LAPORAN AKHIR

KAJIAN PHYSICAL SECURITY KOTA DENPASAR

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS UDAYANA

DENGAN

DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK
KOTA DENPASAR

DENPASAR
TAHUN 2017

KATA PENGANTAR

Puji syukur Kami panjatkan kehadapan Tuhan Yang Maha Esa, karena asung kerta wara nugraha-Nya lah, kami dapat menyelesaikan laporan kegiatan yang berjudul **"Kajian Physical Security Kota Denpasar"**.

Dalam penyusunan Laporan ini, tim pengkaji banyak memperoleh petunjuk dan bimbingan dari berbagai pihak. Sehubungan dengan hal tersebut pada kesempatan ini penulis menyampaikan ucapan terima kasih kepada :

1. Kepala Dinas Komunikasi, Informatika dan Statistik Kota Denpasar
2. Kepala Bidang Smart City Dinas Komunikasi, Informatika dan Statistik Kota Denpasar
3. Staff di Dinas Komunikasi, Informatika dan Statistik Kota Denpasar yang membantu kelancaran administrasi dan kegiatan ini
4. Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Udayana
5. Seluruh Tim pada kegiatan ini.

Penulis menyadari bahwa dalam penyusunan laporan pendahuluan ini masih terdapat kekurangan yang disebabkan karena keterbatasan kemampuan dan waktu yang tersedia. Untuk itu penulis mengharapkan adanya kritik dan saran yang sifatnya membangun demi kesempurnaan pada laporan pendahuluan ini. Akhir kata semoga laporan kajian ini dapat memberikan kontribusi yang bermanfaat bagi kita semua, terutama kemajuan Kabupaten Buleleng.

Denpasar, Nopember 2017

Penulis

DAFTAR ISI

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1.1. Latar Belakang

Smart City merupakan sebuah konsep "kota cerdas" yang mana konsep tersebut dirancang untuk membantu berbagai hal kegiatan masyarakat, melakukan pengelolaan secara lebih efisien dengan tujuan meningkatkan pelayanan kepada seluruh komponen kota tersebut. Dikutip dari laman smartcityindonesia.org, sebuah kota dikatakan cerdas apabila kota tersebut mampu mengetahui seluruh keadaan kota di dalamnya, memahami segala permasalahan secara lebih mendalam, sehingga dapat dilakukan pengambilan solusi untuk segala permasalahan tersebut.

Untuk mendukung konsep "Smart City" tersebut, salah satu pendekatan yang digunakan adalah *E-governance* atau lebih dikenal dengan istilah E-gov. E-gov adalah aplikasi teknologi komunikasi dan informasi (ICT) yang memungkinkan pemberian pelayanan, pertukaran informasi, transaksi komunikasi, perpaduan program-program atau sistem-sistem dan pelayanan antara pemerintah dan masyarakat.

Agar E-gov dapat berjalan dengan baik dan dapat memberikan pelayanan prima setiap waktu, dibutuhkan infrastruktur dan sumber daya yang unggul dan memadai. Faktor terpenting dari infrastruktur dan sumber daya tersebut, salah satunya adalah faktor keamanan dari ancaman-ancaman yang mungkin. Ancaman tersebut dibagi menjadi 2 (dua) jenis, yaitu ancaman siber dan ancaman fisik. Untuk mengantisipasi segala ancaman siber, diperlukan peningkatan keamanan siber (cyber security enhancement); sementara untuk mengantisipasi ancaman fisik, perlu adanya peningkatan keamanan fisik (physical security enhancement). Terlepas dari kedua jenis ancaman tersebut, penting juga untuk meningkatkan pemahaman dan kewaspadaan terhadap keamanan sistem (security awareness) kepada setiap orang yang terkait langsung maupun tidak langsung terhadap sistem.

Peningkatan keamanan fisik dari infrastruktur dan sumber daya yang mendukung E-gov ini menjadi fokus dalam kajian ini. Berdasarkan publikasi dari SANS yang berjudul "*Physical Security and Why It Is Important*", keamanan fisik selalu menjadi topik nomor dua untuk didiskusikan setelah keamanan informasi. Menurut (Harris, 2003), keamanan fisik selalu

diabaikan karena kebanyakan organisasi lebih fokus kepada keamanan sistem berbasis teknologi. Padahal ancaman fisik jauh lebih besar efeknya dibandingkan ancaman siber.

Berdasarkan fakta tersebut kajian ini akan dilaksanakan, agar segala tindakan pencegahan dan peningkatan keamanan yang dianggap perlu dapat dilakukan. Dengan infrastruktur yang lebih kuat, diharapkan pemberian pelayanan prima oleh sistem E-gov dapat selalu diberikan kepada masyarakat, sehingga dapat mewujudkan Denpasar sebagai "kota cerdas" yang unggul.

1.2. Rumusan Masalah

Rumusan masalah yang melatar belakangi pelaksanaan kajian ini adalah bagaimana melakukan kajian keamanan fisik secara menyeluruh terhadap sistem komputer peladen (*server*) di lingkungan Pemerintah Kota Denpasar.

1.3. Tujuan

Pelaksanaan kajian keamanan fisik ini diharapkan dapat menghasilkan dokumen audit keamanan fisik sebagai dasar untuk membuat prosedur standar keamanan fisik sistem E-gov di lingkungan Pemerintah Kota Denpasar.

1.4. Urgensi

Urgensi pelaksaan kajian ini adalah peningkatan keamanan fisik yang merupakan hal penting selain keamanan siber; terutama dalam sistem yang mendukung E-gov.

1.5. Manfaat

Manfaat dari pelaksanaan kajian ini adalah untuk mendapatkan pedoman pengamanan fisik yang sesuai dengan sistem komputer peladen (*server*) di dalam sistem E-gov di lingkungan Pemerintah Kota Denpasar.

1.6. Target

Target yang disasar dalam pelaksanaan kajian ini adalah seluruh sistem yang terdapat di lingkungan komputer peladen pada Pemerintah Kota Denpasar.

1.7. Ruang Lingkup

Ruang lingkup pelaksanaan kajian ini adalah lingkungan tempat komputer peladen ditempatkan, seluruh personal yang dapat mengaksesnya dan seluruh sumberdaya lainnya yang terkait dengan komputer peladen tersebut.

1.8. Batasan

Batasan pelaksanaan kajian keamanan fisik ini akan dititikberatkan kepada 3 (tiga) aspek berikut:

1. *Access control* atau pengendalian akses.
2. *Surveillance* atau monitoring.
3. *Testing* atau pengujian.

BAB II
TINJAUAN PUSTAKA

2.1. Keamanan Fisik

Keamanan fisik bertujuan untuk merancang, menerapkan, memelihara, dan melakukan pencegahan terhadap ancaman-ancaman yang dapat terjadi pada sumber daya fisik organisasi. Pada sebuah sistem seperti E-Gov, keamanan fisik sangat mutlak diperlukan. Keamanan fisik sama pentingnya dengan keamanan logika. Pada keamanan logika, pengujian-pengujian dilakukan terhadap logika yang diterapkan pada sebuah sistem, logika ini dapat berupa algoritma, struktur data, rancangan basis data dan rancangan antar muka sistem. Sementara pada keamanan fisik, pengujian-pengujiannya dilakukan pada fisik dari sistem tersebut, misalnya perangkat keras server, kondisi server router, switch, kabel jaringan dan kondisi lingkungan sistem tersebut berada.

Menurut SANS Institute, Keamanan fisik sering menjadi pemikiran kedua dalam hal keamanan informasi. Karena keamanan fisik memiliki unsur teknis dan administratif, hal ini sering diabaikan karena kebanyakan organisasi fokus pada "penanggulangan keamanan berorientasi teknologi" (Harris, 2013) untuk mencegah serangan hacking. Hacking ke dalam sistem jaringan bukanlah satu-satunya cara agar informasi sensitif dapat dicuri atau digunakan terhadap sebuah organisasi. Keamanan fisik harus diimplementasikan dengan benar untuk mencegah penyerang mendapatkan akses fisik dan mengambil apa yang mereka inginkan. Semua *firewall*, kriptografi dan tindakan pengamanan lainnya akan sia-sia jika itu terjadi. Tantangan penerapan keamanan fisik sekarang jauh lebih bermasalah daripada dekade-dekade sebelumnya.

Laptop, drive USB, tablet, flash drive dan smartphone semuanya memiliki kemampuan untuk menyimpan data sensitif yang bisa hilang atau dicuri. Organisasi memiliki tugas menakutkan untuk mencoba melindungi data, peralatan, orang, fasilitas, sistem, dan aset perusahaan. Perusahaan bisa menghadapi hukuman perdata atau pidana karena kelalaian karena tidak menggunakan kontrol keamanan yang tepat. Tujuan keamanan fisik adalah untuk melindungi personil, informasi, peralatan, infrastruktur TI, fasilitas dan semua aset perusahaan lainnya. Strategi yang digunakan untuk melindungi aset organisasi perlu memiliki pendekatan berlapis. Lebih sulit bagi penyerang untuk mencapai tujuan mereka ketika beberapa lapisan harus

dilewati untuk mengakses sumber daya. Informasi dalam makalah ini akan membahas pentingnya keamanan fisik beserta strategi yang harus diterapkan untuk menerapkan keamanan fisik di fasilitas dengan menggunakan kontrol administratif, teknis dan fisik.

2.2. Standardisasi Keamanan Server

Untuk dapat menerapkan keamanan fisik, ada beberapa dasar yang digunakan dalam sebuah standar keamanan fisik. Standar ini dirancang oleh SANS Institute. Bagian-bagiannya antara lain:

A. Kendali Administratif

Kendali administratif adalah pengendalian keamanan untuk server yang diatur dengan regulasi-regulasi yang ada. Pengendalian ini adalah awal dari keamanan fisik, termasuk pengendalian secara teknis dan fisikal. Seperti diungkapkan oleh (Stewart, J., Chapple, M., & Gibson, D. 2012), pengendalian ini adalah titik pusat yang diaplikasikan untuk mengamankan fisikal dalam rangka melindungi sumber daya manusia, infrastruktur IT dan operasi-operasinya. Pengendalian ini dimaksudkan untuk mencegah penyerang atau memperlambat mereka.

B. Kendali Fisik

Setelah kendali secara administratif, diikuti pengendalian secara fisik. Kendali fisik ini meliputi akses fisik yang mana dapat mengontrol, memantau dan mengelola akses. Mengkategorikan bagian bangunan harus dibatasi, pribadi atau publik. Tingkat kontrol akses yang berbeda diperlukan untuk membatasi zona yang dapat masuk setiap karyawan tergantung pada peran mereka. Banyak mekanisme yang memungkinkan akses kontrol dan isolasi akses di fasilitas. Mekanisme ini dimaksudkan untuk mencegah dan mendeteksi akses dari individu yang tidak berwenang. Mekanisme ini meliputi pengeamanan perimeter, kartu identitas, pendeteksi gerakan, dan alarm untuk pengamanan lingkungan.

C. Kendali Teknis

Fokus utama kontrol teknis adalah kontrol akses karena merupakan salah satu area keamanan yang paling terganggu (Harris, 2013). Kartu pintar adalah kontrol teknis

yang memungkinkan akses fisik ke gedung atau ruang aman dan masuk dengan aman ke jaringan perusahaan dan komputer. Beberapa lapisan pertahanan dibutuhkan untuk tumpang tindih untuk melindungi dari penyerang yang mendapatkan akses langsung ke sumber daya perusahaan. Sistem deteksi intrusi adalah kontrol teknis yang penting karena mendeteksi intrusi. Deteksi adalah suatu keharusan karena memberitahukan kejadian keamanan. Kesadaran akan kejadian tersebut memungkinkan organisasi merespons dan menahan insiden tersebut. Jejak audit dan log akses harus terus dipantau. Mereka memungkinkan organisasi untuk menemukan di mana pelanggaran terjadi dan seberapa sering. Informasi ini membantu tim keamanan mengurangi kerentanan.

Kartu Token memiliki microchip dan sirkuit terpadu yang terpasang pada kartu yang memproses data. Microchip dan integrated circuit memungkinkan smart card melakukan autentikasi dua faktor. Kontrol otentikasi ini membantu mencegah penyerang atau karyawan yang tidak sah mengakses kamar yang tidak diizinkan masuk. Informasi karyawan disimpan di chip untuk membantu mengidentifikasi dan mengotentikasi orang tersebut. Autentikasi dua faktor juga melindungi komputer, server dan pusat data dari individu yang tidak berwenang. Menilai tidak akan diberikan dengan kepemilikan kartu itu sendiri. Bentuk biometrik (sesuatu yang Anda inginkan) atau PIN atau kata sandi (sesuatu yang Anda ketahui) harus dimasukkan untuk membuka kunci kartu tersebut untuk mengotentikasi pengguna.

Kartu cerdas token akses masuk dalam dua tipe, kontak dan tanpa kontak. Menghubungi kartu cerdas memiliki kontak di bagian depan kartu untuk transfer data. Saat kartu dimasukkan, jari dari perangkat membuat sambungan dengan titik kontak chip. Sambungan ke chip itu dan memungkinkan komunikasi dengan perangkat host. Kartu pintar tanpa kontak menggunakan antena yang berkomunikasi dengan gelombang elektromagnetik. Sinyal elektromagnetik memberikan kekuatan untuk kartu cerdas dan berkomunikasi dengan pembaca kartu. Kartu token sukses dianggap tidak tahan terhadap metode perusakan; Namun, kartu ini bukan bukti pembuktian. Keamanan disediakan melalui kerumitan token cerdas. Token cerdas hanya memungkinkan kartu dibaca setelah PIN dimasukkan dengan benar. Metode enkripsi mencegah orang jahat memperoleh data yang tersimpan di microchip. Kartu pintar

juga memiliki kemampuan untuk menghapus data yang tersimpan di dalamnya kartu mendeteksi gangguan. Kost adalah kelemahan teknologi smart card. Adalah mahal untuk membuat smart card dan membeli pembaca kartu. Kartu pintar pada dasarnya adalah komputer kecil dan membawa risiko yang sama. Seiring perkembangan teknologi, kapasitas penyimpanan dan kemampuan untuk memisahkan "perhitungan keamanan kritis" (Harris, 2013) di dalam kartu cerdas. Kartu pintar dapat menyimpan kunci yang digunakan dengan sistem enkripsi yang membantu keamanan. Sirkuit dan penyimpanan mandiri, ijinkan kartu untuk menggunakan algoritma enkripsi. Algoritma enkripsi memungkinkan otorisasi yang dilindungi yang dapat diterapkan di seluruh perusahaan.

Jika peralatan direlokasi tanpa persetujuan, sistem deteksi intrusi (IDSs) bisa

monitor dan memberitahukan entri yang tidak sah. IDS sangat penting untuk keamanan karena sistem dapat mengirim peringatan jika terjadi peristiwa tertentu atau jika akses dilakukan pada waktu yang tidak biasa.

Pengawal adalah bagian penting dari sistem deteksi intrusi karena mereka lebih

mudah beradaptasi dibanding aspek keamanan lainnya. Petugas keamanan bisa dipasang di satu lokasi atau berkeliling dengan berpatroli di kampus. Saat membuat putaran, penjaga bisa memastikan pintu dan jendela terkunci, dan brankas dilindungi. Pengawal mungkin bertanggung jawab untuk menonton IDS dan CCTV dan dapat bereaksi terhadap aktivitas yang mencurigakan. Mereka dapat meminta bantuan cadangan atau polisi setempat untuk membantu menangkap tersangka jika perlu.

Sistem televisi atau sistem surveilans tertutup memanfaatkan kamera dan peralatan perekaman untuk memberikan perlindungan visual. Di area yang dipantau kamera, memiliki cukup cahaya di area yang tepat sangat penting. Mungkin terlalu redup bagi kamera untuk menangkap kualitas video yang layak yang diperlukan untuk mengadili atau mengidentifikasi orang-orang yang berkepentingan tanpa cukup cahaya. Kamera bisa lensa tetap (tidak bergerak) atau lensa zoom (adjustable). Dalam memantau sesuatu yang tidak bergerak, Anda ingin menggunakan jenis lensa tetap yang tepat tergantung jarak dan lebar yang Anda monitor. Lensa tetap tersedia di sudut lebar, sempit atau lebar. Lensa zoom direkomendasikan saat melihat target yang

mungkin memerlukan tampilan yang diperbesar. Jenis kamera lainnya adalah pan, tilt, zoom camera.

Ini adalah kamera gaya kubah yang memiliki kemampuan bergerak ke segala arah sekaligus zoom in.

Kamera PTZ paling baik untuk melacak tersangka karena kamera secara otomatis mendeteksi dan mengikuti tersangka. Kamera PTZ dapat secara otomatis melacak benda bergerak melalui metode mekanis atau aplikasi. Kamera yang menggunakan aplikasi perangkat lunak memiliki kemampuan untuk mengubah target dan bisa menyaring gambar yang stasioner, menghemat bandwidth dan penyimpanan.

Perekam video digital (DVR) digunakan untuk mendukung kamera. Mereka menyimpan apa yang dilihat kamera dan dapat memutar ulang video yang sedang diputar atau untuk bukti. DVR mencakup perangkat lunak yang memungkinkan kontrol PTZ manual, yang kamera diperbesar. Mereka juga memiliki multiplexer yang terpasang sehingga mereka bisa merekam beberapa feed kamera secara bersamaan. Kamera mengalirkan data video melalui alat coax, wireless atau IP. Beberapa sistem DVR memungkinkan pengguna menggabungkannya ke jaringan mereka untuk kapasitas penyimpanan tambahan atau keperluan melihat jarak jauh. Kamera IP juga dapat terhubung ke sistem DVR berbasis komputer yang menginstal perangkat lunak pada mesin induk. Komputer ini memiliki fungsi dan kapasitas penyimpanan lebih banyak daripada DVR dan memerlukannya karena kamera IP memerlukan lebih banyak ruang penyimpanan karena video definisi tinggi.

D. Keamanan Pengguna dan Lingkungan

Keamanan fisik yang paling penting adalah melindungi kehidupan manusia. Keamanan fisik harus selalu diperhatikan secara serius di fasilitas. Mencegah cedera pada karyawan dan melindungi elemen lingkungan dasar di lokasi lokasi harus menjadi prioritas utama dalam program keamanan fisik.

Permasalahan lingkungan dasar harus dipelihara untuk menjaga keselamatan karyawan.

Ancaman kehidupan manusia dan stabilitas situs bisa menjadi akibat langsung dari bencana alam, pelepasan bahan beracun, banjir atau kebakaran. Tim aksi keamanan

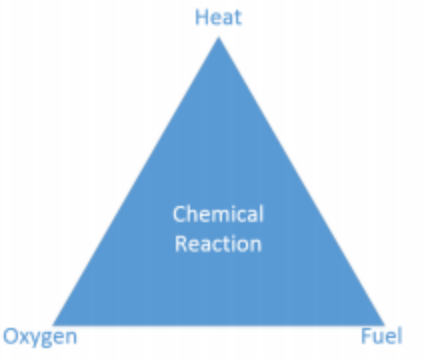
fisik harus memiliki prosedur untuk melindungi terhadap jenis peristiwa ini. Tindakan pertama yang dibutuhkan adalah memusatkan perhatian pada keselamatan manusia. Kedua, pemulihan utilitas yang diperlukan untuk operasi TI dapat dilakukan setelah semua tindakan keselamatan terpenuhi. Dalam kasus ekstrim seperti bencana alam, pedoman dan rencana harus diterapkan untuk mengatasi situasi dengan benar.

Rencana darurat pendudukan (*Occupant Emergency Plans/OEP*) adalah panduan yang membantu keselamatan karyawan setelah terjadinya bencana alam. Panduan ini menguraikan bagaimana mengurangi ancaman hidup manusia, menghindari cedera, melakukan pengaturan perjalanan, cara memantau keselamatan, mengatasi tekanan, dan mempertahankan perusakan properti jika terjadi kejadian fisik yang merusak. *OEP* hanya menangani staf dan kerusakan properti terbatas. Perencanaan kesinambungan bisnis (BCP) dan Perencanaan Pemulihan Bencana (DRP) membahas fungsi bisnis dan TI.

Mengendalikan lingkungan termasuk menjaga iklim fasilitas. Sistem pemanas, ventilasi, dan penyejuk udara (*Heating, Ventilation, and Air-Conditioning/HVAC*) harus dipantau agar orang merasa nyaman dan kelembabannya dalam kisaran yang dapat ditolerir. Komputer harus memiliki kelembaban yang konstan antara 40 dan 60 persen. Listrik statis dihasilkan bila ada sedikit kelembaban dan korosi yang diakibatkan jika ada terlalu banyak.

Asap, api, panas, dan sistem deteksi harus ada untuk melindungi karyawan dari cedera. Menjaga keamanan orang adalah tujuan keamanan fisik yang paling penting. Sistem penekan dipasang untuk membatasi kerusakan akibat asap, api, dan panas. Jika terlalu banyak penekanan diterapkan, infrastruktur dan fasilitas TI dapat rusak oleh sistem ini.

Segitiga api terdiri dari tiga elemen, Heat, oksigen, dan bahan bakar. Reaksi kimia yang berada di tengah, mewakili perubahan apa yang terjadi selama kebakaran. Gambar 2.1 di bawah menggambarkan bahwa jika Anda melepaskan salah satu dari keempat unsur tersebut, reaksi kimia, oksigen, bahan bakar dan atau panas, api dapat dihilangkan.



Gambar 2.1. Segitiga Reaksi Kimia

Kebakaran bisa datang dalam berbagai jenis. Jenis api menentukan pemadam api yang dibutuhkan untuk mengatasinya. Menggunakan alat pemadam api yang salah bisa mengintensifkan api. Misalnya, di kelas B atau kebakaran cair, air tidak bisa digunakan karena cipratan cairan dan bahan kimia biasanya mengapung di atas air. Selain itu, air bisa menyebabkan sengatan listrik saat terjadi kebakaran listrik. Fakta penting yang perlu diingat adalah bahwa alat pemadam kebakaran hanya efektif selama masa kanak-kanak kebakaran. Untuk kelas A, pembakaran api yang umum, asam soda atau air digunakan untuk menghilangkan api. Kelas B, kebakaran cair, membutuhkan karbon monoksida, pengganti halon atau halon, dan asam soda digunakan untuk menahan kebakaran ini. Kelas C, kebakaran listrik, harus mengandung pengganti karbon monoksida atau halon atau halon yang digunakan untuk menghilangkan api. Kelas D, kebakaran logam, harus memiliki penekan tenaga kering yang digunakan untuk pemindahan api.

E. Hukum dan Privasi

Organisasi harus memperhatikan keamanan karyawan dalam kebijakan keamanan. Organisasi harus mematuhi undang-undang dan peraturan yang mengatur di industri dan yurisdiksi tempat mereka berada. Perusahaan harus mempraktekkan uji kelayakan untuk melindungi kehidupan para pekerjanya. Jika uji kelayakan yang tepat mengenai keamanan fisik tidak ditegakkan oleh organisasi, tuntutan hukum perdata dan pidana dapat diajukan.

F. Informasi identitas pribadi (*Personal Identifiable Information/PII*) adalah rincian spesifik tentang orang-orang yang meliputi: nama, nomor jaminan sosial, nomor

telepon, alamat, umur, agama, dan ras. Catatan keuangan, medis dan kriminal juga dianggap informasi PII. Organisasi memiliki persyaratan hukum untuk melindungi informasi PII, dan tidak boleh dikumpulkan tanpa persetujuan atau untuk keuntungan perusahaan. *National Institute of Standards and Technology* (NIST) menguraikan persyaratan penanganan PII dalam publikasi khusus nomor 800-122, Panduan untuk Melindungi Kerahasiaan Informasi Identifikasi Pribadi (PII) (McCallister, E., Grance, T., & Scarfone, K., 2010).

BAB III
METODOLOGI

Pada kajian ini, langkah-langkah yang dilakukan dibagi menjadi 2 (dua), yaitu persiapan dan pelaksanaan. Pada tahap persiapan, dilakukan studi literatur dan penentuan bagian-bagian tempat kajian dilakukan. Kemudian pada tahap pelaksanaan, dilakukan pengambilan data dan analisis.

3.1. Persiapan Kajian

Pada tahap persiapan kajian ini, dilakukan studi literatur dengan mengumpulkan beberapa pustaka dan penelitian terkait dengan keamanan fisik.

3.2. Pelaksanaan Kajian

Kajian dilakukan dengan metode observasi lapangan dan wawancara. Waktu kegiatan dimulai dari pertengahan bulan September 2017. Adapun jadwal kegiatannya :

No	Kegiatan	September				Oktober				November			
		1	2	3	4	1	2	3	4	1	2	3	4
1	Kajian Studi Pustaka												
2	Mengidentifikasi Masalah, Peluang dan Tujuan												
3	Menentukan Syarat-Syarat Informasi												
4	Penyusunan Laporan Pendahuluan												
5	Observasi Lapangan												
	Penyebaran Kuesioner												
	Pengambilan dan Pengolahan Data												
6	Penyusunan Laporan dan Rekomendasi												

3.3. Pengolahan Data

Data yang didapatkan dari pelaksanaan kajian ini dibagi menjadi 2 (dua) jenis, yaitu:

1. Data yang berupa dokumentasi kondisi server dan lingkungan serta wawancara kepada administrator server
2. Data berupa jawaban kuesioner. Kuesioner yang berjumlah 45 butir disebarkan dan dijawab oleh responden.

Pengolahan data dokumentasi dan wawancara serta pemantauan lokasi dilakukan dengan analisis terhadap kelengkapan penunjang server. Sementara pengolahan data hasil kuesioner dari kajian ini dilakukan dengan metode statistik dasar.

3.4. Tahap Analisis

Dari hasil pengolahan data akan dilakukan analisis untuk mencari tingkat keamanan fisik, baik ruang server, lingkungan, kebijakan, maupun kewaspadaan pengguna yangterkait langsung dengan sistem.

3.5. Pembuatan Laporan

Pada tahap pembuatan laporan, akan dicantumkan seluruh langkah-langkah kajian, data yang didapatkan, analisis sampai dengan kesimpulan.

BAB IV
HASIL DAN PEMBAHASAN

Data yang didapatkan melalui 2 (dua) tahap pelaksanaan kajian ini terdiri dari bagian/unit yang memiliki komputer server yang akan dikaji, tingkat kajian yang dilakukan, data kuesioner, data hasil wawancara lisan dan dokumentasi berupa foto keadaan dari lingkungan tempat komputer server berada.

4.1. Hasil Persiapan Kajian

Pada tahapan persiapan kajian, didapatkan hasil sebagai berikut:

A. Aspek kajian
B. Bagian/unit tempat pelaksanaan kajian
C. Metode yang digunakan

4.2. Hasil Pelaksanan Kajian

Dari pelaksanaan kajian, didapatkan hasil sebagai berikut yang dipaparkan berdasarkan tempat pelaksanaan kajian.

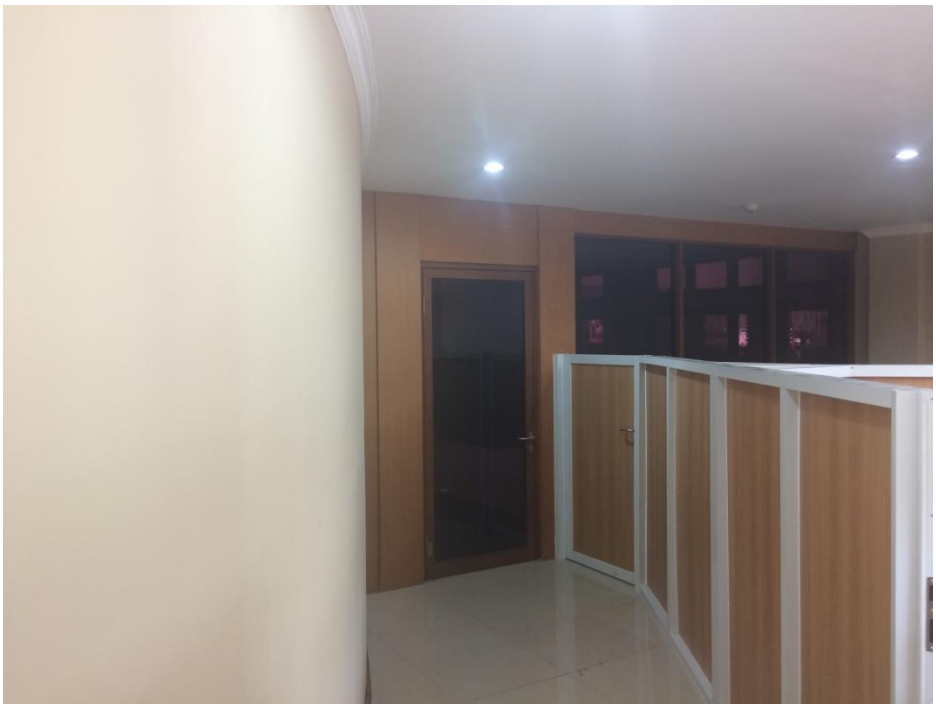
A. Dinas Komunikasi, Informasi dan Statistik

Pada dinas Komunikasi, Informasi dan Statistik, terdapat sebuah ruang server. Ruang server ini terletak di lantai 1 gedung Graha Sewaka Dharma. Berada di sebuah ruangan di belakang bagian pelayanan. Memiliki 1 jalan masuk menuju ruangan tersebut. Memiliki 1 pintu masuk ke ruangan server. Pintu masuk menggunakan akses dengan sistem penguncian manual dan tidak dijaga. Memiliki jendela yang tidak berterali dan menghadap ke luar gedung. Pada sisi yang memiliki jendela tersebut langsung berada pada sebuah akses pejalan kaki. Di sekeliling ruang server tidak terdapat kamera pengawas. Pada ruang server tidak terdapat alat pemadam kebakaran (alat pemadam api ringan/APAR). Terdapat perangkat uninterrupted power supply (UPS) untuk server yang ada di dalamnya. Tidak terdapat alat pemantau suhu dan kelembaban udara. Ruangan memiliki alat pengkondisi udara (air conditioner/AC). Dinding sekeliling ruangan berupa penyekat tipis/partisi, kecuali dinding

yang memiliki jendela menghadap ke luar gedung. Plafon terhubung dengan ruang lain dan memiliki ketinggian kurang lebih 60cm. Kabel jaringan dan kelistrikan dilewatkan plafon.

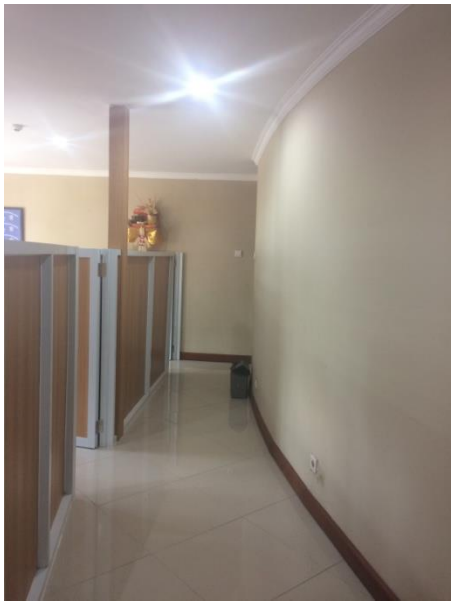
Berikut adalah hasil dokumentasi keadaan dari ruang server:

Gambar 4.2. Jalan menuju ruang server Dinas Kominfo



Gambar 4.3.Pintu masuk ruang server Dinas Kominfo

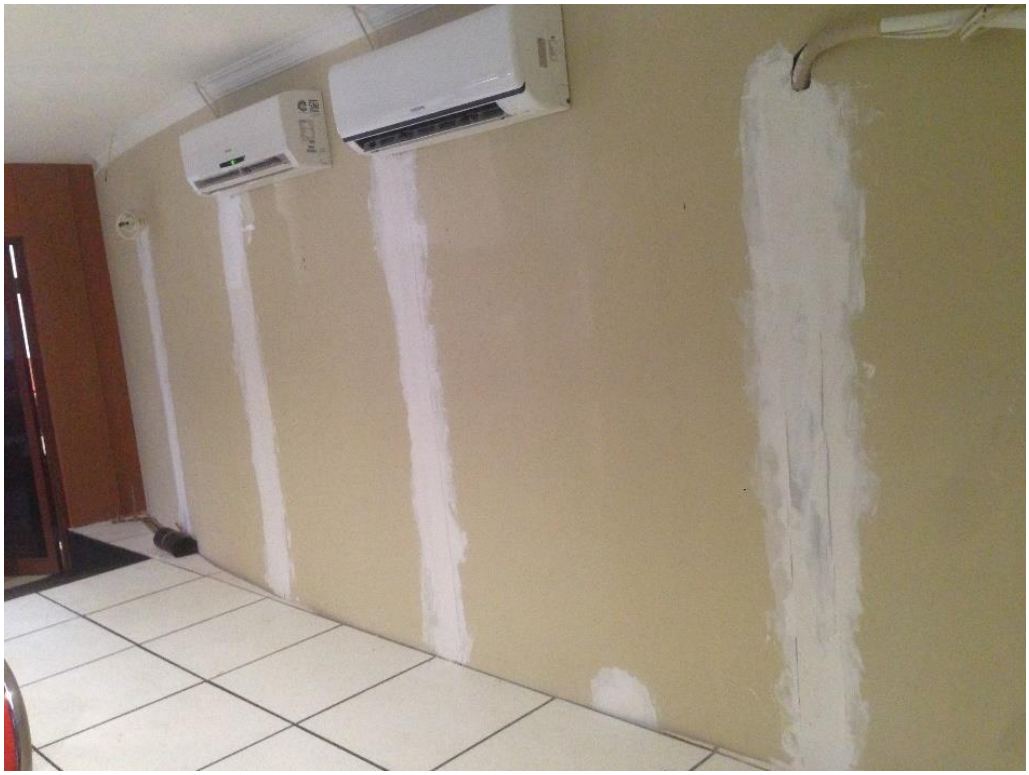
Gambar 4.4. Pintu masuk ke dalam server Dinas Kominfo



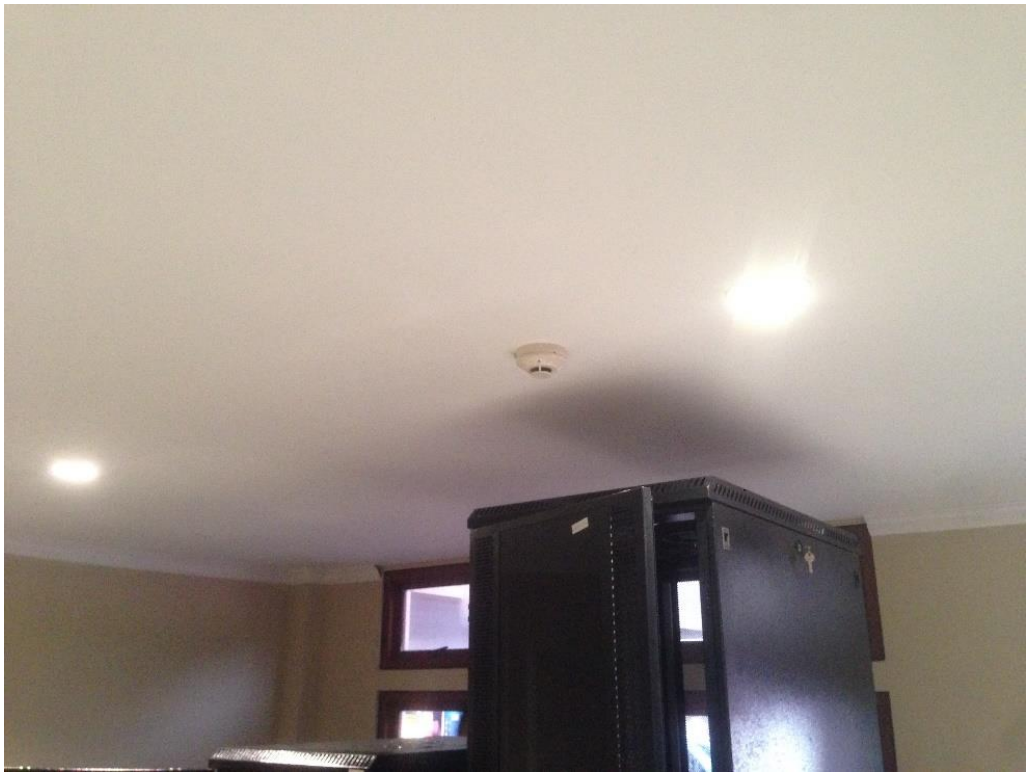
Gambar 4.5. Jalan menuju ruang server Dinas Kominfo

Gambar 4.6. Jendela yang terdapat di ruang server Dinas Kominfo

Gambar 4.7. Rak server dan jendela pada ruang server



Gambar 4.8. Keadaan dinding dan air conditioner pada ruang server



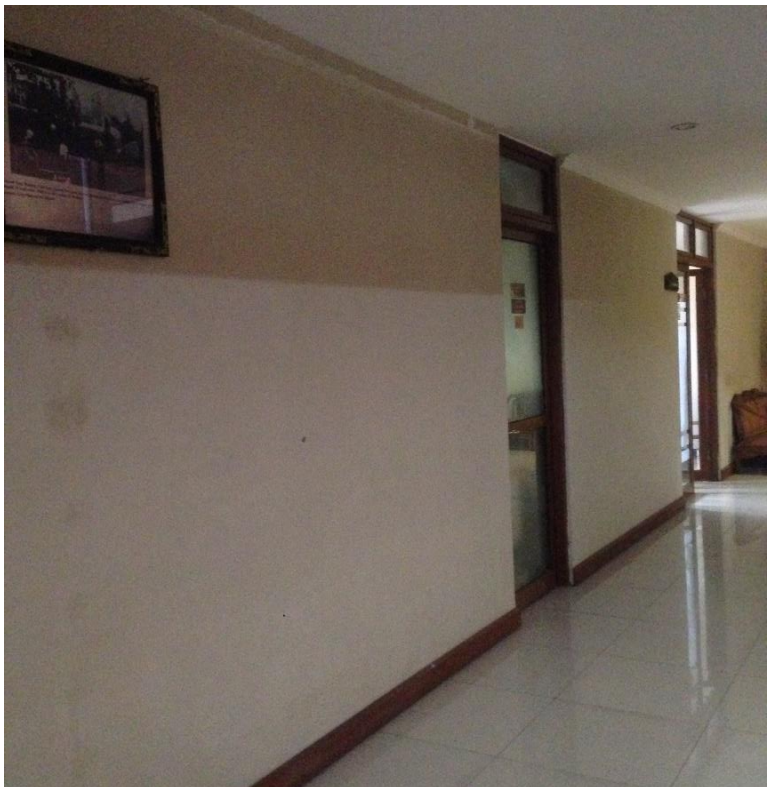
Gambar 4.9. Alat pendeteksi asap di ruang server

Gambar 4.10. Sisi luar gedung pada dinding ruang server Dinas Kominfo

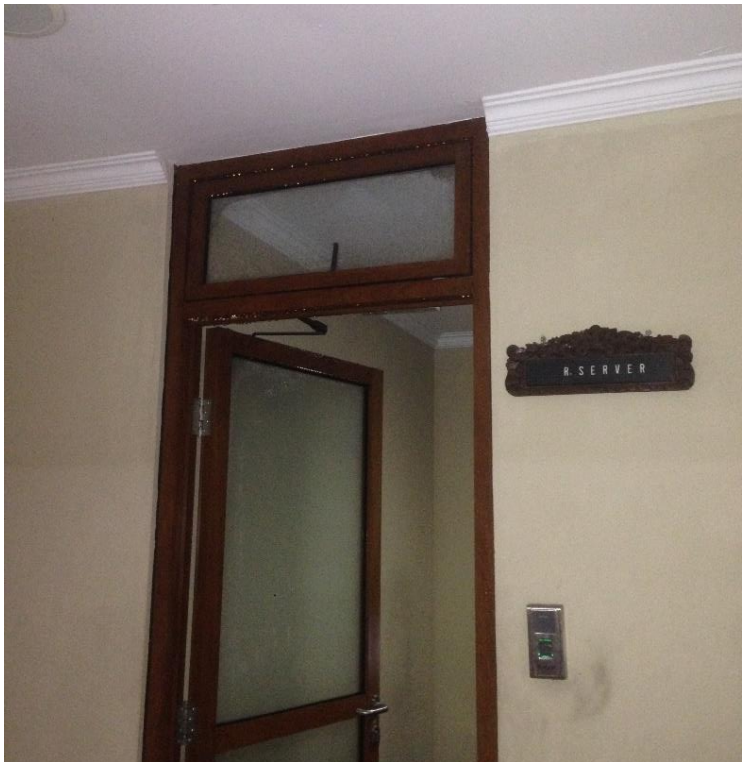
B. Dinas Kependudukan dan Catatan Sipil

Pada dinas Kependudukan dan Catatan Sipil, terdapat sebuah ruang server. Ruang server ini terletak di lantai 2 gedung Graha Sewaka Dharma. Berada di sebuah ruangan di antara 2 ruangan besar (ruang Dinas Kependudukan dan Catatan Sipil; dan ruang Dinas Keuangan). Memiliki 2 jalan masuk menuju ruangan tersebut. Memiliki 2 pintu masuk ke dalam ruang server, namun hanya 1 pintu yang difungsikan. Pintu yang lainnya terkunci dan tidak memiliki terali. Pintu masuk memiliki sistem akses biometric digital dengan menggunakan sidik jari.dan tanpa penjaga. Terdapat sebuah kamera pengawas yang berada di depan pintu masuk ke dalam ruang server. Tidak terdapat kamera pengawas di dalam ruang server. Pada ruang server tidak terdapat alat pemadam kebakaran (alat pemadam api ringan/APAR). Terdapat perangkat uninterrupted power supply (UPS) untuk server yang ada di dalamnya. Tidak terdapat alat pemantau suhu dan kelembaban udara. Ruangan memiliki alat pengkondisi udara (air conditioner/AC). Dinding sekeliling ruangan berupa penyekat tipis/partisi, kecuali dinding yang memiliki pintu masuk. Plafon terhubung dengan ruang lain dan memiliki ketinggian kurang lebih 60cm. Kabel jaringan dan kelistrikan dilewatkan plafon.

Berikut adalah hasil dokumentasi keadaan dari ruang server:



Gambar 4.11. Jalan masuk ruang server Dinas Kependudukan dan Catatan Sipil



Gambar 4.12. Pintu masuk ke ruang server Dinas Kependudukan dan Catatan Sipil

Gambar 4.13. Sistem akses biometric digital di ruang server Dinas Kependudukan dan Catatan Sipil

Gambar 4.14. Jalan masuk menuju ruang server Dinas Kependudukan dan Catatan Sipil

C. Dinas Perijinan

Pada dinas Perijinan, terdapat sebuah ruang server. Ruang server ini terletak di lantai 3 gedung Graha Sewaka Dharma. Ruang server dinas Perijinan dan Dinas Kependudukan dan Catatan Sipil berada pada kolom yang sama di gedung tersebut, namun berbeda lantai. Ruang server ini berada di sebuah ruangan di antara 2 ruangan besar. Memiliki 2

jalan masuk menuju ruangan tersebut. Memiliki 2 pintu masuk ke dalam ruang server, namun hanya 1 pintu yang difungsikan. Pintu yang lainnya terkunci dan tidak memiliki terali. Pintu masuk memiliki sistem manual.dan tanpa penjaga. Kunci diletakkan di sebuah meja dan hanya beberapa orang yang memiliki akses kunci tersebut. Tidak terdapat kamera pengawas di dalam ruang server atau di sekeliling ruang server tersebut. Pada ruang server tidak terdapat alat pemadam kebakaran (alat pemadam api ringan/APAR). Terdapat perangkat uninterrupted power supply (UPS) untuk server yang ada di dalamnya. Terdapat alat pemantau suhu berupa thermometer alcohol dan tidak terdapat alat pemantau kelembaban udara. Ruangan memiliki alat pengkondisi udara (air conditioner/AC). Dinding sekeliling ruangan berupa penyekat tipis/partisi, kecuali dinding yang memiliki pintu masuk. Plafon terhubung dengan ruang lain dan memiliki ketinggian kurang lebih 60cm. Kabel jaringan dan kelistrikan dilewatkan plafon. Terdapat sistem pengendalian inventaris ruang server, berupa kartu inventaris.

Berikut adalah hasil dokumentasi keadaan dari ruang server:

Gambar 4.15. Pintu masuk ruang server Dinas Perijinan

Gambar 4.16. Jalan menuju ruang server Dinas Perijinan

Gambar 4.17. Pintu masuk ruang server Dinas Perijinan

Gambar 4.18. Keadaan di depan pintu masuk ruang server Dinas Perijinan

Gambar 4.19. Alat pendeteksi asap di ruang server Dinas Perijinan

Gambar 4.20. Sistem kontrol inventaris ruang server Dinas Perijinan

D. Dinas Keuangan

Pada dinas Keuangan, terdapat 2 (dua) buah ruang server. Ruang server pertama terletak di gedung Walikota di jalan Gajah Mada, dan ruang server kedua berada di Gedung Dinas Keuangan di jalan Gatot Subroto IV. Pada saat dilakukan peninjauan, ruang server pertama telah disiapkan untuk dipindah ke ruang server kedua. Untuk selanjutnya ruang server yang akan difungsikan adalah ruang server yang kedua.

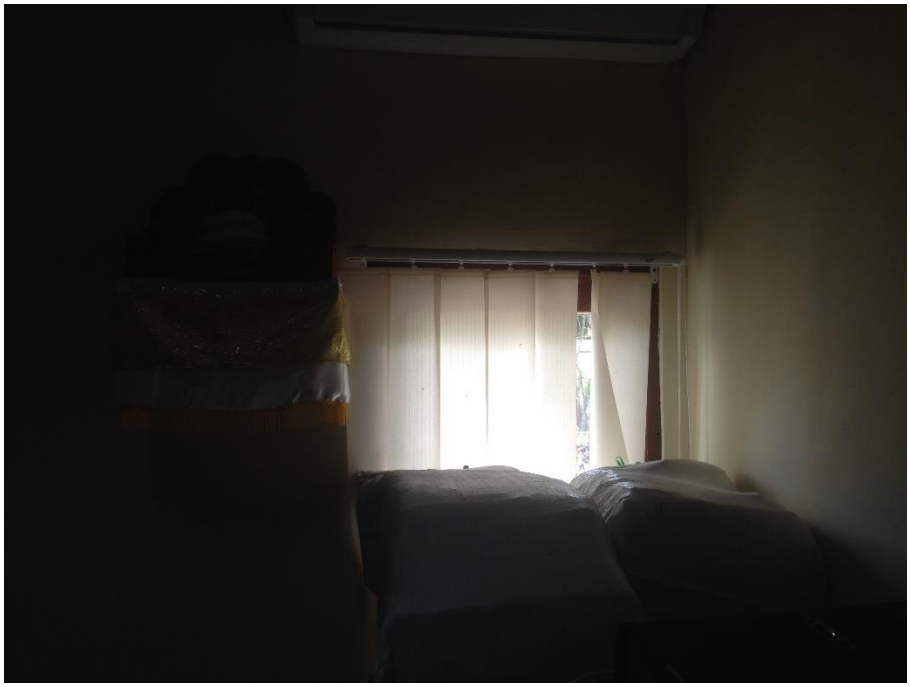
Ruang server pertama Dinas Keuangan ini, berada di sebuah ruangan kecil berpenyekat di dalam ruangan besar yang difungsikan sebagai ruang arsip. Memiliki 1 jalan masuk menuju ruangan tersebut. Memiliki 1 pintu masuk ke dalam ruang server dan 1 pintu masuk menuju ruang arsip. Pintu masuk memiliki sistem manual.dan tanpa penjaga. Kunci dibawa 2 (dua) orang yang memiliki akses ruang tersebut. Tidak terdapat kamera pengawas di dalam ruang server atau di sekeliling ruang server tersebut. Pada ruang server tidak terdapat alat pemadam kebakaran (alat pemadam api ringan/APAR). Terdapat perangkat uninterrupted power supply (UPS) untuk server yang ada di dalamnya. Tidak terdapat alat pemantau suhu dan pemantau kelembaban udara. Ruangan memiliki alat pengkondisi udara (*air conditioner*/AC). Dinding sekeliling ruangan berupa penyekat tipis/partisi, kecuali dinding yang merupakan dinding ruang arsip. Plafon

terhubung dengan ruang lain dan ketinggian tidak diketahui. Kabel jaringan dan kelistrikan dilewatkan plafon.

Ruang server kedua Dinas Keuangan yang berada di jalan Gatot Subroto masih belum difungsikan. Ruangan saat ini digunakan sebagai penyimpan arsip sementara. Dari sisi persiapan, ruangan telah disiapkan dengan baik. Memiliki sistem kelistrikan dan pengatur udara yang baik. Jendela tidak berterali menghadap ke luar gedung. Sebuah pintu akses yang memiliki sistem manual dan tanpa penjaga. Kamera pengawas terdapat di sekeliling ruang server namun tidak terdapat di dalamnya.

Berikut adalah hasil dokumentasi keadaan dari ruang server Dinas Keuangan:

Gambar 4.21. Kelistrikan pada ruang server yang disiapkan Dinas Keuangan

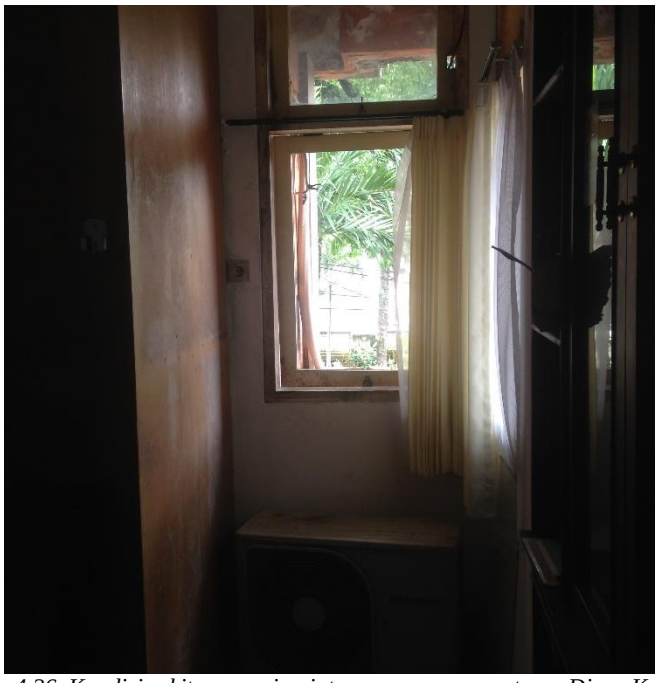


Gambar 4.22. Jendela yang terdapat pada ruang server kedua Dinas Keuangan

Gambar 4.23. Jendela ruang server Dinas Keuangan yang menghadap sisi luar gedung.

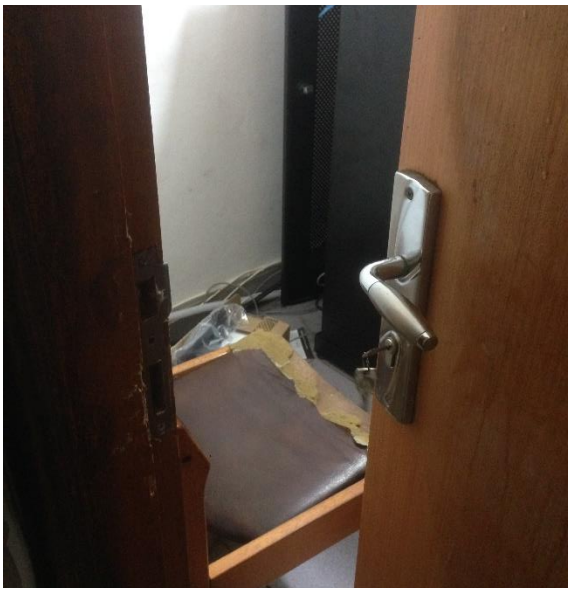
Gambar 4.24. Pintu akses masuk ke ruang server pertama Dinas Keuangan

Gambar 4.25. Plafond an dinding partisi pada ruang server pertama Dinas Keuangan

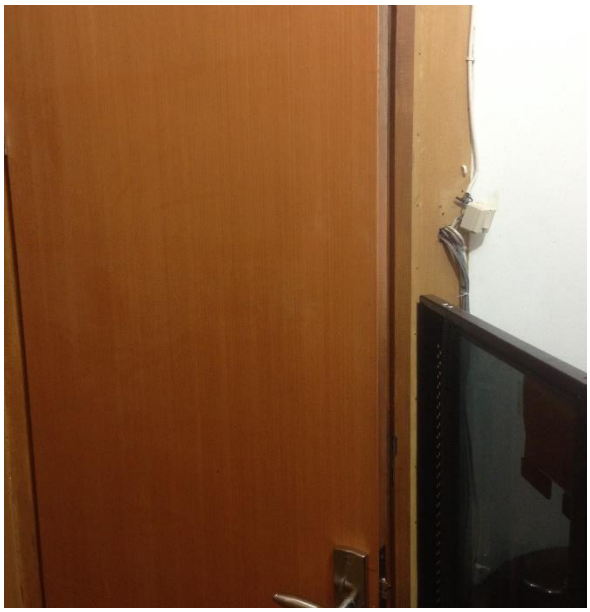


Gambar 4.26. Kondisi sekitar menuju pintu ruang server pertama Dinas Keuangan

Gambar 4.27. Pengkondisi udara di ruang server pertama Dinas Keuangan



Gambar 4.28. Akses pintu ruang server Dinas Keuangan



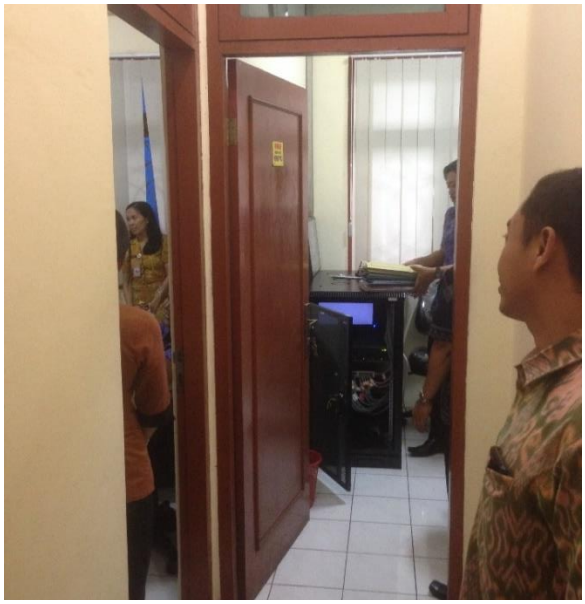
Gambar 4.29. Pintu ruang server Dinas Keuangan (tampak dari dalam ruangan)

E. Dinas Pengadaan

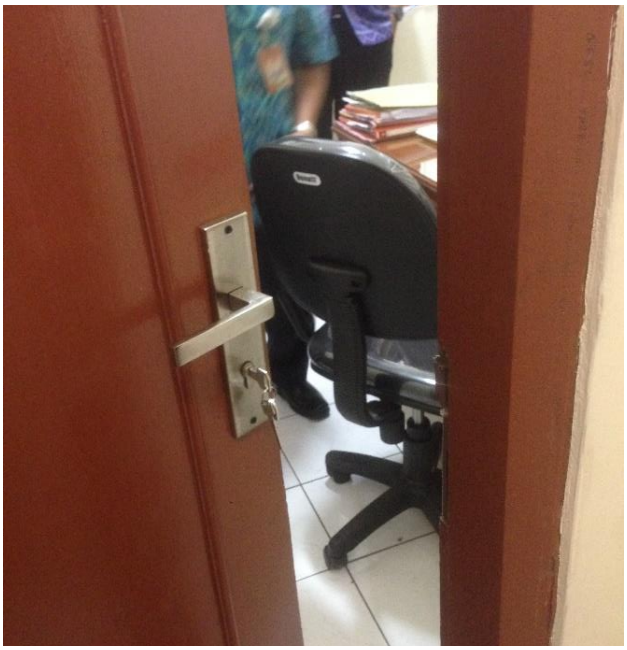
Pada dinas Pengadaan, terdapat sebuah ruang server. Ruang server ini terletak di lantai 1 gedung Dinas Pengadaan. Ruang server ini menjadi satu dengan ruang Kepala Bagian. Memiliki 1 jalan masuk menuju ruangan tersebut. Memiliki 1 pintu masuk ke dalam ruangan tersebut. Pintu masuk memiliki sistem manual.dan tanpa penjaga. Kunci ruangan dibawa oleh Kepala Bagian. Ruangan tersebut memiliki jendela pada satu sisi yang menghadap keluar gedung. Jendela tersebut dilengkapi dengan terali. Tidak terdapat

kamera pengawas di dalam ruang server atau di sekeliling ruang server tersebut. Pada ruang server tidak terdapat alat pemadam kebakaran (alat pemadam api ringan/APAR). Terdapat perangkat uninterrupted power supply (UPS) untuk server yang ada di dalamnya. Tidak terdapat alat pemantau suhu dan kelembaban udara. Ruangan memiliki alat pengkondisi udara (air conditioner/AC). Dinding sekeliling ruangan berupa penyekat/partisi dan sisi yang menghadap ke luar gedung berupa tembok beton. Plafon terhubung dengan ruang lain dan ketinggian tidak ditinjau. Kabel jaringan dan kelistrikan dilewatkan plafon.

Berikut adalah hasil dokumentasi keadaan dari ruang server:



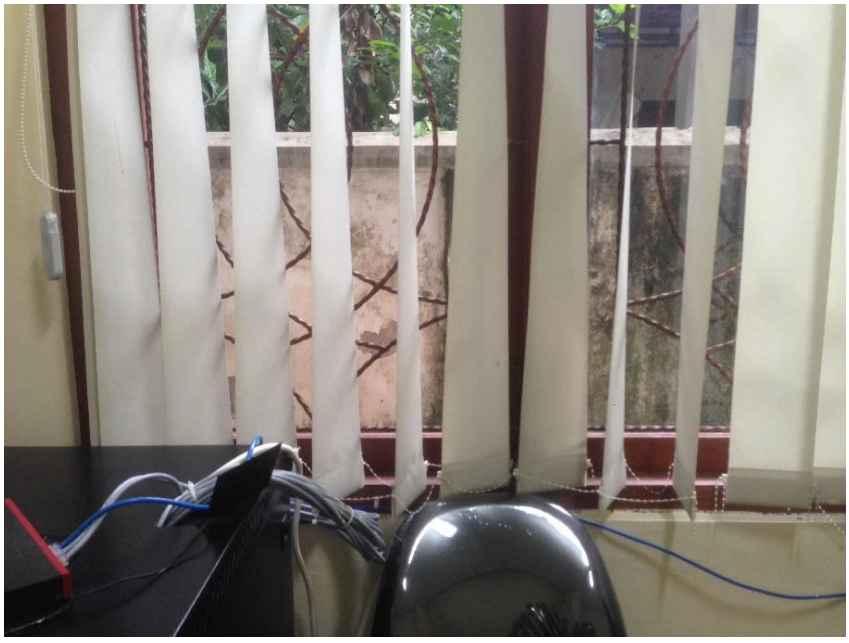
Gambar 4.30. Jalan masuk menuju ruang server yang juga merupakan ruang kerja



Gambar 4.31. Akses pintu ruang server

Gambar 4.32. Pengatur suhu ruangan berupa AC

Gambar 4.33. Peletakan rak server pada ruang server Dinas Pengadaan



Gambar 4.34. Jendela ruang server yang menghadap keluar gedung

4.3. Pengolahan Data

Selain melakukan dokumentasi dan wawancara mengenai tata kelola ruang server. Pada kajian ini juga dilakukan penyebaran kuesioner mengenai kebiasaan pengguna sistem di lingkungan dinas-dinas terkait.

Dari seluruh dinas yang dikaji, disebarkan sebanyak 45 kuesioner, dan sebanyak 42 kuesioner yang terisi. Untuk sebaran responden, dari masing-masing dinas terkait, diambil pengambil kebijakan atau pimpinan dinas, administrator sistem, operator dan pengguna sistem.

Pengolahan data kuesioner menggunakan pengolahan statistik dasar. Dari pengolahan data didapatkan hasil sebagai berikut:

1. **Kebijakan**
   a. Kebijakan untuk pengaksesan ruang server. Dari hasil kuesioner, didapatkan bahwa terdapat pembatasan untuk akses ruang server namun belum berupa atuan tertulis.
   b. Kebijakan pemantauan kinerja server. Dari hasil kuesioner didapatkan bahwa belum ada kebijakan tentang pemantauan kinerja server.
   c. Kebijakan seputar keamanan sistem: dari hasil kuesioner didapatkan bahwa keamanan sistem baik keamanan server dan keamanan perangkat jaringan belum ada.
   d. Kebijakan keamanan pengguna: dari hasil kuesioner, kebijakan tentang keamanan pengguna belum diatur dalam aturan tertulis.
2. **Sistem Pengamanan**
   a. Sistem pengamanan jaringan: sistem pengamanan jaringan seperti *firewall* telah digunakan hampir di seluruh dinas (rata-rata 2,9 dari 5). Penggunaannya sudah sesuai dengan sasaran.
   b. Sistem pemantauan jaringan: untuk pemantauan jaringan, dengan rata-rata 3,69 dari 5 dapat dikatakn bahwa sistem pemantauan yang ada cukup baik
   c. Sistem pengamanan perangkat keras: untuk pengaman perangkat server, didapatkan rata-rata 2,36 dari 5 untuk pengawasan di dalam ruang server dan 3,31 dari 5 untuk pengawasan di lingkungan sekitar ruang server, sehingga dapat dikatakan cukup. Sementara untuk keamanan perangkat PC dan laptop, masih tergolong rendah yaitu 1,74 dari 5 untuk laptop dan 2,79 dari 5 untuk PC
3. **Kewaspadaan Staf terhadap Keamanan**
   a. Kewaspadaan terhadap perangkat keras: dari kuesioner, didapatkan rata-rata 3,31 dari 5 untuk pengguna yang mengunci PC-nya ketika ditinggalkan, dan didapatkan 2,74 dari 5 untuk pengguna yang mengunci laptopnya ketika ditinggalkan.
   b. Kewaspadaan terhadap akun sistem: dari kuesioner didapatkan rata-rata 2,1 dari 5 pengguna menggunakan password/kata sandi yang sama untuk seluruh akunnya.

Sementara itu didapatkan rata-rata 2,55 dari 5 untuk pengguna yang mengubah kata sandinya secara berkala.

4.4. Analisis

A. Analisis Kondisi Fisik dan Lingkungan

Berdasarkan kondisi fisik dan lingkungan dari dinas-dinas tempat kajian ini dilakukan. Secara garis besar, ruang server yang digunakan untuk menempatkan rak server masih jauh dari standar terendah yang dicetuskan oleh SANS Institute. Terdapat satu ruang server yang digunakan berbagi dengan ruang kerja.

Selain alasan keamanan server, terdapat juga alasan kesehatan yang mendorong mengapa ruang server tidak boleh menjadi satu dengan ruang kerja. Radiasi elektromagnetik dari server dapat memengaruhi kondisi kesehatan seseorang. Sehingga disarankan untuk memisahkan server dan/atau rak server di ruangan terpisah.

Kelayakan ruang server, ditinjau dari material bangunannya, untuk standar paling rendah adalah sebuah ruangan tertutup yang bebas dari organisme (tikus, jamur, kutu, dsb), memiliki ventilasi yang baik, pengatur suhu yang baik, material dinding yang kuat (aman dari serangan fisik misalnya: hantaman benda tumpul), plafon dan lantai yang terpisah dari ruangan lainnya. Dalam hal ini, 5 ruang server yang dikaji masih belum memenuhi kelayakan standar ruang server ini. Dinding yang terbuat dari penyekat dapat meningkatkan ancaman pembobolan, baik oleh orang yang tidak bertanggung jawab atau pun organisme lain.

Beberapa jendela dan pintu yang tidak memiliki terali/pengaman ganda akan meningkatkan kerawanan ruang server. Mengingat beberapa ruang server berlokasi di tempat umum, seperti ruang server Dinas Kominfo. Dari 5 ruang server yang ada, seluruhnya tidak memiliki kamera pengawas/pemantau di dalam ruangan. Beberapa memiliki kamera pengawas di luar ruangan, dan sisanya tidak memiliki sama sekali. Hal ini dapat mengurangi tingkat keamanan dari ruang server tersebut. Jika ruang server berada di lokasi umum yang banyak orang melintas, sebaiknya perlu meningkatkan/menambah kamera pengawas/pemantau.

Selain dinding, plafon dan lantai juga memiliki peran yang penting. Seluruh lantai dari 5 ruang server terbuat dari beton dan tidak terdapat ruang yang memungkinkan orang

atau organisme lain menyelinap masuk. Sementara plafon dari seluruh server terbuat dari bahan gypsum/penyekat dan terhubung dengan ruang lain yang bersisian dengan ruang server. Hal ini dapat menurunkan tingkat keamanan, misalnya ada tikus yang berasal dari ruangan sebelah yang dapat masuk melalui plafon.

Selain ruangan, kondisi lingkungan juga memengaruhi keamanan fisik. 3 dari 5 ruang server ini terletak di lantai dasar. Ancaman yang mungkin terjadi adalah ancaman banjir. Sementara 2 server yang berada di tingkat atas (lantai 2 dan lantai 3) dapat meningkatkan keamanan dari ancaman banjir.

Dari 5 ruang server, seluruhnya tidak memiliki alat pemadam api, namun seluruhnya memiliki unit sumber daya listrik cadangan. Hanya 1 ruang server yang memiliki alat pemantau suhu yang berupa thermometer, dan 2 ruang server tidak memiliki alat pendeteksi asap.

Akses ke ruang server yang memiliki sistem pencatatan dan sudah terdigitalisasi adalah server Dinas Kependudukan dan Catatan Sipil. Pencatatan akses ini memungkinkan kita untuk melacak jika terjadi sesuatu pada server. 4 ruang server lainnya menggunakan anak kunci konvensional, yang memiliki kerawanan untuk digandakan. Selain itu, pembatasan akses masuk belum dituangkan ke dalam aturan/surat.

B. Analisis Kebijakan

Aturan mengenai akses ke dalam ruang server belum pernah dibentuk. Hal ini dapat melemahkan kendali atas ruang server. Dari 5 dinas yang dikaji, seluruhnya memiliki ruang server namun belum ada satu dinas yang membuat aturan secara tertulis mengenai cara akses di ruang server, siapa yang diperbolehkan mengakses dan job deskripsi penanggung jawab, dan prosedur operasi standar yang jelas ketika berada di ruang server.

Sementara aturan tentang keamanan dari staf belum didefinisikan, misalnya aturan mengenai penggunaan PC dan laptop kantor, prosedur operasi standar jika menggunakan laptop di luar jaringan kantor, dan mengakses jaringan kantor dari luar.

C. Analisis Pengguna

Pengguna merupakan lini akhir dari sistem yang dapat berinteraksi dengan dunia luar. Pengguna adalah bagian yang rentan disusupi oleh penyerang. Untuk mencegah hal ini, perlu ditingkatkan kesadaran pengguna dalam hal ini staf dari dinas-dinas yang dikaji. Dari data yang didapatkan melalui kuesioner, kesadaran pengguna yang meninggalkan laptop atau PC dalam keadaan terkunci harus ditingkatkan. Selain itu penggunaan aplikasi keamanan di laptop atau PC yang digunakan adalah hal mutlak.

Kesadaran penggantian kata sandi secara berkala juga perlu ditingkatkan. Penggantian kata sandi secara berkala dapat memperkecil kemungkinan untuk dibobol. Salain itu, kesadaran untuk menggunakan kata sandi yang berbeda untuk tiap akun juga perlu ditingkatkan.

4.5 Rekomendasi

Dari hasil analisis kajian yang telah dilakukan, dengan menggunakan standar keamanan fisik yang diuraikan dalam dokumen publikasi NIST yang berjudul "*Physical Security and Why It Is Important*" tahun 2016, didapatkan beberapa rekomendasi yang dapat digunakan sebagai pertimbangan. Rekomendasi tersebut adalah sebagai berikut:

A. Peningkatan Keamanan untuk Server di Dinas Komunikasi, Informasi, dan Statistik

Berikut adalah tabel yang memuat temuan di lapangan dan tindakan yang diperlukan untuk perbaikan, sesuai dengan standar keamanan fisik NIST.

No.	Kondisi Temuan	Tindakan Perbaikan
1.	Akses masuk ke ruang server tidak terjaga atau terawasi.	Menambahkan kamera pengawas di jalan masuk menuju ruang server.
2.	Akses masuk ke ruang server tidak tercatat.	Menambahkan akses pencatatan digital di pintu masuk ruang server.
3.	Akses masuk ke ruang server menggunakan pengamanan/kunci manual.	Menambahkan akses menggunakan biometrik di pintu masuk ruang server. Akses manual sebagai akses cadangan jika terjadi kegagalan sistem.
4.	Dinding ruang server berupa penyekat *calci-board* yang mudah ditembus.	Memperbaiki/mengganti dinding ruang server menjadi dinding rangkap kedap udara untuk mencegah organisme memasuki ruang server.

5.	Ruang server memiliki jendela/akses yang tidak aman.	Mengamankan jendela dengan menambahkan terali atau melakukan penutupan jendela secara permanen.
6.	Ruang server tidak memiliki pemantau keamanan.	Menambahkan alat pemantau keamana di dalam ruang server.
7.	Ruang server tidak memiliki pemantau suhu.	Menambahkan alat pemantau suhu di dalam ruang server.
8.	Ruang server tidak memiliki alat pemadam api.	Menambahkan alat pemadam api ringan di dalam ruang server.
9.	Ruang server terletak di tempat yang terhubung dengan ruang lain secara langsung.	Membatasi keterhubungan ruang server dengan ruang lain. Menambahkan kawat pengaman/terali/pengaman lainnya di sekitar ruang server, contohnya pada plafon.
10.	Regulasi tentang hak akses ruang server yang tidak tersedia.	Membuatkan aturan tentang hak akses ruang server secara tertulis.
11.	Regulasi tentang penggunaan kata sandi dan penggantian kata sandi tidak tersedia.	Membuatkan aturan tentang penggunaan dan penggantian kata sandi secara tertulis.
12.	Regulasi tentang penggunaan atau pemakaian fasilitas kantor ketika di tempat umum/luar wilayah kantor.	Membuatkan aturan tentang penggunaan atau pemakaian fasilitas kantor ketika di tempat umum/luar wilayah kantor.
13.	Sistem inventaris ruang server tidak dilakukan secara berkala.	Perlu dilakukan inventarisasi secara berkala di ruang server.

B. Peningkatan Keamanan untuk Server di Dinas Kependudukan dan Catatan Sipil

Berikut adalah tabel yang memuat temuan di lapangan dan tindakan yang diperlukan untuk perbaikan, sesuai dengan standar keamanan fisik NIST.

No.	Kondisi Temuan	Tindakan Perbaikan
1.	Akses masuk ke ruang server tidak terjaga atau terawasi.	Menambahkan kamera pengawas di jalan masuk menuju ruang server.
2.	Dinding ruang server berupa penyekat *calci-board* yang mudah ditembus.	Memperbaiki/mengganti dinding ruang server menjadi dinding rangkap kedap udara untuk mencegah organisme memasuki ruang server.
3.	Ruang server memiliki pintu/akses yang	Mengamankan pintu dengan menambahkan terali

	tidak aman.	atau melakukan penutupan pintu secara permanen.
4.	Ruang server tidak memiliki pemantau keamanan.	Menambahkan alat pemantau keamana di dalam ruang server.
5.	Ruang server tidak memiliki pemantau suhu.	Menambahkan alat pemantau suhu di dalam ruang server.
6.	Ruang server tidak memiliki alat pemadam api.	Menambahkan alat pemadam api ringan di dalam ruang server.
7.	Ruang server terletak di tempat yang terhubung dengan ruang lain secara langsung.	Membatasi keterhubungan ruang server dengan ruang lain. Menambahkan kawat pengaman/terali/pengaman lainnya di sekitar ruang server, contohnya pada plafon.
8.	Regulasi tentang hak akses ruang server yang tidak tersedia.	Membuatkan aturan tentang hak akses ruang server secara tertulis.
9.	Regulasi tentang penggunaan kata sandi dan penggantian kata sandi tidak tersedia.	Membuatkan aturan tentang penggunaan dan penggantian kata sandi secara tertulis.
10.	Regulasi tentang penggunaan atau pemakaian fasilitas kantor ketika di tempat umum/luar wilayah kantor.	Membuatkan aturan tentang penggunaan atau pemakaian fasilitas kantor ketika di tempat umum/luar wilayah kantor.
11.	Sistem inventaris ruang server tidak dilakukan secara berkala.	Perlu dilakukan inventarisasi secara berkala di ruang server.

C. Peningkatan Keamanan untuk Server di Dinas Perijinan

Berikut adalah tabel yang memuat temuan di lapangan dan tindakan yang diperlukan untuk perbaikan, sesuai dengan standar keamanan fisik NIST.

No.	**Kondisi Temuan**	**Tindakan Perbaikan**
1.	Akses masuk ke ruang server tidak terjaga atau terawasi.	Menambahkan kamera pengawas di jalan masuk menuju ruang server.
2.	Akses masuk ke ruang server tidak tercatat.	Menambahkan akses pencatatan digital di pintu masuk ruang server.
3.	Akses masuk ke ruang server menggunakan pengamanan/kunci manual.	Menambahkan akses menggunakan biometrik di pintu masuk ruang server. Akses manual sebagai akses cadangan jika terjadi kegagalan sistem.
4.	Dinding ruang server berupa penyekat	Memperbaiki/mengganti dinding ruang server

	calci-board yang mudah ditembus.	menjadi dinding rangkap kedap udara untuk mencegah organisme memasuki ruang server.
5.	Ruang server memiliki pintu/akses yang tidak aman.	Mengamankan pintu dengan menambahkan terali atau melakukan penutupan pintu secara permanen.
6.	Ruang server tidak memiliki pemantau keamanan.	Menambahkan alat pemantau keamanan di dalam ruang server.
7.	Ruang server tidak memiliki alat pemadam api.	Menambahkan alat pemadam api ringan di dalam ruang server.
8.	Ruang server terletak di tempat yang terhubung dengan ruang lain secara langsung.	Membatasi keterhubungan ruang server dengan ruang lain. Menambahkan kawat pengaman/terali/pengaman lainnya di sekitar ruang server, contohnya pada plafon.
9.	Regulasi tentang hak akses ruang server yang tidak tersedia.	Membuatkan aturan tentang hak akses ruang server secara tertulis.
10.	Regulasi tentang penggunaan kata sandi dan penggantian kata sandi tidak tersedia.	Membuatkan aturan tentang penggunaan dan penggantian kata sandi secara tertulis.
11.	Regulasi tentang penggunaan atau pemakaian fasilitas kantor ketika di tempat umum/luar wilayah kantor.	Membuatkan aturan tentang penggunaan atau pemakaian fasilitas kantor ketika di tempat umum/luar wilayah kantor.
12.	Sistem inventaris ruang server belum dilakukan secara berkala.	Perlu dilakukan inventarisasi secara berkala di ruang server.

D. Peningkatan Keamanan untuk Server di Dinas Keuangan

Berikut adalah tabel yang memuat temuan di lapangan dan tindakan yang diperlukan untuk perbaikan, sesuai dengan standar keamanan fisik NIST. Rekomendasi yang disarankan untuk server di Dinas Keuangan ini adalah untuk kondisi ruang server yang baru yang akan ditempati berikutnya.

No.	**Kondisi Temuan**	**Tindakan Perbaikan**
1.	Akses masuk ke ruang server tidak terjaga atau terawasi.	Menambahkan kamera pengawas di jalan masuk menuju ruang server.
2.	Akses masuk ke ruang server tidak tercatat.	Menambahkan akses pencatatan digital di pintu masuk ruang server.
3.	Akses masuk ke ruang server menggunakan	Menambahkan akses menggunakan biometrik di

	pengamanan/kunci manual.	pintu masuk ruang server. Akses manual sebagai akses cadangan jika terjadi kegagalan sistem.
4.	Ruang server memiliki jendela/akses yang tidak aman.	Mengamankan jendela dengan menambahkan terali atau melakukan penutupan jendela secara permanen.
5.	Ruang server tidak memiliki pemantau keamanan.	Menambahkan alat pemantau keamana di dalam ruang server.
6.	Ruang server tidak memiliki pemantau suhu.	Menambahkan alat pemantau suhu di dalam ruang server.
7.	Ruang server tidak memiliki alat pemadam api.	Menambahkan alat pemadam api ringan di dalam ruang server.
8.	Ruang server terletak di tempat yang terhubung dengan ruang lain secara langsung.	Membatasi keterhubungan ruang server dengan ruang lain. Menambahkan kawat pengaman/terali/pengaman lainnya di sekitar ruang server, contohnya pada plafon.
9.	Regulasi tentang hak akses ruang server yang tidak tersedia.	Membuatkan aturan tentang hak akses ruang server secara tertulis.
10.	Regulasi tentang penggunaan kata sandi dan penggantian kata sandi tidak tersedia.	Membuatkan aturan tentang penggunaan dan penggantian kata sandi secara tertulis.
11.	Regulasi tentang penggunaan atau pemakaian fasilitas kantor ketika di tempat umum/luar wilayah kantor.	Membuatkan aturan tentang penggunaan atau pemakaian fasilitas kantor ketika di tempat umum/luar wilayah kantor.
12.	Sistem inventaris ruang server tidak dilakukan secara berkala.	Perlu dilakukan inventarisasi secara berkala di ruang server.

E. Peningkatan Keamanan untuk Server di Dinas Pengadaan

Berikut adalah tabel yang memuat temuan di lapangan dan tindakan yang diperlukan untuk perbaikan, sesuai dengan standar keamanan fisik NIST.

No.	**Kondisi Temuan**	**Tindakan Perbaikan**
1.	Penggunaan ruang server dan ruang operasional/kerja secara bersamaan	Ruang server sebaiknya dipisah dengan ruang operasional/kerja. Selain alasan keamanan, gelombang elektromagnetik yang dihasilkan oleh server dan perangkat pendukungnya akan dapat

		mengganggu kesehatan pekerja/orang yang di sekitarnya.
2.	Akses masuk ke ruang server tidak terjaga atau terawasi.	Menambahkan kamera pengawas di jalan masuk menuju ruang server.
3.	Akses masuk ke ruang server tidak tercatat.	Menambahkan akses pencatatan digital di pintu masuk ruang server.
4.	Akses masuk ke ruang server menggunakan pengamanan/kunci manual.	Menambahkan akses menggunakan biometrik di pintu masuk ruang server. Akses manual sebagai akses cadangan jika terjadi kegagalan sistem.
5.	Dinding ruang server berupa penyekat *calci-board* yang mudah ditembus.	Memperbaiki/mengganti dinding ruang server menjadi dinding rangkap kedap udara untuk mencegah organisme memasuki ruang server.
6.	Ruang server tidak memiliki pemantau keamanan.	Menambahkan alat pemantau keamana di dalam ruang server.
7.	Ruang server tidak memiliki pemantau suhu.	Menambahkan alat pemantau suhu di dalam ruang server.
8.	Ruang server tidak memiliki alat pemadam api.	Menambahkan alat pemadam api ringan di dalam ruang server.
9.	Ruang server terletak di tempat yang terhubung dengan ruang lain secara langsung.	Membatasi keterhubungan ruang server dengan ruang lain. Menambahkan kawat pengaman/terali/pengaman lainnya di sekitar ruang server, contohnya pada plafon.
10.	Regulasi tentang hak akses ruang server yang tidak tersedia.	Membuatkan aturan tentang hak akses ruang server secara tertulis.
11.	Regulasi tentang penggunaan kata sandi dan penggantian kata sandi tidak tersedia.	Membuatkan aturan tentang penggunaan dan penggantian kata sandi secara tertulis.
12.	Regulasi tentang penggunaan atau pemakaian fasilitas kantor ketika di tempat umum/luar wilayah kantor.	Membuatkan aturan tentang penggunaan atau pemakaian fasilitas kantor ketika di tempat umum/luar wilayah kantor.
13.	Sistem inventaris ruang server tidak dilakukan secara berkala.	Perlu dilakukan inventarisasi secara berkala di ruang server.

F. Rekomendasi secara umum

Secara garis besar, setelah dilakukan kajian pada 5 (lima) dinas yang terkait dengan pengembangan E-gov di lingkungan pemerintah kota Denpasar. Didapatkan anjuran untuk perbaikan sistem keamanan fisik secara umum, yaitu:

- Aturan tentang keamanan server dan keamanan sistem yang menunjang E-gov perlu dibuat dalam tempo secepatnya. Contoh: aturan tentang pembatasan hak akses ke ruang server.
- Peningkatan ruang server dapat dilakukan dengan membuat sebuah aturan tentang standardisasi atau kebutuhan minimal untuk ruang server dan lingkungan ruang server.

Peningkatan kewaspadaan dan kesadaran staf dapat dilakukan dengan mengadakan pelatihan, workshop atau seminar di lingkungan dinas terkait. Selain itu, aturan yang menunjang kewaspadaan dan kesadaran keamanan sistem juga perlu dibentuk, misalnya peraturan tentang periode penggantian kata sandi dan penggunaan kata sandi.

BAB V
PENUTUP

5.1. Kesimpulan

Hasil analisis dari kajian ini didapatkan kesimpulan sebagai berikut

A. Belum terdapatnya kebijakan tentang keamanan server dan lingkungannya, sehingga perlu dibuat secara jelas dan tertulis dalam bentuk aturan.
B. Kondisi ruang server dan lingkungannya masih dalam kondisi rawan, sehingga perlu ditingkatkan lagi pengamanannya. Selain itu, perlengkapan penting yang menunjang kinerja server perlu ditambahkan, antara lain: alat pemantau suhu dan kelembaban server, kamera pengawas di dalam ruang server, dan alat pemadam kebakaran.
C. Kewaspadaan staf terhadap keamanan sistem terutama keamanan siber dapat dikatakan masih rendah karena masih menggunakan kata sandi yang sama untuk semua akun. Selain itu, penggantian kata sandi jarang dilakukan.
D. Secara garis besar, setelah dilakukan kajian pada 5 (lima) dinas yang terkait dengan pengembangan E-gov di lingkungan pemerintah kota Denpasar. Didapatkan anjuran untuk perbaikan sistem keamanan fisik secara umum, yaitu:
    - Aturan tentang keamanan server dan keamanan sistem yang menunjang E-gov perlu dibuat dalam tempo secepatnya. Contoh: aturan tentang pembatasan hak akses ke ruang server.
    - Peningkatan ruang server dapat dilakukan dengan membuat sebuah aturan tentang standardisasi atau kebutuhan minimal untuk ruang server dan lingkungan ruang server.

5.2. Saran

Beberapa saran yang dapat digunakan sebagai pertimbangan antara lain:

- Aturan tentang keamanan server dan keamanan sistem yang menunjang E-gov perlu dibuat dalam tempo secepatnya. Contoh: aturan tentang pembatasan hak akses ke ruang server.

- Peningkatan ruang server dapat dilakukan dengan membuat sebuah aturan tentang standardisasi ruang server dan lingkungan ruang server.
- Peningkatan kewaspadaan dan kesadaran staf dapat dilakukan dengan mengadakan pelatihan, workshop atau seminar di lingkungan dinas terkait. Selain itu, aturan yang menunjang kewaspadaan dan kesadaran keamanan sistem juga perlu dibentuk, misalnya peraturan tentang periode penggantian kata sandi dan penggunaan kata sandi.

DAFTAR PUSTAKA

Custom Electronic Design and Installation Association (CEDIA). (2008). Basic Electronics. In Electronic Systems Technical Reference Manual (1st ed., pp. 1-30). Indianapolis, IN: Author.

Harris, S. (2013). Physical and Environmental Security. In CISSP Exam Guide (6th ed., pp. 427-502). USA McGraw-Hill;

Harris, S. (2013). Access Control. In CISSP Exam Guide (6th ed., pp. 97, 98, 157- 277). USA McGraw-Hill;

Harris, S. (2013). Information Security Governance and Risk Management. In CISSP-Exam Guide (6th ed., pp. 21-141). USA McGraw-Hill;

Irwin, S. (2014, September 8). Creating a Threat Profile for your Organization. Retrieved from https://www.sans.org/reading-room/whitepapers/threats/creating-threat-profileorganization-35492

Wailgum, T. (2005, February 1). Metrics for Corporate and Physical Security Programs | CSO Online. Retrieved from http://www.csoonline.com/article/2118531/metricsbudgets/metrics-for-corporate-and-physical-security-programs.html