sudah-bisa-diakses-nyatanya-tak-bisa diakses pada 28 juli 2018

Lampung yaitu tahun 2015, LPSE Kabupaten Mesuji juga mendapat serangan hacker. Akibat ulah *hacker* tersebut menyebabkan website LPSE Kabupaten Mesuji tidak dapat di akses atau di buka sehingga dokumen tidak dapat diunduh. Serangan hacker tersebut juga telah mengganggu sistem yang ada.[5]

Pada tahun 2016, terjadi peretasan yang dilakukan oleh *hacker* dengan modus memanipulasi akses LPSE milik Kementerian PUPR dengan cara menerobos atau menjebol sistem pengamanan dengan melakukan *SQL Injection* ke situs Kementerian PUPR, sehingga terdapat laporan dari beberapa penyedia jasa yang tidak dapat login ke dalam sistem LPSE terkait proses lelang.[6] Selain itu, terjadi juga peretasan terhadap situs LPSE Pemkab Mojokerto di tahun yang sama yaitu tahun 2016, akibat peretasan ini membuat proses lelang secara online lumpuh dan mengakibatkan pihak LPSE Pemkab Mojokerto melakukan tender ulang terhadap proyek-proyek yang gagal tender.[7]

Padahal di dalam Buku pertahanan Indonesia tahun 2015, disebutkan bahwa Pemerintah Daerah merupakan bagian dari unsur lain kekuatan bangsa dalam postur pertahanan nirmiliter Indonesia untuk menghadapi ancaman yang bersifat non militer. Ini artinya bahwa pemerintah daerah memiliki peran penting untuk menghadapi ancaman yang bersifat non militer. Dimana salah satu ancaman non militer tersebut ialah ancaman siber. Ancaman siber ini dapat menyebabkan terganggunya sistem pemerintah daerah yang berbasis teknologi informasi. Dan terganggunya sistem pemerintah daerah akan berdampak pada melemahnya sistem pertahanan nirmiliter, sehingga akan

[5] Alzoni. “Situs Mesuji Kerap Dihacker”. Dalam http://le-ut.blogspot.com/2015/08/situs-lpse-mesuji-kerap-dihacker.html diakses pada 4 Agustus 2018

[6] Kurniawati, Putri. “Hacker Pembobol LPSE Kementerian PUPR Terancam Kurungan Empat Tahun Penjara” Dalam https://www.kupastuntas.co/2016/08/hacker-pembobol-lpse-kementerian-pupr-terancam-kurungan-empat-tahun-penjara/ diakses pada 4 Agustus 2018

[7] Julan, Tritus. “Laman LPSE Diretas, Proses Lelang Kacau” Dalam http://koran-sindo.com/page/news/2016-05-10/6/47/Laman_LPSE_Diretas_Proses_Lelang_Kacau diakses pada 4 Agustus 2018

berdampak pula pada stabilitas keamanan nasional. Oleh sebab pemerintah daerah sebagai unsur lain kekuatan bangsa dalam postur pertahanan nirmiliter harus mampu menghadapi ancaman yang bersifat non militer salah satunya ancaman siber.

Untuk menghadapi ancaman siber tersebut maka dibutuhkan pula suatu sistem keamanan yang dapat melindungi sistem informasi tersebut. Hal ini dilakukan agar pemanfaatan dari teknologi informasi pada sistem pengadaan secara elektronik dapat lebih maksimal. Keamanan informasi harus memiliki kehandalan yang tinggi agar dapat mengurangi dan meminimalisir resiko atas kerugian yang mungkin timbul, terkait dengan penggunaan teknologi informasi. Penentuan kebijakan dalam perencanaan keamanan informasi, sebaiknya bukan hanya berdasarkan anggaran yang tersedia, tetapi berdasarkan hasil penilaian/penaksiran resiko keamanan informasi dan strategi untuk menurunkan resiko.

Perencanaan keamanan informasi sebaiknya dilakukan dengan terlebih dahulu melakukan penilaian resiko keamanan informasi dalam rangkaian pengelolaan resiko (*risk management*), yang dapat memberikan informasi secara komprehensif mengenai kerawanan kelemahan (*vulnerability*) dan ancamanan (*threats*) yang mungkin akan dihadapi oleh oraganisasi dimasa yang akan datang.

Beberapa kerangka kerja seperti *ISO/IEC 27001*, *Control Objectives for Information and related Technology (COBIT)*, dan *Defense in Depth* dapat digunakan sebagai dasar atau model untuk membangun dan mengembangkan suatu sistem keamanan informasi. Standar *ISO/IEC 27001* menetapkan persyaratan untuk mendesain dan implementasi sistem manajemen keamanan data yang tepat dalam suatu organisasi, memastikan bahwa kontrol yang memadai dan proporsional dipilih untuk melindungi aset informasi dan memberikan kepercayaan kepada pihak yang berkepentingan. Pada kerangka kerja *COBIT* digunakan sebagai panduan untuk mengarahkan pada *IT governance* yang dapat membantu auditor, manajemen dan pengguna (*user*) untuk menjembatani pemisah

antara resiko bisnis, kebutuhan kontrol, dan permasalahan-permasalahan teknis. Sedangkan pada kerangka kerja *Defense In Depth* memberikan model untuk membangun suatu strategi keamanan informasi dengan menggunakan pertahanan berlapis, artinya semua aspek di dalam sistem informasi akan di lindungi yang meliputi aspek *Governance, People, Processes* dan *Technology*.

Berdasarkan data dari sirup.lkpp.go.id, LPSE Provinsi Lampung sejak tahun 2014 hingga 2018 mengelola pengadaan barang dan jasa yang terdiri dari ribuan paket pengadaan dengan total nilai pagu mencapai triliyunan rupiah. Berikut data paket pengadaan yang dikelola LPSE provinsi Lampung dari tahun 2014 sampai 2018 :

Tabel 1.2 Paket Pengadaan Provinsi Lampung

No.	Tahun	Paket	Pagu
1	2014	2.462	Rp. 1.382.665.270.906
2	2015	2.417	Rp. 1.946.003.028.749
3	2016	2.061	Rp. 1.651.891.384.580
4	2017	2.167	Rp. 2.215.081.648.507
5	2018	1.585	Rp. 2.139.414.806.463

(Sumber: https://sirup.lkpp.go.id/sirup/home/rekapitulasiindex)

Berdasarakan data tersebut kita bisa melihat bahwa peran LPSE provinasi Lampung sangat penting dalam mendukung jalannya pemerintahan provinsi Lampung. Jika sistem pengadaan secara elektronik terganggu maka akan terganggunya program-program yang ada di pemerintah provinsi Lampung, dimana akan berakibat pula pada terhambatnya pelaksanaan pekerjaan di pemerintah provinsi Lampung. Oleh Sebab itu jika ancaman siber ini tidak ditangani secara serius maka dapat mengganggu dan menghambat program-program pemerintah, khususnya pemerintah provinsi Lampung. Maka dari hal tersebut diperlukan suatu upaya yang dapat menghadapi ancaman siber pada Sistem Pengadaan Secara Elektronik (SPSE) di masa yang akan datang.

Guna mewujudkan hal tersebut maka diperlukan sebuah strategi yang dapat mengamankan sistem tersebut. Maka peneliti mencoba mengusulkan sebuah strategi keamanan informasi yang dapat mengamankan sistem dari serangan *hacker* maupun ancaman siber lainnya. Maka dari itu peneliti mengambil judul penelitian:

"Strategi Keamanan Informasi dalam menghadapi Ancaman Siber pada Sistem Pengadaan Secara Elektronik (Studi Serangan *Hacker* Pada SPSE Provinsi Lampung Tahun 2015)".

1.2. Fokus dan Sub Fokus Penelitian

1.2.1 Fokus Penelitian

Fokus penelitian dimaksudkan untuk membatasi masalah yang diteliti, dengan adanya penetapan fokus penelitian, peneliti dapat lebih mendekatkan interaksi antara peneliti dengan fokus penelitian. Sehingga dengan fokus tersebut masalah dapat lebih disederhanakan dan semakin mudah untuk diteliti. Fokus pada penelitian ini yaitu membangun sistem keamanan informasi pada Sistem Pengadaan Secara Elektronik Provinsi Lampung.

1.2.2 Sub Fokus Penelitian

Dari fokus penelitian yang telah disebutkan sebelumnya, Selanjutnya agar penelitian dapat dilaksanakan secara lebih spesifik peneliti membagi fokus penelitian tersebut kedalam sub-subfokus penelitian sebagai berikut :

1 Strategi keamanan informasi dalam menghadapi ancaman siber pada Sistem Pengadaan Secara Elektronik Provinsi Lampung.

2 Pelaksanaan LPSE Provinsi Lampung dalam mengamankan sistem informasi pada Sistem Pengadaan Secara Elektronik.

1.3 Rumusan Masalah

Pada dasarnya masalah dalam penelitian kualitatif bertumpu pada suatu fokus.[8] Menurut Lincoln dan Guba sebagaimana yang di kutip oleh J. Moleong, penentu masalah bergantung pada paradigma apakah yang dianut oleh peneliti, yaitu apakah ia sebagai peneliti, evaluator ataukah sebagai peneliti kebijakan.[9] Berdasarkan hal tersebut maka peneliti membuat rumusan masalah berdasarkan pada fokus dan subfokus penelitian. Dimana penelitian ini mengidentifikasi dua permasalahan dalam penelitian yang akan ditemukan jawabannya, yaitu:

1. Bagaimana strategi keamanan informasi dalam menghadapi ancaman siber pada Sistem Pengadaan Secara Elektronik Provinsi Lampung ?
2. Bagaimana pelaksanaan LPSE Provinsi Lampung dalam mengamankan sistem informasi pada Sistem Pengadaan Secara Elektronik ?

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk menyusun dan membangun suatu strategi yang dapat digunakan untuk menghadapi ancaman siber pada Sistem Pengadaan Secara Elektronik (SPSE) Provinsi Lampung dengan menggunakan strategi keamanan informasi. Dan secara spesifik tujuan penelitian ini di turunkan berdasar pada sub fokus penelitian yang telah di tetapkan sebelumnya yaitu:

1. Untuk merancang strategi keamanan informasi dalam menghadapi ancaman siber pada Sistem Pengadaan Secara Elektronik Provinsi Lampung di masa yang akan datang.

[8] J. Moleong, *Metodologi Penelitian Kualitatif*, Edisi Revisi, (Bandung: Remaja Rosdakarya, 2014), hlm. 93.
[9] Ibid.

2. Untuk Menganalisa pelaksanaan LPSE Provinsi Lampung dalam mengamankan sistem informasi pada Sistem Pengadaan Secara Elektronik.

1.5 Manfaat Penelitian

Penelitian ini memiliki beberapa manfaat, baik manfaat secara teoritis maupun manfaat secara praktis.

1.5.1 Manfaat Teoretis

Dengan adanya penelitian ini diharapkan dapat memberikan landasan bagi para peneliti lain dalam melakukan penelitian yang sejenis dalam rangka meningkatkan kemampuan membangun keamanan sistem informasi pada Sistem Pengadaan Secara Elektronik.

1.5.2 Manfaat Praktis

Selain manfaat teoretis yang telah dikemukakan di atas, dengan adanya penelitian ini diharapakan dapat memberikan manfaat praktis berupa rekomendasi strategi yang dapat lebih meningkatkan keamanan informasi untuk menghadapi ancaman siber pada Sistem Pengadaan Secara Elektronik Provinsi Lampung di masa yang akan datang.

BAB II
KAJIAN TEORETIK

2.1 Landasan Teori

Teori adalah satu set konstruk, konsep, definisi, dan proposisi yang saling berhubungan, yang menyajikan suatu pandangan yang sistematik mengenai suatu fenomena dengan menspesifikkan hubungan antar variabel dengan tujuan untuk menjelaskan dan memprediksi fenomena.[10]

Teori dalam sebuah penelitian merupakan hal yang wajib tersedia, hal ini dikarenakan teori dalam sebuah penelitian berfungsi sebagai pisau analisis yang digunakan untuk mengupas masalah yang akan dibahas. Teori yang digunakan akan menuntun peneliti untuk mencapai tujuan dari peneltian dan sebagai kunci keberhasilan dari penelitian itu sendiri. Teori memiliki peranan yang dapat menghubungkan penemuan-penemuan yang tampak berbeda-beda ke dalam keseluruhan dan memperjelas proses-proses di dalamnya. Teori juga berperan dalam memberikan penjelasan terhadap hubungan-hubungan yang diamati dalam suatu penelitian.[11]

Beberapa teori yang digunakan oleh peneliti untuk mendukung pelaksanaan penelitian yang akan dilaksanakan dalam rencana penelitian ini, sebagai berikut :

2.1.1 Ilmu Pertahanan

Menurut Supriyatno, ilmu pertahanan adalah suatu ilmu yang mempelajari bagaimana mengelola sumber daya dan kekuatan nasional pada saat damai, perang dan pada saat sesudah perang guna menghadapi ancaman dari luar dan dari dalam negeri, baik berupa ancaman militer dan non-militer terhadap keutuhan wilayah, kedaulatan

[10] Fred N. & Howard B. Lee. *Foundations of Behavioral Research*. 4th Edition. (Florida: Harcourt Inc. 2000), hlm.11.
[11] Usman Rianse dan Abdi. *Metodologi Penelitian Sosial dan Ekonomi, Teori dan Aplikasi*. (Bandung: Alfabeta, 2009) hlm. 73.

negara, dan keselamatan segenap bangsa dalam rangka mewujudkan keamanan nasional.[12]

Ilmu pertahanan adalah ilmu mengkaji tentang seluruh aspek yang berhubungan dengan keamanan dalam skala nasional yang melekat pada tujuan penyelenggaraan Negara. Kebutuhan untuk mempelajari masalah-masalah pertahanan secara filosofis berangkat dari keberadaan suatu entitas yang disebut Negara (*state*), dan kebutuhan untuk mempertahankan diri (*survive*) dari ancaman-ancaman (*threats*) terhadap Negara.[13]

Ilmu Pertahanan adalah ilmu digunakan untuk menyelesaikan permasalahan–permasalahan Negara yang dilakukan oleh seluruh *stakeholder* sesuai dengan bidang dan profesinya dalam menjamin kelangsungan hidup bangsa, seiring dengan berkembangnya ancaman (*threat*) yang datang.[14]

Dari definisi tersebut, maka secara jelas dapat ditarik kesimpulan bahwa ilmu pertahanan tidak hanya menjadi bagian dari keilmuan yang membicarakan tentang strategi dan perang saja, namun juga berbicara tentang bagaimana pengelolaan sumber daya nasional untuk mencapai kepentingan nasional yakni menjaga kedaulatan negara, memelihara keutauhan wilayah Kesatuan Negara Republik Indonesia dan menjaga keselamatan bangsa dari ancaman militer maupaun ancaman non-militer. Maka dalam mempelajari ilmu pertahanan, kita akan mendapati materi-materi dari keilmuan lainnya baik yang bersifat ilmu sosial maupun ilmu yang bersifat eksak.

2.1.2 Teori Strategi

Strategi merupakan alat untuk mencapai tujuan, dalam pengembangannya konsep mengenai strategi harus terus memiliki

[12]Supriyatno Makmur. *Tentang Ilmu Pertahanan*. (Jakarta: Yayasan Pustaka Obor Indonesia, 2014), hlm. 20.
[13] Kementerian Pertahanan Republik Indonesia, Media Informasi Pertahanan Volume 54/No.38/Mei-Juni 2015. hlm. 6.
[14] *Ibid.* hlm. 14

perkembangan dan setiap orang mempunyai pendapat atau definisi yang berbeda mengenai strategi.

Menurut Tjiptono (2006), istilah strategi berasal dari bahasa Yunani yaitu *strategia* yang artinya seni atau ilmu untuk menjadi seorang jendral. Strategi juga bisa diartikan suatu rencana untuk pembagian dan penggunaan kekuatan militer pada daerah-daerah tertentu untuk mencapai tujuan tertentu.[15] Menurut Chandler, penentuan tujuan dan sasaran jangka panjang perusahaan, diterapkannya aksi dan alokasi sumber daya yang dibutuhkan untuk mencapai tujuan yang telah ditetapkan.[16]

Menurut David Hunger dan Thomas L. Wheelen (2003), strategi adalah serangkaian keputusan dan tindakan manajerial yang menentukan kinerja perusahaan dalam jangka panjang. Konsep dasar proses manajemen strategis meliputi 4 elemen dasar, yaitu : Pengamatan lingkungan (*Environmental Scanning*), Perumusan strategi (*strategy Formulation*), Implementasi strategi (*strategy implementation*) dan evaluasi dan pengendalian (*evaluation and control*).[17]

Menurut Strickland dalam J. Winardi (2003), strategi dalam suatu organisasi adalah tindakan-tindakan dan pendekatan-pendekatan organisasi yang diterapkan oleh pihak pimpinan guna mencapai kinerja keorganisasian yang telah ditetapkan sebelumnya.[18]

Menurut Onong Uchjana Effendy (2001), strategi adalah perencanaan dan manajemen untuk mencapai tujuan. Tetapi untuk mencapai tujuan tersebut, strategi tidak berfungsi sebagai peta jalan yang

---

[15] Fandy,Tjiptono. *Manajemen Jasa*. (Yogyakarta : Andi, 2006), hlm. 3.
[16] Alfred, D. Chandler, Jr. *Strategy and Structure : Chapters in The History of The industrial Enterprise*. (Cambridge Mass : MIT Press. 1962), hlm.13.
[17] David Hunger dan Thomas L. Wheelen. *Manajemen Strategi*. (Yogyakarta: Andi, 2003), hlm. 9.
[18] Winardi, J. *Entrepreneur dan Entrepreneurship*, Cetakan Kedua. (Jakarta : CV.Kencana, 2003), hlm. 10

hanya menunjukkan arah saja, melainkan harus mampu menunjukkan taktik operasionalnya.[19]

Menurut Ahmad S. Adnanputra (1997), strategi adalah bagian terpadu dari suatu rencana (*plan*), dimana rencana merupakan produk dari perencanaan (*planning*) yang pada akhirnya perencanaan adalah fungsi dasar dari proses manajemen.[20]

Secara *universal*, strategi menunjukkan adanya keterkaitan antara tiga unsur elemen, yakni *Ends* yaitu sasaran atau tujuan yang ingin dicapai, *Means* yaitu sarana atau sumber daya kekuatan yang dimiliki untuk mengejar tujuan dan sasaran tersebut, dan *Ways* yaitu bagaimana cara atau metode untuk mencapai tujuan dengan mengorganisasi dan menggunakan sumber daya tersebut.[21]

Secara matematis, rumus dari strategi adalah sebagai berikut :

$$St = E + M + W$$

Dimana :

St (*Strategy*) = Strategi
E (*Ends*) = Tujuan yang sudah ditentukan dalam kebijakan
W (*Ways*) = Cara yang ditempuh untuk mencapai tujuan
M (*Means*) = Sumber-sumber, sarana dan prasarana yang dapat digunakan dalam mencapai tujuan.

Strategi yang baik dan tepat memiliki proses yang lebih terperinci. Menurut David Proses manajemen strategi terdiri atas tiga tahap:

[19] Effendy, Onong Uchjana*. Ilmu Komunikasi Teori dan Praktek*. (Bandung : PT. Remaja Rosdakarya, 2001) hlm. 32
[20] Ahmad S.Adnanputra dalam Hifni Alifahmi. *Marketing Public Relations*. (Jakarta: Lembaga Manajemen FEUI, 1997). Hlm.106
[21] Arthur F. Lykke Jr., *Defining Military Strategy*, (Military Review 69, no. 5. 1989), hlm. 3.

perumusan strategi, penerapan strategi, dan penilaian strategi. Tahapan tersebut, yaitu : [22]

1. Perumusan Strategi

   Perumusan strategi terdiri dari:

   - Pengembangan Visi dan Misi
   - Identifikasi peluang dan ancaman eksternal suatu organisasi
   - Kesadaran akan kekuatan dan kelemahan internal
   - Penetapan tujuan jangka panjang
   - Pencarian strategi-strategi aternatif
   - Pemilihan strategi tertentu untuk mencapai tujuan

2. Penerapan Strategi

   Tahap penerapan strategi terdiri dari :

   - Pengembangan budaya yang suportif pada strategi
   - Penciptaan struktur organisasional yang efektif
   - Pengerahan ulang upaya-upaya pemasaran
   - Penyiapan anggaran
   - Pengembangan serta pemanfaatan sistem informasi
   - Pengaitan kompensasi karyawan dengan kinerja organisasi

3. Penilaian Strategi

   Tahap aktivitas penilaian strategi tediri dari :

   - Peninjauan ulang faktor-faktor eksternal dan internal yang menjadi landasan bagi strategi saat ini
   - Pengukuran kinerja
   - Pengambilan langkah korektif

[22] David, Fred.R. *Manajemen Strategis: Konsep-Konsep*. Edisi Duabelas. (Jakarta: Salemba Empat. 2011), hlm.6.

2.1.3 Keamanan Informasi

2.1.3.1 Definisi Keamanan Informasi

Menurut Whitman & Mattord (2011), keamanan informasi merupakan perlindungan terhadap kerahasiaan, integritas dan ketersediaan aset informasi, baik dalam penyimpanan, pengolahan, atau transmisi. Hal ini dicapai melalui penerapan kebijakan, pendidikan, pelatihan dan kesadaran, serta teknologi.[23]

Keamanan informasi adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis (*business continuity*), meminimalisasi resiko bisnis (*reduce business risk*) dan memaksimalkan atau mempercepat pengembalian investasi dan peluang bisnis (ISO/IEC 27001, 2005).[24]

2.1.3.2 Aspek Keamanan Sistem Informasi

Garfinkel mengemukakan bahwa keamanan komputer (*computer security*) melingkupi empat aspek, yaitu *privacy*, *integrity*, *authentication*, dan *availability*. Selain keempat hal di atas, masih ada dua aspek lain yang juga sering dibahas dalam kaitannya dengan *electronic commerce*, yaitu access control dan nonrepudiation.[25]

a. Privacy / Confidentiality

Inti utama aspek privacy atau confidentiality adalah usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. *Privacy* lebih kearah data-data yang sifatnya *private* sedangkan *confidentiality* biasanya berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu (misalnya sebagai bagian dari pendaftaran sebuah *service*) dan hanya diperbolehkan untuk keperluan tertentu tersebut.

---

[23] Whitman, E. & Mattord, H. 2011. Principles of Information Security, 4th edition. (2011)
[24] International Organization for Standardization. ISO/IEC 27001. (2005)
[25] Simson Garfinkel, “PGP: Pretty Good Privacy,” O’Reilly & Associates, Inc., (1995).

b. Integrity

Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi. Adanya *virus*, *trojan horse*, atau pemakai lain yang mengubah informasi tanpa ijin merupakan contoh masalah yang harus dihadapi. Sebuah *e-mail* dapat saja "ditangkap" (*intercept*) di tengah jalan, diubah isinya, kemudian diteruskan ke alamat yang dituju. Dengan kata lain, integritas dari informasi sudah tidak terjaga.

c. Authentication

Aspek ini berhubungan dengan metode untuk menyatakan bahwa informasi betul-betul asli, atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud. Masalah pertama, membuktikan keaslian dokumen, dapat dilakukan dengan teknologi watermarking dan digital signature.

d. Availability

Aspek *availability* atau ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang atau dijebol dapat menghambat atau meniadakan akses ke informasi. Contoh hambatan adalah serangan yang sering disebut dengan "denial of service attack" (*DoS attack*), dimana server dikirimi permintaan (biasanya palsu) yang bertubi-tubi atau permintaan yang diluar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai *down, hang, crash*.

e. Access Control

Aspek ini berhubungan dengan cara pengaturan akses kepada informasi. Hal ini biasanya berhubungan dengan masalah authentication dan juga *privacy*. *Access control* seringkali dilakukan dengan menggunakan kombinasi *userid/password* atau dengan menggunakan mekanisme lain.

f. Non-repudiation

Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi. Sebagai contoh, seseorang yang mengirimkan email untuk memesan barang tidak dapat menyangkal bahwa dia telah mengirimkan email tersebut. Aspek ini sangat penting dalam hal *electronic commerce*. Penggunaan digital signature dan teknologi kriptografi secara umum dapat menjaga aspek ini.

Serangan terhadap keamanan sistem informasi, dapat dilihat dari sudut peranan komputer atau jaringan komputer yang fungsinya adalah sebagai penyedia informasi. Menurut W. Stallings ada beberapa kemungkinan serangan (*attack*):[26]

a. *Interruption*: Perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan kepada ketersediaan (*availability*) dari sistem. Contoh serangan adalah "*denial of service attack*".

b. *Interception*: Pihak yang tidak berwenang berhasil mengakses aset atau informasi. Contoh dari serangan ini adalah penyadapan (*wiretapping*).

c. *Modification*: Pihak yang tidak berwenang tidak saja berhasil mengakses, akan tetapi dapat juga mengubah (tamper) aset. Contoh dari serangan ini antara lain adalah mengubah isi dari *website* dengan pesan-pesan yang merugikan pemilik *website*.

d. *Fabrication*: Pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem. Contoh dari serangan jenis ini adalah memasukkan pesan-pesan palsu seperti *e-mail* palsu ke dalam jaringan komputer.

[26] William Stallings. *Network and Internetwork Security*. (Prentice Hall. 1995)

2.1.3.3 *Framework* Keamanan Informasi

a. ISO/IEC 27001

ISO/IEC 27001 dikembangkan oleh *The International Organization for Standardization (ISO)* dan *The International Electrotechnical Commission (IEC)* merupakan suatu standar Internasional dalam menerapkan sistem manajemen kemanan informasi atau lebih dikenal dengan *Information Security Management Systems (ISMS)*. Menerapkan standar *ISO/IEC 27001* akan membantu organisasi atau perusahaan dalam membangun dan memelihara sistem manajemen keamanan informasi (SMKI). *Information Security Management Systems (ISMS)* merupakan seperangkat unsur yang saling terkait dengan organisasi atau perusahaan yang digunakan untuk mengelola dan mengendalikan risiko keamanan informasi dan untuk melindungi serta menjaga kerahasiaan (*confidentiality*), integritas (*integrity*) dan ketersediaan (*availability*) informasi.

ISO/IEC 27001:2013 memiliki sepuluh klausa pendek, ditambah lampiran yang panjang, yang meliputi:

- Lingkup standar
- Bagaimana dokumen direferensikan
- Istilah dan definisi dalam *ISO/IEC 27000*
- Hubungan organisasi dan stakeholder
- Kepemimpinan keamanan informasi dan dukungan tingkat tinggi untuk kebijakan
- Perencanaan sistem manajemen keamanan informasi; perkiraan risiko; kontrol terhadap resiko
- Mendukung sistem manajemen keamanan informasi
- Membuat operasional sistem manajemen keamanan informasi
- Meninjau kinerja sistem
- Tindakan korektif

b. *Control Objectives for Information and related Technology (COBIT)*

COBIT adalah sekumpulan dokumentasi dan panduan yang mengarahkan pada *IT governance* yang dapat membantu auditor, manajemen dan pengguna (*user*) untuk menjembatani pemisah antara resiko bisnis, kebutuhan kontrol, dan permasalahan-permasalahan teknis.

COBIT Framework dikembangkan oleh *IT Governance Institute*, sebuah organisasi yang melakukkan studi tentang model pengelolaan TI yang berbasis di Amerika Serikat. *COBIT Framework* terdiri atas 4 domain utama yaitu: PO (*Planning and Organisation*), AI (*Acquisition and Implementasion*), DS (*Delivery and Support*) dan ME (*Monitoring and Evaluation*).

1) Planning and Organization (PO)

Domain ini mencakup strategi dan taktik, dan perhatian atas identifikasi bagaimana TI secara maksimal dapat berkontribusi dalam pencapaian tujuan bisnis. Selain itu, realisasi dari visi strategis perlu direncanakan, dikomunikasikan, dan dikelola untuk berbagai perspektif yang berbeda. Terakhir, sebuah pengorganisasian yang baik serta infrastruktur teknologi harus di tempatkan di tempat yang semestinya.

2) Acquisition and Implementation (AI)

Untuk merealisasikan strategi TI, solusi TI perlu diidentifikasi, dikembangkan atau diperoleh, serta diimplementasikan, dan terintegrasi ke dalam proses bisnis. Selain itu, perubahan serta pemeliharaan sistem yang ada harus di cakup dalam domain ini untuk memastikan bahwa siklus hidup akan terus berlangsung untuk sistem ini.

3) Delivery and Support (DS)

Domain ini memberikan fokus utama pada aspek penyampaian/ pengiriman dari TI. Domain ini mencakup area-area seperti pengoperasian aplikasi-aplikasi dalam sistem TI dan hasilnya, dan

juga, proses dukungan yang memungkinkan pengoperasian sistem TI tersebut dengan efektif dan efisien.

4) Monitoring and Evaluation (ME)

Semua proses IT perlu dinilai secara teratur sepanjang waktu untuk menjaga kualitas dan pemenuhan atas syarat pengendalian. Domain ini menunjuk pada perlunya pengawasan manajemen atas proses pengendalian dalam organisasi serta penilaian independen yang dilakukan baik auditor internal maupun eksternal atau diperoleh dari sumber-sumber alternatif lainnya.

c. *Defense In Depth*

Defense in depth adalah konsep perlindungan jaringan komputer dengan serangkaian mekanisme pertahanan sehingga jika satu mekanisme gagal, yang lain akan ada untuk menggagalkan serangan. Karena ada banyak penyerang potensial dengan berbagai macam metode serangan yang tersedia, dengan memanfaatkan strategi *defense in depth* akan mengurangi risiko karena serangan yang sukses membutuhkan biaya yang sangat mahal.[27]

Defense in depth adalah manajemen keamanan dari *people*, *processes* and *technology* dalam sebuah pendekatan manajemen resiko holistik. Konsep ini didasarkan pada strategi militer yang mengatakan bahwa pertahanan yang utama adalah menunda daripada mencegah sebuah penyerangan. Dalam konteks militer, ini bergantung pada asumsi bahwa serangan akan kehilangan momentum selama periode waktu tertentu, dan waktu akan memungkinkan mereka diserang untuk merespon secara tepat.[28]

Dalam bidang Teknologi Informasi, *defense in depth* juga dimaksudkan untuk meningkatkan biaya dan upaya serangan terhadap organisasi, dengan mendeteksi serangan, memungkinkan waktu untuk

[27] SANS Institute InfoSec Reading Room, *Defense in depth*. (United State: 2001), hlm. 1.
[28] Trusted Information Sharing Network, *Defense in depth.* (Australia : 2008). hlm. 6

menanggapi serangan tersebut, dan memberikan pertahanan lapisan sedemikian rupa sehingga bahkan serangan yang sukses tidak akan sepenuhnya dikompromi oleh suatu organisasi.[29]

Prinsip mendasar dalam *defense in depth* adalah pendekatan keseimbangan dan koordinasi antara *people*, *process (operation)* dan *technology*[30], sedangkan unsur *governance* bertanggungjawab mengelola koordinasi elemen-elemen ini. Agar *defense in depth* dapat berhasil diimplementasikan dalam strategi organisasi, perencanaan dan struktur harus memasukkan elemen-elemen inti dari *defense in depth* yaitu *governance*, *people*, *process and technology*. Seperti didefinisikan oleh *Australian Government Attorney-General's Department*, sebagai berikut:

Gambar 2.1 Elemen *Defense In Depth*

(Sumber : Trusted Information Sharing Network, Australia)

1) Governance

Komponen ini mengacu pada kerangka manajemen yang digunakan untuk memberikan pengawasan dan koordinasi *people*, *process* dan *technology*, yang meliputi :

- Manajemen resiko
- Keamanan Informasi

[29] *Ibid.*

[30] United State, National Security Agency, "Defense in Depth" dalam www.nsa.gov/snac/support/defenseindepth.pdf dikases pada 4 Agustus 2018

- Kebijakan dan penyesuaian manajemen

2) *People*

Komponen ini menguraikan definisi, pemeliharaan, dan penegakan peran dan tanggung jawab keamanan bagi karyawan dan vendor internal dan eksternal, yaitu :

- Keamanan Personal (termasuk kesadaran pengguna).

3) *Process*

Komponen ini menggambarkan definisi, pemeliharaan, dan tindakan standar yang digunakan untuk mengembangkan dan memastikan bahwa keamanan tetap pada basisnya, yang meliputi :

- Manajemen akses pengguna
- Manajemen respon
- Manajemen audit

4) *Technology*

Komponen ini menjelaskan teknologi dan solusi produk yang digunakan untuk memungkinkan pencapaian tujuan bisnis secara berkelanjutan, yang meliputi :

- Manajemen komunikasi
- Manajemen infrastruktur
- Manajemen arsitektur jaringan
- Keamanan Aplikasi

Dari ke tiga framework tersebut, yaitu *ISO 27001*, *COBIT* dan *Defense in depth*. Peneliti memilih untuk menggunkan *defense in depth framework* sebagai model yang akan digunakan untuk membangun strategi keamanan informasi pada Sistem Pengadaan Secara Elektronik provinsi Lampung, karena framework ini paling mudah diimplementasikan pada sistem pengadaan elektronik dan handal digunakan untuk menghadapi ancaman siber. Sebab *defense in depth framework* merupakan konsep atau model keamanan informasi dengan pertahanan berlapis yang dapat melindungi dari berbagai macam ancaman siber. Hal

ini didasarkan bahwa dalam membangun keamanan informasi tidak bisa dari satu aspek saja, melainkan semua aspekl harus di lindungi sehingga *defense in depth framework* sangat cocok untuk di implementasikan dalam membangun strategi keamanan informasi khususnya pada sistem pengadaan Secara Elektronik.

2.2 Deskripsi Konseptual

Sebelumnya peneliti telah menjelaskan bahwa fokus dari rencana penelitian adalah terkait dengan strategi dalam menghadapi ancaman Siber pada Sistem Pengadaan Secara Elektronik (SPSE) Provinsi Lampung. Fokus ini ditetapkan dengan asumsi bahwa ancaman siber pada Sistem Pengadaan Secara Elektronik (SPSE) Provinsi Lampung adalah salah satu ancaman yang sangat serius yang dapat mengganggu jalannya pemerintahan khususnya pada proses pengadaan barang dan jasa di provinsi Lampung. Dimana dalam membangun suatu sistem keamanan siber dibutuhkan strategi yang handal, hal ini disebabkan bahwa ancaman diruang siber sangat kompleks yang membutuhkan pengamanan berlapis dan pengamanan dari berbagai aspek.

Oleh sebab itu agar fokus penelitian ini memiliki pijakan ilmiah yang dapat dipertanggungjawabkan, maka peneliti akan menggunakan strategi *defense in depth* sebagai strategi yang dapat menjadi solusi untuk menghadapi ancaman siber dimasa yang akan datang pada Sistem Pengadaan Secara Elektronik (SPSE) Provinsi Lampung. Sebab dengan menggunakan model *defense in depth* dalam strategi keamanan informasi dapat melindungi 4 aspek keamanan informasi yaitu *privacy*, *integrity*, *authentication*, dan *availability*. Sehingga dapat menghadapi serangan terhadap keamanan informasi berupa serangan *Interruption, Interception, Modification* dan *Fabrication.* Hal ini dikarenakan didalam model keamanan informasi *defense in depth* terdapat empat komponen utama yang di lindungi yaitu *governance*, *people, process,* dan *technology*. Dengan melindungi 4 komponen ini maka akan menutup celah kerentanan

terhadap keamanan informasi, sehingga serangan akan sulit menembus pertahanan.

Setiap konsep dalam fokus ini, tidak menutup kemungkinan akan digunakan juga sebagai konsep pembahasan untuk analisis dari sub-subfokus penelitian yang telah ditetapkan. Konsep tersebut akan dijabarkan lebih rinci secara berturut-turut sebagai berikut:

2.2.1 Definisi Sistem

Menurut Romney dan Steinbart, Sistem adalah rangkaian dari dua atau lebih komponen-komponen yang saling berhubungan, yang berinteraksi untuk mencapai suatu tujuan. Sebagian besar sistem terdiri dari subsistem yang lebih kecil yang mendukung sistem yang lebih besar.[31]

Menurut Anastasia Diana & Lilis Setiawati, Sistem merupakan "serangkaian bagian yang saling tergantung dan bekerja sama untuk mencapai tujuan tertentu".[32]

Menurut Mulyadi, Sistem adalah "suatu jaringan prosedur yang dibuat menurut pola yang terpadu untuk melaksanakan kegiatan pokok perusahaan".[33]

Berdasarkan pengertian diatas dapat disimpulkan bahwa sistem adalah kumpulan dari komponen-komponen yang saling berkaitan satu dengan yang lain untuk mencapai tujuan dalam melaksanakan suatu kegiatan pokok perusahaan..

2.2.2 Sistem Pengadaan Secara Elektronik (SPSE)

SPSE merupakan aplikasi *e-Procurement* yang dikembangkan oleh Direktorat *e-Procurement* - LKPP untuk digunakan oleh LPSE di seluruh K/L/D/I. Aplikasi ini dikembangkan dengan semangat efisiensi nasional

[31] Romney, Marshal R. & Paul John Steinbart. *Sistem Informasi Akuntansi.* (Jakarta : Salemba Empat. 2015), hlm. 3.
[32] Anastasia Diana, Lilis Setiawati. *Sistem Informasi Akuntansi, Perancangan, Prosedur dan Penerapan*. Edisi 1. (Yogyakarta: Andi Yogyakarta. 2011), hlm. 3.
[33] Mulyadi. *Sistem Akuntansi,* (Jakarta : Salemba Empat. 2016), hlm. 5.

sehingga tidak memerlukan biaya lisensi, baik lisensi SPSE itu sendiri maupun perangkat lunak pendukungnya.

SPSE dikembangkan oleh LKPP bekerja sama dengan:

1. Badan Siber dan Sandi Negara (BSSN) untuk fungsi enkripsi dokumen.
2. Badan Pengawasan Keuangan dan Pembangunan (BPKP) untuk sub sistem audit.

Di dalam Peraturan Presiden RI Nomor 4 Tahun 2015 tentang Perubahan Keempat Atas Peraturan Presiden Nomor 54 Tahun 2010 tentang Pengadaan Barang/Jasa Pemerintah, *e-Procurement* didefinisikan sebagai Pengadaan Barang/Jasa yang dilaksanakan dengan menggunakan teknologi informasi dan transaksi elektronik sesuai dengan ketentuan perundang-undangan. Sedangkan beberapa ahli mendefinikan *e-Procurement* sebagai berikut :

- Turban, mengemukakan bahwa e-procurement adalah penggunaan teknologi internet untuk membeli atau menyediakan barang dan jasa, yang memerlukan penggunaan sistem database yang terintegrasi, sistem komunikasi *WA*N, sistem berbasis *web*, sistem persediaan, dan interaksi dengan sistem akuntansi.[34]
- Croom dan Jones menjelaskan bahwa *e-procurement* merujuk pada penggunaan penggabungan sistem teknologi informasi untuk fungsi pengadaan, meliputi pencarian sumber daya, negosiasi, pemesanan, dan pembelian.[35]
- Tatsis dkk, mendefinisikan *e-procurement* sebagai penggabungan manajemen, otomatisasi, dan optimisasi dari suatu proses pengadaan organisasi dengan menggunakan

[34] Turban, Efraim, et al. *Electronic Commerce 2008: A Managerial Perspective*. (New Jersey: Prentince Hall, Inc., 2008), hlm.184.

[35] Croom, S.R., Brandon-Jones, A., "Impact of E-procurement: experiences from implementation in the UK public sector", Journal of Purchasing & Supply Management, Vol. 13, 2007, hlm. 294–303.

sistem elektronik berbasis *web*.[36]

- Sedangkan Davila dkk., menambahkan definisi tentang *e-procurement* yaitu sebuah teknologi yang dirancang untuk memfasilitasi pengadaan barang melalui internet.[37]

2.2.3 Definisi *Hacker*

Hacker adalah orang yang mempelajari, menganalisis, memodifikasi, menerobos masuk ke dalam komputer dan jaringan komputer, baik untuk keuntungan atau dimotivasi oleh tantangan.[38]

Hacker merupakan 'seni' tersendiri yang melibatkan proses mencari serpihan-serpihan informasi yang bertebaran di mana-mana dan seolah-olah tidak ada hubungannya satu sama lain. cara kerja hacker mengakses suatu sistem, secara sederhana dapat digambarkan dengan langkah-langkah sebagai berikut:

- *Footprinting* yaitu mencari rincian informasi terhadap sistem-sistem untuk dijadikan sasaran, mencakup pencarian informasi dengan mesin pencari, *whois*, dan *DNS one transfer*.
- *Scanning* yaitu terhadap sasaran tertentu dicari pintu masuk yang paling mungkin. Digunakan ping sweep dan port scan
- *Enumeration* yaitu telaah intensif terhadap sasaran, yang mencari *user account* absah, *network resource and share*, dan aplikasi untuk mendapatkan mana yang proteksinya lemah.
- *Gaining Access* yaitu Mendapatkan data lebih banyak lagi untuk memulai mencoba mengakses sasaran. Meliputi atau merampas kata sandi, menebak kata sandi, serta melakukan *buffer overflow*
- *Escalating Privilege* yaitu apabila baru mendapatkan *user*

[36] Tatsis,V., Mena,C., VanWassenhove, L.N., Whicker,L., "Procurement in the Greek Food and Drink Industry", Journal of Purchasing & Supply Management, Vol. 12, 2006. hlm. 63–74.
[37] Davila, A., Gupta, M., Palmer, R., "Moving procurement systems to the internet : the adoption and use of e-Procurement technology models ", European Management Journal, Vol.21, No. 1, 2003. hlm 11.
[38] Definisi Hacker. "https://id.wikipedia.org/wiki/Peretas" di akses pada 4 agustus 2018

password di tahap sebelumnya, di tahap ini di usahakan mendapat *privilese* admin jaringan dengan *password cracking* atau eksploit sejenis *getadmin*, *sechole* atau *lc_messages*.

- *Pilfering* yaitu proses pengumpulan informasi dimulai lagi untuk mengidentifikasi mekanisme untuk mendapatkan akses ke *trusted system*. Mencakup evaluasi *trust* dan pencarian *cleartext password* di *registry*, *config file*, dan *user data*.
- *Convering Tracks* yaitu begitu kontrol penuh terhadap sistem diperoleh, maka menutup jejak menjadi prioritas. Meliputi membersihkan *network log* dan penggunaan *hide tool* seperti macam-macam *rootkit* dan *file streaming.*
- *Creating Backdoors* yaitu pintu belakang diciptakan pada berbagai bagian dari sistem untuk memudahkan masuk kembali ke sistem ke sistem ini dengan cara membentuk *user account* palsu, menjadwalkan *batch joob*, mengubah *startup file*, menambahkan servis pengendali jarak jauh serta *monitoring tool*, dan menggantikan aplikasi dengan *qtrojan*.
- *Denial of Service* yaitu apabila semua usaha diatas gagal, penyerang dapat dilumpuhkan sasaran sebagai usaha terakhir. Meliputi *SYN flood*, teknik-teknik *ICMP*, *supernuk*e, *land/ latierra*, *teardrop*, *bonk, newtear, trincoo, smurf,* dan lain-lain.
- *Distributed Denial of Service* atau lebih dikenal dengan nama *DDoS* adalah sebuah percobaan penyerangan dari beberapa sistem komputer yang menargetkan sebuah *server* agar jumlah *traffic* menjadi terlalu tinggi sampai *server* tidak bisa *handle request*.

2.3 Hasil Penelitian Terdahulu yang Relevan

Hasil penelitian terdahulu yang relevan merupakan hasil-hasil penelitian atau kejadian terdahulu yang pernah dilakukan oleh peneliti sebelumnya yang tentu saja relevan dengan penelitian yang akan dilakukan.[39] Hasil penelitian terdahulu dapat berupa disertasi, tesis, jurnal atau karya-karya tulis ilmiah lainnya.

Manfaat dari penelitian terdahulu di antaranya agar peneliti dapat memperjelas masalah, menjajagi kemungkinan dilanjutkannya penelitian dan juga agar peneliti dapat mengetahui apa yang sudah dihasilkan orang lain bagi penelitian serupa dan bagian permasalahan yang belum terpecahkan[40]. Tujuan utama dari penelitian terdahulu adalah agar mempermudah calon peneliti mendalami dan memperjelas permasalahan yang akan diteliti.[41]

Berikut ini peneliti akan uraikan hasil penelitian terdahulu yang relevan dengan penelitian yang akan dilakukan oleh peneliti sesuai dengan format penulisan tesis Universitas Pertahanan. Format penelitian terdahulu terdiri atas nama peneliti, tahun penelitian/penulisan dilakukan, judul penelitian, metode penelitian yang digunakan dan hasil penelitian.

Hasil penelitian terdahulu yang relevan dengan penelitian yang akan dilakukan adalah sebagai berikut:

2.3.1 Implementasi Sistem Pengadaan Barang/Jasa Secara Elektronik (SPSE) Dalam Mewujudkan Transparansi Pemerintahan

Nama peneliti Firli Satriawan, penelitian dilakukan pada tahun 2018 dengan judul penelitian “Implementasi Sistem Pengadaan Barang/Jasa Secara Elektronik (SPSE) Dalam Mewujudkan Transparansi Pemerintahan (Studi Pada Badan Layanan Pengadaan Barang/Jasa

[39] Peraturan Rektor Universitas Pertahanan Nomor 30 Tahun 2017 tentang Buku Pedoman Penulisan Tesis dan Disertasi Universitas Pertahanan.
[40]Etta Mamang Sangadji dan Sopiah. *Metodologi Penelitian, Pendekatan Praktis dalam Penelitian,* (Yogyakarta: Andi. 2010), hlm. 9.
[41]*Ibid*. hlm. 10.

(BLPBJ) dan Layanan Pengadaan Secara Elektronik (LPSE) Provinsi Lampung)". Penelitian ini dilakukan dengan metode penelitian kualitatif dan pendekatan secara deskriptif. Hasil dari penelitian yang dilakukan oleh Firli Satriawan yaitu Implementasi pengadaan barang/jasa secara elektronik Layanan Pengadaan Secara Elektronik (LPSE) Provinsi Lampung telah berhasil menciptakan transparansi dalam pelaksanaan pengadaan secara elektronik. Namun masih terdapat beberapa hambatan dalam pelaksanaannya. Hambatan-hambatan yang ditemukan disebabkan oleh beberapa hal yaitu: pertama, belum adanya peraturan perundang-undangan yang mengatur lebih rinci terhadap penggunaan tanda tangan elektronik, besaran serta format file yang dapat digunakan dalam proses pengadaan barang/jasa secara elektronik. Kedua, masih terdapat kekurangan dalam hal sumber daya yang terdiri dari faktor internal yaitu kurangnya ketersediaan aparatur pemerintah dalam instansi pemerintah, masih adanya aparatur yang belum mampu melaksanakan tugasnya dengan kompeten dan maksimal.

Penelitian yang dilakukan oleh Firli Satriawan memiliki beberapa kesamaan dalam beberapa hal seperti yang dilakukan oleh peneliti, yakni: 1) Metode penelitian sama-sama menggunakan metode penelitian kualitatif, 2) teknik pengumpulan data memiki kesamaan yakni dengan metode wawancara, observasi dan dokumentasi. dan 3) objek penelitian yang sama. Adapun perbedaan antara penelitian ini yakni : 1) Indikator teori yang digunakan dalam penelitian berbeda dengan yang digunakan oleh peneliti; 2) penelitian tidak membahas tentang keamanan siber seperti dilakukan oleh peneliti.

2.3.2 Perencanaan Keamanan Informasi dengan Menggunakan Metode ISO 27001:2005 Di LPSE Kab. Bandung Barat.

Nama peneliti Chandra, penelitian dilakukan pada tahun 2017 dengan judul Perencanaan Keamanan Informasi dengan Menggunakan Metode ISO 27001:2005 Di LPSE Kab. Bandung Barat. Penelitian ini

dilakukan dengan metode penelitian kualitatif deskriptif. Penelitian yang dilakukan oleh Muhammad Chandra ini adalah penelitian yang bertujuan merancang keamanan informasi dengan menggunakan pendekatan standar ISO 27001:2005 lampiran anek A. Klausul A.7 Pengelolaan Aset, A.8 Keamanan sumber daya manusia, A.9 keamanan fisik dan lingkungan sebagai pisau analisis. Sedangkan Metode penilaian risiko keamanan informasi pada penelitian ini menggunakan metode FMEA (Failure Mode and Effect Analysis). Hasil dari penelitian ini berupa penyusunan Standar Operasi Prosedur (SOP) berdasarkan ISO 27001:2005. Dalam Penelitian yang dilakukan oleh Muhammad Chandra terdapat persamaan dan perbedaan. Persamaan: menggunakan metode penelitian kualitatif, Perbedaannya: Pada penelitian yang dilakukan oleh Muhammad Chandra dilakukan di LPSE Kabupaten Bandung Barat, sedangkan yang peneliti lakukan di LPSE Provinsi Lampung. Perbedaan berikutnya pada pisau analisis, penelitian yang dilakukan oleh Muhammad Chandra menggunakan ISO 27001:2005 sedangkan pada penelitian ini menggunakan Strategi *Defense in Depth.*

2.3.3 Evaluasi Celah Keamanan *Web Server* pada LPSE Kota Palembang

Nama peneliti Muhammad Ilham Daniel, Leon Andretti Abdillah, Kiky Rizky Nova Wardani, penelitian dilakukan pada tahun 2015 dengan judul “Evaluasi Celah Keamanan *Web Server* pada LPSE Kota Palembang”. Penelitian ini menggunakan metode penelitian tindakan atau *action research*. Diamana penelitian ini dilakukan di LPSE Kota Palembang. Berdasarkan hasil penelitian didapat kesimpulan: Masih terdapat celah keamanan pada *web server* LPSE. Perbaikan yang dilakukan hanya pada beberapa celah keamanan. Perlu dilakukan pengujian untuk memeriksa kerentanan yang ada pada *web server*. Saran yang diberikan pada penelitian tersebut antara lain: a) Perlu dilakukan evaluasi terhadap celah keamanan web server secara berkala, dan b)

Melakukan update aplikasi-aplikasi yang sudah kadaluwarsa. Pada penelitian yang di lakukan Muhammad Ilham Daniel, dkk. Terdapat perbedaan dan persamaan. Perbedaan pada penelitian Muhammad Ilham Daniel, dkk menggunakan metode penelitian tindakan atau *action research* sedangkan pada penelitian ini menggunakan metode penelitian kualitatif. Adapun persamaan dari penelitian yang Muhammad Ilham Daniel, dkk adalah sama-sama menggali masalah terkait keamanan sistem pengadaan secara elektronik. Adapun persamaan penelitian tersebut dengan penelitian ini adalah sama-sama meneliti tentang keamanan sistem informasi pada sistem LPSE. Sedangkan perbedaan penelitian tersebut dengan penelitian ini, penelitian yang dilakukan oleh Muhammad Ilham Daniel, dkk menggunakan metode penelitian *action research* sedangkan pada penelitian ini menggunakan metode penelitian deskriptif kualitatif. Selain itu terdapat perbedaan waktu dan tempat penelitian.

2.3.4 *Layered Defense in Depth Model for IT Organizations*

Nama peneliti Azra Shamim, Bushra Fayyaz, and Vimala Balakrishnan, penelitian dilakukakan pada tahun 2014 dengan judul "*Layered Defense in Depth Model for IT Organizations".* Penelitian ini menggunakan strategi *Defense in Depth* dimana hasil dari penelitian ini sebagai berikut: Dalam model *defense in depth* menyajikan kerangka kerja yang paling komprehensif untuk tujuan keamanan. Karena sifatnya yang dapat diadopsi dan skalabilitas yang alamiah, ini dapat dengan mudah memberikan pertahanan terhadap ancaman baru yang muncul dengan memanfaatkan mekanisme baru. Pembelian, pengaturan, dan pendidikan administrator adalah komponen utama dari model ini. Pada penelitian yang dilakukan oleh Azra Shamim, dkk. terdapat perbedaan dan persamaan. Perbedaannya: penerapan strategi yang dilakukan oleh Azra Shamim, dkk. digunakan pada organisasi IT sedangkan pada penelitian ini digunakan pada Sistem Pengadaan Secara Elektronik. Persamaanya: menggunakan strategi *Defense in Depth* sebagai pisau analisis.

2.3.5 Implementasi Perlindungan Peretasan *Google In App Purchase* dengan Metode *One Time Server Side Verfication*, *Verification Bypass Detection*, dan *Obfuscator* pada Aplikasi Informasi Cuaca Android.

Nama peneliti M Faizal Putra Pradana, Agi Putra Kharisma dan Komang Candra Brata, penelitian dilakukan pada tahun 2017 dengan judul "Implementasi Perlindungan Peretasan *Google In App Purchase* dengan Metode *One Time Server Side Verfication*, *Verification Bypass Detection*, dan *Obfuscator* pada Aplikasi Informasi Cuaca Android". Dalam penelitian ini peneliti mencoba menerapkan sistem pengamanan dengan menggunakan 3 metode sekaligus yaitu *Server Side Verification, Verification Bypass Detection, dan Obfuscator* untuk melindungi sistem *In App Purchase* pada *Google Play Store* dari peretasan menggunakan sistem peretas *VirtualSwindler* yaitu suatu sistem yang dapat memanipulasi proses verifikasi dan menyimpan data pembelian yang tidak otentik pada perangkat pengguna. Dari hasil penelitian di dapat hasil bahwa Sistem perlindungan dengan kombinasi 3 metode tersebut memiliki tingkat keberhasilan 100% dalam melindungi sistem *In App Purchase.* Penelitian yang dilakukan oleh M Faizal Putra Pradana, dkk ini memiliki perbedaan dan persamaan. Perbedanya, objek penelitian yaitu *In App Purchase* pada *Google Play Store* sedangkan yang peneliti lakukan saat ini pada sistem pengadaan secara elektronik. perbedaan berikutnya pada kerangka kerja yang digunakan yaitu menggunakan *Server Side Verification, Verification Bypass Detection, dan Obfuscator* sedangkan kerangka kerja yang digunakan peneliti saat ini ialah *Defense in Depth.* Persamaan antara penelitian yang dilakukan oleh M Faizal Putra Pradana, dkk dengan peneliti lakukan saat ini ialah sama-sama menerapkan sistem pengamanan informasi untuk melindungi dari ancaman siber berupa serangan *hacker.*

Tabel 2.1 Persamaan dan perbedaan penelitian terdahulu

No	Nama Peneliti	Judul Peneltitian	Metode Penelitian & Teori	Objek Penelitian	Hasil Penelitian	Persamaan	Perbedaan
1	Firli Satriawan (2018)	Implementasi Sistem Pengadaan Barang/Jasa Secara Elektronik (SPSE) Dalam Mewujudkan Transparansi Pemerintahan (Studi Pada Badan Layanan Pengadaan Barang/Jasa (BLPBJ) dan	Menggunakan metode penelitian kualitatif dengan pendekatan deskriptif. Teori Implementasi Kebijakan	Badan Layanan Pengadaan Barang/ Jasa (BLPBJ) dan Layanan Pengadaan Secara Elektronik (LPSE)	Implementasi pengadaan barang/jasa LPSE Provinsi Lampung telah berhasil menciptakan transparansi dalam pelaksanaan pengadaan secara elektronik. Namun terdapat hambatan dalam pelaksanaannya. yaitu: belum adanya peraturan perundang-undangan yang mengatur lebih rinci terhadap tatakelola LPSE. Dan masih terdapat kekurangan dalam hal	Menggunakan metode penelitian yang sama yaitu penelitian kualitatif Dan objek penelitian yang sama yaitu LPSE Provinsi Lampung	Berbeda teori yang digunakan.

		Layanan Pengadaan Secara Elektronik (LPSE) Provinsi Lampung)			sumber daya yang mampu melaksanakan tugasnya dengan kompeten dan maksimal.		
2	Muhammad Chandra (2017)	Perencanaan Keamanan Informasi dengan Menggunakan Metode ISO 27001:2005 Di LPSE Kab. Bandung Barat	Metode penelitian yang digunakan adalah metode penelitian deskriptif dengan pendekatan kualitatif. Dan	LPSE Kab. Bandung Barat	Dalam Penelitian ini menggunakan pendekatan standar ISO 27001:2005 lampiran anek A. Klausul A.7 Pengelolaan Aset, A.8 Keamanan sumber daya manusia, A.9 keamanan fisik dan lingkungan sebagai pisau analisis. Sedangkan Metode penilaian risiko keamanan informasi. Hasil penelitian	Menggunakan metode penelitian yang sama yaitu penelitian kualitatif dan membahas tentang keamanan informasi	Berbeda lokasi penelitian dan framework kemanan informasi yaitu menggunakn framework ISO 27001

			menggunakan ISO 27001:2005 Klausul A		ini berupa penyusunan SOP berdasarkan ISO 27001:2005.	pada LPSE	
3	Muhammad Ilham Daniel, Leon Andretti Abdillah, Kiky Rizky Nova Wardani (2015)	Evaluasi Celah Keamanan Web Server pada LPSE Kota Palembang	Menggunakan metode penelitian tindakan atau *action research*	LPSE Kota Palembang	Berdasarkan hasil analisis dan uji coba terhadap celah keamanan web server pada LPSE, didapat masih terdapat celah keamanan pada web server LPSE dan perbaikan yang dilakukan hanya pada beberapa celah keamanan. Sehingga perlu dilakukan pengujian untuk memeriksa kerentanan yang ada pada web server.	membahas tentang keamanan informasi pada LPSE	Berbeda lokasi penelitian dan Metode penelitian yaitu *action research*

4	Azra Shamim, Bushra Fayyaz, and Vimala Balakrishnan (2014)	Layered Defense in Depth Model for IT Organizations	Menggunakan model *Defense in Depth*	Perusahaan IT secara umum	Menghasilkan model *defense in depth* menyajikan kerangka kerja yang komprehensif untuk tujuan keamanan informasi. Karena sifatnya yang dapat memberikan pertahanan terhadap ancaman baru yang muncul dengan memanfaatkan mekanisme baru ketika tersedia.	Menggunakan framework keamanan informasi yang sama yaitu defense in depth	Berbeda lokasi penelitian.
5	M Faizal Putra Pradana, Agi Putra Kharisma dan Komang	Implementasi Perlindungan Peretasan *Google In App Purchase* dengan Metode *One Time*	Menggunakan metode penelitian studi literatur dengan metode	*In App Purchase* pada *Google Play Store*	Dengan melakukan pengamanan menjadi 3 tahapan. Yaitu tahap dalam mendeteksi apakah proses verifikasi otentik atau tidak, Pemeriksaan hasil verifikasi dan tahap	Menerapkan sistem Keamanan informasi untuk menghadapi ancaman	Berbeda objek penelitian dan kerangka kerja yang digunakan

	Candra Brata (2017)	*Server Side Verfication*, *Verification Bypass Detection*, dan *Obfuscator* pada Aplikasi Informasi Cuaca Android	perlindungan *One Time Server Side Verfication*, *Verification Bypass Detection*, dan *Obfuscator*		penyimpanan data verifikasi. Kemudian untuk mengetahui tingkat keberhasilan pengamanan Sistem *In App Purchase* akan dilakukan dengan 2 tahap. Yakni validasi dengan kebutuhan fungsional pengamanan In App Purchase dan pengujian tingkat keberhasilan. Dan di dapat hasil bahwa Sistem perlindungan dengan kombinasi 3 metode tersebut memiliki tingkat keberhasilan 100% dalam melindungi sistem *In App Purchase.*	siber berupa serangan *hacker.*	untuk menerapkan sistem keamanan informasi

Dari ke lima penelitian terdahulu yang telah peneliti uraikan sebelumnya maka penelitian yang dilakukan oleh Muhammad Chandra (2017) dengan judul Perencanaan Keamanan Informasi dengan Menggunakan Metode *ISO 27001:2005* Di LPSE Kab. Bandung Barat merupakan penelitian yang paling banyak memiliki kemiripan dengan penelitian yang dilakukan peneliti saat ini dari sisi penerapan sistem keamanan informasi yang pada sistem pengadaan secara elektronik hanya saja perbedaannya pada kerangka kerja yang digunakan, Muhammad Chandra (2017) menggunakan *ISO 27001:2005* yaitu menggunakan clausul-clausul yang ada pada *ISO 27001:2005* untuk penerapan keamanan sistem informasi, sedangkan yang peneliti gunakan saat ini ialah model keamanan informasi *Defense in Depth* dengan cara melindungi 4 aspek di dalam sistem informasi yaitu aspek *Governance, People, Pracesses* dan *Technology*.

Sedangkan Kebaruan yang peneliti lakukan pada penelitian saat ini yaitu terletak pada kerangka kerja yang digunakan, jika kerangka kerja *ISO 27001:2005* pernah digunakan pada sistem pengadaan secara elektronik seperti yang telah dilakukan oleh Muhammad Chandra (2017) maka penerapan kerangka kerja atau model keamanan informasi *defense in depth* belum pernah sama sekali diterapkan pada sistem pengadaan secara elektronik di Indonesia. Sehingga penerapan model keamanan informasi d*efense in depth* pada sistem pengadaan secara elektronik ini merupakan penelitian yang pertama dilakukan. Selain itu penerapan strategi keamanan informasi pada sistem pengadaan secara elektronik provinsi Lampung belum pernah dilakukan sebelumnya. Sehingga penerapan strategi keamanan informasi untuk menghadapi ancaman siber pada sistem pengadaan secara elektronik provinsi Lampung ini merupakan yang pertama dilakukan.

BAB III
METODOLOGI PENELITIAN

3.1 Desain Peneiltian

Penelitian ini merupakan sebuah penelitian dengan metode kualitatif berdasarkan studi serangan *hacker* pada SPSE Provinsi Lampung Tahun 2015. Bogdan dan Taylor dalam Moleong mendefinisikan penelitian kualitatif sebagai prosedur penelitian yang menghasilkan data deskriptif berupa kata-kata tertulis atau lisan dari orang-orang dan perilaku yang diamati dari fenomena yang terjadi.[42] Lebih lanjut Moleong mengemukakan bahwa penelitian deskriptif menekankan pada data berupa kata-kata, gambar, dan bukan angka-angka yang disebabkan oleh adanya penerapan metode kualitatif. Selain itu, semua yang dikumpulkan berkemungkinan menjadi kunci terhadap apa yang sudah diteliti.[43]

Adapun pelaksanaan penelitian ini akan fokus pada studi serangan *hacker* pada Sistem Pengadaan Secara Elektronik Provinsi Lampung tahun 2015. Berikut ini peneliti akan menguraikan kerangka metodologi penelitian yang akan digunakan dalam proses pelaksanaan penelitian.

3.2 Tempat dan Waktu Penelitian

3.2.1 Tempat Penelitian

Tempat penelitian atau yang disebut juga lokus penelitian adalah lokasi-lokasi yang telah ditentukan secara *purposive* oleh peneliti untuk mendapatkan data penelitian. Proses penentuan tempat penelitian dilakukan secara logis sesuai dengan kebutuhan data yang ingin digali. Hal ini bertujuan agar penelitian dapat dikendalikan sehingga dapat dilaksanakan sesuai dengan waktu yang telah ditentukan. Penelitian ini akan dilaksanakan di LPSE Provinsi Lampung sesuai dengan rumusan masalah.

[42] J. Moleong, Op. cit. hlm. 4.
[43] *Ibid*. hlm 11.

3.2.2 Waktu Penelitian

Proses penelitian akan dilaksanakan pada bulan Juni 2018 hingga bulan November 2018, dengan rincian jadwal sebagai berikut:

Tabel 3.1 Jadwal Penelitian

No	Kegiatan	2018							2019	
		Jun	Jul	Ags	Sep	Okt	Nov	Des	Jan	Feb
1	Studi Pendahuluan									
2	Bimbingan Proposal									
3	Seminar Proposal									
4	Pengumpulan Data									
5	Analisis Data									
6	Penyusunan Tesis									
7	Konsultasi dan bimbingan									
8	Ujian Tesis									
9	Perbaikan Tesis									
10	Penyerahan Tesis									

3.3 Subyek dan Obyek Penelitian

3.3.1 Subyek Penelitian

Subjek penelitian oleh Moleong dideskripsikan sebagai informan, yang bermakna bahwa seseorang yang dimanfaatkan untuk memberikan informasi tentang situasi dan kondisi latar penelitian dikarenakan yang bersangkutan dinilai memiliki kapabilitas untuk memberikan informasi terkait penelitian[44]. Sejalan dengan definisi tersebut, dalam Buku Pedoman Penulisan Tesis dan Disertasi Unhan, disebutkan bahwa subjek penelitian yaitu orang-orang atau siapa saja yang dapat dijadikan sebagai

[44] Lexy J. Moleong, *op. cit.,* hlm. 132.

informan/narasumber yang dijadikan sumber data/informasi dalam penelitian.

Adapun subyek dari penelitian ini disesuaikan dengan lokus penelitian, yakni orang-orang yang memiliki kewenangan dan kapasitas untuk memberikan data/informasi pada lembaga yang menjadi lokus penelitian. Penentuan subyek penelitian ini menggunakan teknik *purposive sampling*, yakni teknik pengambilan sampel sumber data dengan pertimbangan tertentu[45]. Makna dari pertimbangan tersebut adalah orang yang dijadikan sebagai narasumber dinilai paling tahu tentang apa yang peneliti harapkan. Hal tersebut dikarenakan narasumber merupakan orang yang memiliki kapasitas yang memahami situasi sosial yang diteliti. Beberapa subyek tersebut adalah:

1. Dodi Hendrawan, ST. (Kepala Kepala Bagian LPSE Provinsi Lampung);
2. Yusron, ST (Kepala Subbagian Pengembangan Sistem Informasi LPSE Provinsi Lampung);
3. Andi Ahmad Yusuf, S.Kom., MM. (Kepala Subbagian Pengendalian dan Administrasi Pembangunan Provinsi Lampung);

3.3.2 Obyek Penelitian

Obyek penelitian adalah variabel atau apa yang menjadi titik perhatian suatu penelitian, sedangkan subyek penelitian merupakan tempat dimana variabel melekat[46]. Oleh karena itu, obyek pada penelitian ini adalah strategi keamanan informasi dalam menghadapi ancaman siber pada Sistem Pengadaan Secara Elektronik.

[45] Sugiyono, *op. cit.,* hlm. 218-219.
[46] Suharsimi Arikunto, *Prosuder Penelitian Suatu Pendekatan Praktek.* (Jakarta: PT. Rineka Cipta, 1998), hlm. 15.

3.4 Teknik Pengumpulan Data

Teknik pengumpulan data dalam penelitian kualitatif secara umum dapat dikelompokkan ke dalam dua cara yatu teknik pengumpulan data yang bersifat interaktif dan non interaktif.[47]

Dalam penelitian ini peneliti menggunakan teknik interaktif termasuk di dalamnya meliputi:

1. Wawancara

Dalam penelitian kualitatif pada umumnya wawancara tidak dilakukan secara terstruktur ketat. Wawancara dilakukan dengan pertanyaan yang mengarah pada kedalaman informasi serta dilakukan dengan cara tidak secara formal terstruktur. Wawancara mendalam dapat dilakukan pada waktu dan kondisi konteks yang dianggap paling tepat guna mendapat data yang rinci, jujur dan mendalam. Narasumber yang akan diwawancarai adalah Ketua dan Admin Sistem Layanan Pengadaan Secara Elektronik (LPSE) Provinsi Lampung, Kepala Direktorat Pengembangan Sistem Pengadaan Secara Elektronik (SPSE) LKPP. serta para pemangku kepentingan dan pengambil kebijakan dalam lembaga atau organisasi yang akan dijadikan sebagai lokus dari penelitian ini.

2. Observasi

Teknik Observasi digunakan untuk menggali data dari sumber data yang berupa peristiwa, tempat atau lokasi, dan benda, serta rekaman gambar.[48] Observasi ini dilakukan dengan melihat langsung aktivitas, dalam penelitian ini melihat langsung kegiatan di Layanan Pengadaan Secara Elektronik (LPSE) provinsi Lampung.

---

[47] Sutopo, *Metodologi Penelitian Kualitatif*, (Surakarta: Sebelas Maret University Press, 2002), hlm. 50.
[48] Ibid. hlm. 64-65

3. Dokumentasi

Dokumen merupakan catatan peristiwa yang sudah berlalu[49]. Dokumen dapat berbentuk tulisan, gambar maupun karya. Dokumen berupa tulisan seperti catatan harian, sejarah kehidupan, biografi, peraturan dan kebijakan. Dokumen berbentuk gambar misalnya foto, gambar hidup, sketsa dan lain-lain. Dokumen berbentuk karya misalnya karya seni seperti patung, gambar, film dan lain-lain[50]. Dengan demikian, peneliti akan menggunakan dokumen-dokumen yang dimiliki oleh lembaga atau subjek yang akan diteliti yakni dokumen yang ada pada LPSE Provinsi Lampung dan Lembaga Kebijakan Pengadaan Pemerintah (LKPP).

4. Studi Kepustakaan

Menurut Koentjaraningrat teknik kepustakaan merupakan cara pengumpulan data bermacam-macam material yang terdapat di ruang kepustakaan seperti koran, buku-buku, majalah, naskah, dokumen dan sebagainya yang relevan dengan penelitian[51].

3.5 Pemeriksaan Keabsahan Data

Keabsahan data dalam penelitian kualitatif memegang peranan yang sangat penting. Hal ini dikarenakan penelitian kualitatif harus memaparkan kebenaran secara objektif. Kredibilitas penelitian kualitatif dapat tercapai apabila data yang diperoleh memiliki tingkat keabsahan yang dapat dipertanggungjawabkan. Untuk mendapatkan keabsahan data dalam penelitian ini diterapkan cara triangulasi. Dimana dalam pengertiannya triangulasi adalah teknik pemeriksaan keabsahan data yang memanfaatkan sesuatu yang lain dalam membandingkan hasil wawancara terhadap objek penelitian[52]. Denzin dalam Moloeng,

[49] Sugiyono, *op. cit.,* hlm. 240.
[50] *Ibid.*
[51] Koentjaraningrat, *Metode-Metode Penelitian Masyarakat*, (Jakarta: Gramedia, 1983), hlm. 420.
[52] J. Moleong. Op. cit. hlm. 330

membedakan empat macam triangulasi diantaranya dengan memanfaatkan penggunaan sumber, metode, penyidik dan teori. Pada penelitian ini penulis menggunakan teknik pemeriksaan dengan memanfaatkan sumber.[53]

Menurut Patton, Triangulasi dengan sumber artinya membandingkan dan mengecek balik derajat kepercayaan suatu informasi yang diperoleh melalui waktu dan alat yang berbeda dalam penelitian kualitatif.[54] Adapun untuk mencapai kepercayaan itu, maka dalam penelitian ini ditempuh langkah sebagai berikut:

1. Membandingkan data hasil pengamatan dengan data hasil wawancara;
2. Membandingkan hasil wawancara dan pengamatan dengan pendapat-pendapat para pakar/akademisi;
3. Membandingkan keadaan dan perspektif seseorang dengan berbagai pendapat dan pandangan masyarakat yang turut berpartisipasi;
4. Membandingkan hasil wawancara dengan isi suatu dokumen /data yang berkaitan.

3.6 Teknik Analisis Data

Teknik analisis data adalah proses pengumpulan data secara sistematis untuk mempermudah peneliti dalam memperoleh kesimpulan. Analisis data menurut Bogdan dalam Sugiyono yaitu proses mencari dan menyusun secara sistematik data yang diperoleh dari hasil wawancara, catatan lapangan, dan bahan-bahan lain sehingga dapat mudah dipahami dan temuannya dapat diinformasikan kepada orang lain.[55] Analisis data kualitatif bersifat induktif, yaitu analisis berdasarkan data yang diperoleh.

---

[53] *Ibid*.
[54] Patton, Michael Quinn. *Qualitative Education Methods*, (Beverly Hills: Sage Publication, 1987) hlm. 331
[55] Sugiyono, Op. cit. hlm. 334.

Dalam penelitian ini, teknik analisis data yang digunakan adalah teknik analisis data di lapangan model Miles dan Huberman. Menurut Miles & Huberman analisis terdiri dari tiga alur kegiatan yang terjadi secara bersamaan yaitu: reduksi data, penyajian data, penarikan kesimpulan/verifikasi.[56] Mengenai ketiga alur tersebut secara lebih lengkapnya adalah sebagai berikut:

1. Reduksi Data

Reduksi data diartikan sebagai proses pemilihan, pemusatan perhatian pada penyederhanaan, pengabstrakan, dan transformasi data kasar yang muncul dari catatan-catatan tertulis di lapangan. Reduksi data berlangsung terus-menerus selama proyek yang berorientasi penelitian kualitatif berlangsung. Antisipasi akan adanya reduksi data sudah tampak waktu penelitiannya memutuskan (seringkali tanpa disadari sepenuhnya) kerangka konseptual wilayah penelitian, permasalahan penelitian, dan pendekatan pengumpulan data mana yang dipilihnya. Selama pengumpulan data berlangsung, terjadilan tahapan reduksi selanjutnya (membuat ringkasan, mengkode, menelusur tema, membuat gugus-gugus, membuat partisi, membuat memo). Reduksi data/transformasi ini berlanjut terus sesudah penelian lapangan, sampai laporan akhir lengkap tersusun.

2. Penyajian Data

Miles & Huberman membatasi suatu penyajian sebagai sekumpulan informasi tersusun yang memberi kemungkinan adanya penarikan kesimpulan dan pengambilan tindakan. Mereka meyakini bahwa penyajian-penyajian yang lebih baik merupakan suatu cara yang utama bagi analisis kualitatif yang valid, yang meliputi: berbagai jenis matrik, grafik, jaringan dan bagan.

[56] Milles dan Huberman, *Analisis Data Kualitatif*, (Jakarta: Universitas Indonesia Press, 1992), hlm. 16.

Semuanya dirancang guna menggabungkan informasi yang tersusun dalam suatu bentuk yang padu dan mudah diraih. Dengan demikian seorang penganalisis dapat melihat apa yang sedang terjadi, dan menentukan apakah menarik kesimpulan yang benar ataukah terus melangkah melakukan analisis yang menurut saran yang dikisahkan oleh penyajian sebagai sesuatu yang mungkin berguna.

3. Penarikan Kesimpulan

Penarikan kesimpulan menurut Miles & Huberman hanyalah sebagian dari satu kegiatan dari konfigurasi yang utuh. Kesimpulan-kesimpulan juga diverifikasi selama penelitian berlangsung. Verifikasi itu mungkin sesingkat pemikiran kembali yang melintas dalam pikiran penganalisis (peneliti) selama ia menulis, suatu tinjauan ulang pada catatan-catatan lapangan, atau mungkin menjadi begitu seksama dan menghabiskan tenaga dengan peninjauan kembali serta tukar pikiran di antara teman sejawat untuk mengembangkan kesepakatan intersubjektif atau juga upaya-upaya yang luas untuk menempatkan salinan suatu temuan dalam seperangkat data yang lain. Singkatnya, makna-makna yang muncul dari data yang lain harus diuji kebenarannya, kekokohannya, dan kecocokannya, yakni yang merupakan validitasnya. Kesimpulan akhir tidak hanya terjadi pada waktu proses pengumpulan data saja, akan tetapi perlu diverifikasi agar benar-benar dapat dipertanggungjawabkan.

BAB IV
HASIL PENELITIAN DAN PEMBAHASAN

4.1 Hasil Penelitian

Penelitian sebagai upaya pengumpulan data telah dilaksanakan dengan cara wawancara, observasi, studi dokumentasi dan studi kepustakaan. Hasil penelitian ini akan diuraikan sesuai dengan subfokus yang telah ditetapkan sebelumnya yaitu: pelaksanaan LPSE Provinsi Lampung dalam mengamankan sistem informasi pada sistem pengadaan secara elektronik dan strategi keamanan informasi dalam menghadapi ancaman siber pada sistem pengadaan secara elektronik.

4.1.1 Gambaran Umum Provinsi Lampung

Lampung adalah sebuah provinsi paling selatan di Pulau Sumatera, Indonesia, dengan Ibukota yang terletak di Bandar Lampung. Provinsi ini memilki 2 Kota dan 13 Kabupaten. Kota yang dimaksud adalah Kota Bandar Lampung dan Kota Metro. Di sebelah utara berbatasan dengan Bengkulu dan Sumatera Selatan. Secara Geografis Provinsi Lampung memiliki luas 35.376,50 km² dan terletak pada kedudukan: Timur-Barat berada antara : 103º 40’ – 105º 50’ Bujur Timur Utara-Selatan berada antara : 6º 45’ – 3º 45’ Lintang Selatan. Beberapa pulau termasuk dalam wilayah Provinsi Lampung, yang sebagian besar terletak di Teluk Lampung, di antaranya: Pulau Darot, Pulau Legundi, Pulau Tegal, Pulau Sebuku, Pulau Ketagian, Pulau Sebesi, Pulau Poahawang, Pulau Krakatau, Pulau Putus dan Pulau Tabuan. Ada juga Pulau Tampang dan Pulau Pisang di yang masuk ke wilayah Kabupaten Lampung Barat.[57]

Provinsi Lampung lahir pada tanggal 18 Maret 1964 dengan ditetapkannya Peraturan Pemerintah Nomor 3 tahun 1964 yang kemudian menjadi Undang-undang Nomor 14 tahun 1964. Sebelum itu Provinsi Lampung merupakan Karesidenan yang tergabung dengan Provinsi

[57] Provinsi Lampung, https://id.wikipedia.org/wiki/Lampung, diakses pada 28 Januari 2018

Sumatera Selatan. Pada tahun 1997 wilayah Provinsi Lampung dimekarkan menjadi 7 kabupaten/kota, kemudian dengan diundangkannya UU No.12 Tahun 1999 dimekarkan lagi menjadi 10 kabupaten/kota. Berdasarkan UU No. 33 Tahun 2008 terbentuklah Kabupaten Pesawaran yang sebelumnya merupakan bagian dari Kabupaten Lampung Selatan. Dengan demikian Provinsi Lampung terdiri dari 9 kabupaten dan 2 kota. Tahun 2010 berubah menjadi 12 Kabupaten dan 2 kota. Adanya Pemekaran Kabupaten Lampung Barat dan Pesisir Barat berdasarkan UU RI no 22 tahun 2012, menjadikan Provinsi Lampung terdiri dari 13 Kabupaten dan 2 Kota. Di Provinsi Lampung terdapat 228 kecamatan dengan 2.643 desa/kelurahan.[58]

Penduduk Provinsi Lampung berdasarkan proyeksi penduduk tahun 2017 sebanyak 8.289.577 jiwa yang terdiri atas 4.247.121 jiwa penduduk laki-laki dan 4.042.456 jiwa penduduk perempuan. Dibandingkan dengan proyeksi jumlah penduduk tahun 2016, penduduk Lampung mengalami pertumbuhan sebesar 1,03 persen. Kepadatan penduduk di Provinsi Lampung tahun 2017 mencapai 239 jiwa/km2. Kepadatan Penduduk di 15 kabupaten/kota cukup beragam dengan kepadatan penduduk tertinggi terletak di Kota Bandar Lampung dengan kepadatan sebesar 3.432 jiwa/km^2 dan terendah di Kabupaten Pesisir Barat sebesar 52 jiwa/Km^2.

Berdasarkan data dari Peraturan Menteri Dalam Negeri Nomor 137 tahun 2017 tentang Kode Dan Data Wilayah Administrasi Pemerintahan. Disebutkan bahwa data jumlah penduduk dan luas wilayah kabupaten/kota di provinsi Lampung sebagai berikut :[59]

[58] Badan Pusat Statistik Provinsi Lampung. *Provinsi Lampung Dalam Angka 2018*. (Lampung : CV. Jaya Wijaya. 2018) hlm. xi

[59] Data jumlah penduduk dan luas wilayah kabupaten/kota di Provinsi Lampung dalam Peraturan Menteri Dalam Negeri Nomor 137 tahun 2017 tentang Kode Dan Data Wilayah Administrasi Pemerintahan.

Tabel 4.1 Data Jumlah Penduduk dan Luas Wilayah Kabupaten/Kota di Provinsi Lampung

No	Kabupaten /Kota	Luas Wilayah (Km^2)	Jumlah Penduduk	Jumlah Kecamatan	Jumlah Kelurahan /Desa
1	Kabupaten Lampung Barat	2.142,78	301.131	15	5/131
2	Kabupaten Lampung Selatan	700,32	1.269.262	17	4/256
3	Kabupaten Lampung Tengah	3.802,68	1.468.875	28	10/301
4	Kabupaten Lampung Timur	5.325,03	1.113.976	24	-/264
5	Kabupaten Lampung Utara	2.725,87	885.591	23	15/232
6	Kabupaten Mesuji	2.184,00	315.813	7	-/105
7	Kabupaten Pesawaran	2.243,51	546.160	11	-/144
8	Kabupaten Pesisir Barat	2.907,23	155.964	11	2/116
9	Kabupaten Pringsewu	625	421.180	9	5/126
10	Kabupaten Tanggamus	3.020,64	640.588	20	3/299
12	Kabupaten Tulang Bawang Barat	1.201,00	268.119	9	3/93
13	Kabupaten Way Kanan	3.921,63	479.256	14	6/221
14	Kota Bandar Lampung	296	1.175.397	20	126/-
15	Kota Metro	61,79	165.368	5	22/-

(Sumber : Pemendagri Nomor 137 Tahun 2017)

4.1.2 LPSE Provinsi Lampung

LPSE adalah unit kerja yang dibentuk di seluruh Kementerian/ Lembaga/Satuan Kerja Perangkat Daerah/Institusi Lainnya (K/L/D/I) untuk menyelenggarakan sistem pelayanan pengadaan barang/jasa secara elektronik serta memfasilitasi ULP/Pejabat Pengadaan dalam melaksanakan pengadaan barang/jasa secara elektronik. Dasar hukum pembentukan LPSE adalah Pasal 111 Nomor 54 Tahun 2010 tentang pengadaan barang/jasa pemerintah yang ketentuan teknis operasionalnya diatur oleh Peraturan Kepala LKPP Nomor 2 Tahun 2010 tentang Layanan Pengadaan Secara Elektronik. LPSE dalam menyelenggarakan sistem pelayanan Pengadaan Barang/Jasa secara elektronik juga wajib memenuhi persyaratan sebagaimana yang ditentukan dalam Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Layanan yang tersedia dalam Sistem Pengadaan Secara Elektronik saat ini adalah *e-tendering* yang ketentuan teknis operasionalnya diatur dengan Peraturan Kepala LKPP Nomor 1 Tahun 2011 tentang Tata Cara *E-Tendering*. Selain itu LKPP juga menyediakan fasilitas Katalog Elektronik (*e-Catalogue*) yang merupakan sistem informasi elektronik yang memuat daftar, jenis, spesifikasi teknis dan harga barang tertentu dari berbagai penyedia barang/jasa pemerintah, proses audit secara online (*e-Audit*), dan tata cara pembelian barang/jasa melalui katalog elektronik (*e-Purchasing*).

LPSE Provinsi Lampung merupakan salah satu bagian yang terdapat pada Biro Administrasi Pembangunan yang dibentuk berdasarkan Peraturan Daerah Provinsi Lampung No. 8 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Provinsi Lampung. Sebelum adanya peraturan daerah ini status LPSE Provinsi Lampung adalah *ad-hoc* (kepanitian). LPSE Provinsi Lampung terbentuk sejak tahun 2010 dan pada tahun 2011 untuk pertama kalinya melakukan proses pengadaan barang/jasa secara elektronik menggunakan aplikasi

SPSE versi 3.2, adapun struktur organisasi LPSE Provinsi Lampung saat ini sebagai berikut:

Gambar 4.1 Struktur Organisasi LPSE Provinsi Lampung

(Sumber : Laporan kegiatan dan kinerja LPSE Provinsi Lampung tahun 2017)

Dalam pelaksanaan Pengadaan Barang/Jasa LPSE Provinsi Lampung menerapkan prinsip-prinsip sebagai berikut:

a. Efisien
b. Efektif
c. Transparan
d. Terbuka
e. Bersaing
f. Adil/tidak diskriminatif, dan
g. Akuntabel

Dalam Peraturan Presiden 54 Tahun 2010 sebagaimana telah diubah dengan Peraturan Presiden 70 Tahun 2012, ketentuan tentang *e-procurement* dijelaskan bahwa Pengadaan barang secara elektronik

dilakukan dengan cara *e-tendering* dan *e-purchasing*. Pengadaan barang/jasa secara elektronik bertujuan untuk :

a. Meningkatkan transparansi dan akuntabilitas
b. Meningkatkan akses pasar dan persaingan usaha yang sehat
c. Memperbaiki tingkat efisiensi proses Pengadaan
d. Mendukung proses *monitoring* dan audit, dan
e. Memenuhi kebutuhan akses informasi yang *real time*

Fungsi LPSE Provinsi Lampung dalam kegiatan layanan pengadaan secara elektronik meliputi:

a. Pengelolaan seluruh sistem informasi Pengadaan Barang/Jasa dan infrastrukturnya
b. Pelaksanaan registrasi dan verifikasi pengguna seluruh sistem informasi Pengadaan Barang/Jasa, dan
c. Pengembangan sistem informasi yang dibutuhkan oleh pemangku kepentingan.

Penyelenggaraan Pengadaan Barang/Jasa dilakukan secara elektronik menggunakan sistem informasi yang terdiri atas Sistem Pengadaan Secara Elektronik (SPSE) dan sistem pendukung. Ruang lingkup SPSE terdiri atas:

a. Perencanaan Pengadaan
b. Persiapan Pengadaan
c. Pemilihan Penyedia
d. Pelaksanaan Kontrak
e. Serah Terima Pekerjaan
f. Pengelolaan Penyedia, dan
g. Katalog Elektronik.

Semua pihak yang terlibat dalam Pengadaan Barang/Jasa di LPSE Provinsi lampung harus mematuhi etika sebagai berikut:

a. Melaksanakan tugas secara tertib, disertai rasa tanggung jawab untuk mencapai sasaran, kelancaran, dan ketepatan tujuan Pengadaan Barang/Jasa
b. Bekerja secara profesional, mandiri, dan menjaga kerahasiaan informasi yang menurut sifatnya harus dirahasiakan untuk mencegah penyimpangan Pengadaan Barang/Jasa
c. Tidak saling mempengaruhi baik langsung maupun tidak langsung yang berakibat persaingan usaha tidak sehat
d. Menerima dan bertanggung jawab atas segala keputusan yang ditetapkan sesuai dengan kesepakatan tertulis pihak yang terkait
e. Menghindari dan mencegah terjadinya pertentangan kepentingan pihak yang terkait, baik secara langsung maupun tidak langsung, yang berakibat persaingan usaha tidak sehat dalam Pengadaan Barang/Jasa
f. Menghindari dan mencegah pemborosan dan kebocoran keuangan negara
g. Menghindari dan mencegah penyalahgunaan wewenang dan/atau kolusi, dan
h. Tidak menerima, tidak menawarkan, atau tidak menjanjikan untuk memberi atau menerima hadiah, imbalan, komisi, rabat, dan apa saja dari atau kepada siapapun yang diketahui atau patut diduga berkaitan dengan Pengadaan Barang/Jasa.

Pelaksanaan pengadaan barang/jasa secara elektronik di LPSE provinsi Lampung melalui Tender/Seleksi meliputi:

a. Pelaksanaan Kualifikasi
b. Pengumuman dan/atau Undangan
c. Pendaftaran dan Unduh Dokumen Pengadaan
b. Pemberian Penjelasan
a. Unggah Dokumen Penawaran

b. Evaluasi Dokumen Penawaran
c. Penetapan dan Pengumuman Pemenang, dan
d. Sanggah.

Tender/Seleksi dalam proses pengadaan secara elektronik gagal apabila dalam hal:

a. Terdapat kesalahan dalam proses evaluasi
b. Tidak ada peserta yang menyampaikan dokumen penawaran setelah ada pemberian waktu perpanjangan
c. Tidak ada peserta yang lulus evaluasi penawaran
d. Ditemukan kesalahan dalam Dokumen Pemilihan atau tidak sesuai dengan ketentuan dalam Peraturan Presiden ini
e. Seluruh peserta terlibat Korupsi, Kolusi, dan Nepotisme (KKN)
f. Seluruh peserta terlibat persaingan usaha tidak sehat
g. Seluruh penawaran harga Tender Barang/ Pekerjaan Konstruksi/ Jasa Lainnya di atas HPS
h. Negosiasi biaya pada Seleksi tidak tercapai, dan/atau
i. KKN melibatkan Pokja Pemilihan/ PPK.

Tindak lanjut dari Tender/Seleksi gagal dalam proses pengadaan secara elektronik maka Pokja Pemilihan segera melakukan:

a. Evaluasi penawaran ulang
b. Penyampaian penawaran ulang, atau
c. Tender/Seleksi ulang.

LPSE Provinsi Lampung sebagai salah satu unit kerja yang memberikan layanan dan fasilitasi pengadaan barang/jasa secara elektronik kepada Penyedia, Pokja, Intansi dan Auditor di lingkungan Pemerintah Provinsi Lampung memberikan pelayanan yang meliputi :

a. Pelayanan terhadap Penyedia
   1) Registrasi dan Verifikasi penyedia
   2) Lupa *user Id* dan atau *pasword* penyedia

3) Penanganan Gagal *Reset Password* Penyedia
4) Mendaftar sebagai Penyedia di LPSE
5) Mengubah Alamat *Email*
6) Muncul *Error* di Menu Pengguna
7) Pendampingan Proses Pengisian Data Penyedia
8) Pendampingan Proses *Upload* Dokumen Penawaran
9) Penggunaan *Bidding Room*;
10) Bimbingan Teknis/ Pelatihan Penggunaan Aplikasi SPSE.

b. Pelayanan terhadap Pokja
1) Ubah Jadwal Pelelangan;
2) Muncul *Error* di Menu Pengguna;
3) Uji Forensik File RHS;
4) Bimbingan Teknis / Pelatihan Penggunaan Aplikasi SPSE

c. Pelayanan kepada Instansi
1) Registrasi Admin *Agency*;
2) Registrasi Auditor;
3) Lupa *User ID* dan atau *Password* Admin *Agency*;
4) Lupa *User ID* dan atau *Password* Auditor;
5) Bimbingan Teknis/Pelatihan Penggunaan Aplikasi SPSE, SiRUP, dan Monev OL

d. Pelayanan kepada Auditor
1) Registrasi Auditor
2) Bimbingan Teknis / Pelatihan Penggunaan Aplikasi SPSE

Sebagai salah satu unit kerja yang memberikan layanan dan fasilitasi pengadaan barang/jasa secara elektronik, LPSE Provinsi Lampung juga memiliki beberapa fasilitas guna mendukung kinerja organisasi agar pemenuhan kebutuhan terkait pengadaan barang/jasa secara elektronik bagi *stakeholder* bisa terpenuhi secara maksimal. Adapun beberapa fasilitas yang di miliki tersebut sebagai berikut:

a. **_Server_ Utama dan _Server Backup_**

1) *Server* Utama *Coolocation* di Jakarta

Gambar 4.2 Server Utama LPSE Provinsi Lampung

(Sumber : Laporan kegiatan dan kinerja LPSE Provinsi Lampung tahun 2017)

Untuk *server* utama SPSE Provinsi Lampung *coolocation* di Jakarta, *colocation server* maksudnya ialah meletakan/menitipkan *server* pada sebuah ruangan di data center miliki sebuah perusahaan penyedia layanan internet dengan membayar sewa tempat dan jasa pengelolaan *server*.

1) *Server Backup* yang berada di LPSE Provinsi Lampung

Gambar 4.3 Server Backup LPSE Provinsi Lampung

(Sumber : Laporan kegiatan dan kinerja LPSE Provinsi Lampung tahun 2017)

Ruangan ini merupakan ruangan yang digunakan untuk pengelolaan *server backup* SPSE yang terletak di Kantor LPSE Provinsi Lampung. Selain digunakan untuk ruang pengelolaan *server backup* SPSE ruangan ini juga digunakan untuk pengelolaan *server* pelaporan milik Biro Administrasi Pembangunan Provinsi Lampung.

b. **Ruang *Helpdesk***

Gambar 4.4 Ruang *Helpdesk* LPSE Provinsi Lampung

(Sumber : Laporan kegiatan dan kinerja LPSE Provinsi Lampung tahun 2017)

Ruangan ini merupakan ruangan yang disediakan oleh LPSE Provinsi Lampung yang dimaksudkan untuk tujuan konsultasi dan pemberian layanan/bantuan kepada penyedia, pokja dan pihak organsasi perangkat daerah (OPD) yang terlibat di dalam sistem pengadaan barang dan jasa secara elektronik. adapun layanan/bantuan yang diberikan *helpdesk* LPSE Provinsi Lampung meliputi layanan pendaftaran dan pembuatan akun, layanan *reset password* jika pengguna lupa dengan *login* akunnya maka *helpdesk* bisa membantu *reset password,* dan juga memberikan konsultasi terkait aturan, mekanisme dan permasalahan pengadaan barang dan jasa secara elektronik.

c. Ruang *Bidding*

Gambar 4.5 Ruang *Bidding* LPSE Provinsi Lampung

(Sumber : Laporan kegiatan dan kinerja LPSE Provinsi Lampung tahun 2017)

Ruangan ini merupakan ruangan yang difasilitasi dengan adanya perangkat komputer dan jaringan internet, fungsi dari ruang *bidding* ini untuk memberikan kemudahan dan akses kepada penyedia, pokja ataupun instansi dalam kegiatan pengadaan secara elektronik. Selain itu ruangan ini juga bisa digunakan penyedia untuk mengikuti proses pengadaan secara elektronik mulai dari proses pendaftaran, *download* dokumen pengadaan, *upload* dokumen kualifikasi, *upload* dokumen penawaran, hingga sanggah. Meskipun ruangan ini dapat digunakan oleh Penyedia maupun Pokja, akan tetapi Penyedia dan Pokja di larang menggunakan ruangan ini secara bersama-sama dalam satu waktu. Hal ini dilakukan agar menghindari kecurangan yang dilakukan oleh Pokja dan Penyedia. Karena bisa memungkinkan terjadinya kesepakatan antara Pokja dan Penyedia dalam penentuan pemenang lelang. Sehingga proses lelang menjadi tidak transparan.

d. Ruang Pelatihan Dan Rapat

Gambar 4.6 Ruang Pelatihan dan Rapat LPSE Provinsi Lampung

(Sumber : Laporan kegiatan dan kinerja LPSE Provinsi Lampung tahun 2017)

Ruangan ini digunakan sebagai ruang rapat internal LPSE Provinsi Lampung untuk membahas program-program kerja LPSE Provinsi Lampung, akan tetapi ruangan ini juga digunakan untuk pelatihan penggunaan aplikasi SPSE baik pelatihan untuk penyedia, pojka maupun pelatihan untuk pihak OPD.

Untuk mempermudah pengguna dalam melakukan proses pengadaan barang/jasa secara elektronik maka dibangunlah suatu aplikasi *interface* (tatap muka) untuk pelaksanaan pengadaan barng/jasa secara elektronik tersebut. Kegunakan aplikasi ini sebagai media *interface* yang dapat menjembatani dan penghubung antara *stakeholder* yang terlibat dalam sistem pengadaan barang/jasa, dengan adanya aplikasi *interface* Penyedia dan Pokja bisa tanya jawab terkait paket pekerjaan yang sedang di lelang, Penyedia dan Pokja dan unduh dan unggah dokumen sehingga tidak perlu melakukan pencetakan dokumen. Serta dengan adanya aplikasi ini proses pengadaan bisa dilakukan dan di pantau dari manapun dan kapan pun dikarenakan aplikasi ini bisa di akses

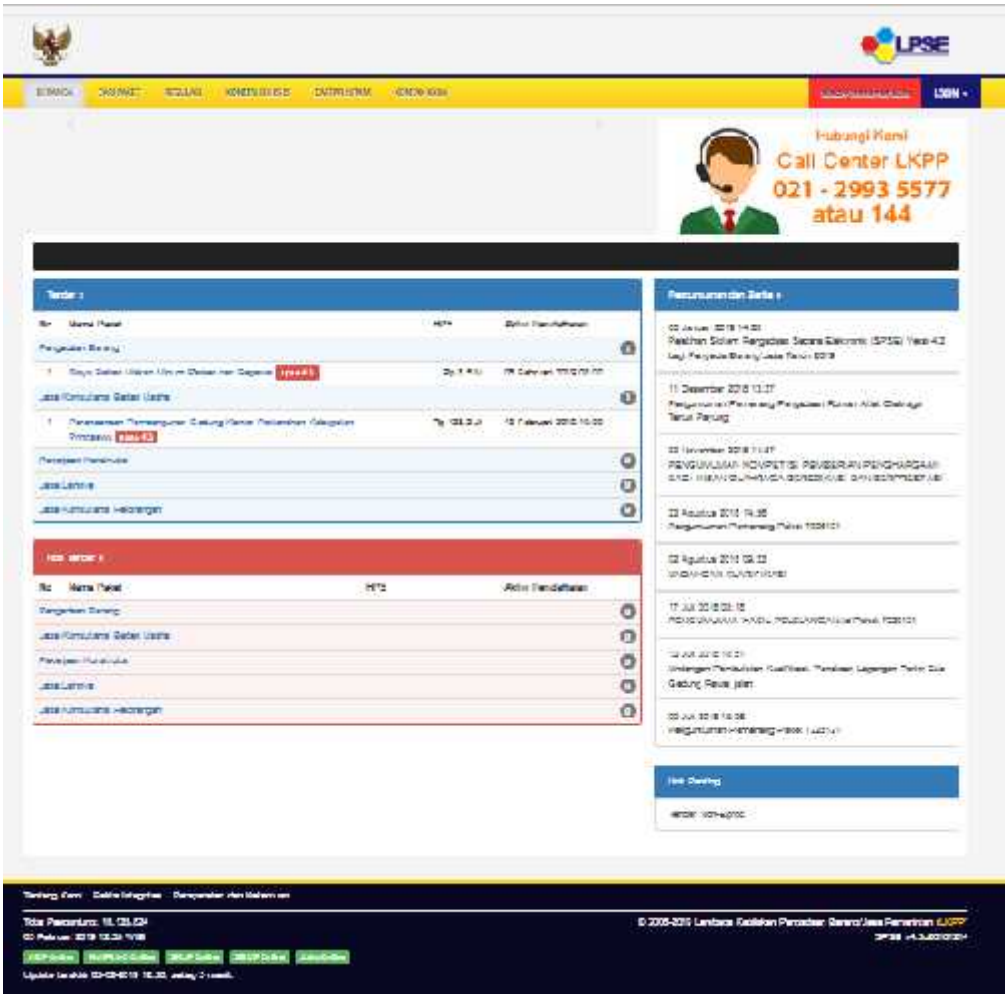
melalui internet. Semua stakeholder dapat melihat dan memantau tender mulai dari proses pengumuman paket pelelangan hingga pengumuman pemenang paket pelelangan. Aplikasi Sistem Pengadaan Secara Elektronik (SPSE) sendiri terus dikembangankan hingga saat ini. dan sudah dikembangkan dari versi 1 hingga menjadi SPSE versi 4.2. Namun penggunaan SPSE secara nasional baru bisa terealisasi melalui SPSE Versi 3.0 pada versi sebelumnya masih dalam tahap uji coba. Aplikasi SPSE sendiri merupakan aplikasi berbasis website dengan sistem *open source* yang artinya siapapun dapat berkontribusi untuk mengembangkan aplikasi ini. Adapun tampilan aplikasi SPSE tersebut sebagai berikut :

a. Tampilan Aplikasi SPSE Versi 3.2

Gambar 4.7 Tampilan SPSE Versi 3.2

(Sumber : http://lpse.tanggamus.go.id/eproc)

b. Tampilan Aplikasi SPSE Versi 4.2



Gambar 4.8 Tampilan Aplikasi SPSE Versi 4.2

(Sumber : http://lpse.tanggamus.go.id/eproc4)

4.1.3 Serangan *Hacker* Pada SPSE Provinsi Lampung Tahun 2015

Dari hasil penelitian didapatkan data bahwa pada tahun 2015 memang telah terjadi serangan *hacker* pada SPSE Provinsi Lampung yang menyebabkan 168 dari 169 paket pengadaan yang saat itu sedang proses lelang harus dilakukan tander ulang, hal ini diakibatkan oleh serangan *hacker* dengan teknik *Distributed Denial of Service (DDos)* yang membuat *server* SPSE Provinsi Lampung *down* (tidak dapat diakses).

Menurut Kepala Subbagian Pengembangan Sistem Informasi, Yusron, ST., yang sekaligus *admin PPE* pada sistem pengadaan secara elektronik saat diwawancarai oleh peneliti pada Senin, 14 Desember 2018 di ruang kerjanya, menjelaskan bagaimana kronologi serangan *hacker* yang terjadi pada tahun 2015 tersebut, Kepala Subbagian Pengembangan Sistem Informasi, Yusron, ST., mengatakan bahwa serangan tersebut terjadi tepatnya pada bulan April tahun 2015. Sebelum *server* SPSE Provinsi Lampung *down* (tidak dapat diakses) terjadi serangan secara besar dan terus-menerus menyerang *server* SPSE Provinsi Lampung yang mengakibatkan *floading* yaitu suatu kondisi dimana terlalu banyak yang mengakses *server* diwaktu yang bersamaan, hal ini menyebabkan *server down* sehingga tidak dapat diakses.

Kemudian Kepala Subbagian Pengendalian dan Administrasi Pembangunan, Andi Ahmad Yusuf, S.Kom., MM., yang sekaligus sebagai admin sistem saat diwawancarai oleh peneliti di hari yang sama menjelaskan kronologi serangan *hacker* secara lebih rinci, Kepala Subbagian Pengendalian dan Administrasi Pembangunan, Andi Ahmad Yusuf, S.Kom., MM., mengatakan bahwa sebelum serang besar tersebut terjadi, *hacker* tersebut sebelumnya telah meletakan *file java script* kedalam *server* SPSE Provinsi Lampung. Ketika *file* tersebut diaktifkan maka *file* tersebut seperti halnya sinyal yang memberikan tanda dimana lokasi sasaran untuk dilakukannya serangan secara besar-besaran. Namun sampai sekarang siapa pelaku dan bagaimana pelaku bisa memasukan *file java script* tersebut masih belum diketahui. Kepala Subbagian Pengendalian dan Administrasi Pembangunan, Andi Ahmad Yusuf, S.Kom., MM., mengatakan bahwa akibat serangan tersebut, proses pengadaan secara elektronik di LPSE Provinsi Lampung harus ditunda selama satu bulan yang mengakibatkan 168 dari 169 paket yang saat itu sedang proses lelang terpaksa harus tender ulang satu bulan kemudian. Untuk mengatisipasi serangan serupa terjadi lagi, pihak LPSE Provinsi Lampung mengganti *server* yang lama dengan *server* yang baru.

Sehingga membutuhkan waktu yang lama untuk instalasi ulang dan penginputan data ulang. Selain menyebabkan tertundanya pelaksanaan pekerjaan proyek pemerintah Provinsi Lampung juga menyebabkan kerugian secara materil akibat serangan tersebut, hal ini dikarenakan LPSE Provinsi Lampung harus menganggarkan dana untuk pembelian *server* baru.

Kepala Subbagian Pengendalian dan Administrasi Pembangunan, Andi Ahmad Yusuf, S.Kom., MM., mengakui bahwa pihak LPSE Provinsi Lampung sebelumnya telah melakukan kelalain dalam tata kelola sistem pengadaan secara elektronik yang mengakibatkan serangan *DDos* itu bisa terjadi. Menurut Kepala Subbagian Pengendalian dan Administrasi Pembangunan, Andi Ahmad Yusuf, S.Kom., MM., sebelum serangan itu terjadi, LPSE Provinsi Lampung menggunakan jasa pihak ke-3 (Penyedia) untuk mengelola *server* SPSE Provinsi Lampung sepenuhnya, mulai dari instalasi *operating sistem (OS)* hingga instalasi Aplikasi SPSE. Semua dilakukan oleh pihak ke-3. Dengan memberikan akses penuh kepada pihak ke-3 tersebut maka pihak ke-3 tersebut dapat mengakses secara penuh kedalam sistem. Sehingga bisa leluasa keluar masuk kedalam sistem. Termasuk mengubah atau mengganti data di dalam sistem. Sehingga setelah terjadinya serangan *hacker* pada bulan April 2015 tersebut, pihak LPSE Provinsi Lampung mengambil langkah cepat dengan mengganti penyedia yang mengelola *server* SPSE Provinsi Lampung tersebut dengan penyedia yang baru. Namun agar peristiwa serupa tidak terjadi lagi maka pihak LPSE provinsi Lampung tidak memberikan akses penuh dalam pengelolaan *server* SPSE kepada pihak penyedia yang baru. Pihak penyedia yang baru hanya bertanggung jawab untuk memastikan bahwa server dapat hidup 24 jam *non-stop* dan *server* dapat terkoneksi dengan internet sehingga dapat diakses oleh siapapun dan dimanapun. Sistem kerjasama ini banyak diterapkan oleh LPSE yang ada di Indonesia. Sistem ini disebut dengan sistem *Coolocation*.

Dari hasil wawancara dengan Kepala Subbagian Pengendalian dan Administrasi Pembangunan, Andi Ahmad Yusuf, S.Kom., MM., dan Kepala Subbagian Pengembangan Sistem Informasi, Yusron, ST., peneliti menemukan fakta baru bahwa ternyata pada bulan juli 2018 serangan *hacker* kembali lagi terjadi pada SPSE Provinsi Lampung. Namun serangan kali ini berbeda dari serangan sebelumnya. Kepala Subbagian Pengendalian dan Administrasi Pembangunan, Andi Ahmad Yusuf, S.Kom., MM., menjelaskan serangan *hacker* yang terjadi pada bulan juli 2018 tersebut tidak sampai mengakibatkan kerusakan terhadap *server* SPSE provinsi Lampung. *Hacker* hanya mengganggu 3 paket pengadaan yang sedang proses lelang di LPSE provinsi Lampung. Akibat gangguan yang dilakukan oleh *hacker* tersebut membuat 3 paket pengadaan harus tander ulang. Dan 1 dari ke 3 paket tersebut harus di ulang sebanyak 3 x, bahkan harus memaksa Pokja untuk melakukan tender di LPSE lain yaitu LPSE Poli Teknik Negeri Lampung (Polinela). Kepala Subbagian Pengendalian dan Administrasi Pembangunan, Andi Ahmad Yusuf, S.Kom., MM., mengatakan bahwa teknik yang dilakukan oleh *hacker* tersebut yaitu dengan mengubah atau mengganti *file* penawaran yang sudah di *upload* oleh penyedia dengan *file* yang berbeda. Sehingga ketika proses pembukaan penawaran oleh Pokja, *file* penawaran berubah dan tidak sesuai dengan aslinya. Namun Kepala Subbagian Pengendalian dan Administrasi Pembangunan, Andi Ahmad Yusuf, S.Kom., MM., menduga bahwa hal ini bukanlah murni serangan *hacker* yang menerobos kedalam sistem. Sebab setelah dilakukan pengecekan kedalam sistem ternyata tidak aktifitas yang mencurigakan didalam sistem. Kepala Subbagian Pengendalian dan Administrasi Pembangunan, Andi Ahmad Yusuf, S.Kom., MM., menambahkan bahwa kemungkinan besar ada faktor kelalaian yang dilakukan oleh pihak penyedia yang bersangkutan. Sebab sebelumnya pihak penyedia tersebut sudah beberapa kali meminjamkan perusahaannya kepada pihak lain. Dengan meminjamkan perusahaan tersebut tentu juga meminjamkan *login* SPSE-nya kepada pihak tersebut.

Sehingga ada banyak pihak yang sudah mengetahui *login* dari perusahaan tersebut. Hal ini yang mungkin dimanfaatkan oleh oknum yang tidak bertanggung jawab untuk mengubah atau mengganti dokumen penawaran yang telah di *upload* oleh penyedia tersebut.

Kepala Subbagian Pengendalian dan Administrasi Pembangunan, Andi Ahmad Yusuf, S.Kom., MM., mengatakan untuk menghindari hal serupa terjadi kembali, pihak LPSE provinsi Lampung saat ini kerap kali mengingatkan kepada pihak penyedia dan panitia di sela-sela pelatihan penggunaan SPSE untuk pentingnya menjaga kerahasian *login* mereka dengan mengubah *login* secara berkala minimal 1 bulan sekali dan membatasi penggunaan *login* mereka kepada pihak lain.

4.1.4 Strategi Keamanan Informasi Dalam Menghadapi Ancaman Siber Pada Sistem Pengadaan Secara Elektronik Provinsi Lampung.

Dari hasil wawancara, observasi dan studi dokumentasi yang dilakukan oleh peneliti terhadap objek penelitian yaitu LPSE Provinsi Lampung, peneliti menemukan banyak data dan fakta terkait keamanan infomasi yang ada pada LPSE Provinsi Lampung. Dalam model keamanan informasi *defense in depth* terdapat 4 aspek penting yang harus dilindungi yang meliputi aspek: *governace*, *people*, *process* dan *technology*. Dari hasil pengumpulan data terkait 4 aspek tersebut pada LPSE Provinsi lampung sebagai berikut:

a. Aspek *Governace*

Pada Aspek ini mengacu pada kerangka manajemen yang digunakan untuk memberikan pengawasan dan koordinasi pada aspek *people, process*es dan *technology* yang meliputi: manajemen resiko, keamanan informasi dan penyesuaian kebijakan. Dari wawancara yang dilakukan oleh peneliti kepada Kepala Bagian LPSE, Dodi Hendrawan, ST., mengatakan bahwa sebelum keluarnya Peraturan Presiden dan Peraturan LKPP yang baru yaitu Peraturan Presiden No. 16 Tahun 2018

tentang Pengadaan Barang/Jasa Pemerintah, Peraturan LKPP No.14 Tahun 2018 tentang Unit Kerja Pengadaan Barang/Jasa dan Peraturan LKPP No.19 Tahun 2018 Tentang Pengembangan Sistem dan Kebijakan Pengadaan, pihak LPSE Provinsi Lampung memiliki turunan berupa Peraturan Daerah No. 8 Tahun 2016 yang mengatur tentang tata kelola LPSE Provinsi Lampung. Namun setelah keluarnya Peraturan yang baru tersebut saat ini LPSE Provinsi Lampung belum memiliki aturan turunan yang baru. Kepala Bagian LPSE, Dodi Hendrawan, ST., mengatakan bahwa alasan LPSE Provinsi Lampung belum mengeluarkan regulasi turunan tersebut dikarenakan pihak LPSE Provinsi Lampung menilai bahwa di dalam Peraturan Presiden No. 16 Tahun 2018, Peraturan LKPP No.14 Tahun 2018 dan Peraturan LKPP No.19 Tahun 2018 sudah mengatur dengan sangat jelas terkait pengadaan barang dan jasa. Sehingga saat ini pihak LPSE Provinsi Lampung hanya berpedoman pada peraturan yang sudah ada tanpa membuat aturan turunan. Sedangkan terkait regulasi yang berupa aturan tertulis atau SOP tentang keamanan informasi dan manajemen resiko belum ada. Saat ini LPSE Provinsi Lampung lebih fokus kepada upaya pencapaian standar yang telah ditetapkan oleh LKPP, yaitu terdapat 17 standar yang harus di penuhi oleh setiap LPSE di Indonesia. Dari 17 standar tersebut, LPSE Provinsi Lampung sudah mendapatkan 12 sertifikat terkait standar pengelolaan LPSE yaitu sertifikat untuk standar: 1. Pengelolaan Layanan Helpdesk, 2. Pengelolaan Kelangsungan Layanan, 3. Pengelolaan Pendukung Layanan, 4. Pengelolaan Resiko Layanan, 5. Pengorganisasian Layanan, 6. Kebijakan Layanan, 7. Pengelolaan Anggaran Layanan, 8. Pengelolaan Aset Layanan, 9. Pengelolaan Hubungan Dengan Layanan, 10. Pengelolaan Kapasitas, 11. Pengelolaan Perubahan, 12. Pengelolaan Sumber Daya Manusia. Sedangkan 5 standar yang belum dicapai yaitu standar : 1. Pengelolaan Keamanan Perangkat, 2. Keamanan Operational Layanan, 3. Keamanan Server dan Jaringan, 4. Pengelolaan Kepatuhan, 5. Penilaian Internal.

Namun yang disayangkan dari 12 pencapaian standar yang sudah di raih LPSE Provinsi Lampung belum ada yang terkait dengan pengelolaan keamanan informasi. Justru 3 standar tentang keamanan informasi yaitu: 1. Pengelolaan Keamanan Perangkat, 2. Keamanan Operational Layanan, 3. Keamanan Server belum tercapai.

Dari apa yang telah diuraikan diatas dapat disimpulkan bahwa pada aspek Governance ini LPSE Provinsi Lampung belum memenuhi standar model keamanan defense in depth hal ini dikarenakan LPSE Provinsi Lampung belum memiliki aturan atau standar terkait pengelolaan keamanan informasi dan manajemen resiko.

b. Aspek *People*

Pada aspek people menguraikan definisi tentang pemeliharaan dan penegakan peran dan tanggung jawab keamanan bagi pegawai dan vendor internal dan eksternal yaitu keamanan personil (termasuk kesadaran pengguna). Dalam wawancara dengan peneliti terkait aspek people ini Kepala Bagian LPSE, Dodi Hendrawan, ST., mengatakan bahwa saat ini LPSE Provinsi Lampung belum memiliki sumber daya manusia yang cukup khususnya yang dapat memahami *IT,* saat ini LPSE Provinsi Lampung hanya memiliki satu orang pegawai lulusan sarjana komputer. Sehingga hal tersebut masih belum cukup. Terkait kerahasian data dan login, Kepala Bagian LPSE, Dodi Hendrawan, ST., mengatakan bahwa setiap pegawai yang berada di LPSE Provinsi Lampung diikat secara hukum dengan pakta integritas. Sedangkan terkait pembekalan pengetahuan dan kemampuan dalam hal keamanan informasi Kepala Bagian LPSE, Dodi Hendrawan, ST., mengatakan saat ini LPSE Provinsi Lampung belum pernah mengadakan pelatihan khusus keamanan informasi kepada pengguna SPSE termasuk personil LPSE Provinsi Lampung. Sejauh ini pelatihan hanya berupa pelatihan penggunaan SPSE. Hal ini dibenarkan oleh Kepala Subbagian Pengembangan Sistem Informasi, Yusron, ST., saat di wawancarai oleh peneliti. Kepala

Subbagian Pengembangan Sistem Informasi, Yusron, ST., mengatakan bahwa saat ini memang LPSE Provinsi Lampung belum pernah mengadakan pelatihan khusus terkait keamanan informasi termasuk keamanan pengguna/personil. Terkait keamanan informasi Kepala Subbagian Pengembangan Sistem Informasi, Yusron, ST., mengatakan saat ini LPSE Provinsi Lampung hanya sebagai memberikan sosialisai tentang pentingnya kerahasian login, pentingnya perubahan login secara berkala. Sosialisasi tersebut disampaikan pada saat pelatihan penggunaan SPSE versi terbaru.

Dari apa yang telah diuraikan terkait aspek *people,* LPSE Provinsi Lampung belum memenuhi aspek *people*. Walaupun dalam hal keamanan personil atau pengguna LPSE Provinsi Lampung telah menggunakan pakta integritas untuk mengikat secara hukum pegawai LPSE, akan tetapi pada hal pengetahuan dan kemampuan tetang keamanan informasi pengguna/personil LPSE Provinsi Lampung belum pernah ada pembekalan dalam bentuk pelatihan. Dan sosialisasi terkait kesadaran pengguna juga belum maksimal karena hanya sebatas pada disampaikan pada sela-sela pelatihan penggunaan aplikasi SPSE.

c. Aspek *Processes*

Pada aspek *processes* menguraikan tentang bagaimana pemeliharaan dan tindakan standar yang digunakan untuk mengembangkan dan memastikan bahwa keamanan tetap pada basisnya, yang meliputi: manajemen akses pengguna, manajemen respon, dan manajemen audit. Dalam wawancara terkait permasalahan pada aspek *processes* Kepala Bagian LPSE, Dodi Hendrawan, ST., mengatakan bahwa saat ini LPSE Provinsi Lampung belum memiliki SOP terkait manajemen respon, selama ini penanganan permasalahan yang muncul harus berdasarkan keputusan pimpinan. Sehingga belum ada standar baku tentang bagaimana menangani permasalahan. Kemudian terkait manajemen audit, Kepala Bagian LPSE, Dodi Hendrawan, ST.,

mengatakan bahwa saat ini LPSE Provinsi Lampung belum memiliki tim audit internal. Audit yang selama ini hanya dilakukan oleh LKPP selaku pemangku kebijakan. Namun pada sisi manajemen akses pengguna sistem SPSE sendiri sudah menerapkan hal tersebut, hal ini dilakukan dengan membuat level hak akses pengguna. Dengan adanya sistem ini masing-masing pengguna hanya dapat mengakses sesuai dengan tugas dan tanggung jawabnya.

Berdasarkan uraian tersebut dapat disimpulkan bahwa pada aspek processes ini LPSE Provinsi Lampung belum memenuhi standar yang ada. Walaupun pada aspek manajemen akses pengguna sudah memenuhi, namun pada aspek manajemen audit dan manajemen respon belum memenuhi.

d. Aspek *Technology*

Pada aspek ini menjelaskan tentang teknologi dan solusi produk yang digunakan untuk memungkinkan pencapaian tujuan secara berkelanjutan yang meliputi: manajeman komunikasi, manajemen infrastruktur, manajemen arsitektur jaringan dan keamanan apilkasi. Berdasarkan pengamatan langsung yang dilakukan oleh peneliti manajemen infrastruktur yang ada, peneliti melihat bahwa dalam hal pengamanan fisik pada server LPSE Provinsi Lampung belum dilakukan. Terlihat bahwa siapapun bisa keluar masuk ruang *server* tanpa pengamanan. Sedangkan untuk artsitektur jaringan internet LPSE provinsi lampung menggunakan jasa layanan PT. Telkom. Kemudian pada sisi manajemen komunikasi, LPSE Provinsi Lampung belum membuat suatu standar atau tata kelola terkait manajemen komunikasi. Berdasarkan wawancara yang peneliti lakukan dengan Kepala Subbagian Pengendalian dan Administrasi Pembangunan, Andi Ahmad Yusuf, S.Kom., MM, di ketahui bahwa saat ini pihak LPSE Provinsi Lampung sudah menerapkan beberapa teknik pengamanan aplikasi diantaranya dengan menggunakan *server backup* untuk mengantisipasi jika terjadi

serangan terhadap server utama sehingga bisa digantikan dengan *server backup,* selain itu pengamanan aplikasi juga menggunakan *firewall yang* berfungsi sebagai pembatas dan pelindung dari akses-akses yang tidak resmi, selain itu penggunaan *VPN* juga merupakan langkah yang dilakukan oleh LPSE Provinsi Lampung untuk membatasi pengguna yang dapat mengakses secara langsung pada server.

Berdasarkan hasil penelitian tersebut maka dapat disimpulkan bahwa pada aspek *Technology* ini LPSE Provinsi Lampung belum memenuhi standar yang ada pada *defense in depth*. Hal ini dikarenakan LPSE Provinsi Lampung belum menerapkan manajemen komunikasi dan manajamen infrastruktur. Walaupun pada aspek manajemen arsitektur jaringan dan keamanan aplikasi sudah memenuhi.

4.1.5 Pelaksanaan LPSE Provinsi Lampung dalam mengamankan sistem informasi pada Sistem Pengadaan Secara Elektronik

Kepala Bagian LPSE, Dodi Hendrawan, ST., dalam wawancara dengan peneliti mengatakan bahwa setelah keluarnya Peraturan Presiden No. 16 Tahun 2018 tentang Pengadaan Barang/Jasa Pemerintah, Peraturan LKPP No.14 Tahun 2018 tentang Unit Kerja Pengadaan Barang/Jasa dan Peraturan LKPP No.19 Tahun 2018 Tentang Pengembangan Sistem dan Kebijakan Pengadaan, saat ini LPSE Provinsi Lampung belum memiliki regulasi turunan terkait perubahan peraturan yang baru tersebut. Kepala Bagian LPSE, Dodi Hendrawan, ST., mengatakan bahwa alasan LPSE Provinsi Lampung belum mengeluarkan regulasi turunan tersebut dikarenakan pihak LPSE Provinsi Lampung menilai bahwa di dalam Peraturan Presiden No. 16 Tahun 2018 tentang Pengadaan Barang/Jasa Pemerintah, Peraturan LKPP No.14 Tahun 2018 tentang Unit Kerja Pengadaan Barang/Jasa dan Peraturan LKPP No.19 Tahun 2018 Tentang Pengembangan Sistem dan Kebijakan Pengadaan sudah mengatur dengan sangat detail terkait pengadaan barang dan jasa. Sehingga saat ini pihak LPSE Provinsi Lampung hanya berpedoman pada

peraturan yang sudah ada tanpa membuat aturan turunan. Kepala Bagian LPSE, Dodi Hendrawan, ST., juga mengatakan bahwa sebelum keluarnya Peraturan Presiden dan Peraturan LKPP yang baru tersebut, pihak LPSE Provinsi Lampung memiliki Peraturan Daerah No. 8 Tahun 2016 yang mengatur tentang tata kelola LPSE Provinsi Lampung. Sedangkan terkait regulasi yang berupa aturan tertulis atau SOP tentang keamanan informasi dan pengelolaan resiko belum ada. Saat ini LPSE Provinsi Lampung lebih fokus kepada upaya pencapaian standar yang telah ditetapkan oleh LKPP, yaitu terdapat 17 standar yang harus di penuhi oleh setiap LPSE di Indonesia. Dari 17 standar tersebut, LPSE Provinsi Lampung sudah mendapatkan 12 sertifikat terkait standar pengelolaan LPSE yaitu sertifikat untuk standar: 1. Pengelolaan Layanan Helpdesk, 2. Pengelolaan Kelangsungan Layanan, 3. Pengelolaan Pendukung Layanan, 4. Pengelolaan Resiko Layanan, 5. Pengorganisasian Layanan, 6. Kebijakan Layanan, 7. Pengelolaan Anggaran Layanan, 8. Pengelolaan Aset Layanan, 9. Pengelolaan Hubungan Dengan Layanan, 10. Pengelolaan Kapasitas, 11. Pengelolaan Perubahan, 12. Pengelolaan Sumber Daya Manusia. Sedangkan 5 standar yang belum dicapai yaitu standar : 1. Pengelolaan Keamanan Perangkat, 2. Keamanan Operational Layanan, 3. Keamanan Server dan Jaringan, 4. Pengelolaan Kepatuhan, 5. Penilaian Internal.

Seperti yang telah diungkapkan oleh Kepala Subbagian Pengendalian dan Administrasi Pembangunan, Andi Ahmad Yusuf, S.Kom., MM., bahwa sebelum peristiwa serangan *hacker* tahun 2015, pihak LPSE Provinsi Lampung sepenuhnya menyerahkan pengelolaan *server* SPSE dan keamanan informasinya kepada pihak ke-3. Hal ini dikarenakan keterbatasan sumber daya manusia di LPSE Provinsi Lampung yang mampu mengelola *server*. Sebab saat itu di LPSE Provinsi Lampung tidak ada satu pegawai pun yang merupakan lulusan IT. Dan setelah peristiwa serangan *hacker* tahun 2015. Barulah Kepala Subbagian Pengendalian dan Administrasi Pembangunan, Andi Ahmad

Yusuf, S.Kom., MM., di tarik sebagai staf di LPSE Provinsi Lampung dan menjadi satu-satunya lulusan *IT* di LPSE Provinsi Lampung dan kini Andi Ahmad Yusuf, S.Kom., MM., menjabat sebagai Kepala Subbagian Pengendalian dan Administrasi Pembangunan di Biro Administrasi Pembangunan.

Kepala Subbagian Pengendalian dan Administrasi Pembangunan, Andi Ahmad Yusuf, S.Kom., MM., mengatakan saat wawancara dengan peneliti bahwa setelah peristiwa serangan *hacker* tahun 2015 pihak LPSE Provinsi Lampung mengambil langkah cepat dengan mengambil beberapa tindakan penting yaitu, 1. Mengganti pihak pengelola *server* LPSE Provinsi Lampung dan untuk membatasi akses terhadap *server*, pihak pengelola yang baru hanya diberi wewenang untuk memastikan *server* dapat diakses 24 jam. Sedangkan untuk instalasi baik *operating system* dan Aplikasi SPSE, pihak LPSE Provinsi Lampung meminta bantuan langsung dari pihak LKPP. Sehingga keamanan informasi dari sistem bisa terjamin. 2. Pihak LPSE Provinsi Lampung segera mengganti *server* yang sudah terserang oleh *hacker* dengan *server* yang baru. Hal ini dilakukan untuk mengantisipasi kemungkinan masih ada ancaman siber di *server* yang lama.

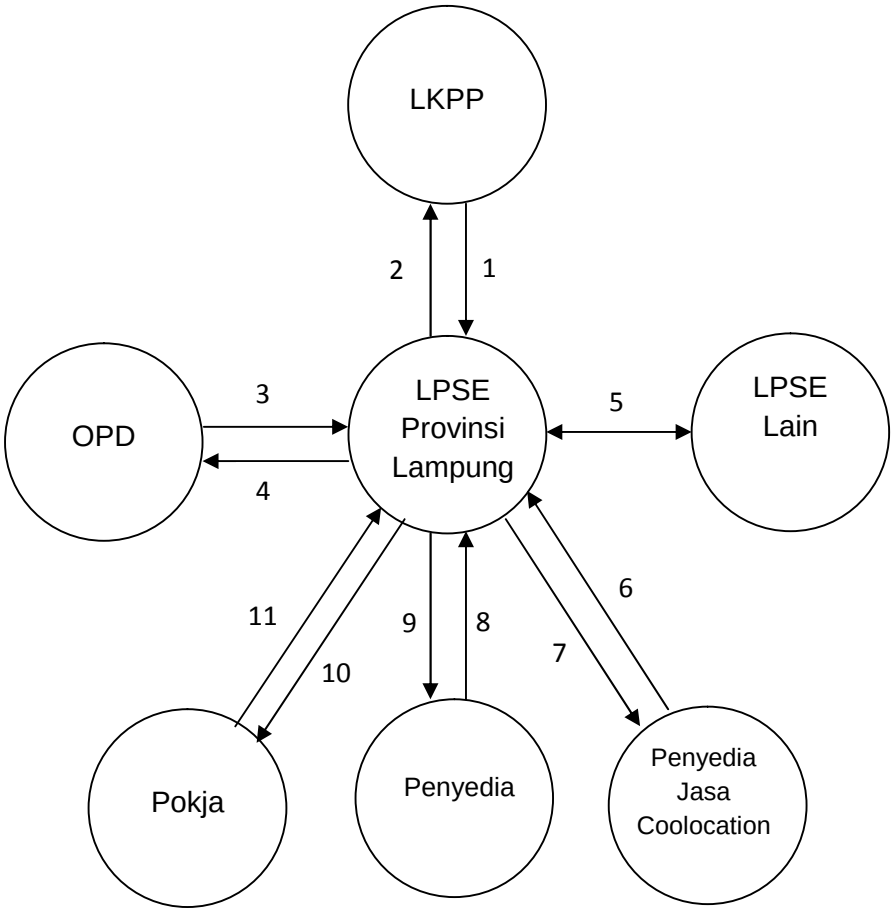
Kepala Subbagian Pengendalian dan Administrasi Pembangunan, Andi Ahmad Yusuf, S.Kom., MM., mengatakan dengan mengambil langkah tersebut keamanan informasi sistem pengadaan elektronik jauh lebih baik. Namun seiring berjalannya waktu dan berkembangnya teknologi, belum lama ini yaitu pada bulan juli 2018 SPSE Provinsi Lampung kembali di serang oleh *hacker*. Namun pada serangan kali ini sedikit berbeda, *hacker* tidak menerobos kedalam sistem, melainkan diduga bahwa pihak *hacker* tersebut masuk melalui *login* penyedia. Hal ini di perkuat karena setelah di cek tidak ada aktifitas mencurigakan di dalam sistem. Hal ini kemungkinan besar bahwa pihak *hacker* sebelumnya pernah mendapat *login* penyedia tersebut. Sebab seperti yang dikatakan oleh pihak penyedia tersebut, bahwa sebelumnya ia beberapa kali pernah

meminjamkan perusahaannya untuk di pakai mengikuti lelang di LPSE lain. Dan penyedia tersebut tidak mengubah *login* setelah perusahanan itu dipinjamkan. Sehingga hal ini dimanfaatkan oleh pihak bertanggung jawab untuk masuk dengan *login* penyedia tersebut untuk mengubah data penawaran peruasahaan yang saat ini sedang mengikuti lelang di LPSE Provinsi Lampung. Sehingga ketika tahap pembukaan penawaran, penawaran yang di *upload* oleh penyedia tersebut berbeda atau berubah. Akibat gangguan dari serangan *hacker* ini, membuat 3 paket pekerjaan yang sedang proses tender terpaksa tander ulang akibat ada beberapa penawarn yang di *upload* oleh penyedia berubah tidak sesuai aslinya.

Kepala Subbagian Pengendalian dan Administrasi Pembangunan, Andi Ahmad Yusuf, S.Kom., MM., mengatakan bahwa agar hal serupa tidak terjadi lagi, pihak LPSE Provinsi Lampung mengambil langkah untuk memberikan sosialisasi terkait penggunaan *login* kepada pihak penyedia di sela-sela pelatihan penggunaan SPSE versi 4.2. Dan untuk mengantisipasi hal-hal yang tidak diinginkan dimasa yang akan datang, pihak LPSE Provinsi Lampung kini memliki *server backup*. Diharapkan dimana ketika nantinya ada gangguan terhadap *server* utama, *server backup* dapat menggantikannya segera. *Server backup* sendiri di kelola oleh pihlak LPSE Provinsi Lampung dimana *server* berada di kantor LPSE Provinsi Lampung sedangkan *server* utamanya dikelola oleh pihak ke-3 yang berada di Jakarta.

Kepala Subbagian Pengendalian dan Administrasi Pembangunan, Andi Ahmad Yusuf, S.Kom., MM., juga mengatakan bahwa untuk lebih meningkatkan keamanan informasi pada SPSE, pihak LPSE Provinsi Lampung secara intensif berkerjasama dengan LKPP. Dengan adanya kerjasama ini LKPP akan melakukan pengawasan dan pengontrolan secara langsung terhadap SPSE Provinsi Lampung. Kemudian LPSE Provinsi Lampung juga bekerjasama dengan penyedia jasa *coolocation* untuk pengelolaan server utama. Serta LPSE Provinsi Lampung juga bekerjasama dengan semua *stakeholder* yang terlibat secara langsung

dengan sistem pengadaan secara elektronik di Pemerintah Provinsi Lampung. Hubungan kerjasama yang dilakukan oleh LPSE Provinsi Lampung dalam mengamankan sistem informasi SPSE dapat digambarkan dengan gambar berikut ini:



Gambar 4.9 Hubungan Antar Stakeholder Pada SPSE

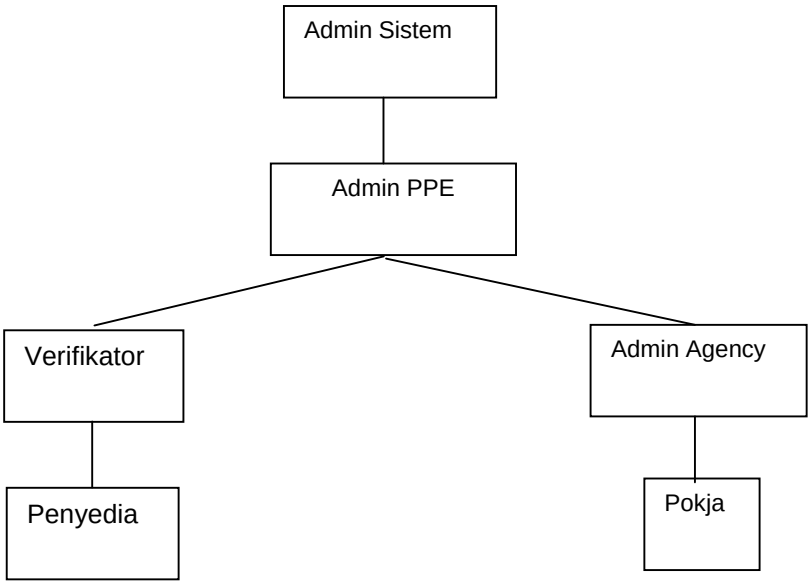
(Sumber: dibuat oleh peneliti berdasarkan data hasil penelitian)

Dari gambar tersebut kita dapat melihat hubungan antar stakeholder yang ditunjukan dengan angka dimana penjelasannya sebagai berikut:

1. LKPP mengawasi dan mengontrol LPSE Provinsi Lampung.
2. LPSE Provinsi Lampung berkoordinasi dengan LKPP terkait tata kelola dan keamanan informasi.

3. OPD melakukan konsultasi dan pengaduan kepada LPSE Provinsi Lampung terkait masalah pengadaan barang/jasa.
4. LPSE Provinsi Lampung mensosialisasikan dan menangani masalah terkait pengaduan OPD
5. LPSE Provinsi Lampung dan LPSE lain saling bertukar pengalaman dalam hal keamanan informasi SPSE.
6. LPSE Provinsi Lampung melakukan pengawasan dan kontrol terkait pengelolaan *server* yang dilakukan oleh penyedia jasa layanan *coolocation.*
7. Penyedia jasa *coolocation* berkoordinasi dengan LPSE Provinsi Lampung dalam hal pengelolaan dan pengembangan pengamanan *server*.
8. Penyedia melakukan pengaduan kepada LPSE Provinsi Lampung jika terjadi *trauble* terhadap SPSE.
9. LPSE Provinsi Lampung memberikan pelatihan dan menyelesaikan masalah pengaduan dari pihak Penyedia.
10. Pokja melakukan pengaduan kepada LPSE Provinsi Lampung jika terjadi *trauble* terhadap SPSE.
11. LPSE Provinsi Lampung memberikan pelatihan. Dan menyelesaikan masalah pengaduan dari pihak Pokja.

Sedangkan dari sisi teknologi keamanan aplikasi SPSE sendiri sudah cukup baik, pengembangan aplikasi SPSE dari waktu ke waktu juga terus memperhatikan keamanan informasi sehingga kerahasian dokumen dapat dijaga. Dalam hal akses pengguna, aplikasi ini menerapkan level akses pengguna dan membatasi akses pengguna. Sehingga setiap pengguna memiliki fungsi dan perannya masing-masing sehingga tidak bisa mengganggu fungsi lain. Ada pun level akses login sebagai berikut :



Gambar 4.10 Level Hak Akses Pengguna

(Sumber: dibuat oleh peneliti berdasarkan data hasil penelitian)

Admin sistem merupakan admin tertinggi di dalam sistem, perannya sebagai pengelola server dari instalasi (*operating system* dan aplikasi SPSE) dan bertanggung jawab terhadap keamanan sistem informasi. Selain itu admin sistem juga dapat menghapus, mengubah, mengganti data yang ada di dalam server. Sebab admin sistem mempunyai akses penuh terhadap server. Melakukan backup data juga termasuk tugas admin sistem. Selanjutnya Admin PPE atau Admin SPSE merupakan admin tertinggi di aplikasi SPSE. Admin PPE memiliki peran sebagai pembuat akun Verifikator dan Admin *Agency*. Selain itu admin PPE dan mengawasi proses lelang dan *log* akses pengguna. Kemudian Verifikator merupakan salah satu pengguna dalam aplikasi yang memiliki tugas memverifikasi pendaftaran penyedia yang mendaftar di dalam sistem. Verifikator memiliki hak untuk menerima atau menolak pendaftaran penyedia. Kemudian admin *agency*, admin agency ialah pengguna pada aplikasi SPSE yang mewakili instansi yang akan melelangkan paket pengadaannya di LPSE Provinsi Lampung adapun tugasnya membuat akun Pojka. Selanjutnya Pokja, Pokja merupakan pengguna di dalam

aplikasi SPSE yang bertugas mengumumkan, mengevaluasi dan menetapkan pemenang tender. Dan yang terakhir Penyedia, penyedia merupakan pengguna aplikasi SPSE yang berperan sebagai perusahaan peserta tender.

Selain menggunakan sistem level hak akses, untuk mengamankan informasi dokumen penawaran peserta agar tetap terjaga kerahasiannya. Dalam SPSE menggunakan aplikasi pendukung untuk kriptografi dokumen. Aplikasi ini disebut dengan Apendo (Aplikasi Pengaman Dokumen) dengan menggukan aplikasi ini file dokumen penawaran dapat di enkripsi dan di deskripsi. Mekanisme enkripsi dan deskripsi dokumen penawaran sebagai berikut:

a. Proses Enskripsi Dokumen

Gambar 4.11 Proses Enskripsi Dokumen

(Sumber: dibuat oleh peneliti berdasarkan data hasil penelitian)

Untuk melakukan enskripsi dokumen menggunakan aplikasi Apendo Peserta, langkahnya dengan membuka aplikasi Apendo Peserta kemudian login ke aplikasi. Setelah berhasil masuk kemudian *browse file* yang akan di enskripsi kemudian aplikasi akan meminta 2 kunci untuk mengenskripsi file, pertama kunci private (bisa di dapat dengan login penyedia ke aplikasi SPSE) dan Kunci Publik (bisa di dapat dengan login penyedia ke aplikasi SPSE kemudian dengan milih paket pengadaan yang akan di ikuti nantinya pada paket tersebut ada kunci publik yang dapat di

copy. Dan setelah memasukan kunci private dan kunci publik maka dokumen akan terenskripsi sehingga tidak dapat di baca.

b. Proses Deskripsi Dokumen

Gambar 4.12 Proses Deskripsi Dokumen

(Sumber: dibuat oleh peneliti berdasarkan data hasil penelitian)

Untuk melakukan deskripsi dokumen menggunakan aplikasi Apendo Panitia, langkahnya dengan membuka aplikasi Apendo Panitia kemudian login ke aplikasi. Setelah berhasil masuk kemudian *browse file* yang akan di deskripsi. Perbedaan antara enskrpsi dan deskripsi, jika pada proses enskripsi membutuhkan 2 kunci (private dan publik) maka pada proses deskripsi hanya membutuhkan kunci publik. Untuk mendapatkan kunci publik langkahnya dengan login panitia ke aplikasi SPSE kemudian dengan milih paket pengadaan sesuai dengan yang diikuti nantinya pada paket tersebut ada kunci publik yang dapat di *copy*. Dan setelah memasukan kunci publik maka dokumen yang terenskripsi bisa di deskripsi dan bisa di baca kembali.

Dari apa yang telah diuraikan diatas dapat disimpulkan bahwa saat ini dalam pelaksanaan pengelolaan sistem pengadaan barang/jasa secara elektronik di LPSE Provinsi Lampung berpedoman pada Peraturan Presiden No. 16 Tahun 2018 tentang Pengadaan Barang/Jasa Pemerintah, Peraturan LKPP No.14 Tahun 2018 tentang Unit Kerja Pengadaan Barang/Jasa dan Peraturan LKPP No.19 Tahun 2018 Tentang Pengembangan Sistem dan Kebijakan Pengadaan. Selain berpedoman

pada peraturan yang ada, untuk memberikan pelayanan yang maksimal LPSE Provinsi Lampung menjalin kerjasama dengan LKPP terkait pengelolaan keamanan informasi sistem pengadaan secara elektronik dan secara rutin LKPP melakukan audit terhadap LPSE Provinsi Lampung. Sedangkan untuk memastikan ketersediaan akses internet terhadap server SPSE, pihak LPSE Provinsi Lampung bekerjasama dengan pihak penyedia jasa coolocation.

Kerjasama-kerjasama ini dilakukan untuk memastikan ketercapainya tujuan dari LPSE Provinsi Lampung sesuai dengan peraturan yang ada yaitu: meningkatkan transparansi dan akuntabilitas, meningkatkan akses pasar dan persaingan usaha yang sehat, memperbaiki tingkat efisiensi proses Pengadaan, mendukung proses monitoring dan audit, dan memenuhi kebutuhan akses informasi yang *real time.*

Untuk mencapai tujuan dan memastikan keamanan informasi sistem pengadaan secara elektronik tersebut, LPSE Provinsi Lampung mengambil langkah-langkah yang meliputi: pengadaan server backup untuk mengantisipasi jika terjadi serangan hacker pada server utama; penggunaan *firewall* untuk melindungi aplikasi dan jaringan dari ancaman siber, penggunaan *VPN* untuk membatasi akses langung pada server, mengunakan level hak akses, menggunakan aplikasi Apendo untuk kriptografi dokumen, pelatihan penggunaan SPSE versi terbaru agar penguna selalu *update* terhadap SPSE versi terbaru, menyelenggarakan rapat koordinasi (Rakor) teknis LPSE se-Provinsi Lampung, melaksanakan sosialisasi kepada pengguna SPSE (Pokja, Penyedia dan Instansi) terkait pentingnya kerahasian login, berkoordinasi secara rutin dengan LKPP jika terjadi trouble terhadap sistem SPSE, berkoordinasi dengan Penyedia jasa coolocation jika terjadi trouble terhadap jaringan internet SPSE, dan secara rutin LPSE Provinsi Lampung di audit oleh LKPP.

4.2 Pembahasan

Dalam bagian Pembahasan ini, peneliti akan memberikan interprestasi atau verifikasi terhadap temuan atau hasil penelitian yang akan dihubungkan dengan berbagai konsep atau teori yang relevan yang telah ditentukan dalam Bab II. Pembahasan akan disesuaikan dengan temuan penelitian pada subfokus masing-masing.

4.2.1 Strategi Keamanan Informasi Dalam Menghadapi Ancaman Siber Pada Sistem Pengadaan Secara Elektronik Provinsi Lampung.

Dalam pembahasan pada rumusan masalah pertama ini peneliti menggunakan model keamanan informasi *defense in depth* sebagai pisau analisis. Model keamanan informasi *defense in depth* yang peneliti gunakan dalam merancang strategi keamanan informasi ini merupakan model keamanan informasi yang dikembangkan oleh *IT Security Expert Advisory Group (ITSEAG)* yang merupakan bagian dari *Trusted Information Sharing Network (TISN)* Pemerintah Australia. Pada model defense in depth yang dikembangkan oleh *IT Security Expert Advisory Group (ITSEAG)* berfokus pada perlindungan 4 elemen/aspek yaitu *People*, *Process*, *Technology*, dan *Governance*. Pada aspek *people,* menguraikan definisi tentang pemeliharaan dan penegakan peran dan tanggung jawab keamanan bagi pegawai dan vendor internal dan eksternal yaitu keamanan personal (termasuk kesadaran pengguna). Pada aspek *Process*, menguraikan definisi pemeliharaan dan tindakan standar yang digunakan untuk mengembangkan dan memastikan bahwa keamanan tetap pada basisnya, yang meliputi: manajemen akses pengguna, manajemen respon, dan manajemen audit. Pada aspek *Technology,* menjelaskan tentang teknologi dan solusi produk yang digunakan untuk memungkinkan pencapaian tujuan secara berkelanjutan yang meliputi: manajeman komunikasi, manajemen infrastruktur, manajemen arsitektur jaringan dan keamanan apilkasi. Sedangkan pada

aspek *Governance*, mengacu pada kerangka manajemen yang digunakan untuk memberikan pengawasan dan koordinasi aspek *People*, *Process* dan *Technology* yang meliputi: Manajemen Resiko, Manajemen Keamanan Informasi dan Kebijakan serta penyesuaian manajemen.

Dari hasil penelitian yang telah dijelaskan sebelumnya maka, peneliti membahasnya berdasarkan aspek-aspek yang terdapat pada model keamanan informasi defense in depth tersebut sebagai berikut:

a. Governance (Tata Kelola)

Pada aspek ini mengambarkan tentang bagaimana tata kelola yang dijalankan oleh instansi terkait yaitu LPSE Provinsi Lampung dalam pengelolaan tugas dan tanggung jawab khususnya pada keamanan informasi serta bagaimana kebijakan dan regulasi yang di gunakan dalam implementasi tersebut. Dan didapat bahwa saat ini LPSE Provinsi Lampung belum memiliki regulasi atau kebijakan yang mengatur tentang keamanan informasi, manajemen resiko, dan LPSE Provinsi lampung belum memiliki regulasi terbaru yang mengatur tata kelola layanan pengadaan barang/jasa secara elektronik. Saat ini LPSE Provinsi Lampung hanya berpegangan pada Peraturan Presiden No. 16 Tahun 2018 dan Peraturan Lembaga Kebijakan Pengadaan Pemerintah (LKPP) No.14 dan No.19 Tahun 2018. Untuk mencapai kesesuaian terhadap aspek *Governace* ini maka langkah yang dilakukan sesuai dengan model *defense in depth* sebagai berikut :

1) Manajemen Resiko

Tabel 4.2 Manajemen Resiko

Deskripsi	Manajemen risiko terdiri dari proses bisnis dan kerangka kerja kebijakan untuk mengidentifikasi ancaman terhadap organisasi, menentukan risiko bisnis mereka dan menerapkan strategi mitigasi untuk mengurangi tingkat risiko ke tingkat yang

	dapat diterima
Tujuan	• Mengidentifikasi kerentanan dan ancaman • Menentukan risiko dan Melindungi organisasi dari risiko tersebut • Memfasilitasi penerimaan bisnis terhadap risiko residual • Memberikan masukan untuk perencanaan kelangsungan bisnis • Mendukung unit bisnis dalam kegiatan manajemen risiko yang sedang berlangsung
Implementasi	a. Mengembangkan dan menetapkan kebijakan internal untuk manajemen risiko • Melibatkan pemangku kepentingan (Dalam hal ini melibatkan LKPP, Pokja, Penyedia, dan Instansi di Lingkungan Pemerintah Provinsi Lampung dalam pengelolaan resiko) • Menentukan prioritas risiko (Dalam hal ini resiko terbesar ialah serangan hacker) • Menentukan ruang lingkup risiko (meliputi keamanan data, keamanan jaringan dan keamanan personal) • Kemudian membentuk Kerangka kerja Pengelolaan Resiko. b. Mengevaluasi lingkungan resiko • Melakukan *workshop* atau rapat koordinasi terkait manajemen risiko dengan para pemangku kepentingan (LKPP, Pokja, Penyedia dan Instansi terkait) dengan pakar/ahli dalam bidang manajemen resiko

	• Melakukan penilaian dan penentuan prioritas aset c. Menilai lingkungan internal dan eksternal • Ancaman (*Hacker, Malware*) • Kerentanan (Kerusakan *Server*, pencurian data, kehilangan data) d. Menentukan risiko bisnis • *Governance* (Belum ada kerangka kerja atau SOP terkait manajemen resiko) • *People* (Belum ada pelatihan khusus terkait keamanan informasi bagi pengguna) • *Process* (Lemahnya audit internal) • *Technology* (Kurang memadainya fasilitas khususnya standar untuk ruangan *server*)

(Sumber: Dikelola oleh peneliti berdasarkan model *defense in depth*)

2) Keamanan Informasi

Tabel 4.3 Keamanan Informasi

Deskripsi	Keamanan informasi adalah serangkaian proses dan kontrol bisnis yang memberikan jaminan kerahasiaan, integritas, dan ketersediaan informasi dalam suatu organisasi.
Tujuan	3) Memberikan jaminan keamanan sistem • Kerahasiaan (Data dan *Login*) • Integritas (Keaslian data) • Ketersediaan (Akses Internet) 4) Menilai, memahami dan menerima risiko • Melibatkan Seluruh komponen yang terlibat dalam kemanan informasi (LPSE Provinsi

	Lampung, LKPP, Penyedia Jasa *Coolocation*, Pokja, Penyedia, dan OPD) • Memfasilitasi pengambilan keputusan terkait keamanan informasi 5) Sosialisasi kesadaran keamanan informasi
Implementasi	a. Pemenuhan standar keamanan informasi • Mengalokasikan sumber daya sesuai Kebutuhan (Petugas keamanan, Tenaga ahli bidang IT, Pencapaian standar fasilitas, keamanan personal, keamanan data, keamanan jaringan, dan keamanan aplikasi) • Usulan peningkatan sistem atau jaringan (*upgrade server*) b. Melakukan tinjauan keamanan informasi (melalui *monitoring* dan evaluasi secara berkala) c. Melakukan pelatihan khusus terkait keamanan informasi

(Sumber: Dikelola oleh peneliti berdasarkan model *defense in depth*)

b. *People* (Pengguna/Personil)

Pada aspek ini menjelaskan bagaimana peran pengguna dalam sistem yang dapat mempengaruhi keamanan informasi dalam sistem itu sendiri. Aspek ini memiliki pengaruh yang besar terhadap berjalan atau tidaknya keamanan informasi. Sebab pengguna yang berinteraksi langsung terhadap sistem. Sehingga keamanan pengguna menjadi sangat penting di lindungi. Dari apa yang telah diuraikan terkait aspek *people,* LPSE Provinsi Lampung belum memenuhi aspek *people*. Walaupun dalam hal keamanan personil atau pengguna LPSE Provinsi Lampung telah menggunakan pakta integritas untuk mengikat secara hukum pegawai LPSE, akan tetapi pada hal pengetahuan dan kemampuan

tentang keamanan informasi pengguna/personil LPSE Provinsi Lampung belum pernah ada pembekalan dalam bentuk pelatihan. Dan sosialisasi terkait kesadaran pengguna juga belum maksimal karena hanya sebatas pada disampaikan pada sela-sela pelatihan penggunaan aplikasi SPSE.

Sedangkan berdasarkan kasus serangan *hacker* yang terjadi di LPSE Provinsi Lampung tahun 2015 dan tahun 2018 bisa di nilai bahwa adanya kelemahan terhadap keamanan pengguna/personil didalam tim LPSE Provinsi Lampung. Pada tahun 2015 LPSE Provinsi Lampung mempercayakan sepenuhnya pengelolaan *server* kepada pihak ke-3 sehingga pihak ke-3 mempunyai akses penuh ke dalam *server* sedangkan banyak data rahasia yang harusnya pihak ke-3 tidak boleh mengetahuinya. Sehingga kebocoran sistem akan sangat terbuka. Kemudian pada tahun 2018 adanya kelalaian pengguna dalam hal ini penyedia yang ikut sebagai peserta tender di LPSE provinsi Lampung yang memberikan loginnya kepada pihak lain sehingga ada pihak yang tidak bertanggung jawab menggunakan login tersebut untuk kepentingan tertentu. Sehingga pihak tersebut secara sengaja mengubah data penawaran yang sudah di *upload* oleh penyedia tersebut dengan data yang tidak sesuai. Sehingga ketika proses pembukaan penawaran oleh pokja didapat dokumen penawarannya berbeda dengan yang asli. Berdasarkan hasil penelitian yang telah diuraikan pada bagian sebelumnya maka untuk mencapai kesesuaian terhadap aspek *People* dalam model *defense in depth* ini, langkah yang harus dilakukan oleh LPSE Provinsi Lampung dalam mengamankan sistem pengadaan secara elektronik sebagai berikut :

1) Keamanan Personil / Pengguna

Tabel 4.4 Keamanan Pengguna

Deskripsi	Keamanan personel adalah serangkaian proses dan kontrol bisnis yang melindungi organisasi dari

	perilaku pegawai/pengguna yang lalai, curang atau jahat.
Tujuan	• Melindungi dari penipuan, memata-matai, dan serangan bermotif politik • Mencegah akses atau penggunaan aset/ informasi yang tidak sah • Mencegah pegawai dengan resiko tinggi bergabung dengan organisasi • Melindungi pengguna dari bahaya • Mengidentifikasi dan mengatasi ancaman yang sedang dilakukan oleh pengguna
Implementasi	• Pegawai yang bergabung sebagai tim LPSE Provinsi Lampung di ikat dengan pakta integritas yang salah satunya terkait kerahasian data dan login sehingga ketika ada pelanggaran pegaai tersebut bisa dituntut secara hukum. • Rekrutmen pegawai baru harus melihat rekam jejak dan riwayat pekerjaan sebelumnya apakah yang bersangkutan pernah mengalami masalah hukum. • Pegawai dan pengguna sistem dibekali pelatihan penggunaan SPSE versi terbaru dan pelatihan tentang keamanan informasi

(Sumber: Dikelola oleh peneliti berdasarkan model *defense in depth*)

c. *Processes* (Proses)

Pada aspek ini menguraikan bagaimana pemeliharaan dan tindakan standar yang digunakan untuk mengembangkan dan memastikan bahwa keamanan tetap pada basisnya, yang meliputi:

manajemen akses pengguna, manajemen respon, dan manajemen audit. Berdasarkan data yang peneliti peroleh baik melalui wawancara, observasi dan studi dokumentasi, peneliti melihat bahwa adanya kelemahan terhadap proses audit. Selama ini LPSE Provinsi Lampung berpaku pada audit yang dilakukan oleh LKPP, dimana audit yang dilakukan LKPP tidak rutin dilakukan. Audit sifatnya hanya dilakukan jika pihak LPSE Provinsi Lampung ingin mengajukan sertiftiasi standar yang yang telah ditetapkan LKPP. Audit yang dilakukan oleh pihak internal sendiri belum pernah dilakukan. Lemahnya audit akan berdampak lemahnya pengawasan sehingga kesesuaian terhadap SOP pun menjadi tidak maksimal. Berdasarkan data yang peneliti peroleh dilapangan maka agar aspek *Process* ini bisa sesuai dengan model kemanan informasi defense in depth maka langkah yang harus dilakukan sebagai berikut:

1) Manajemen Respon

Tabel 4.5 Manajemen Respon

Deskripsi	Manajemen respons insiden adalah serangkaian proses dan kontrol bisnis yang dibentuk untuk meminimalkan dampak insiden keamanan dan membatasi pengulangannya.
Tujuan	• Menghindari insiden melalui pemantauan dan respons yang proaktif • Meminimalkan dampak insiden keamanan • Menetapkan proses untuk secara akurat mendeteksi pelanggaran kebijakan dan memberikan penahanan/mitigasi • Mengidentifikasi sumber pelanggaran dan menyediakan pelaporan untuk membantu dalam penyelesaian insiden • Mengembalikan sistem/lingkungan ke status

	sesuai SOP
Implementasi	• Penerapan kontrol melalui monitoring dan evaluasi terhadap (jaringan internet, *server* SPSE, dan keamanan pengguna) • Menerapkan sistem pemantauan jarak jauh sehingga admin sistem dapat memantau dan mengawasi. • Mengembangkan sistem pengaduan elektronik sehingga ketika ada tarouble terhadap sistem, pengguna bisa melakukan pengaduan secara mudah dan cepat kepada pihak LPSE Provinsi Lampung.

(Sumber: Dikelola oleh peneliti berdasarkan model *defense in depth*)

2) Manajemen Audit

Tabel 4.6 Manajemen Audit

Deskripsi	Manajemen audit adalah serangkaian proses bisnis dan kontrol yang mengatur akuntabilitas departemen dan personel, evaluasi kesesuaian kontrol yang diterapkan, dan pelaporan hasil audit kepada manajemen.
Tujuan	• Memastikan akuntabilitas unit kerja dan personel di LPSE Provinsi Lampung. • Mengevaluasi kecukupan dan kesesuaian kontrol • Menentukan keselarasan kegiatan keamanan informasi dan strategi *defense in depth* • Mengetahui hasil audit
Implementasi	a. Menentukan ruang lingkup audit

	• Analisis risiko terhadap sistem SPSE • Proses yang diamati dan benda-benda fisik (kondisi server, jaringan dan kesesuaian operasional) • Dokumentasi • Representasi • Analisis secara keseluruhan b. Mengumpulkan bukti audit (Penyelidikan, observasi, inspeksi, konfirmasi, monitor) • Laporan akses pengguna (IP address) • Proses perawatan (pemindaian anti virus) • Kuesioner personel • Survei Aplikasi SPSE c. Meninjau pelanggaran pengguna / layanan dengan identifikasi penyebab dan penanggulangan yang tepat. d. Uji kontrol • Kontrol pengguna/pegawai dengan wawancara atau diskusi dengan pengguna/ pegawai) • Kontrol aplikasi (kontrol otentikasi, dan log akses aplikasi) • Kontrol sistem (Pemeliharaan anti-virus) • Kontrol jaringan (Pengujian penetrasi) • Kontrol fisik (Akses ke infrastruktur) e. Kemudian mendokumentasikan hasil temuan audit, yang selanjutnya disimpulankan dan rekomendasi kepada pemangku kebijakan.

(Sumber: Dikelola oleh peneliti berdasarkan model defense in depth)

3) Manajemen Akses Pengguna

Tabel 4.7 Manajemen Akses Pengguna

Deskripsi	Manajemen akses pengguna adalah serangkaian proses dan kontrol bisnis yang membatasi akses ke suatu organisasi adalah informasi dan sumber daya dan membatasi kemampuan pengguna untuk menipu proses bisnis.
Tujuan	• Memastikan hanya pengguna resmi yang memiliki akses ke informasi dan sumber daya • Membatasi kerusakan yang dapat dilakukan oleh pengguna • Membatasi akses pengguna kedalam sistem • Mengijinkan akses pengguna bisa dilacak dan diaudit • Membatasi kemampuan pengguna untuk menipu proses
Implementasi	a. Menerapkan infrastruktur manajemen pengguna: • Penyimpanan identitas terpusat • Layanan direktori • Layanan otentikasi • Sistem pelacakan untuk menangkap permintaan akses dan perubahan b. Menjalankan proses bisnis manajemen pengguna yang terdefinisi dengan baik: • Penyediaan pengguna (Log in) • Pengakhiran pengguna (Log out) • Manajemen kata sandi (Ganti Password) c. Mengembangkan prosedur audit yang mencakup:

	• Semua perubahan akses pengguna • Penggunaan hak istimewa khusus • Upaya dan kegagalan otentikasi

(Sumber: Dikelola oleh peneliti berdasarkan model *defense in depth*)

d. *Technology* (Teknologi)

Aspek ini menjelaskan tentang teknologi dan solusi yang digunakan untuk memungkinkan pencapaian tujuan secara berkelanjutan, yang meliputi: Manajemen komunikasi, Manajemen infrastruktur, Manajemen arsitektur jaringan, Keamanan Aplikasi. Berdasarkan hasil wawancara, observasi dan studi dokumentasi yang peneliti lakukan didapatkan hasil bahwa saat ini di LPSE Provinsi Lampung untuk aspek teknologi ini sudah cukup baik. Mulai dari manajemen infrastruktur, manajemen arsitektur jaringan, manajmen komunikasi dan keamanan aplikasi yang cukup baik. Hal ini dikarenakan pengembangan aplikasi sendiri dilakukan oleh LKPP dengan sangat memperhatikan keamanan informasi. Hal semua hal tersebut masih belum cukup untuk memenuhi standar aspek teknologi dalam model keamanan informasi defense in depth sehingga diperlukan beberapa penyesuaian sebagai berikut :

1) Keamanan Infrastruktur

Tabel 4.8 Keamanan Infrastruktur

Deskripsi	Keamanan infrastruktur adalah serangkaian kontrol teknis dan proses bisnis yang menentukan persyaratan infrastruktur untuk pengiriman layanan bisnis dan menerapkan langkah-langkah untuk melindungi sistem dan perangkat.
Tujuan	• Mengidentifikasi persyaratan standar untuk keamanan infrastruktur pada sistem pengadaan barang/jasa secara elektronik (SPSE)

	• Melaksanakan pengiriman, penyimpanan, perlindungan, dan pemulihan data yang aman pada sistem pengadaan barang/jasa secara elektronik (SPSE) • Menerapkan prosedur perawatan yang efektif • Memberikan keamanan fisik pada *server* SPSE
Implementasi	a. Melakukan Peninjauan terhadap infrastruktur yang ada meliputi: • Ketersediaan ruangan khusus untuk server harus sesuai dengan standar (Suhu, kelembaban, ukuran ruangan dan ketersediaan listrik) • Ketersediaan jaringan internet harus lancar minimal 10mbps • Kemampuan backup server dengan kemampuan backup yang real time b. Menilai kerentanan infrastruktur (saat ini masih kurangnya pengamanan fisik sehingga diperlukan petugas keamanan yang dapat menjaga ruang server) c. Mendesain infrastruktur untuk menghindari serangan umum maupun untuk menghindari pencurian server. d. Spesifikasi server harus sesuai dengan standar yaitu kapasitas penyimpanan minimal 1 TB dan RAM minimal 4 GB. e. Menerapkan aturan terkait akses keluar masuk ruangan server f. Pemeliharaan infrastruktur secara rutin g. Melakukan perencanaan berkesinambungan

	untuk peningkatan kapasitas dan fasilitas infrastruktur yang ada.

(Sumber: Dikelola oleh peneliti berdasarkan model *defense in depth*)

2) Keamanan Komunikasi

Tabel 4.9 Keamanan Komunikasi

Deskripsi	Keamanan komunikasi adalah serangkaian kontrol teknis dan proses bisnis yang menentukan persyaratan komunikasi untuk informasi dan melindungi data terhadap ancaman saat dalam perjalanan.
Tujuan	1) Melindungi komunikasi dari: • Akses tidak sah • Penyadapan • Pembajakan • Pencurian identitas 2) Meningkatkan kesadaran akan risiko keamanan komunikasi
Implementasi	• Menggunakan teknologi enskripsi data (saat ini sudah menggunakan aplikasi Apendo untuk enskripsi dan deskripsi data) • Mengunakan *VPN* untuk membatasi pengguna yang dapat masuk langsung kedalam sistem keamanan *server* SPSE • Tidak menggunakan email gratisan melainkan menggunakan email yang dikelola dengan domain sendiri. • Menerapkan sistem 2 langkah otentifikasi

(Sumber: Dikelola oleh peneliti berdasarkan model *defense in depth*)

3) Keamanan Arsitektur Jaringan

Tabel 4.10 Keamanan Arsitektur Jaringan

Deskripsi	Keamanan arsitektur jaringan adalah serangkaian kontrol desain dan proses pemantauan yang melindungi informasi selama pemrosesan, transmisi, dan penyimpanan.
Tujuan	• Melindungi informasi selama pemrosesan, pengiriman dan penyimpanan pada SPSE • Mengisolasi akses publik dari sistem kritis • Memfasilitasi pemantauan data jaringan untuk insiden keamanan
Implementasi	a. Menggunakan jasa konsultan untuk melakukan tinjauan terhadap arsitektur jaringan b. Melakukan pengujian terhadap keamanan perimeter, jaringan, aplikasi, dan host c. Menerapkan penguatan keamanan jaringan dengan melakukan modifikasi arsitektur jaringan dan penggunaa Firewall d. Peninjauan terhadap koneksi jaringan eksternal • Menentukan penyedia jasa layanan internet yang dapat dipercaya • Menerapkan kerjasama keamanan jaringan dengan kontrak yang mengikat secara hukum dengan penyedia jasa layanan internet

(Sumber: Dikelola oleh peneliti berdasarkan model *defense in depth*)

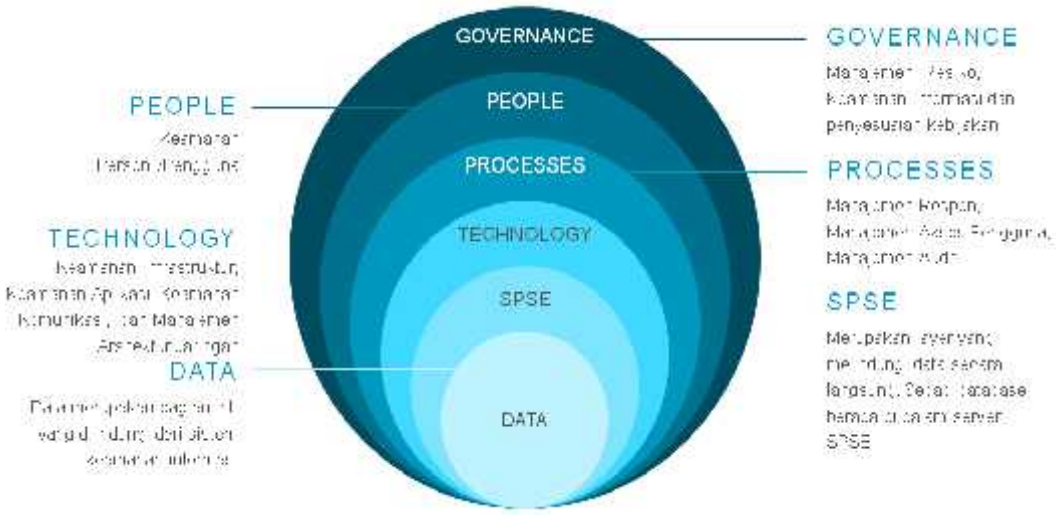
4) Keamanan Aplikasi

Tabel 4.11 Keamanan Aplikasi

Deskripsi	Keamanan aplikasi adalah serangkaian kontrol teknis yang menentukan risiko keamanan aplikasi dan mengurangi risiko yang diidentifikasi melalui proses siklus pengembangan yang aman.
Tujuan	• Melindungi aplikasi dari ancaman keamanan • Meningkatkan kesadaran akan persyaratan keamanan dalam desain, pengembangan, dan pemeliharaan aplikasi • Menilai keamanan aplikasi dengan melakukan analisis kerentanan / ancaman • Mengembangkan proses untuk mendorong pengembangan aplikasi yang aman
Implementasi	a. Mengamankan *source code* aplikasi SPSE b. Melakukan pelatihan untuk personel pengembangan aplikasi SPSE c. Mengidentifikasi kerentanan aplikasi SPSE • *Injection attacks* • *Buffer overflow* • *Scripting attacks* d. Mengidentifikasi dan menilai komponen yang terkait langsung dengan aplikasi • Sistem operasi (Mengunakan *Linux*) • Kerangka Kerja (Menggunakan *J2EE*) • Basis data (*Apache Tomcat*) • *Firewall* e. Melakukan penilaian dengan cara *testing*

(Sumber: Dikelola oleh peneliti berdasarkan model *defense in depth*)

Dari tabel-tabel yang telah disajikan diatas terkait penyesuaian ke-4 aspek model keamanan informasi *defense in depth* yaitu aspek *Governance* (tata kelola), aspek *People* (personil/pengguna), aspek *Processes* (proses), dan aspek *Technology* (teknologi) dengan disesuaikan dengan data yang telah peneliti kumpulkan melalui wawancara, observasi dan studi dokumentasi terkait sistem pengadaan secara elektronik di LPSE Prrovinsi Lampung maka peneliti mencoba membuat desain strategi *defense in depth* dalam menghadapi ancaman siber pada sistem pengadaan secara elektronik tersebut kedalam bentuk gambar sebagai berikut :



Gambar 4.13 Strategi Keamanan Informasi *Defense In Depth* Dalam Menghadapi Ancaman Siber Pada Sistem Pengadaan Secara Elektronik

(Sumber : dibuat oleh peneliti)

Berdasarkan gambar diatas dapat disimpulkan tentang bagaimana strategi keamanan informasi dalam menghadapi ancaman siber pada sistem pengadaan secara elektronik Provinsi Lampung yang meliputi perlindungan secara berlapis terhadap semua aspek di dalam sistem pengadaan secara elektronik. Bisa dilihat bahwa pada bagian inti atau bagian utama yang di lindungi pada sistem keamanan informasi ialah

data, data pada sistem pengadaan secara elektronik berupa: dokumen penawaran, dokumen kualifikasi, dokumen pengadaan dan data rahasia lain yang harus dilindungi dari berbagai ancaman yang bisa membuat data menjadi hilang, berubah, dan rusak. Pada bagian ini, akan dilindungi secara langsung oleh Aplikasi SPSE dimana data berada langsung di dalam database pada Aplikasi SPSE. Selanjutnya Aplikasi SPSE akan dilindungi oleh aspek teknologi dimana perlindungan tersebut berupa keamanan infrastruktur yaitu keamanan secara fisik, keamanan aplikasi, keamanan komunikasi, dan manajemen arsitektur jaringan. Kemudian aspek teknologi akan terlindung melalui pelaksanaan aspek proses yang baik yang dijalankan sesuai dengan prosedur standar yang ada meliputi manajemen akses pengguna, manajemen respon dan manajemen audit. Pada lapisan aspek proses ini, selanjutnya akan dilindungi oleh aspek personil/pengguna yang meliputi keamanan dan kesadaran penggunaan. Mustahil aspek proses akan terlindung jika penggunanya yang terlibat secara langsung pada sistem tidak menjalankan prosedur keamanan informasi sesuai dengan standar. Dan pada akhirnya semua aspek akan dilindungi melalui tata kelola yang baik dengan regulasi yang kuat yang dapat mendukung pengelolaan keamanan informasi pada sistem pengadaan secara elektronik.

Hal ini sesuai dengan apa telah disebutkan pada Bab II tentang model keamanan informasi d*efense in depth,* dimana disebutkan bahwa d*efense in depth* adalah konsep perlindungan jaringan komputer dengan serangkaian mekanisme pertahanan sehingga jika satu mekanisme gagal, yang lain akan ada untuk menggagalkan serangan. Karena ada banyak penyerang potensial dengan berbagai macam metode serangan yang tersedia, dengan memanfaatkan strategi *defense in depth* akan mengurangi risiko. Ini berarti bahwa model keamanan informasi *defense in depth* ini merupakan konsep perlindungan secara berlapis dengan melindungi semua aspek yang ada pada sistem. Sehingga dalam membangun dan menerapkan strategi keamanan informasi tidak bisa

hanya dilakukan pada satu atau dua aspek saja, melainkan semua aspek yang ada di dalam sistem informasi harus dilindungi. Hal ini dikarenakan setiap aspek di dalam sistem informasi saling berkaitan dan ancaman siber saat ini merupakan ancaman yang sifatnya sangat kompleks. Sehingga sesuai dengan model keamanan informasi *defense in depth* maka semua aspek yang ada di dalam sistem yaitu *Governance, People, Processes* dan *Technology* harus mendapat perlindungan.

Namun dalam upaya implementasi model keamanan informasi *defense in depth* ini ke dalam strategi keamanan informasi LPSE Provinsi Lampung bukanlah hal yang mudah, namun memiliki beberapa kendala dan hambatan diantaranya: terbatasnya alokasi anggaran untuk peningkatan sarana dan prasarana seperti terbatasnya anggaran untuk *upgrade server* penambahan *bandwidth* internet dan penambahan perangkat komputer. Kemudian terbatasnya sumber daya manusia yang memiliki kemampuan di bidang *IT* sehingga ketika terjadi trouble terhadap *server* maupun jaringan penangan akan menjadi lebih lambat ditangani. Selain itu lemahnya regulasi yang ada pada LPSE Provinsi Lampung menjadi hambatan tersendiri dalam upaya pelaksanaan kegiatan di LPSE Provinsi Lampung. Hal ini dikarena pihak LPSE Provinsi Lampung belum memiliki SOP terkait bagaimana manajemen keamanan informasi dan bagaimana manajemen resiko.

4.2.2 Pelaksanaan LPSE Provinsi Lampung Dalam Mengamankan Sistem Informasi Pada Sistem Pengadaan Secara Elektronik

Dalam pembahasan pada rumusan masalah 1 ini peneliti menggunakan teori strategi *Ends, Means dan Ways* oleh Karl Von Clausewitz sebagai pisau analisis. Clausewitz merumuskan strategi kedalam tiga hal yang harus dilalui, yakni *Ends, Means dan Ways*. Berdasarkan hasil penelitian yang telah diuraikan sebelumnya terkait pelaksanaan LPSE Provinsi Lampung dalam mengamankan sistem

pengadaan secara elektronik maka peneliti akan menguraikan strategi tersebut kedalam elemen *Ends, Means dan Ways* sebagai berikut:

a. *Ends*

Ends adalah segala sesuatu yang menjadi tujuan dari strategi yang dilakukan. Memperjelas tujuan akan memberikan kemungkinan yang lebih besar untuk tercapainya keinginan yang telah direncanakan atau ditetapkan. Untuk elemen *Ends* dari strategi yang dimiliki oleh LPSE Provinsi Lampung tertuang jelas dalam tujuan LPSE Provinsi Lampung yaitu: Meningkatkan transparansi dan akuntabilitas, Meningkatkan akses pasar dan persaingan usaha yang sehat, Memperbaiki tingkat efisiensi proses Pengadaan, Mendukung proses monitoring dan audit, dan Memenuhi kebutuhan akses informasi yang *real time*.

b. Means

Means merupakan sarana dan prasarana dalam upaya mewujudkan dari tujuan yang telah ditetapkan. Melalui penggunaan sarana dan prasarana baik akan menjadikan proses pencapaian tujuan menjadi lebih menjanjikan. Sebagai upaya pencapaian tujuan tersebut LPSE Provinsi Lampung dalam melakukan pengelolaan sistem pengadaan secara elektronik berpedoman pada Peraturan Presiden No. 16 Tahun 2018 tentang Pengadaan Barang/Jasa Pemerintah, Peraturan LKPP No.14 Tahun 2018 tentang Unit Kerja Pengadaan Barang/Jasa dan Peraturan LKPP No.19 Tahun 2018 Tentang Pengembangan Sistem dan Kebijakan Pengadaan.

Selain itu *means* yang juga diterapkan oleh LPSE Provinsi Lampung yakni dengan membangun kolaborasi dengan beberapa *stakeholder* dalam rangka mencegah ancaman siber melalui kerjasama yang aktif dengan LKPP sebagai pengawas dan pengontrol sistem, dengan Penyedia jasa *coolocation* yang memberikan layanan ketersedian akses internet 24 jam *non-stop*, dan menjalin kerjasama dengan OPD yang ada di lingkungan pemerintah Provinsi Lampung, serta aktif

membangun komunikasi dengan pihak pokja dan Penyedia yang menjadi perserta tender di LPSE Provinsi Lampung.

c. Ways

Ways merupakan cara atau metode yang dilaksanakan untuk mencapai tujuan. Secara sederhana, *Ways* adalah sebuah taktik yang dijalankan untuk mencapai tujuan yang telah ditetapkan tersebut. *Ways* yang dilakukan oleh LPSE Provinsi Lampung yaitu: memperkuat kerjasama dengan LKPP dengan secara aktif dan rutin membangun komunikasi yang baik. LKPP dapat terlibat langsung kedalam sistem SPSE Provinsi Lampung sehingga keamanan sistem informasi bisa jauh lebih baik. Kemudian membangun kerjasama dengan pihak Penyedia jasa *coolocation* sehingga kebutuhan akan jaringan internet bisa jauh lebih baik. Selain itu secara rutin setiap tahun LPSE Provinsi Lampung mengadakan rapat koordinasi teknis LPSE se-provinsi Lampung.

Terhadap penguatan kapasitas sumber daya manusia ways yang dilakukan oleh LPSE Provinsi Lampung yaitu secara rutin mengadaan pelatihan penggunaan SPSE versi terbaru kepada pokja dan penyedia sehingga pihak pokja dan penyedia bisa selalu *update* terhadap sistem SPSE terbaru. .

Sedangkan *Ways* dari sisi teknologi, LPSE Provinsi Lampung meningkatkan sarana dan prasarana dengan pengadaan *server backup*, memberikan *proteksi firewall* pada sistem SPSE, menggunakan sistem *VPN* untuk membatasi akses langsung terhadap *server*, menggunakan level hak akses dan menggunakan metode kriptografi untuk menjaga kerahasian dokumen.

Dari uraian di atas maka dapat kita ketahui bahwa berdasarkan teori strategi *Ends, Means, Ways* oleh Karl Von Clauswitz, LPSE Provinsi Lampung telah memiliki strategi dalam menghadapi ancaman siber pada sistem pengadaan barang/jasa secara elektronik.

Berikut strategi keamanan informasi yang telah dilakukan LPSE Provinsi Lampung dalam menghadapi ancaman siber yang peneliti sajikan dalam bentuk tabel berdasarkan teori strategi Karl Von Clauswitz *(Ends, Means, Ways).*

Tabel 4.12 Pelaksanaan LPSE Provinsi Lampung Dalam Mengamankan Sistem Informasi Pada Sistem Pengadaan Secara Elektronik

Ends	Meningkatkan transparansi dan akuntabilitas, Meningkatkan akses pasar dan persaingan usaha yang sehat, Memperbaiki tingkat efisiensi proses Pengadaan, Mendukung proses monitoring dan audit, dan Memenuhi kebutuhan akses informasi yang *real time*
Means	Peraturan Presiden No. 16 Tahun 2018, Peraturan LKPP No.14 Tahun 2018, dan Peraturan LKPP No.19 Tahun 2018
	Membangun kerjasama dengan LKPP dalam hal pengelolaan sistem pengadaan secara elektronik dan keamanan informasi SPSE. Dan Membangun kerjasama dengan dengan Penyedia Jasa *Coolocation* untuk pengelolaan *server* utama.
	Menyusun program-program kegiatan yang terkait tata kelola LPSE dan upaya pencegahan serangan siber
Ways	Pengadaan server backup;
	Penggunaan Firewall;
	Penggunaan VPN;
	Mengunakan level hak akses
	Menggunakan Aplikasi Apendo untuk kriptografi
	Pelatihan Penggunaan SPSE versi terbaru;
	Menyelenggarakan Rapat Koordinasi (Rakor) teknis LPSE se-Provinsi Lampung;

	Melaksanakan sosialisasi kepada pengguna SPSE (Pokja, Penyedia dan OPD) terkait pentingnya kerahasian login.
	Berkoordinasi secara rutin dengan LKPP jika terjadi *trouble* terhadap sistem SPSE;
	Berkoordinasi secara rutin dengan PT. jika terjadi *trouble* terhadap jaringan internet SPSE
	Secara rutin dilakukan audit oleh LKPP

(Sumber : Dikelola oleh peneliti)

Namun dari strategi yang telah dilakukan oleh LPSE Provinsi Lampung ini masih memiliki kelemahan, hal ini terbukti bahwa pada tahun 2018 yang lalu, terjadi serangan *hacker* kembali pada sistem pengadaan secara elektronik LPSE Provinsi Lampung. Dari sisi teknologi yang dimiliki oleh LPSE Provinsi Lampung memang sudah sangat baik. Namun pada sisi tatakelola dan sumber daya manusia masih lemah. Sehingga strategi yang di miliki oleh LPSE Provinsi Lampung dalam menghadapi ancaman siber di masa yang akan datang masih belum maksimal.

Hal ini sesuai dengan hasil penelitian terdahulu yang telah dilakukan oleh Firli Satriawan (2018) dengan judul penelitian "Implementasi Sistem Pengadaan Barang/Jasa Secara Elektronik (SPSE) Dalam Mewujudkan Transparansi Pemerintahan (Studi Pada Badan Layanan Pengadaan Barang/Jasa (BLPBJ) dan Layanan Pengadaan Secara Elektronik (LPSE) Provinsi Lampung)" yang telah disebutkan sebelumnya pada Bab II. Dimana di dapat hasil bahwa belum adanya peraturan perundang-undangan yang mengatur lebih rinci terkait pengeloaan pengadaan barang/jasa secara elektronik. masih terdapat kekurangan dalam hal sumber daya yang terdiri dari faktor internal yaitu kurangnya ketersediaan aparatur pemerintah dalam instansi pemerintah, masih adanya aparatur yang belum mampu melaksanakan tugasnya dengan kompeten dan maksimal. Sehingga hal ini sesuai dengan apa

yang penelti dapatkan pada penelitian ini yaitu adanya kelemahan pada aspek *Governance* dan aspek *People.*

Berdasarkan landasan teori pada Bab II terkait ancaman terhadap keamanan informasi yang diungkapkan oleh Garfinkel bahwa ancaman terhadap keamanan komputer (*computer security*) melingkupi empat aspek, yaitu *privacy*, *integrity*, *authentication*, dan *availability*. Dan didapatkan hasil bahwa dengan menggunakan model keamanan informasi *defense in depth* dapat menghadapi ancaman terhadap *privacy*, *integrity*, *authentication*, dan *availability*.

*Privac*y atau *confidentiality* adalah usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. *Privacy* lebih kearah data-data yang sifatnya *private* sedangkan *confidentiality* biasanya berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu (misalnya sebagai bagian dari pendaftaran sebuah *service*) dan hanya diperbolehkan untuk keperluan tertentu tersebut. Melalui perlindungan pada aspek *people dan technology* pada model *defense in depth*, dapat menghadapi ancaman terhadap *privac*y atau *confidentiality*. Hal ini dikarenakan adanya keamanan personil/pengguna pada aspek *people* dan adanya manajemen komunikasi dan keamanan aplikasi pada aspek *technology* sehingga dapat menghadapi ancaman terhadap kerahasiaan data.

Integrity merupakan aspek yang menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi. Adanya virus, trojan horse, atau pemakai lain yang mengubah informasi tanpa ijin. Penyadapan merupakan salah satu ancaman terhadap aspek *integrity* ini. Melalui perlindungan pada aspek *technology* pada model *defense in depth*, dapat menghadapi ancaman terhadap *integrity*. Hal ini dikarenakan adanya manajemen komunikasi dan keamanan aplikasi yang salah satunya dengan teknik kriptografi pada aspek *technology* sehingga dapat menghadapi ancaman terhadap keaslian data.

Authentication merupakan aspek yang berhubungan dengan metode untuk menyatakan bahwa informasi betul-betul asli, atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud. Melalui perlindungan pada aspek *processes* pada *defense in depth*, dapat menghadapi ancaman terhadap *Authentication*. Hal ini dikarenakan adanya manajemen hak akses yang salah satunya dengan penerapan *login* dan level hak akses pada aspek *processes* sehingga orang yang dapat masuk kedalam sistem ialah orang yang memang memiliki hak akses.

Availability merupakan aspek yang berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang atau dijebol dapat menghambat atau meniadakan akses ke informasi. Contoh hambatan adalah serangan yang sering disebut dengan *denial of service attack (DoS attack)*, dimana server dikirimi permintaan (biasanya palsu) yang bertubi-tubi atau permintaan yang diluar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai *down, hang, crash.* Melalui perlindungan pada aspek *technology* pada model *defense in depth*, dapat menghadapi ancaman terhadap a*vailability*. Hal ini dikarenakan adanya manajemen arsitektur jaringan dan keamanan aplikasi pada aspek *technology* dengan menggunakan *firewall* dan *VPN* akan membatasi dan memblokir akses-akses yang tidak resmi/ mencurigakan/ tidak wajar sehingga sistem akan menolak atau memblokir IP tersebut. Melalui perlindungan aspek *technology* pada *defense in depth* ini tentu akan dapat menghadapi ancaman terhadap a*vailability.*

Dan pada akhirnya dengan menerapkan model keamanan informasi defense in depth yang terdiri aspek Governance, People, Processes dan Technology ini akan melindungi aspek *privacy*, *integrity*, *authentication*, dan *availability*.

BAB V
KESIMPULAN DAN REKOMENDASI

5.1. Kesimpulan

Kesimpulan yang dapat peneliti sajikan dari penelitian yang telah dilakukan ini adalah sebagai berikut:

5.1.1 Strategi Keamanan Informasi Dalam Menghadapi Ancaman Siber Pada Sistem Pengadaan Secara Elektronik Provinsi Lampung.

Dalam strategi keamanan informasi dengan menggunakan model keamanan informasi *defense in depth* yang dikembangkan oleh *IT Security Expert Advisory Group (ITSEAG)* di LPSE Provinsi Lampung guna menghadapi ancaman siber pada sistem pengadaan secara elektronik berdasarkan 4 aspek yaitu *People*, *Process*, *Technology*, dan *Governance*. Dihasilkan bahwa:

1. Aspek *Governance*, pada aspek ini LPSE Provinsi Lampung belum memenuhi standar model keamanan informasi *defense in depth* hal ini dikarenakan LPSE Provinsi Lampung belum memiliki aturan atau standar terkait pengelolaan keamanan informasi dan manajemen resiko.
2. Aspek *People*, pada aspek ini LPSE Provinsi Lampung belum memenuhi standar model keamanan informasi *defense in depth* hal ini dikarenakan belum adanya kesadaran dan kapasitas terhadap keamanan informasi bagi pengguna/personil.
3. Aspek *Processes*, pada aspek ini LPSE Provinsi Lampung belum memenuhi standar model keamanan informasi *defense in depth* hal ini dikarenakan masih lemahnya manajemen audit dan belum adanya manajemen respon terhadap suatu *trouble*.
4. Aspek *Technology*, pada aspek ini LPSE Provinsi Lampung belum memenuhi standar model keamanan informasi *defense in depth* hal

ini dikarenakan LPSE Provinsi Lampung belum menerapkan manajemen komunikasi dan manajamen infrastruktur khususnya pengamanan fisik ruang server.

5.1.2 Pelaksanaan LPSE Provinsi Lampung Dalam Mengamankan Sistem Informasi Pada Sistem Pengadaan Secara Elektronik.

Dalam rangka mengamankan informasi pada sistem pengadaan secara elektronik LPSE Provinsi Lampung telah melaksanaakan suatu strategi berdasarkan teori strategi Karl Von Clauswitz yaitu *Ends, Means and Ways* sebagai berikut:

1. *Ends,* pengamanan informasi pada SPSE dalam rangka untuk pencapaian terhadap tujuan LPSE yaitu meningkatkan transparansi dan akuntabilitas dan memenuhi kebutuhan akses informasi yang *real time*.
2. *Means*, sarana dan prasarana yang digunakan dalam mencapai tujuan LPSE yaitu berpedoman pada Peraturan Presiden No. 16 Tahun 2018 Peraturan LKPP No.14 Tahun 2018 dan Peraturan LKPP No.19 Tahun 2018. Serta membangun kerjasama dengan LKPP dan Penyedia jasa *coolocation* untuk pengelolaan *server* utama.
3. *Ways*, LPSE Provinsi Lampung dalam upaya pengamanan sistem informasi guna mencapai tujuan melakukan langkah-langkah: pengadaan *server backup*, pemasangan *firewall* dan *VPN*, pelatihan dan sosialisasi penggunaan SPSE, serta menyelenggarakan rapat koordinasi (rakor) teknis LPSE se-Provinsi Lampung.

5.2. Rekomendasi

Peneliti memberikan rekomendasi yang bersifat teoritis dan bersifat praktis.

5.2.1 Rekomendasi Teoretis

Ditujukan kepada pihak-pihak terkait untuk menjadikan hasil penelitian ini sebagai rujukan dalam melakukan penelitian lanjutan dengan fokus/subfokus yang serupa.

5.2.2 Rekomendasi Praktis

Ditujukan kepada LPSE Provinsi Lampung agar dapat melakukan hal-hal sebagai berikut:

1. Mengajukan permohonan kepada Sekretaris Provinsi Lampung selaku Pengguna Anggaran (PA) untuk menambahkan alokasi anggaran pada LPSE Provinsi Lampung guna meningkatkan sarana dan prasarana keamanan informasi pada sistem pengadaan secara elektronik;
2. Meningkatkan kapasitas sumber daya manusia di LPSE Provinsi Lampung yang mampu dan memahami bidang *IT* melalui rekrutmen, pelatihan dan sosialisasi.
3. Harus di buat dan ditetapkannya SOP terkait keamanan informasi yang dapat dilaksanaakan dan dikembangkan secara berkelanjutan.

DAFTAR PUSTAKA

BUKU

Alfred, D. Chandler. 1962. *Strategy and Structure: Chapters in The History of The industrial Enterprise*. Cambridge Mass : MIT Press.

Anastasia, Diana dan Lilis Setiawati. 2011. *Sistem Informasi Akuntansi, Perancangan, Prosedur dan Penerapan*. Edisi 1. Yogyakarta: Andi Yogyakarta.

David, Fred. R. 2011. *Manajemen Strategis: Konsep-Konsep*. Edisi Duabelas. Jakarta: Salemba Empat.

Fandy,Tjiptono. 2006. *Manajemen Jasa*. Yogyakarta : Andi.

Fred N. & Howard B. Lee. 2000. *Foundations of Behavioral Research*. 4th Edition. Florida: Harcourt Inc.

Garfinkel, Simson. 1995. *PGP: Pretty Good Privacy*. O'Reilly & Associates, Inc.

Hasan, M. Iqbal. 2002. *Pokok-pokok Materi Metodologi Penelitian dan Aplikasinya.* Bogor : Ghalia Indonesia.

Hunger, David dan Thomas L. Wheelen. 2003. *Manajemen Strategi*. Yogyakarta: Andi.

Jasin, Mochammad. 2007. *Mencegah Korupsi Melalui E-procurement.* Jakarta : Komisi Pemberantasan Korupsi.

Kementerian Informasi dan Komunikasi. 2018. *Kebijakan Cybersecurity Dalam Perspektif Multistakeholder*. Jakarta : Seri Literasi Digital

Kementerian Pertahanan Republik Indonesia, *Buku Putih Pertahanan Indonesia 2015*. Jakarta:

Kementerian Pertahanan Republik Indonesia, Media Informasi Pertahanan Volume 54/No.38/Mei-Juni 2015.

Makmur, Supriyatno. 2014. *Tentang Ilmu Pertahanan*. Jakarta: Yayasan Pustaka Obor Indonesia.

Milles dan Huberman. 1992. *Analisis Data Kualitatif*. Jakarta: Universitas Indonesia Press

Moleong, J. 2014. *Metodologi Penelitian Kualitatif*, Edisi Revisi. Bandung: Remaja Rosdakarya.

Mulyadi. 2016. *Sistem Akuntansi.* Jakarta : Salemba Empat

Patton, Michael Quinn. 1987. *Qualitative Education Methods*. Beverly Hills: Sage Publication

Rianse, Usman. 2009. *Metodologi Penelitian Sosial dan Ekonomi, Teori dan Aplikasi*. Bandung: Alfabeta.

Romney, Marshal R. & Paul John Steinbart. 2015. *Sistem Informasi Akuntansi.* Jakarta : Salemba Empat.

Sangadji, Etta Mamang dan Sopiah. 2010. *Metodologi Penelitian, Pendekatan Praktis dalam Penelitian.* Yogyakarta: Andi.

SANS Institute InfoSec Reading Room. 2001. *Defense in depth*. United State:

Sutopo. 2002. *Metodologi Penelitian Kualitatif*. Surakarta: Sebelas Maret University Press.

Trusted Information Sharing Network. 2008. *Defense in depth.* Australia :

Turban, Efraim, et al. 2008. *Electronic Commerce 2008: A Managerial Perspective*. New Jersey: Prentince Hall, Inc.

William, Stallings. 1995. *Network and Internetwork Security*. Prentice Hall.

TESIS

Chandra, Muhammad. 2017. *Perencanaan Keamanan Informasi dengan Menggunakan Metode ISO 27001:2005 Di LPSE Kab. Bandung Barat*.

Ilham, Muhammad, 2015. *Evaluasi Celah Keamanan Web Server pada LPSE Kota Palembang*.

Suryani, Wiwik. 2015. *Implementasi Kebijakan E-Procurement Pada Layanan Pengadaan Barang Dan Jasa Secara Elektronik (LPSE) Pemerintah Provinsi Riau*.

JURNAL

Arthur F. Lykke Jr. 1989. *Defining Military Strategy*, (Military Review 69, no. 5.)

Croom, S.R., Brandon-Jones, A., *"Impact of E-procurement: experiences from implementation in the UK public sector"*, Journal of Purchasing & Supply Management, Vol. 13, 2007

Davila, A., Gupta, M., Palmer, R., *"Moving procurement systems to the internet : the adoption and use of e-Procurement technology models"*, European Management Journal, Vol.21, No. 1, 2003.

Tatsis,V., Mena,C., VanWassenhove, L.N., Whicker,L., *"Procurement in the Greek Food and Drink Industry"*, Journal of Purchasing & Supply Management, Vol. 12, 2006.

UNDANG-UNDANG

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Republik Indonesia Nomor 14 tahun 2008 Tentang Keterbukaan Infromasi.

PERATURAN

Instruksi Presiden No 3 tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan E-Government

Peraturan Kepala LKPP Nomor 2 Tahun 2010 tentang Layanan pengadaan Secara Elektronik.

Peraturan Kepala LKPP Nomor 1 Tahun 2011 tentang Tata Cara *E-Tendering*.

Peraturan Presiden pasal 111 Nomor 54 tahun 2010 Tentang Pengadaan Barang atau Jasa Pemerintah.

Peraturan Presiden Nomor 70 Tahun 2012 Tentang Pengadaan Barang atau Jasa Pemerintah

Peraturan Rektor Universitas Pertahanan Nomor 30 Tahun 2017 tentang Buku Pedoman Penulisan Tesis dan Disertasi Universitas Pertahanan.

INTERNET

Anonim. *"Dunia Maya"* Dalam https://id.wikipedia.org/wiki/Dunia_maya diakses Pada 10 Mei 2018

Biro Humas, Kementerian Komunikasi Dan Informatika. *"Himbauan Agar Segera Melakukan Tindakan Pencegahan Terhadap Ancaman Malware Khususnya Ransomware Jenis WannaCRY"* Dalam https://www.kominfo.go.id/content/detail/9636/siaran-pers-no-55hmkominfo052017-tentang-himbauan-agar-segera-melakukan-tindakan-pencegahan-terhadap-ancaman-malware-khususnya-ransomware-jenis-wannacry/0/siaran_pers diakses pada 4 agustus 2018.

Julan, Tritus. *"Laman LPSE Diretas, Proses Lelang Kacau"* Dalam http://koran-sindo.com/page/news/2016-05-10/6/47/Laman_LPSE_Diretas_Proses_Lelang_Kacau diakses pada 4 Agustus 2018

Kurniawati, Putri. *"Hacker Pembobol LPSE Kementerian PUPR Terancam Kurungan Empat Tahun Penjara"* Dalam https://www.kupastuntas.co/2016/08/hacker-pembobol-lpse-kementerian-pupr-terancam-kurungan-empat-tahun-penjara/ diakses pada 4 Agustus 2018.

Maulana, Rizqi F. *"Aksi Hacker Meretas Situs KPAI yang Mendukung Pemblokiran Game Online Patut Disayangkan"* Dalam https://id.techinasia.com/aksi-hacker-meretas-situs-kpai-patut-disayangkan diakses pada 4 Agustus 2018.

Prayudi, Yudi. *"Ransomware, Kejahatan Pemerasan Cyber yang Mengancam Sistem Komputer di Dunia"* Dalam http://jogja.tribunnews.com/2017/05/14/ransomware-kejahatan-pemerasan-cyber-yang-mengancam-sistem-komputer-di-dunia di akses pada 4 Agustus 2018

Rizki, Ramadhan. *"Dalih Peretasan Situs KPU di Balik Transparansi Suara Pilkada"*, dalam https://www.cnnindonesia.com/nasional/20180703143616-32-311113/dalih-peretasan-situs-kpu-di-balik-transparansi-suara-pilkada diakses pada 4 Agustus 2018

Yulianto, Beni. *"Awalnya Diserang Hacker, Katanya Sudah Bisa Diakses, Nyatanya Tak Bisa"* Dalam http://lampung.tribunnews.com/2015/05/23/awalnya-diserang-hacker-katanya-sudah-bisa-diakses-nyatanya-tak-bisa diakses pada 28 juli 2018.

United State, National Security Agency, "*Defense in Depth*" dalam www.nsa.gov/snac/support/defenseindepth.pdf dikases pada 4 Agustus 2018

LAMPIRAN 1

SURAT IJIN PENELITIAN

KEMENTERIAN PERTAHANAN RI
UNIVERSITAS PERTAHANAN

Nomor : B / 2319 / IX/2018
Klasifikasi : Biasa
Lampiran : -
Hal : Permohonan Izin Penelitian

Bogor, 07 September 2018

Kepada
Yth. Pejabat Terlampir
di
Tempat

1. Dasar:
   a. Peraturan Presiden RI Nomor 5 Tahun 2011 tentang Universitas Pertahanan sebagai Perguruan Tinggi yang diselenggarakan oleh Pemerintah;
   b. Kalender Pendidikan Program Studi Peperangan Asimetris Fakultas Strategi Pertahanan Unhan TA. 2017/2018.
2. Sehubungan dasar tersebut di atas, mohon dapatnya Pejabat dalam lampiran berkenan mengizinkan mahasiswa Prodi Studi Peperangan Asimetris Fakultas Strategi Pertahanan Universitas Pertahanan atas nama Adi Wijaya, Nomor Induk Mahasiswa 12017012001, untuk melaksanakan wawancara dan atau memberikan kuesioner guna mengumpulkan data-data penelitian yang diperlukan dalam penyusunan Tesis dengan judul "Strategi Keamanan Informasi dalam Menghadapi Ancaman Siber Pada Sistem Pengadaan Secara Elektronik (Suatu Studi Serangan *Hacker* pada SPSE Provinsi Lampung Tahun 2015)"
3. Mohon konfirmasi waktu serta tempat pelaksanaan wawancara dan pemberian kuesioner kepada Adi Wijaya, NIM. 12017012001, HP. 082269112269, email. adi.wijaya@idu.ac.id dan adidontgiveup@gmail.com.
4. Demikian untuk menjadikan periksa.

a.n. Rektor Universitas Pertahanan
Warek I Bidang Akademik dan
Kemahasiswaan,

Prof. Dr. Ir. Dadang Gunawan, M.Eng
Pembina Utama IV/e

Tembusan:
1. Rektor Unhan
2. Dekan FSP Unhan
3. Karo Akademik & Kemahasiswaan Unhan.

Lampiran Surat Rektor Unhan
Nomor : B/ 2319 / IX/2018
Tanggal : 07 September 2018

DAFTAR NAMA PEJABAT

1. Kepala Lembaga Kebijakan Pengadaan Barang dan Jasa Pemerintah (LKPP)
2. Kedeputian Bidang Monitoring Evaluasi dan Pengembangan Sistem Informasi, LKPP
3. Kepala Bappeda, Provinsi Lampung
4. Ketua LPSE, Provinsi Lampung
5. Ketua ULP, Provinsi Lampung
6. Admin PPE, LPSE Provinsi Lampung
7. Admin Sistem, LPSE Provinsi Lampung
8. Verifikator, LPSE Provinsi Lampung
9. Dekan Fakultas Ilmu Komputer, Universitas Bandar Lampung
10. Kepala Prodi Informatika, Universitas Bandar Lampung

a.n. Rektor Universitas Pertahanan
Warek I Bidang Akademik dan
Kemahasiswaan,

Prof. Dr. Ir. Dadang Gunawan, M.Eng
Pembina Utama IV/e

LAMPIRAN 2

PEDOMAN WAWANCARA

PEDOMAN WAWANCARA

STRATEGI KEAMANAN INFORMASI
DALAM MENGHADAPI ANCAMAN SIBER
PADA SISTEM PENGADAAN SECARA ELEKTRONIK
(STUDI SERANGAN *HACKER* PADA SPSE PROVINSI LAMPUNG
TAHUN 2015)

INFORMASI UMUM

Peneliti mengharapkan kesediaan Bapak/Ibu/Saudara/i, berkenan untuk menjawab pertanyaan yang telah dibuat peneliti dalam rangka penelitian mahasiswa Universitas Pertahanan. Mohon jawaban atas pertanyaan ini diisi dengan benar dan sejujurnya. Terima Kasih atas partisipasi Bapak/ Ibu/ Saudara/ i dalam menjawab pertanyaan yang ada. Apabila terdapat keluhan, kritik dan saran, maka Bapak/Ibu/Saudara/i dapat menghubungi:

Nama	:	Adi Wijaya
Fakultas / Prodi	:	Strategi Pertahanan / Peperangan Asimetris
Perguruan Tinggi	:	Universitas Pertahanan.
Alamat	:	Kawasan IPSC, Sentul, Sukahati, Citeureup, Bogor Jawa Barat – 16810.
No Telp / Email	:	082269112269 / adidontgiveup@gmail.com

A. Identitas Informan.

Nama : ……

Pangkat/ Korps : ……....

Satuan : ……

Jabatan : ……

Alamat : ……

B. Deskripsi Penelitian.

Dalam sistem pertahanan negara, sebagaimana disebutkan dalam Peraturan Menteri Pertahanan Republik Indonesia Nomor 38 Tahun 2015 tentang Doktrin Pertahanan Negara 2015, pemerintah daerah adalah salah satu Unsur Lain Kekuatan Bangsa yang harus terlibat sebagai pertahanan nirmiliter untuk menghadapi ancaman yang bersifat nonmiliter. Dimana ancaman siber digolongkan sebagai ancaman yang bersifat non militer. Pemerintah daerah sangat berperan penting dalam pembangunan sistem pertahanan nirmiliter untuk menghadapi ancaman non militer dalam hal ini ancaman siber. Sebab jika ancaman siber ini tidak ditangani secara serius maka dapat mengganggu berjalannya roda pemerintahan.

Layanan Pengadaan Secara Elektronik (LPSE) provinsi Lampung sebagai instansi yang bertanggungjawab memberikan pelayanan pengadaan barang dan jasa pemerintah memiliki peranan yang sangat penting. Hal ini dikarena semua pengadaan barang dan jasa yang akan dilaksanakan oleh pemerintah provinsi Lampung harus melalui proses tender di LPSE provinsi Lampung. Terganggunya sistem pengadaan ini tentu akan berdampak pada terhambatnya proyek pemerintah. Maka dari hal tersebut perlu dilakukanya pengamanan sistem informasi tersebut guna memastikan berjalanannya sistem sesuai yang dharapkan. Namun kenyataannya pada tahun 2015 SPSE Provinsi Lampung mendapat serangan *hacker* yang mengakibatkan sistem pengadaan secara elektronik tidak bisa digunakan. Hal ini menyebabkan paket yang sedang tender harus dihentikan dan dilakukan tender dari awal atau tender ulang.

Maka dari hal tersebut perlu adanya upaya yang harus dilakukan agar serangan *hacker* tersebut tidak terulang kembali pada Sistem Pengadaan Secara Elektronik (SPSE) provinsi Lampung. Sehingga untuk mewujudkan hal tersebut diperlukan sebuah strategi yang dapat mengamankan sistem tersebut. Maka peneliti mencoba mengusulkan sebuah strategi pertahanan berlapis yang dapat mengamankan sistem dari serangan *hacker* maupun ancaman siber lainnya. Oleh sebab itu peneliti mengusulkan strategi *Defense in Depth* untuk digunakan sebagai strategi mengamankan sistem informasi.

C. Panduan Wawancara

Dalam membahas mengenai penelitian ini dibutuhkan informasi mengenai strategi dalam menghadapi ancaman siber pada Sistem Pengadaan Secara Elektronik Provinsi Lampung.

1. Governance

a. Bagaimana pemahaman LPSE provinsi Lampung terhadap manajemen resiko ?
b. Apakah LPSE Provinsi Lampung sudah mempunyai manajemen resiko ?
c. Bagaimana implementasi manajemen resiko tersebut di LPSE Provinsi Lampung ?
d. Apa kendala yang membuat LPSE Provinsi Lampung belum mempunyai manajemen resiko ?
e. Bagaimana pemahaman LPSE provinsi Lampung terhadap sistem keamanan informasi ?
f. Apakah LPSE Provinsi Lampung sudah mempunyai sistem keamanan informasi ?
g. Bagaimana implementasi sistem keamanan informasi tersebut di LPSE Provinsi Lampung ?
h. Apa kendala yang membuat LPSE Provinsi Lampung belum mempunyai sistem keamanan informasi ?

i. Apakah LPSE Provinsi Lampung sudah menetapkan kebijakan terkait pengadaan barang dan jasa di LPSE Provinsi Lampung ?

2. *People*

a. Apakah SDM yang ada di LPSE provinsi Lampung sudah mendapat pelatihan terkait penggunaan SPSE ?

b. Apakah SDM yang ada di LPSE provinsi Lampung sudah mendapat sosialisasi terkait pentingnya kesadaran keamanan informasi ?

3. *Proccess*

a. Bagaimana pemahaman LPSE provinsi Lampung terhadap manajemen akses pengguna ?

b. Apakah LPSE Provinsi Lampung sudah mempunyai manajemen akses pengguna ?

c. Bagaimana implementasi manajemen akses pengguna tersebut di LPSE Provinsi Lampung ?

d. Apa kendala yang membuat LPSE Provinsi Lampung belum mempunyai manajemen akses pengguna ?

e. Bagaimana pemahaman LPSE provinsi Lampung terhadap manajemen respon ?

f. Apakah LPSE Provinsi Lampung sudah mempunyai manajemen respon ?

g. Bagaimana implementasi manajemen respon tersebut di LPSE Provinsi Lampung ?

h. Apa kendala yang membuat LPSE Provinsi Lampung belum mempunyai manajemen respon ?

i. Bagaimana pemahaman LPSE provinsi Lampung terhadap manajemen audit ?

j. Apakah LPSE Provinsi Lampung sudah mempunyai manajemen audit ?

k. Bagaimana implementasi manajemen audit tersebut di LPSE Provinsi Lampung ?
l. Apa kendala yang membuat LPSE Provinsi Lampung belum mempunyai manajemen audit ?

4. *Technology*
   a. Bagaimana pemahaman LPSE provinsi Lampung terhadap manajemen komunikasi ?
   b. Apakah LPSE Provinsi Lampung sudah mempunyai manajemen komunikasi ?
   c. Bagaimana implementasi manajemen komunikasi tersebut di LPSE Provinsi Lampung ?
   d. Apa kendala yang membuat LPSE Provinsi Lampung belum mempunyai komunikasi ?
   e. Bagaimana pemahaman LPSE provinsi Lampung terhadap manajemen infrastruktur ?
   f. Apakah LPSE Provinsi Lampung sudah mempunyai manajemen infrastruktur ?
   g. Bagaimana implementasi manajemen infrastruktur tersebut di LPSE Provinsi Lampung ?
   h. Apa kendala yang membuat LPSE Provinsi Lampung belum mempunyai manajemen infrastruktur ?
   i. Bagaimana pemahaman LPSE provinsi Lampung terhadap manajemen arsitektur jaringan ?
   j. Apakah LPSE Provinsi Lampung sudah mempunyai manajemen arsitektur jaringan ?
   k. Bagaimana implementasi manajemen arsitektur jaringan tersebut di LPSE Provinsi Lampung ?
   l. Apa kendala yang membuat LPSE Provinsi Lampung belum mempunyai manajemen arsitektur jaringan ?

LAMPIRAN 3
CATATAN HASIL WAWANCARA

Wawancara dengan Kepala Bagian LPSE Provinsi Lampung

Hari : Selasa, 18 Desember 2018

Tempat : Ruang Kepala Bagian LPSE Provinsi Lampung

Narasumber : Dodi Hendrawan, ST.

Waktu : 09.00 WIB – selesai

T	**:**	**Sejak kapan bapak menjabat sebagai Ketua LPSE?**
J	:	Saya menjabat sebagai ketua LPSE sejak september 2015, sebelumnya saya dari Badan Perencanaan Pembangunan Daerah (Bappeda) Provinsi Lampung. Kemudian pimpinan meminta saya untuk menangani LPSE Provinsi Lampung sebagai ketuanya.
T	**:**	**Sejauh ini apakah LPSE Provinsi Lampung sudah memiliki aturan atau standar tentang pengelolaan keamanan informasi ?**
J	:	Sebenarnya sebelum keluarnya No. 16 Tahun 2018 tentang Pengadaan Barang/Jasa Pemerintah, Peraturan LKPP No.14 Tahun 2018 tentang Unit Kerja Pengadaan Barang/Jasa dan Peraturan LKPP No.19 Tahun 2018 Tentang Pengembangan Sistem dan Kebijakan Pengadaan, LPSE Provinsi Lampung memiliki peraturan turunan dari Perpres sebelumnya yaitu Perpres No.70 Tahun 2012 Tentang Perubahan Kedua Atas Peraturan Presiden Nomor 54 Tahun 2010 Tentang Pengadaan Barang/Jasa Pemerintah. Peraturan ini berupa Peraturan Daerah Provinsi Lampung No. 8 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Provinsi Lampung. Di dalam perda tersebut memuat tentang bagaimana tata kelola LPSE provinsi lampung termasuk tupoksinya. Namun setelah peraturan yang baru keluar, LPSE Provinsi lampung belum memiliki aturan turunan. Terkait

		aturan atau standar pengelolaan keamanan informasi belum ada. Saat ini LPSE Provinsi Lampung hanya fokus kepada pencapaian terhadap standar yang telah di tetapkan yaitu ada 17 standar dan LPSE Provinsi Lampung telah memperoleh 12 standar. Tinggal 5 lagi yang belum tercapai. Untuk lebih jelasnya lagi terkait apa saja standarnya bisa di tanyakan kepada staf saya.
T	**:**	**Apa alasan LPSE Provinsi Lampung belum membuat aturan turunan terhadap perpres yang baru?**
J	:	Itu karena kami menilai bahwa peraturan yang baru ini sudah sangat detail mengatur tentang tata kelola LPSE dan semakin diperjelas dengan adanya peraturan LKPP yang baru. Sehingga kami merasa bahwa peraturan turunan tersebut belum diperlukan
T	**:**	**Lalu terkait pengelolaan keamanan informasi bagaimana implementasi yang sudah di lalukan oleh LPSE Provinsi Lampung?**
J	:	Untuk memastikan keamanan informasi pada sistem pengadaan elektronik kami, kami bekerja sama dengan LKPP untuk pengelolaan server utama kami. Kami juga bekerja sama dengan penyedia jasa *coocation*. Jadi server utama kami, kami titipkan di jakarta.
T	**:**	**Apakah LPSE Provinsi Lampung juga sudah memiliki aturan atau standar tentang pengelolaan resiko?**
J	:	Sama dengan pengelolaan keamanan informasi, untuk pengeloaan resiko kami juga belum memiliki aturan atau standar pengeloaan resiko berupa SOP atau sejenisnya.
T	**:**	**Lalu bagaimana penanganan resiko sejauh ini di LPSE Provinsi Lampung**
J	:	Sejauh ini untuk penanganan resiko di LPSE Provinsi Lampung keputusan berada di level pimpinan yaitu gubernur. Ini untuk yang sifatnya masalah besar. Sebagai contoh waktu terjadi serangan

		hacker tahun 2015, pimpinan yang langsung menginstruksikan untuk pengadaan server baru sebagai pengganti server yang lama akibat rusak oleh serangan hacker.
T	**:**	**Dalam keamanan informasi kan tidak hanya mengamankan sistemnya saja tetapi pengguna atau orangnya juga perlu pengamanan, sejauh ini bagaimana pengamanan terhadap pengguna LPSE?**
J	:	Terkait keamanan pengguna, semua pegawai kami terikat oleh pakta integritas yang terikat secara hukum hal ini dilakukan untuk menjaga agar pegawai kami tetap pada koridornya dan tetap menjaga kerahasiaan yang ada di LPSE. Namun untuk masalah kapasitas kemampuan pengelolaan keamanan informasi kami belum pernah memberikan pembekalan atau bimtek (bimbingan teknis) terkait hal tersebut. Sejauh ini kami hanya mensosialisasikan kepada pegawai dan pengguna yaitu pokja dan penyedia untuk melebih memprioritaskan keamanan informasi. Khususnya kerahasian login mereka. Bisanya kami mneympaikannya di saat ada pelatihan penggunaan apilkasi SPSE versi terbaru.
T	**:**	**Lalu untuk memastikan agar semua telah berjalan sesuai dengan apa yang seharusnya, apakah LPSE sudah memiliki manajemen audit ?**
J	:	Sejauh ini yang mengaudit kami hanya LKPP. Jika kami mengajukan sertifikasi untuk standar LKPP maka LKPP akan langsung mengaudit kami. Sedangkan untuk manajemen audit internal kami belum ada
T	**:**	**Terkait dengan aritektur jaringan, bagaimana keamanan aritektur jaringan di LPSE Provinsi Lampung?**
J	:	Untuk masalah arsitektur jaringan dan keamanan jaringan kami menggunakan jasa layanan telkom, jadi pihak telkom yang mealkukan setting terhadap topologi jaringan di LPSE Provinsi

		Lampung termasuk keamanan terhadap jaringan tersebut.
T	**:**	**Terkait hak akses pengguna pada SPSE, apakah LPSE Provinsi Lampung sudah menerapkan manajemen hak akses ?**
J	:	Untuk masalah ini di sistem kami sudah ada manajemen hak akses, dimana verifikator hanya bisa mengakses halaman verifikator saja begitu pula yang lain. Sehingga akses kepada sistem sesuai dengan tanggung jawabnya masing-masing.
T	**:**	**Kemudian terkait keamanan aplikasi, apa saja yang di lakukan oleh LPSE Provinsi Lampung untuk mengamankan aplikasi?**
J	:	Untuk teknis bagaimana pengamanan aplikasi nanti bisa ditanyakan kepada admin sistem kami.
T	**:**	**Bagaimana dengan keamanan infrastruktur di LPSE Provinsi Lampung khususnya pengaman fisik server backup?**
J	:	Untuk pengelolaan server, kami menggunakan ruang khusus yang kebetulan memang satu gedung dengan kantor kami. Nanti bisa dilihat secara langsung.

Wawancara dengan Kepala Subbagian Pengembangan Sistem Informasi LPSE Provinsi Lampung

Hari : Selasa, 18 Desember 2018

Tempat : Ruang LPSE Provinsi Lampung

Narasumber : Yusron, ST

Waktu : 10.00 WIB – selesai

T	**:**	**Sejak kapan bapak menjadi admin PPE di LPSE Provinsi Lampung?**
J	:	Saya sejak akhir tahun 2010 sudah menangani LPSE Provinsi Lampung, karena saya salah satu orang yang menjadi tim pendiri LPSE Provinsi Lampung.
T	**:**	**Sejak Kapan LPSE Provinsi Lampung didirikan ?**
J	:	LPSE Provinsi Lampung berdiri menjadi salah satu bagian di biro administrasi pembangunan berdasarkan Peraturan Daerah Provinsi Lampung No. 8 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Provinsi Lampung. Sebelum adanya peraturan daerah ini status LPSE Provinsi Lampung adalah *ad-hoc* (kepanitian). Namun LPSE Provinsi Lampung terbentuk sejak tahun 2010 dan pada tahun 2011 untuk pertama kalinya melakukan proses pengadaan barang/jasa secara elektronik.
T	**:**	**Bagaimana serangan hacker tahun 2015 bisa terjadi ?**
J	:	Serangan tahun 2015 itu terjadi akibat serangan hacker yang membuat kondisi server awtu itu mengalami floading. Yaitu kondisi server diserang dengan akses yang bertubi-tubi secara besar-besaran sehingga mengakibatkan server kami down.
T	**:**	**Lalu apa dampak dari serang hacker tersebut ?**
J	:	Akibat serangan tersebut membuat server kami down, padahal saat ini kami sedang ada lelang sehingga terpaksa lelang di ulang dan di tunda selama kurang lebih satu bulan. Karena serang tersebut

		membuat kami harus membeli server baru, kami takut untuk menggunakan server yang lama karena mengantisipasi hacker tersebut menyerang lagi untuk kedua kalinya.
T	**:**	**Lalu langkah apa yang di lakukan LPSE Provinsi Lampung untuk mengatasi hal tersebut ?**
J	:	Langkah yang pertama kami ambil ialah dengan membeli server baru dan mengganti penyedia yang mengelola server kami. Dimana kami sekarang sudah bekerjasama dengan penyedia jasa coocation yang ada di jakarta. Sebenarnya baru-baru ini kami juga mendapat serangan hacker kembali sekitar bulan juli 2018 yang lalu. Tapi serangan yang terjadi tidak separah yang dulu. Hacker hanya mengganggu 3 paket yang sedang lelang. Modusnya dengan mengganti dokumen penawaran yang sudah di upload dengan penawaran yang berbeda. Sehingga ketika dokumen tersebut di buka oleh pokja tidak sesuai dengan aslinya.
T	**:**	**Terkait dengan personil yang ada di LPSE Provinsi Lampung, apakah banyak yang memiliki kapasitas atau lulusan IT?**
J	:	Untuk di tempat kami yang lulusan IT hanya satu orang, dia yang menjadi admin sistem di LPSE Provinsi lampung. Saya saja lulusan teknik sipil. Kami memang memiliki keterbatasan terhadap SDM yang memiliki kapasitas di bidang IT.
T	**:**	**Bapak sebagai admin PPE yang merupakan admin tertinggi di SPSE sering melakukan pengawasan atau kontrol terhadap sistem?**
J	:	Ya sesekali saya mengawasi namun ya tidak terlalu sering. Saya hanya mengawasi log akses. Tapi yang sesekali saja, karena tidak mungkin mau mengawasi IP yang begitu banyak secara rutin
T	**:**	**Terkait dengan kapasitas SDM di LPSE Provinsi Lampung, apakah ada pembekalan terhadap pengetahun IT khususnya keamanan informasi?**

J	:	Sejauh ini kami belum pernah memberikan atau mengirimkan pegawai kami untuk mendapat pelatihan tentang keamanan informasi. Sejauh ini kami hanya memberikan pelatihan tentang penggunaan aplikasi SPSE saja.
T	**:**	**Menurut bapak apa yang menjadi kendala mengapa keamanan informasi belum menjadi prioritas di LPSE Provinsi Lampung?**
J	:	Masalah kami selain pada SDM yang di miliki, kami juga terkendala dengan anggaran. Untuk pembelian perangkat baru saja terkadang kami harus menghemat SPPD (belanja perjalanan dinas) kami. Sehingga terkadang kalau ada undangan bimtek kami tidak ikut.

Wawancara dengan Kepala Subbagian Pengendalian dan Administrasi Pembangunan

Hari : Selasa, 18 Desember 2018

Tempat : Ruang Biro Administrasi Pembangunan Provinsi Lampung

Narasumber : Andi Ahmad Yusuf, S.Kom., MM.

Waktu : 14.00 WIB – selesai

T	**:**	**Sejak kapan bapak di LPSE Provinsi Lampung ?**
J	:	Sebenarnya saat ini saya bukan pegawai di LPSE Provinsi Lampung saat ini saya pegawai di bagian pengendalian administrasi pembangunan dan kebetulan saya kasubbagnya. Sebelumnya saya memang saya staf di LPSE akan tetapi sejah 2018 ini saya ditarik menjadi kasubbag pengendalian dan pembangunan administrasi lampung. Berhubung LPSE dan tempat baru saya masih di dalam biro yang sama yaitu administrasi pembangunan, jadi saya masih diamanahkan sebagai admin sistem yang mengelola server LPSE.
T	**:**	**Terkait serangan hacker tahun 2015 apakah bapak tahu kronologinya ?**
J	:	Sebenernya kalo secara langsung saya tidak tahu, karena saat ini server LPSE masih dikelola oleh pihak ke-3. Yang saya bilang termasuk kelalaian kami saat itu. Sebab saat ini kami belum memiliki kapasitas untuk mengelola server. Sehingga pengelolaan server sepenuhnya kami serahkan kepada pihak ke-3 tersebut. Berdasarkan diskusi saya dengan pihak IT LKPP, ada dugaan bahwa sebelum peristiwa serangan hacker terjadi, ada pihak yang sengaja menyusupkan java script kedalam server. File ini ini seperti halnya malware atau virus, padahal ukuran filenya sangat kecil tapi ketika file ini di aktifkan, file ini memberikan sinyal lokasi untuk penyerangan. Maka ketika file diaktifkan kemudian serangan secara

		besar dan bertubi-tubi menyerang server kita sehingga server menjadi down dan tidak dapat diakses. Ini semacam serangan DDos.
T	**:**	**Lalu apa yang dilakukan oleh pihak LPSE saat itu ?**
J	:	Kami segera memutus kerjasama dengan pihak ke-3 tersebut dan menggantinya dengan yang lebih kompeten dengan sistem colocation. Kami menggunakan pihak penyedia jasa coolocation yang ada di jakarta. Karena banyak LPSE di Indonesia juga menggunakan penyedia tersebut. Dan kami juga membangun kerjasama dengan LKPP untuk pengamanan server
T	**:**	**Lalu apa dampak dari serang hacker tersebut ?**
J	:	Akibat serangan tersebut membuat server kami down, padahal saat ini kami sedang ada lelang sehingga terpaksa lelang di ulang dan di tunda selama kurang lebih satu bulan. Karena serang tersebut membuat kami harus membeli server baru, kami takut untuk menggunakan server yang lama karena mengantisipasi hacker tersebut menyerang lagi untuk kedua kalinya.
T	**:**	**Apakah langkah-langkah yang telah dilakukan tersebut efektif ?**
J	:	Dibilang efektif sih iya. Tapi belum maksimal, karena nyatanya belum lama ini kami diserang hacker lagi. Namun serangannya agak berbeda. Hacker tidak masuk menerobos kedalam server, sebab waktu kami cek bersama LKPP tidak akses yang anomali. Kemungkinan besar ada pihak yang secara sengaja menggunakan login penyedia untuk masuk dke aplikasi SPSE. Sebab saat ini banyak penyedia barang/jasa meminjamkan perusahaannya ke pihak lain termasuk login SPSEnya. Dan setelah perusahanan dikembalikan pihaknya lupa untuk mengubah login. Sehingga ada oknum yang memanfaatkanhal tersebut untuk tujuan tertentu. Akibat gangguan ini menyebabkan 3 paket harus tander ulang.

		Malah karena si hacker ini berulang kali mengubah dokumen penawaran yang sudah di upload di paket tersebut membuat kami terpaksa melelangkan 1 paket di LPSE Poli Teknik Negeri Lampung
T	**:**	**Lalu langkah-langkah apa saja yang sudah dilakukan saat ini untuk mengahadpi ancaman dikemudian hari nanti?**
J	:	Untuk di jaringan dan aplikasi kami menggunakan firewall hal ini standar bisanya di lakukan dalam keamanan informasi. Tapi kami juga menggunakan VPN, dimana VPN ini langsung melalui LKPP. Jadi ketika mau masuk ke dalam sistem server harus melalui akses dari LKPP. Sehingga LKPP bisa mengawasi aktifitas di SPSE Provinsi Lampung. Selain itu kami juga menggunakan server backup untuk mengantisipasi jika terjadi serangan terhadap server utama, server backup kami bisa stanby untuk menggantikan.

RIWAYAT HIDUP PENELITI

Adi Wijaya, lahir pada tanggal 18 Oktober 1990, di Desa Bergen, Kecamatan Tanjung Bintang, Kabupaten Lampung Selatan, Provinsi Lampung. Menyelesaikan pendidikan di SDN 4 Kertosari pada tahun 2003, SMPN 1 Tanjung Sari pada tahun 2006, dan SMA Assalam Tanjung Sari pada tahun 2009, Kemudian mendapat beasiswa 100% S1 Teknik Informatika di Universitas Bandar Lampung tahun 2010 dan menyelesaikan gelar sarjananya pada tahun 2014. Pada tahun 2017, peneliti mendapatkan kesempatan Beasiswa Program Pascasarjana (S2) dengan mengambil Program Studi Peperangan Asimetris, Fakultas Strategi Pertahanan, Universitas Pertahanan.

Peneliti saat ini masih aktif sebagai Pegawai Non PNS pada Bagian Pengadaan Barang dan Jasa, Sekretariat Daerah Kabupaten Tanggamus. Berikut daftar singkat riwayat pekerjaan peneliti:

No	Riwayat Pekerjaan	Jabatan	Tahun	Instansi
1	2	3	4	5
1	Pengajar	Guru Matematika	2010 s/d 2011	Smart English Course
2	Staf Magang	Verifikator	2012 s/d 2014	LPSE Universitas Bandar Lampung
3	Staf Non PNS	Pelaksana	2016 s/d Sekarang	Bagian Pengadaan Barang dan Jasa Sekretariat Daerah Kabupaten Tanggamus