ANALISIS *SOFTWARE* KEAMANAN DENGAN MENGGUNAKAN INDIKATOR *GARTNER MAGIC QUADRAN* UNTUK DINAS KOMUNIKASI DAN INFORMASI JAWA TIMUR

KERJA PRAKTIK

Program Studi
S1 Sistem Informasi

Oleh :
M Syifaul Fuadi Z A
16.41010.0114

FAKULTAS TEKNOLOGI DAN INFORMATIKA
UNIVERSITAS DINAMIKA
2020

ANALISIS *SOFTWARE* KEAMANAN DENGAN MENGGUNAKAN INDIKATOR *GARTNER MAGIC QUADRAN* UNTUK DINAS KOMUNIKASI DAN INFORMASI JAWA TIMUR

Diajukan sebidang salah satu syarat untuk menyelesaikan
Program Sarjana

Disusun Oleh :

Nama : **M SYIFAUL FUADI Z A**
NIM : **164101000114**
Program : **S1 (Strata Satu)**
Jurusan : **Sistem Informasi**

FAKULTAS TEKNOLOGI DAN INFORMATIKA

UNIVERSITAS DINAMIKA

2020

LEMBAR PENGESAHAN

ANALISIS *SOFTWARE* KEAMANAN DENGAN MENGGUNAKAN INDIKATOR *GARTNER MAGIC QUADRAN* UNTUK DINAS KOMUNIKASI DAN INFORMASI JAWA TIMUR

Laporan Kerja Praktik oleh

M Syifaul Fuadi Z A.

Nim : 164101000114

Telah dipriksa, diuji dan disetujui

Surabaya, 9 Juli 2020

Disetujui:

Pembimbing	Penyelia
Ayouvi Peerna Wardhanie, S.M.B, M.M.	**Dra. Fe. Nirmala Dewi, M.M**
NIDN. 0721068904	NIP. 19650909 199403 006

Mengetahui,

Ketua Program Studi S1 Sistem Informasi

Anjik Sukmaaji

Digitally signed by Anjik Sukmaaji
Date: 2020.07.24 07:41:26 +07'00'

Dr. Anjik Sukmaaji, S.Kom., M.Eng.

NIDN. 0731057301

"Hidup itu pilihan, kamu memilih dia tapi dia memilih orang lain"

Ku persembahkan kepada

Keluargaku yang ku sayangi,

Beserta semua teman dan sahabat yang selalu

Mendukungku saat dirojo.

SURAT PERNYATAAN
PERSETUJUAN PUBLIKASI DAN KEASLIAN KARYA ILMIAH

Sebagai mahasiswa Universitas Dinamika, saya :

Nama	:	M Syifaul Fuadi Z A.
Nim	:	16410100114
Program Studi	:	S1 Sistem Informasi
Fakultas	:	Fakultas Teknologi dan Informatika
Jenis Karya	:	Laporan Kerja Praktek
Judul Karya	:	**Analisis Software Keamanan Dengan Menggunakan Indikator *Gartner Magic Quadran* Untuk Dinas Komunikasi Dan Informasi Jawa Timur**

Menyatakan dengan sesungguhnya bahwa:

1. Demi pengembangan Ilmu Pengetahuan, Teknologi dan Seni, saya menyetujui memberikan kepada Institut Bisnis dan Informatika Stikom Surabaya Hak Bebas Royalti Non-Eksklusif *(Non-Exclusive Royalti Free Right)* atas seluruh isi/ sebagian karya ilmiah saya tersebut di atas untuk disimpan, diahlimediakan dan dikelola dalam bentuk pangkalan data *(database)* untuk selanjutnya didistribusikan atau dipublikasikan demi kepentingan akademis dengan tetap mencantumkan nama saya sebagai penulis atau pencipta dan sebagai pemilik Hak Cipta
2. Karya tersebut di atas adalah karya asli saya, bukan plagiat baik sebagian maupun keseluruhan, Kutipan karya atau pendapat orang lain yang ada dalam karya ilmiah ini adalah semata hanya rujukan yang dicantumkan dalam Daftar Pustaka saya
3. Apabila dikemudian hari ditemukan dan terbukti terdapat tindakan plagiat pada karya ilmiah ini, maka saya bersedia untuk menerima pencabut terhadap gelar kerjasama yang telah diberikan kepada saya.

Demikian surat pernyataan ini saya buat dengan sebenarnya.

M Syifaul Fuadi Z A.

NIM : 16410100114

ABSTRAK

Dinas Komunikasi dan Informatika Provinsi Jawa Timur merupakan unsur pelaksana otonomi daerah, dipimpin oleh seorang kepala dinas, yang berada dibawah dan bertanggung jawab kepada Gubernur melalui Sekretaris Daerah. Dinas Komunikasi dan Informatika Provinsi Jawa Timur memiliki tugas yaitu membantu Gubernur menyiapkan bahan pelaksanaan urusan pemerintahan yang menjadi kewenangan Pemerintah Provinsi di bidang komunikasi dan informasi serta tugas pembantuan.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur mempunyai beberapa masalah dalam hal keamanan data. Berdasarkan hasil wawancara dan observasi ke empat bidang yaitu Kepala Bidang Informasi Publik, Kepala Bidang Komunikasi Publik, Kepala Bidang Aplikasi Informatika, dan Kepala Bidang Infrastruktur Teknologi Informatika dan Komunikasi bahwa kurangnya keamanan pada penyimpanan data yang sering kali disalah gunakan oleh pihak yang tidak bertanggung jawab. Data dari komputer satu ke komputer lain biasanya dipindah melalui *Flasdisk* dan juga dikirim melalui email. Dampak yang ditimbulkan dari permasalahan tersebut dapat menyebabkan kurang terjaganya data utama dari Instansi tersebut, mudahnya orang lain dalam hal mengetahui data penting yang ada di bidang lain, dan juga adanya orang yang tidak bertanggung jawab yang dapat menghapus data penting tersebut.

Berdasarkan permasalahan di atas maka penulis memberikan solusi yaitu analisis *software* keamanan dari perbandingan beberapa *software* menggunakan indikator *Magic Quadran* dengan metode wawancara dan obervasi di ke empat bidang, yang mana analisis tersebut menghasilkan sebuah rekomendasi berupa sebuah *software* keamanan Forcepoint untuk digunakan sebagai sistem keamanan data di ke empat bidang tersebut.

Kata kunci: *Software* Keamanan, *Gardner Magic Quadran*, Dinas Komunikasi dan Informatika Provinsi Jawa Timur

KATA PENGANTAR

Puji syukur kehadirat Allah Subhanahuwata'ala atas segala nikmat yang diberikan sehingga penulis dapat melaksanakan kerja praktik dan menyelesaikan pembuatan laporan dari kerja praktik ini. Laporan ini disusun berdasarkan kerja praktik dan hasil studi yang dilakukan selama lebih kurang satu bulan di Dinas Komunikasi dan Informatika Provinsi Jawa Timur.

Kerja Praktik ini menganalisa tentang sebuah *software* keamanan yang cocok untuk melindungi data penting pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur agar tidak di salah gunakan oleh pihak yang tidak bertanggung jawab. Penyelesaian laporan kerja praktik ini tidak terlepas dari bantuan berbagai pihak yang telah memberikan banyak masukan,nasihat,saran,kritik dan dukungan moral maupun materil kepada penulis. Oleh karena itu penulis menyampaikan rasa terima kasih kepada:

1. Abi dan ibuku tercinta serta keluarga besarku yang selalu mendoakan, mendukung, dan memberikan semangat di setiap langkah dan aktifitas penulis.
2. Bapak Prof. Dr. Budi Jatmiko, M.Pd. selaku rektor Universitas Dinamika yang telah mengesahkan dan memberikan kesempatan secara resmi dalam melakukan kerja praktik.
3. Bapak Dr. Anjik Sukmaaji, S.Kom., M.Eng selaku Kepala Program Studi Sistem Informasi Universitas Dinamika Surabaya
4. Ibu Ayouvi Poerna Wardhanie, S.M.B., M.M. sebagai dosen pembimbing dalam kegiatan kerja praktik yang telah memberikan izin kepada penulis untuk melakukan kerja praktik.
5. Dra. Ec. NIRMALA DEWI, M.M selaku Kepala Bidang Aptika Dinas Komunikasi dan Informatika Provinsi Jawa Timur yang telah memberikan dukungan serta kesempatan dalam melakukan kerja praktik kepada penulis.
6. Pak Aulia Bahar Pernama selaku pembimbing yang ada di instansi yang selalu membantu penulis dan menyelsaikan laporan kerja praktik ini,

Semoga Allah SWT memberikan balasan yang setimpal kepada semua pihak yang telah memberikan bantuan, bimbingan, dan nasehat dalam proses kerja praktik ini. Penulis menyadari bahwa kerja praktik ini yang dikerjakan masih banyak terdapat kekurangan, sehingga kritik yang bersifat membangun dan saran dari semua pihak sangatlah diharapkan agar aplikasi ini dapat diperbaiki menjadi lebih baik lagi dikemudian hari. Semoga laporan kerja praktik ini dapat diterima dan bermanfaat bagi penulis dan semua pihak.

Surabaya, Juli 2020

M Syifaul Fuadi Z A

DAFTAR ISI

Halaman

ABSTRAK vii

KATA PENGANTAR viii

DAFTAR ISI ix

DAFTAR GAMBAR xi

BAB I PENDAHULUAN 1

1.1 Latar Belakang 1

1.2 Rumusan Masalah 3

1.3 Batasan Masalah 3

1.4 Tujuan 4

1.5 Manfaat 4

1.6 Sistematika Penulisan 4

BAB II GAMBARAN UMUM INSTANSI 7

2.1. Gambaran Umum 7

2.2 Logo Perusahaan 7

2.4 Visi dan Misi Instansi 9

2.5 Struktur Organisasi 9

BAB III LANDASAN TEORI 11

3.1 *Data Loss Prevention (DLP)* 11

3.2 *Gartner Magic Quadran* 11

3.3 Symantec 14

3.4 Forcepoint.....14

3.5 McAfee 14

3.6 Trend Micro.....14

BAB IV DESKRIPSI PEKERJAAN 16

4.1.1. Bidang Informasi Publik 16

4.1.2. Bidang Komunikasi Publik.....17

4.1.3. Bidang Aplikasi Informatika 19

4.1.4. Bidang Infrastruktur Teknologi dan Informasi.....20

4.1.5. Hasil Analisis Wawancara.....21

4.2.1. Hasil Observasi.....26

4.2.2. Hasil Analisis Observasi.....27

4.2.3. Hasil Kesimpulan Analisis Dari Wawancara dan Observasi 27

BAB V PENUTUP.....29

5.1. Kesimpulan.....29

5.2. Saran 29

DAFTAR PUSTAKA 30

DAFTAR GAMBAR

Halaman

Gambar 2.1 Dinas Komunikasi dan Informatika Provinsi Jawa Timur 7
Gambar 2.2 Logo Provinsi Jawa Timur 8
Gambar 2.3 Struktur Organisasi Di Dinas Komunikasi dan Informatika Provinsi Jawa Timur..... 10
Gambar 3.1 Magic Quadran 2018…….....12

BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada saat ini Teknologi Informasi (TI) tidak hanya diharapkan sebagai perangkat pembantu kegiatan berorganisasi tetapi sudah merupakan bidang strategi dari suatu perusahaan untuk mencapai tujuannya (Effendy, F., & Nuqoba, B. 2016). Data merupakan input yang setelah diolah berubah bentuknya menjadi output yang disebut informasi. Keamanan dalam sistem informasi merupakan bidang yang sangat penting. Keamanan yang dimaksud adalah untuk menjaga suatu sistem dari ancaman dan gangguan dari dalam dan luar. Kesalahan tersebut sangat krusial bagi ke akurasian informasi yang dihasilkan oleh sistem. Ancaman terhadap sistem informasi yang paling berbahaya adalah kejahatan komputer yang dilakukan di dunia maya.

Sistem informasi menjadi hal yang sangat rawan terhadap kejahatan yang terjadi di dunia maya tersebut, baik melalui *Email*, *Message*, *WhastApp*, *Website* dan lain lain. Kejahatan dunia maya adalah ancaman yang berkembang di dalam masyarakat yang diakibatkan oleh tindakan seseorang yang tidak bertanggung jawab dari para individu yang mengambil keuntungan dari pemanfaatan komputer dan teknologi informasi lainnya tanpa memerhatikan pihak – pihak yang dirugikan (Effendy, F., & Nuqoba, B. 2016).

Dinas Komunikasi dan Informatika Provinsi Jawa Timur merupakan unsur pelaksana otonomi daerah, dipimpin oleh seorang kepala dinas, yang berada dibawah dan bertanggung jawab kepada Gubernur melalui Sekretaris Daerah. Dinas Komunikasi dan Informatika Provinsi Jawa Timur memiliki tugas yaitu membantu Gubernur menyiapkan bahan pelaksanaan urusan pemerintahan yang menjadi kewenangan Pemerintah Provinsi di bidang komunikasi dan informasi serta tugas pembantuan. Ada banyak bidang yang ada di Dinas Komunikasi dan Informatika Provinsi Jawa Timur, akan tetapi ada empat bidang yang memliki masalah dengan keamanan data, yaitu : Komunikasi Publik, Bidang Informasi Publik, Bidang Aplikasi Informatika, dan Bidang Infrastruktur Teknologi dan Informasi.

Bidang Komunikasi Publik adalah bidang yang bertanggung jawab atas komunikasi dan melaksanakan kebijakan pengelolaan opini publik. Bidang ini juga sering mengirimkan beberapa data penting untuk Dinas via email. Akan tetapi pernah terjadi kebobolan data via email karena tidak ada nya sistem keamanan untuk email dibidang tersebut.

Bidang Informasi Publik adalah bidang yang bertanggung jawab atas informasi – informasi yang akan disampaikan kepada publik, dan permasalahan yang terjadi adalah ada salah satu karyawan yang dengan sengaja meminta sebuah data menggunakan *Flasdisk* akan tetapi data yang diambil adalah informasi mengenai denda karyawan sedangkan denda karyawan tidak boleh sampai bocor ke beberapa karyawan.

Bidang Aplikasi Informatika adalah bidang yang bertangungg jawab atas pengembangan perangkat lunak dan juga pengoordinasian kebijakan aplikasi informatika untuk digunakan oleh Gubernur dan juga dari Dinas Komunikasi dan Informatika Provinsi Jawa Timur itu sendiri. Akan tetapi banyak juga dari bidang lain yang meminta data ke bidang ini melalui *Flashdisk*. Di bidang ini terdapat *software* keamanan Firewall, tetapi di tahun 2019 pernah terjadi kebobolan karena sistem tidak dapat mengenali IP. Ditakutkan suatu hari nanti terjadi pengambilan data penting yang tidak diketahui oleh bidang tersebut.

Bidang Infrastruktur Teknologi dan Informasi adalah bidang yang bertanggung jawab atas penyediaan infrastruktur berupa server, jaringan, hosting, dan juga kebutuhan infrastruktur lainnya. Di bidang ini juga menggunakan sistem keamanan Firewall, tetapi di tahun 2019 pernah terjadi kebobolan jaringan yang membuat orang lain bisa masuk ke email instansi. Belum adanya sistem keamanan yang lebih baik, ditakutkan terjadi penyerangan lagi terhadap jaringan yang ada di bidang ini.

Salah satu fitur pencegah yang dapat digunakan untuk keperluan sistem keamanan itu adalah DLP (*Data Loss Prevention*) yang berarti pencegahan kehilangan data/sebuah tambahan lapisan keamanan pada data perusahaan yang berisi informasi sensitif agar tidak tereskpose oleh pihak yang tidak berwenang (Ariata., 2019). *Gartner Magic Quadran* merupakan kuadran yang menunjukkan tren pasar khususnya dalam bidang IT, untuk melihat beberapa vendor *software*

keamanan dunia sesuai tren pasaran. Penulis menggunakan *Gartner Magic Quadran* sebagai indikator, karena di *Gartner Magic Quadran* memberikan informasi seputar perkembangan teknologi informasi menyangkut pemain-pemainnya dari seluruh dunia (Lintasarta, 2018).

Dari permasalahan tersebut maka penulis merekomendasikan *software* keamanan menggunakan indikator *Gartner Magic Quadran* yang memiliki beberapa vendor DLP yang telah disaring menjadi beberapa bidang. Vendor yang ada di indikator *Gartner Magic Quadran* antara lain: Forcepoint, McAfee, Trend Micro, dan Symantec. Dari hasil analisis empat vendor DLP dengan menggunakan indikator *Gartner Magic Quadran* ini, hasil analisis tersebut akan digunakan oleh Dinas Komunikasi dan Informatika Provinsi Jawa Timur untuk kebutuhan yang ada di Bidang Komunikasi Publik, Bidang Informasi Publik, Bidang Aplikasi Informatika, dan Bidang Infrastruktur Teknologi dan Informasi, dan teknik yang digunakan untuk mendapatkan hasil analisis yaitu dengan melakukan wawancara dan juga observasi di ke empat bidang tersebut.

1.2 Rumusan Masalah

Berdasarkan latar balakang yang dijabarkan diatas, maka yang menjadi rumusan masalah adalah bagaimana menganalisis *software* keamanan dengan menggunakan indikator *Gartner Magic Quadran* untuk Dinas Komunikasi dan Informatika Provinsi Jawa Timur.

1.3 Batasan Masalah

Adapun batasan masalah dalam sistem informasi keamanan ini yaitu :

a. Vendor yang akan di analisa hanya 4, yaitu : Symantec, Trend Micro, Forcepoint, dan McAfee.
b. *Software* yang dipilih nantinya hanya digunakan untuk beberapa bidang penting yang ada di Dinas Komunikasi dan Informatika Provinsi Jawa Timur.
c. Indikator yang digunakan adalah *Gartner Magic Quadrant*
d. Bidang yang di sarankan untuk menggunakan vendor ini adalah Bidang Informasi Publik, Bidang Informasi Publik, Bidang Aplikasi

Informatika, dan Bidang Infrastruktur Teknologi Informasi dan Komunikasi.

1.4 Tujuan

Berdasarkan latar belakang dan rumusan masalah, maka tujuan dari kerja praktik ini adalah menganalisis *Data Loss Prevention* menggunakan indikator *Gartner Magic Quadran* untuk menentukan penggunaan *software* keamanan pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur.

1.5 Manfaat

Diharapkan hasil dari analisis ini nanti akan memberikan manfaat yaitu :

a. Bidang Informasi Publik

   Melindungi data dari serangan pihak luar yang menyampaikan berita *hoax* yang didengar publik.

b. Bidang Komunikasi Publik

   Melindungi data dan juga informasi yang masuk kedalam email dan juga *website*.

c. Bidang Infrastruktur Teknologi Informasi dan Komunikasi

   Melindungi jaringan agar tidak mudah dilihat dan dimasuki oleh pihak dalam maupun luar.

d. Bidang Aplikasi Informatika

   Melindungi data penting perusahaan dan juga server.

e. Bagi Instansi

   Terjaganya data yang dikirim via email dari pihak dalam maupun luar, terjaganya *website* dari serangan, dan menjaga informasi rahasia yang dimiliki oleh Dinas Komunikasi dan Informatika Provinsi Jawa Timur.

1.6 Sistematika Penulisan

Untuk memberikan gambaran menyeluruh terhadap masalah yang dibahas, maka sistematika penulisan dibagi ke dalam beberapa bab yaitu :

BAB I PENDAHULUAN

Pada bab ini menjelaskan tentang latar belakang dari hal-hal yang berhubungan dengan perusahaan, rumusan masalah, batasan masalah, tujuan yang ingin dicapai, manfaat yang diperoleh dengan adanya aplikasi yang telah dibuat, serta sistematika penulisan dari proposal.

BAB II GAMBARAN UMUM INSTANSI

Bab ini menjelaskan tentang Dinas Komunikasi dan Informatika Provinsi Jawa Timur, mulai dari visi & misi perusahaan, dan stuktur organisasi.

BAB III LANDASAN TEORI

Pada bab ini membahas tentang teori-teori yang dianggap berhubungan dengan kerja praktik yang dilakukan, dimana teori-teori tersebut akan menjadi acuan untuk penyelesaian masalah.

BAB IV DESKRIPSI PEKERJAAN

Bab ini menguraikan tentang hasil analisis dari wawancara dan observasi. Pada bab ini juga membahas tentang implementasi dari analisis yang telah dilakukan di *GRANDNER MAGIC QUADRAN* pada vendor DLP.

BAB V PENUTUP

Pada bab ini dibahas mengenai kesimpulan dari analisis ini untuk sistem keamanan pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur. Terkait dengan tujuan dan permasalahan, beserta dengan saran yang bermanfaat untuk pengembangan dalam analisis yang dijalankan

BAB II
GAMBARAN UMUM INSTANSI

2.1. Gambaran Umum

Dinas Komunikasi dan Informatika Provinsi Jawa Timur merupakan unsur pelaksana otomoni daerah, dipimpin oleh seorang kepala dinas, yang berada dibawah dan bertanggung jawab kepada Gubernur melalui Sekretaris Daerah. Dinas Komunikasi dan Informatika Provinsi Jawa Timur berlokasi di JL. Ahmad Yani No. 242-244, gayungan, Kota SBY, Jawa Timur (60235). Berikut adalah gambar Dinas Komunikasi dan Informatika Provinsi Jawa Timur bisa di lihat di gambar 2.1

Gambar 2.1 Dinas Komunikasi dan Informatika Provinsi Jawa Timur

2.2 Logo Perusahaan

Pada gambar 2.2 merupakan logo dari Dinas Komunikasi dan Informatika Provinsi Jawa Timur yang memakai logo Provinsi Jawa Timur karena berada di

bawah dan bertanggung jawab kepada Gubernur Jawa Timur melalui Sekretaris Daerah seperti pada gambar 2.1..

Gambar 2.2 Logo Provinsi Jawa Timur

2.3 Tugas dan Fungsi

Adapun tugas dan fungsi dari Dinas Komunikasi dan Informatika Pemerintah Provinsi Jawa Timur akan diuraikan dalam penjelasan di bawah ini :

2.3.1 Tugas

Membantu Gubernur menyiapkan bahan pelaksanaan urusan pemerintahan yang menjadi kewenangan Pemerintahan Provinsi di bidang komunikasi dan informasi serta tugas pembantuan.

2.3.2 Fungsi

Fungsi dari Komunikasi dan Informatika Pemerintah Provinsi Jawa Timur yaitu :

1. Perumusan kebijakan di bidang komunikasi dan informasi
2. Pelaksanaan kebijakan di bidang komunikasi dan informasi
3. Pelaksanaan evaluasi dan pelaporan di bidang komunikasi dan informasi
4. Pelaksanaan administrasi dinas di bidang komunikasi dan informasi
5. Pelaksanaan fungsi lain yang diberikan oleh Gubernur terkait dengan tugas dan fungsinya.

2.4 Visi dan Misi Instansi

Visi

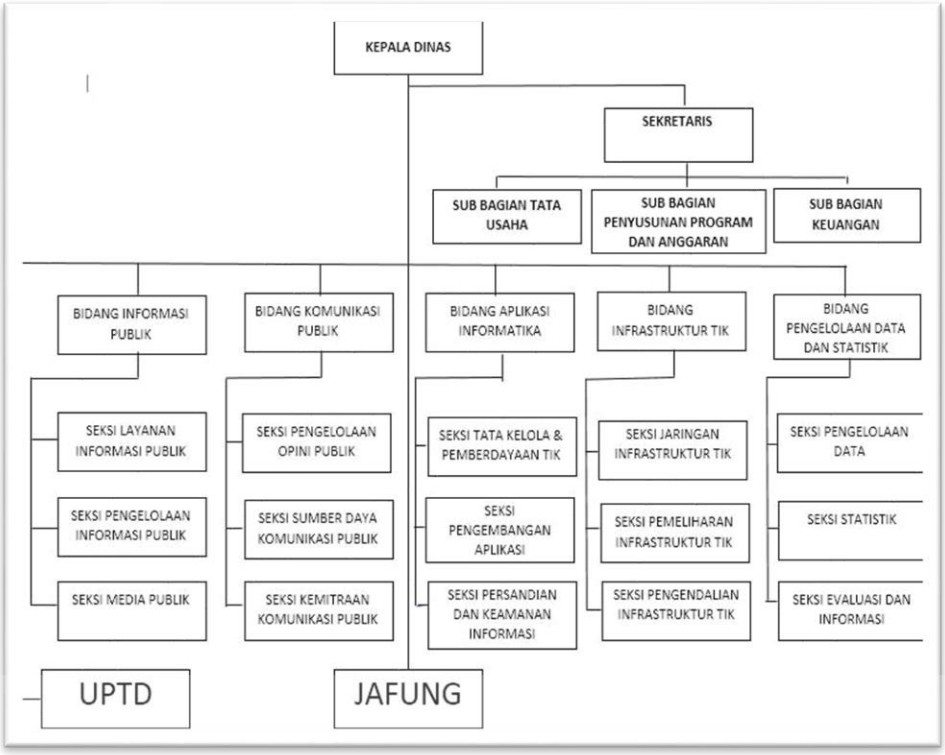
Terwujudnya Masyarakat Jawa Timur yang mandiri dan beretika melalui komunikasi dan informatika.

Misi

1. Meningkatkan kapasitas layanan informasi, memberdayakan potensi masyarakat dan kerjasama lembaga komunikasi dan informatika.
2. Meningkatkan profesionalisme aparatur bidang komunikasi dan informatika *dane-literacy* masyarakat.
3. Mengembangkan infrastruktur TIK melalui pengembangan aplikasi, muatan layanan public, standarisasi dan pemnfaatan jaringan TIK dalam rangka peningkatan pelayanan public.
4. Meningkatkan pembinaan, pengawasan dan pengendalian terhadap perusahaan penyelenggaraan jasa Pos, dan Telekomunikasi

2.5 Struktur Organisasi

Struktur organisasi pada Dinas Komunikasi dan Informatika dapat dilihat pada gambar 2.3. Berikut adalah struktur organisasi Dinas Komunikasi dan Informatika Provinsi Jawa Timur :



Gambar 2.3 Struktur Organisasi Di Dinas Komunikasi dan Informatika Provinsi Jawa Timur

BAB III
LANDASAN TEORI

3.1 *Data Loss Prevention (DLP)*

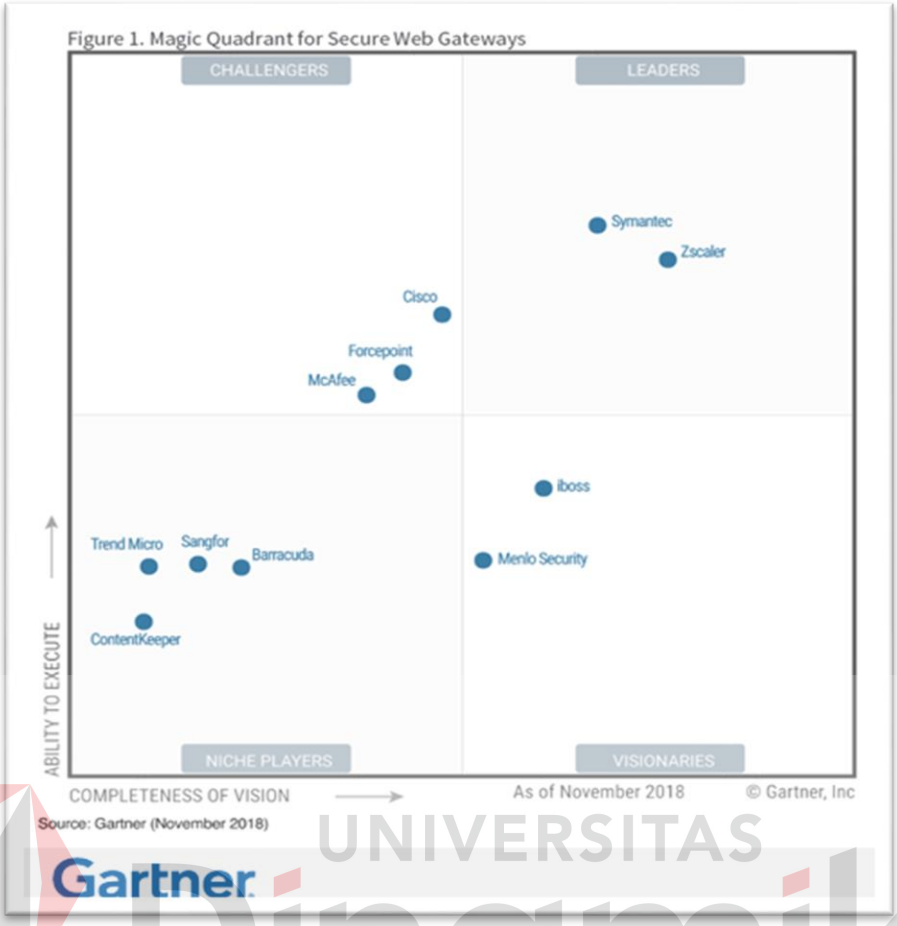
Secara umum keamanan adalah keadaan bebas dari bahaya dan ancaman, sedangkan keamanan informasi adalah perlindungan informasi dari berbagai ancaman agar menjamin kelanjutan proses bisnis, mengurangi resiko bisnis, dan meningkatkan *Return Of Investment* serta peluang bisnis (Chaeikar,etc.,2012)

DLP atau biasa yang di kenal dengan *Data Loss Prevention* menurut (Ariata, 2019) adalah sebuah fitur yang menambah lapisan keamanan pada data perusahaan yang berisi informasi sensitive agar tidak terekspos pada pihak yang tidak berwenang. Asset informasi perusahaan perlu dijaga dengan ketat untuk menjamin kelangsungan hidup perusahaan, untuk itulah beberapa yang dapat di lakukan IT manager untuk manajemen keamanan informasi diantaranya adalah :

1. Memberi enskripsi pada semua akses informasi.
2. Laporan audit.
3. Memberika sharingfile dan dokumen.
4. Manajemen perangkat mobile.
5. Verifikasi 2 langkah.

3.2 *Gartner Magic Quadran*

GartnerMagic Quadrant merupakan *Quadrant* yang menunjukkan tren pasar khususnya dalam bidang IT. Dengan adanya *Quadrant* ini, diharapkan bisa mengetahui kondisi dan juga perkembangan pasar IT yang sedang berlangsung.Pada gambar 3.1. Menunjukkan Magic Quadrant untuk *software* keamanan pada tahun 2018.



Gambar 3.1 *MagicQuadran* 2018

Nama kuadran ini diambil dari nama pencetusnya, yakni Gideon Gartner. Gideon Gartner merupakan pendiri perusahaan *Gartner* yang bermarkas di Stamford Amerika Serikat. Perusahaan ini pertama kali didirikan pada tahun 1979. Adapun tujuan dari pendirian perusahaan ini adalah untuk memberikan informasi seputar perkembangan teknologi informasi menyangkut pemain-pemainnya dari seluruh dunia.

Informasi ini sangat penting mengingat saat ini teknologi informasi semakin berkembang. Data yang mereka hasilkan diperlukan oleh banyak pihak terutama perusahaan teknologi, agensi pemerintahan, investor, dan juga perusahaan-perusahaan besar lainnya, seperti *National Rural Electric Cooperative Association* di Amerika Serikat. Dengan informasi yang mereka dapat dari kuadran Gartner ini, para pemain di dunia tersebut bisa memetakan ataupun memprediksi kondisi teknologi ke depannya.

Gartner Magic Quadrant menilai vendor melalui beberapa pembidang *rating*. Sejauh ini, ada empat *rating* yang mereka keluarkan untuk mengelompokkan status para *vendor*. Yang pertama adalah kuadran *Niche Player*. Kuadran ini merupakan *rating* terendah dalam hasil analisis *Gartner Magic Quadrant*. Para vendor yang berada di kuadran ini adalah mereka yang umumnya hanya menyediakan layanan untuk segmen tertentu secara terbatas. Selain "dihuni" oleh vendor semacam itu, kuadran ini juga biasanya ditempati oleh vendor-vendor yang masih dalam tahap menyesuaikan produk mereka untuk kepentingan pasar.

Selanjutnya, *rating* setingkat di atas *Niche Player* adalah *Visionaries*. Vendor ini lebih canggih dan besar dari pada yang ada di kuadran sebelumnya. Para vendor di kuadran *Visionaries* sudah bisa memberikan inovasi produk untuk digunakan oleh perusahaan tingkat dunia. Biasanya, vendor-vendor tersebut masih dimiliki oleh perusahaan perorangan. Namun pada umumnya, vendor-vendor tersebut asih belum mumpuni untuk menangkap pangsa pasar secara berkelanjutan.

Kemudian ada kuadran *Challengers*. Seperti namanya, vendor-vendor yang ada di sini siap menantang vendor-vendor yang ad adi kuadran dengan *rating* teratas. Para vendor di sini tak hanya bisa menunjukkan kualitasnya dalam pasar tapi juga bisa menjadi ancaman bagi para vendor yang ad adi kuadran dengan *rating* terbaik. Para vendor di kuadran *Challengers* memiliki produk yang sudah tak diragukan lagi kualitasnya dan dalam kondisi "aman" untuk terus menumbuhkan perusahaan mereka secara berkelanjutan karena memiliki sumber daya yang mumpuni.

Terakhir, ada kuadran *Leadres*. Ini merupakan *rating* tertinggi yang keluarkan oleh Gartner. Para vendor di sini tahu dengan pasti apa yang dibutuhkan oleh pasar sehingga mampu memberikan inovasi-inovasi terbaru. Mereka adalah vendor yang akan berusaha memberikan yang terbaik bagi para konsumen dengan menyediakan infrastruktur yang dapat diandalkan. Dibanding para vendor di kuadran *Challengers*, vendor di sini memiliki skala perusahaan yang jauh lebih besar dan cukup berpengaruh (Lintasarta, 2018).

3.3 Symantec

Menurut *website* (https://m.merdeka.com/symantec/profil/) Symantec adalah perusahaan asal Amerika yang memproduksi *software* pengamanan data. Perusahaan yang bermarkas di Mountain *View* California ini didirikan oleh Gary Hendrix, bersama dengan *National Science Foundation*. Perusahaan ini telah berkembang menjadi salah satu perusahaan perangkat lunak terbesar di dunia dengan lebih dari 18.500 karyawan di lebih dari 50 negara (https://www.broadcom.com/404-symantec).

3.4 Forcepoint

DLP Forcepoint ™ memungkinkan pengguna untuk menemukan dan melindungi data sensitif di Cloud. Pengguna dapat mengamankan data pribadi, kekayaan intelektual, dan memenuhi persyaratan kepatuhan dengan cepat, dengan kustom atau *out-of-the-box* (https://www.forcepoint.com/).

3.5 McAfee

McAfee, Inc.*NYSE*: *MFE* adalah perusahaan perangkat lunak antivirus dan keamanan komputer yang berpusat di Santa Clara, California. Beberapa produknya adalah McAfee *VirusScan*, McAfee *SpamKiller*, *IntruShield*, *Entercept*, *dan Foundstone*. Didirikan pada 1987 sebagai McAfee *Associates*, dinamai menurut pendiri John McAfee, mereka kemudian bergabung dengan *Network General* dan membentuk *NetworkAssociates* pada 1997. Pada 2004 mereka kembali menggunakan nama McAfee. Salah satu perusahaan yang dibeli McAfee adalah *Trusted Information Systems*, pencipta *Firewall Toolkit*.

Produk yang diberikan dari McAfee adalah Email and *Web Security, Data Protection, Security-as-a-Service (SaaS), Mobile Security, Network Security, Risk and Compliance, System Security, Virtualization Security* (https://www.mcafee.com/en-us/index.html)

3.6 Trend Micro

Trend Micro didirikan oleh Steve Chang, Jenny Chang, dan Eva Chen pada tahun 1988 untuk mengembangkan perangkat lunak antivirus. Namun, mereka tidak

berhenti begitu saja. Selama tiga dekade terakhir, Trend Micro telah menjadi pemimpin pasar dalam keamanan *cloud* gabungan, pertahanan jaringan, keamanan usaha kecil, dan keamanan *endpoint*.

Infrastruktur TI terus berubah, perilaku pengguna menjadi kian berisiko, dan ancaman terus berkembang. Trend Micro senantiasa berinovasi agar selalu selangkah di depan pergerakan kejahatan siber. Pendiri Trend Micro telah menentukan standar, budaya, dan jalan Trend Micro menuju inovasi – membentuk tim karyawan unggulan yang bekerja bersama demi membantu menjadikan dunia terhubung dengan masyarakat dan menjadikan tempat yang lebih aman untuk melakukan pertukaran informasi digital.

Selama hampir 30 tahun, kegigihan visi Trend Micro telah menjadikan dunia tempat yang lebih aman untuk melakukan pertukaran informasi digital. Keamanan adalah fokus utama Trend Micro dan Trend Micro membuktikannya. Semangat visi tunggal ini telah mengilhami inovasi Trend Micro untuk terus mengimbangi pergerakan kejahatan siber, sekalipun di tengah lanskap TI yang terus berubah, perilaku pengguna yang kian berisiko, dan ancaman yang senantiasa berkembang.

Kedalaman pengalaman Trend Micro tetap tidak tertandingi. Dari *endpoint* ke jaringan dan menuju *cloud*, Trend Micro siap melindungi Anda dengan pertahanan ancaman terhubung yang diakui oleh analis, pelanggan, dan tokoh industri dalam berbagai bidang (https://www.trendmicro.com/in_id/business.html)

BAB IV
DESKRIPSI PEKERJAAN

Berikut ini merupakan pengumpulan data menggunakan teknik observasi dan wawancara. Hasil wawancara dan observasi berikut ini didapatkan dengan beberapa pertanyaan dan observasi langsung di masing – masing bidang dan juga memberikan penjelasan tentang empat vendor DLP yaitu: Symantec, Forcepoint, McAfee, dan Trend Micro. Penulis juga menjelaskan fitur, kelebihan dan kekurangan dari ke empat vendor tersebut.

4.1. Metode Wawancara

Untuk mengumpulkan data di bidang Dinas Komunikasi dan Informatika Provinsi Jawa Timur, peneliti melakukan wawancara secara terstruktur kepada beberapa bidang yang ada di Dinas Komunikasi dan Informatika Provinsi Jawa Timur yaitu Kepala Bidang Informasi Publik, Kepala Bidang Komunikasi Publik, Kepala Bidang Aplikasi Informatika, dan Kepala Bidang Infrastruktur Teknologi Informatika dan Komunikasi. Berikut rangkuman hasil dari wawancara berdasarkan pertanyaan peneliti.

4.1.1. Bidang Informasi Publik

Pada tabel 1 berikut ini adalah hasil dari wawancara yang di lakukan kepada kepala bidang Bidang Informasi Publik beserta solusi untuk memecahkan masalah yang terjadi di bidang Informasi Publik.

Tabel 1. Hasil Wawancara Bidang Informasi Publik

No	Pertanyaan	Jawaban	Narasumber
1	Bagaimana cara mengambil data dari luar? Apakah melalui media *Email* atau yang lainnya ?	Melalui *Email* dan juga link. Untuk *Email* jarang digunakan	Edi Supaji, SH, MM (Kepala Bidang)

No	Pertanyaan	Jawaban	Narasumber
2	Informasi seperti apa yang di bagikan kepada publik?	Informasi seputar yang ada di Jawa Timur**,** Informasi Gubernur, dan acara acara acara penting.	
3	Apakah bidang ini pernah menerima Email dari pihak luar?	Sering, tapi kebanyakan biasanya melalui surat	
4	Apakah di bidang ini memerlukan sebuah keamanan untuk menjaga data dari pihak – pihak yang mengambil data penting tanpa sepengetahuan kepala bidang ?	Sangat perlu	
5	Keamanan yang di sarankan ada empat, yaitu: Symantec, *McAfee, Forcepoint, dan Trend Micro.* Dari 4 *Software* keamanan tersebut apa pilihan anda ? dan kenapa memerlukan *software* tersebut ?	*Software* keamanan yang kami pilih adalah Forcepoint, karena Forcepoint sendiri memiliki fitur yang lengkap untuk dipakai di bidang ini. Forcepoint juga sangat berguna dalam hal mengamankan data data penting kami, tidak hanya itu fitur di Forcepoint juga sangat mudah untuk di pahami, karena saya pribadi pernah menggunakan Forcepoint.	

4.1.2. Bidang Komunikasi Publik

Pada tabel 2 berikut ini adalah hasil dari wawancara yang di lakukan kepada kepala Bidang Komunikasi Publik beserta solusi untuk memecahkan masalah yang terjadi di bidang Komunikasi Publik.

Tabel 2. Hasil Wawancara dengan Bidang Komunikasi Publik

No	Pertanyaan	Jawaban	Narasumber
1	Apakah ada kaitannya dengan pengiriman data melalui email instansi ?	Ada, tapi pengiriman email melalui instansi jarang digunakan dan biasanya di gunakan untuk mengirim undangan melalui Gubernur dan Dinas	Danu Ardhiarso, SSTP (Kepala Bidang)
2	Bagaimana cara mengambil data dari bidang bidang lain?	Biasanya pihak luar di berikan *link* untuk undangan, Kalau internal menggunakan (*Dropbox*), Dan WhatsApp.	
3	Apakah di bidang ini memerlukan sebuah keamanan untuk menjaga data dari pihak – pihak yang mengambil data penting tanpa sepengetahuan kepala bidang ?	Sangat perlu	
4	Keamanan yang di sarankan ada 4, yaitu : Symantec, *McAfee, Forcepoint, dan Trend Micro.* Dari 4 *Software* keamanan tersebut apa pilihan anda ?dan kenapa memerlukan *software* tersebut ?	Untuk keamanan sendiri kita memilih Forcepoint, karena fiturnya yang mudah di pahami dan juga mudahnya dalam memakai fitur – fitur tersebut. Yang jelas dari bidang ini sangat butuh keamanan, karena kita sering juga mengambil data melalui *Flashdisk* dan itu merupakan sebuah ancaman ketika data yang di *copy* ke dalam *Flashdisk* merupakan	

No	Pertanyaan	Jawaban	Narasumber
		data penting yang tidak kita ketahui	

4.1.3. Bidang Aplikasi Informatika

Pada tabel 3 berikut ini adalah hasil dari wawancara yang di lakukan kepada kepala Bidang Komunikasi Publik beserta solusi untuk memecahkan masalah yang terjadi di bidang Aplikasi Informatika.

Tabel 3. Hasil Wawancara pada Bidang Aplikasi Informatika

No	Pertanyaan	Jawaban	Narasumber
1	Keamanan apa saja yang di kendalikan oleh bidang aplikasi informatika ?	Email server, *Hosting* (Kominfo.Jatimprov.id), Keamanan aplikasi = *Finger* absen, *Big* Data, *ISO* (Data data yang di amankan),Pergub (Peraturan pembuatan aplikasi), Rencana induk *TIK* (5 tahun sekali).	Devan Astiko (Perwakilan di Bidang Aplikasi Informatika)
2	Bagaimana cara mengambil data dari bidang bidang lain yang ada di instansi ?	Kalau di *internal* memakai jaringan *LAN*, Kalau dari bidang lain menggunakan *WhatsApp*, dan *Flasdisk*, Kalau data penting langsung cetak	
3	Apakah ada system keamanan untuk melindungi data dari luar ataupun dalam ?	Firewall	
4	Bagaimana cara mengirimkan data *server* ke *developer* program ?	Pakai *LAN*	

No	Pertanyaan	Jawaban	Narasumber
5	Bagaimana sistem penyimpanan *server* pada bidang ini ? apakah bidang lain boleh melihat server ?	Hanya bidang tertentu yang boleh melihat server yaitu: a. Kepala bidang b. SeksiBidangTerkait c. Kepala Dinas	
6	Apakah di bidang ini memerlukan sebuah keamanan untuk menjaga data dari pihak – pihak yang mengambil data penting tanpa sepengetahuan kepala bidang ?	Sangat perlu	
7	Keamanan yang di sarankan ada empat, yaitu : Symantec, *McAfee, Forcepoint, dan Trend Micro.* Dari 4 *Software* keamanan tersebut apa pilihan anda ?dan kenapa memerlukan *software* tersebut ?	Dari kami memilih Forcepoint, yak arena sesuai dengan fungsi dan juga kegunaan	

4.1.4. Bidang Infrastruktur Teknologi dan Informasi

Pada tabel 4 berikut ini adalah hasil dari wawancara yang di lakukan kepada kepala IT Bidang Komunikasi Publik beserta solusi untuk memecahkan masalah yang terjadi di bidang Bidang Infrastruktur Teknologi dan Informasi.

Tabel 4. Hasil Wawancara pada Bidang Infrastruktur Teknologi dan Informasi

No	Pertanyaan	Jawaban	Narasumber
1	Bagaimana cara mengambil data dari bidang lain ?	Email, *WhastApp* untuk bidang dalam , dan juga memakai IP untuk antar dinas.	Ir. Arif Lukman Hakin, MM (Kepala bidang Infrastruktur

No	Pertanyaan	Jawaban	Narasumber
2	Apakah ada sistem keamanan untuk melindungi jaringan dari serangan-serangan pihak luar ?	Ada, nama sistem keamanannya adalah Firewall yang memakai (DMZ), (IPS),(IDS) sistem keamanan Firewall pernah di bobol oleh IP yang belum pernah di kenali oleh sistemnya	Teknologi dan Informasi)
3	Apakah di bidang ini memerlukan sebuah keamanan untuk menjaga data dari pihak – pihak yang mengambil data penting tanpa sepengetahuan kepala bidang ?	Sangat Butuh, karena ditakutkan suatu hari nanti ada orang yang tidak bertanggung jawab yang mengambil data penting	
4	Keamanan yang di sarankan ada 4, yaitu : Symantec, *McAfee, Forcepoint, dan Trend Micro.* Dari 4 *Software* keamanan tersebut apa pilihan anda ?dan kenapa memerlukan *software* tersebut ?	Forcepoint, karena selain untuk jaga jaga nanti ketika mau kebobolan, dibidang ini banyak data penting yang tidak boleh orang luar ada yang tau	

4.1.5. Hasil Analisis Wawancara

Berikut adalah hasil analisis dari wawancara beserta solusi yang penulis berikan kepada ke empat bidang yang ada di Dinas Komunikasi dan Informatika Provinsi Jawa Timur. Hasil dapat dilihat pada tabel 5.

Tabel 5. Hasil Analisis Wawancara

No	Permasalahan	Sebab-akibat	Solusi
Bidang Bidang Informasi Publik			
1	Masih Menggunakan Email, dan juga terbiasa pakai *Link* untuk membagikan file data	Email pernah diretas, dan juga server pernah di bobol	Dengan adanya fitur keamanan email dan juga keamanan server yang ada di Forcepoint akan sangat memudahkan dalam hal mengamankan data penting di email dan juga tidak akan terjadinya server yang dibobol
Bidang Komunikasi Publik			
1.	Pengiriman data di bidang ini menggunakan *email*, akan tetapi email instansi biasanya digunakan untuk mengirim hal yang urgent ke gubernur dan juga kantor dinas.	Tanpa adanya keamanan yang jelas, ditakutkan ketika mengirim data dari email instansi ke bidang dinas terkait dapat menyebabkan kebobolan.	Untuk mencegah terjadinya kebobolan data disuatu hari nanti dengan menggunakan email instansi maka perlu sebuah *software* keamanan Forcepoint karena dapat mengetahui ID siapa yang masuk ke email dan juga memiliki hak akses tersendiri ketika ingin membuka email tersebut, jadi sangat susah untuk membobol karena adanya keamanan dari Forcepoint
2.	Untuk mengirim berkas di internal instansi biasanya	Tanpa adanya keamanan data ketika mengirim file melalui Dropbox atau	Dengan menggunakan Forcepoint, keamanan untuk cloud dan juga di

No	Permasalahan	Sebab-akibat	Solusi
	menggunakan (*Dropbox*), *WhastApp* dan juga terkadang memakai *Flasdisk*	menggunakan *Flasdisk* ketika memindah file, ditakutkan akan terjadinya pengambilan data penting di Dropbox dan *Flashdisk*	*Flasdisk* sekalipun bisa terjaga dengan aman. Harus ada izin sebelum file yang ada di *Flashdisk* dibuka atau pindahkan
Bidang Bidang Aplikasi Informatika			
1	Untuk pengiriman data di internal bidang menggunakan LAN, tapi untuk diluar bidang menggunakan *WhatsApp* dan *Flashdisk*	Di Bidang ini sudah ada keamanannya yaitu Firewall, akan tetapi kelemahan dari Firewall sendiri adalah tidak bisa membaca IP yang belum dikenal oleh sistem Firewall. Tanpa adanya keamanan data yang memungkinkan ketika mengirim file melalui LAN atau menggunakan *Flasdisk* ketika memindah file, ditakutkan akan terjadinya pengambilan data penting di LAN dan *Flashdisk*	Dengan menggunakan Forcepoint, keamanan untuk Cloud dan juga di *Flasdisk* sekalipun bisa terjaga dengan aman. Harus ada izin sebelum file yang ada di *Flashdisk* dibuka atau pindahkan
Bidang Infrastruktur Teknologi Informatika dan Komunikasi			
1	Dibidang ini untuk mengirim file di internal menggunakan email dan *WhatsApp* dan untuk pengiriman antar dinas atau *external* menggunakan IP	Dibidang ini pernah terjadi kebobolan data melalui *email* dan juga server, padahal sudah ada keamanan seperti Firewall, akan tetapi Firewall tidak dapat mengenali IP yang belum pernah Firewall identifikasi, karena ditakutkan ada kebobolan	Dengan menggunakan Forcepoint, keamanan untuk email akan sangat terjaga dan terjamin, karena ketika dibobol oleh orang yang tidak dikenal Forcepoint akan membaca orang tak dikenal itu dan akan meminta hak akses ke

No	Permasalahan	Sebab-akibat	Solusi
		lagi, maka bidang ini membutuhkan tambahan sebuah *software* untuk mengamankan data penting perusahaan	pemilik email untuk menerima atau menolak

Dari hasil wawancara yang telah dilakukan dengan empat bidang penting yang ada di Dinas Komunikasi dan Informatika Provinsi Jawa Timur, bahwa data yang mereka kirim rata – rata menggunakan *Flashdisk*, Email, dan juga *Link* yang ada di *WhatsApp*. Data yang *Loss* tersebut karena belum adanya keamanan data yang menjaga data mereka dari orang yang tidak bertanggung jawab. Bahkan ada dua bidang yaitu di bidang Aplikasi Informatika dan bidang Infrastruktur Teknologi Informasi dan Komunikasi yang memiliki keamanan sendiri berupa Firewall, akan tetapi pernah kebobolan karena Firewall mereka tidak bisa membaca IP yang belum pernah dikenali oleh sistem. Dari pilihan empat vendor yang sudah dijelaskan oleh peneliti, hasilnya adalah ke empat bidang memilih *Software* Forcepoint untuk bidang mereka. Alasan empat bidang memilih Forcepoint karena Forcepoint memiliki fitur yang lengkap dan juga mudah digunakan. Akan tetapi dari sisi harga, Forcepoint termasuk ke dalam kategori yang relatif mahal, namun ke empat bidang yang telah penulis wawancara lebih memprioritaskan Forcepoint guna menjaga data yang penting di setiap bidangnya agar data nya tidak kebobolan.

Adapaun kelebihan dari *Software* Forcepoint tersebut adalah :

1. *Forcepoint* berkomitment untuk memberikan pelindungan keamanan terhadap permasalahan yang terjadi di sebuah perusahaan, dengan keunggulan keunggalan yang banyak.
2. Strategi dari *Forcepoint* itu sendiri adalah untuk memblokir situs web tertentu yang dirasa kurang aman , memeriksa lalu lintas jaringan, mem*filter* email, dan *controlling* terhadap file *sensitive* yang dapat dengan mudah di akses.
3. Produk yang ditawarkan oleh *Forcepoint* itu sendiri terbilang banyak, diantara nya adalah :

a. Keamanan *Cloud* : yaitu menjaga/mengamankan Akses *Cloud*, mencegah akun yang ingin menyusup, dan juga mengamankan akses seluler ke aplikasi *Cloud*.

b. Keamanan *Web* : yaitu menjaga keamanan *website* yang memiliki kemanjuran 52% lebih baik dari pada pesaing lainnya

c. *Filter web – URL* : Di filter web ini sendiri, Forcepoint dapa mengumpulkan dan menganalisis hingga 5 miliar insiden tiap hari (lebih dari 155 negara), yang menghasilkan analisis ancaman terbaru untuk solusi Forcepoint hingga 3,2 pembaruan perdetik.

d. Keamanan jaringan : Menghindari seseorang yang ingin menyerang ke dalam jaringan, mengamankan seluruh jaringan dipusat data perusahaan, dan juga kantor cabang.

e. Keamanan ancaman data dan orang dalam : Keamanan ini membantu memahami perilaku yang mencurigakan dan motivasi membantu melindungi data dan IP dari tindakan jahat.

f. Keamanan Lintas domain : yang berguna untuk misi keamanan nasional badan pemerintah *global* bergantung pada akses *Cross Domain* dan solusi transfer untuk berbagi informasi yang cepat dan aman sambil memastikan data sensitif dan perlindungan jaringan yang kuat.

g. Keamanan *email* : Menjaga *email* dari orang2 dalam yang mencoba mengirimkan data penting perusahaan keluar, atau mencegah adanya *email* yang membahayakan perusahaan.

Disamping itu Forcepoint juga memiliki kekurangan yaitu :

a. Kurangnya iklan publikasi untuk informasi produk, karena kebanyakan masyarakat indonesia masih belum paham dengan cara kerja ataupun mekanisme dari produk - produk yang ada di Forcepoint itu sendiri.

b. Kurangnya informasi produk yang lebih detail sehingga susah untuk mengenali produk dan memilih apakah produk ini cocok untuk perusahaan atau tidak.

4.2. Metode Observasi

Untuk mengumpulkan data, peneliti juga melakukan observasi untuk mencari informasi tentang kegiatan yang berlangsung untuk kemudian dijadikan objek kajian penelitian. Berikut hasil dari observasi yang dilakukan.

4.2.1. Hasil Observasi

A. Bidang Informasi Publik

Data yang diperoleh dari lapangan saat melakukan observasi di bidang Bidang Informasi Publik yakni: Pengambilan data yang dilakukan dibidang ini dengan menerima dan mengirim data melalui Email dan *Link* yang dibagikan melalui Via *WhatsApp.* Terkadang beberapa karyawan meminta data ke bidang lain melalui *Flashdisk* begitu juga bidang lain ketika meminta data ke bidang ini. Kegiatan meminda data ini di lakukan setiap hari dan sudah menjadi rutinitas tanpa adanya *software* keamanan yang mengamankan data penting mereka.

B. Bidang Komunikasi Publik

Data yang diperoleh dari lapangan saat melakukan observasi di bidang Bidang Komuikasi Publik yakni: Untuk pengiriman data bidang ini sangat jarang menggunakan Email, bidang ini menggunakan email hanya untuk mengirim undangan ke Gubernur dan Dinas. Dan beberapa karyawan ketika memindai data menggunakan *Flashdisk* karena dinilai lebih efisien. Akan tetapi belum adanya *software* keamanan ketika mencolokkan *Flashdisk* membuat kurang amannya pengambilan data tersebut. Untuk pihak luar sendiri menggunakan *Link*.

C. Bidang Aplikasi Informatika

Data yang diperoleh dari lapangan saat melakukan observasi di bidang Bidang Aplikasi Informatika yakni: Di bidang ini mereka mengendalikan beberapa keamanan yaitu keamanan Email, Server, *Big Data*, ISO, Peraturan Gubernur, dan rencana induk TIK. Untuk mengirim data mereka biasanya menggunakan jaringan LAN di *internal* mereka, dan untuk ke bidang lain mereka menggunakan *Flashdisk* dan *Link* yang

dibagikan melalui *WhatsApp.* Ketika ada seseorang yang ingin membobol email mereka, maka dengan intesif Firewall mereka akan mendeteksi IP yang masuk, tetapi jika IP tidak di kenali oleh sistem maka sistem dengan mudah kebobolan.

D. Bidang Infrastruktur Teknologi Informatika dan Komunikasi

Data yang diperoleh dari lapangan saat melakukan observasi di bidang Bidang Infrastruktur Teknologi Informatika dan Komunikasi yakni: Bidang ini dalam mengambil mengambil data di internal melalui *WhatsApp* dan untuk antar dinas menggunakan IP. Dibidang ini untuk data keamananya memakai keamanan firewall seperti bidang Aplikasi Informatika. Akan tetapi pernah kebobolan juga karena IP yang belum pernah di kenali oleh sistem.

4.2.2. Hasil Analisis Observasi

Berdasarkan hasil pengamatan yang dilakukan, dari empat bidang yang diobservasi ada dua bidang yang tidak menggunakan keamanan seperti Firewall. Pemindahan file dari bidang satu ke bidang lain yang masih menggunakan *Flashdisk* membuat kurang amannya data yang dipindah bahkan transaksi data menggunakan *Flashdisk* ini pernah membuat *Loss* data penting yang ada di bidang tersebut. Seperti informasi tentang denda karyawan, gaji yang dipotong, dan juga email yang terbobol.

4.2.3. Hasil Kesimpulan Analisis Dari Wawancara dan Observasi

Hasil kesimpulan wawancara berdasarkan dari beberapa masalah yang penulis observasi dan gali melalui wawancara dan pengamatan langsung, terdapat beberapa masalah yang terjadi disetiap bidang, dari keempat permasalahan diatas mayoritas permasalahannya ada di kehilangan data, oleh sebab itu solusi yang tepat untuk permasalahan kehilangan data disemua bidang tersebut dengan menggunakan aplikasi *software* keamanan Forcepoint karena keamanan lintas *Domain* yang dimana sangat

berguna di bidang informasi public, agar informasi yang dipublikasikan di *website* aman. Dibidang bidang aplikasi informatika *Forcepoint* sangat berguna, karena bisa menjaga data keamanan seperti *server* umum, keamanan jaringan, keamanan data dari beberapa orang yang mengambil data dari flashdisk. Kelebihan – kelebihan yang dimiliki *Forcepoint* sangat cocok untuk digunakan untuk Dinas Komunikasi dan Informatika Provinsi Jawa Timur.

BAB V
PENUTUP

5.1. Kesimpulan

Kesimpulan yang dapat diperoleh dari analisa diatas adalah sebagai berikut: Berdasarkan permintaan penyelia untuk melakukan analisis keamanan pada beberapa *software* yang masuk kategori *Gartner Magic Quadran*. Dari kategori tersebut penulis mengambil beberapa *software* yang ada di dalamnya di antaranya adalah: Symantec, *Trend Micro*, *Forcepoint*, *McAfee* dan sesuai dengan keinginan serta kebutuhan dari penyelia. Akhirnya penulis menyimpulkan bahwa *software* Forcepoint cocok untuk kantor Dinas Komunikasi dan Informatika Jawa Timur.

Dari hasil analisis yang sudah ditemukan bahwa penulis merekomendasikan untuk menggunakan vendor Forcepoint, karena fitur – fitur yang ada di *software* tersebut memenuhi *standart* kebutuhan yang ada di Dinas Komunikasi dan Informatika Provinsi Jawa Timur. Dari hasil wawancara banyak sekali kecocokan fitur yang ada di Forcepoint untuk memenuhi keamanan pada bidang – bidang yang ada di Dinas Komunikasi dan Informatika Provinsi Jawa Timur.

5.2. Saran

Saran yang dapat diberikan untuk pengembangan Analisis *Software* Keamanan Dengan Menggunakan Indikator *Gartner Magic Quadran* Untuk Dinas Komunikasi dan Informasi Jawa Timur sebagai berikut :

1. Untuk bidang nya sebisa mungkin di perluas lagi untuk dianalisis agar keamanan yang ada pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur lebih banyak
2. Sebisa mungkin untuk harga di jelaskan lagi.
3. Untuk wawancara harus ada tanda tangan dari narasumber.

DAFTAR PUSTAKA

Adi, L., Akbar, R. J., & Khotimah, W. N. (2017). Platform E-Learning untuk Pembelajaran Pemrograman Web Menggunakan Konsep Progressive Web Apps. *JURNAL TEKNIK ITS Vol. 6*, A579.

Ariata. (2019, January 23). *Apa Itu Data Loss Prevention? Pengertian Data Loss Prevention Serta Kelebihan dan Kekurangannya*. Retrieved August 08, 2019, from Hostinger: https://blog.eikontechnology.com/data-loss-prevention-tingkatkan-sistem-manajemen-keamanan-informasi/

Aziz, A., & Tampati, T. (2015). Analisis Web Server untuk Pengembangan Hosting Server Institusi: Pembandingan Kinerja Web Server Apache dengan Nginx. *Analisis Web Server untuk Pengembangan Hosting Server Institusi: Pembandingan Kinerja Web Server Apache dengan Nginx*, 13.

Billy. (2016, June 4). *Membuat Website Header dengan Bootstrap Carousel*. Retrieved from codepolitan: https://www.codepolitan.com/membuat-website-header-bootstrap-carousel

Effendy, F., & Nuqoba, B. (2016). PENERAPAN FRAMEWORK BOOTSRAP DALAM PEMBANGUNAN SISTEM INFORMASI PENGANGKATAN DAN PENJADWALAN PEGAWAI (STUDI KASUS:RUMAH SAKIT BERSALIN BUAH DELIMA SIDOARJO). *Jurnal Informatika Mulawarman Vol. 11*, 9 - 10.

Kecil, L. (2015, Mei 5). *Makna Sebuah Senyuman*. Retrieved from lentera kecil: https://lenterakecil.com/makna-sebuah-senyuman/

Kurniawan, A., & Areni, I. S. (2017). Implementasi Progressive Web Application pada Sistem Monitoring Keluhan Sampah Kota Makassar. *Jurnal JPE, Vol.21,*, 34 - 38.

Lavarino, D., & Yustanti, W. (2016). RANCANG BANGUN E – VOTING BERBASIS WEBSITE DI UNIVERSITAS NEGERI SURABAYA. *Jurnal Manajemen Informatika. Volume 6*, 73 - 74.

Nurlif, A., Kusumadewi2, S., & Kariyam. (2014). ANALISIS PENGARUH USER INTERFACE TERHADAP KEMUDAHAN PENGGUNAAN SISTEM PENDUKUNG KEPUTUSAN SEORANG DOKTER . *Prosiding SNATIF Ke-1*, 333 - 334.

Web, J. (2016, August 23). *6 Kelebihan ReactJS dan Alasan Menggunakan ReactJS Untuk Membuat Aplikasi Web*. Retrieved June 4, 2019, from www.jurnalweb.com

Yasha. (2018, August 09). *Pentingnya User Experience*. Retrieved from dewaweb: https://www.dewaweb.com/blog/user-experience/

https://blog.lintasarta.net/article/apa-itu-gartner-quadrant/