Nama : **Rian Fauza Dinata**

Nim : **312210083**

Kelas : **TI.22.A2**

Matkul : **Analisa Kebutuhan Sistem**

---

1. Identifikasi Permasalahan Dan Latar Belakang Kebutuhan Sistem

Deskripsi Permasalahan:

Terdapat beberapa permasalahan dalam sistem keamanan jaringan saat ini yang perlu diatasi:

- **Risiko Keamanan:** Sistem saat ini rentan terhadap ancaman luar yang dapat mengakibatkan pencurian data atau gangguan layanan.
- **Keterbatasan Monitoring:** Monitoring jaringan yang kurang efektif dalam mendeteksi dan mencegah serangan siber atau aktivitas mencurigakan.
- **Kebijakan Keamanan yang Kurang Jelas:** Tidak ada kebijakan keamanan jaringan yang jelas dan terdokumentasi dengan baik.

Dampak Permasalahan:

- Potensi kebocoran informasi sensitif.
- Gangguan pada layanan yang dapat mengganggu produktivitas.
- Potensi kerugian finansial akibat serangan atau pelanggaran keamanan.

Latar Belakang:

Organisasi ABC, sebuah perusahaan teknologi layanan finansial, menghadapi peningkatan ancaman keamanan siber terkait serangan malware, phishing, dan kebocoran data. Untuk mengatasi hal ini, perusahaan perlu meningkatkan sistem keamanan jaringan dan memastikan kepatuhan terhadap regulasi industri. Tujuan perubahan sistem adalah untuk meningkatkan keamanan data pelanggan, memenuhi standar keamanan, dan memperkuat kepercayaan pelanggan. Manajemen perubahan sistem diperlukan untuk mengelola implementasi perubahan dengan efisien, mengingat keterbatasan sumber daya perusahaan. Dengan pemahaman latar belakang ini, Organisasi ABC dapat merencanakan strategi perubahan yang tepat untuk meningkatkan keamanan dan kinerja keseluruhan perusahaan.

Kuesioner Keamanan Jaringan

Bagian 1: Informasi Demografis

1. **Nama:**

2. **Departemen:**

3. **Jabatan:**

4. **Lama bekerja di perusahaan:**

Bagian 2: Persepsi dan Pengalaman

5. Seberapa sering Anda menggunakan sistem jaringan perusahaan?

- Setiap hari
- Beberapa kali seminggu
- Beberapa kali sebulan
- Jarang

6. Bagaimana Anda menilai tingkat keamanan jaringan saat ini?

- Sangat aman
- Aman
- Cukup aman
- Tidak aman
- Sangat tidak aman

7. Pernahkah Anda mengalami masalah keamanan jaringan (misalnya, serangan malware, phishing) di tempat kerja?

- Ya
- Tidak

8. Jika ya, seberapa sering masalah tersebut terjadi?

- Setiap bulan
- Beberapa kali setahun
- Setahun sekali
- Kurang dari setahun sekali

9. Seberapa puas Anda dengan respons dan dukungan IT terhadap masalah keamanan jaringan?

- Sangat puas
- Puas
- Cukup puas
- Tidak puas
- Sangat tidak puas

Bagian 3: Kebutuhan dan Rekomendasi

10. Fitur keamanan apa yang menurut Anda paling penting untuk ditingkatkan?

- Firewall
- Antivirus/Antimalware
- Sistem Deteksi Intrusi (IDS/IPS)
- Enkripsi data
- Manajemen akses pengguna
- Pemantauan keamanan secara real-time

11. Apakah Anda merasa memerlukan pelatihan tambahan tentang keamanan jaringan?

- Ya
- Tidak

12. Seberapa penting Anda merasa perlu adanya sistem monitoring keamanan real-time?

- Sangat penting
- Penting
- Cukup penting
- Tidak penting
- Sangat tidak penting

13. Adakah saran atau rekomendasi lain yang ingin Anda berikan terkait peningkatan keamanan jaringan perusahaan?

- [Open-ended response]

Hasil Kuesioner

Jumlah Responden: 50 orang

Bagian 1: Informasi Demografis

• **Nama:** [Dirahasiakan]

• **Departemen:** IT, Keuangan, Pemasaran, dll.

• **Jabatan:** Staf, Manajer, Supervisor, dll.

• **Lama bekerja di perusahaan:** Rata-rata 5 tahun

Bagian 2: Persepsi dan Pengalaman

Frekuensi penggunaan sistem jaringan perusahaan:

- Setiap hari: 70%
- Beberapa kali seminggu: 20%
- Beberapa kali sebulan: 7%
- Jarang: 3%

Penilaian tingkat keamanan jaringan saat ini:

- Sangat aman: 10%
- Aman: 40%
- Cukup aman: 35%
- Tidak aman: 10%
- Sangat tidak aman: 5%

Pengalaman masalah keamanan jaringan:

- Ya: 60%
- Tidak: 40%

Frekuensi masalah keamanan:

- Setiap bulan: 20%
- Beberapa kali setahun: 25%
- Setahun sekali: 10%
- Kurang dari setahun sekali: 5%

Kepuasan terhadap respons IT:

- Sangat puas: 15%
- Puas: 35%
- Cukup puas: 30%
- Tidak puas: 15%
- Sangat tidak puas: 5%

Bagian 3: Kebutuhan dan Rekomendasi

Fitur keamanan yang perlu ditingkatkan:

- Firewall: 50%
- Antivirus/Antimalware: 60%
- IDS/IPS: 40%
- Enkripsi data: 45%
- Manajemen akses pengguna: 30%
- Pemantauan keamanan secara real-time: 70%

Kebutuhan pelatihan tambahan:

- Ya: 80%
- Tidak: 20%

Pentingnya sistem monitoring keamanan real-time:

- Sangat penting: 55%
- Penting: 30%
- Cukup penting: 10%
- Tidak penting: 5%
- Sangat tidak penting: 0%

Saran atau rekomendasi lain:

- "Perlu peningkatan enkripsi data dan autentikasi multi-faktor."
- "Adakan pelatihan berkala tentang ancaman keamanan terbaru."
- "Tingkatkan dukungan IT dalam respons terhadap insiden keamanan."

Wawancara Keamanan Jaringan

Pewawancara: [Nama Pewawancara]

Wawancara dengan: [Nama Responden]

Jabatan: [Jabatan Responden]

Departemen: [Departemen Responden]

Tanggal: [Tanggal Wawancara]

Pertanyaan Wawancara:

1. Bagaimana Anda menilai keamanan jaringan perusahaan saat ini? Apakah Anda merasa data dan informasi terlindungi dengan baik?

2. Apakah Anda pernah mengalami atau mengetahui insiden keamanan jaringan (seperti serangan malware, kebocoran data) di perusahaan ini? Jika ya, bisakah Anda menceritakan pengalaman tersebut?

3. Fitur keamanan apa yang menurut Anda paling penting untuk ditingkatkan dalam sistem jaringan kita? Mengapa?

4. Seberapa puas Anda dengan dukungan yang diberikan oleh tim IT terkait masalah keamanan jaringan? Apa yang bisa ditingkatkan?

5. Apakah Anda merasa perlu adanya pelatihan tambahan tentang keamanan jaringan? Jika ya, pelatihan apa yang menurut Anda paling bermanfaat?

6. Bagaimana menurut Anda dampak dari peningkatan sistem keamanan jaringan terhadap pekerjaan sehari-hari Anda?

7. Adakah saran atau rekomendasi lain yang ingin Anda berikan terkait peningkatan keamanan jaringan perusahaan?

Hasil Wawancara

Pewawancara: John Doe

Wawancara dengan: Jane Smith

Jabatan: Manajer Keuangan

Departemen: Keuangan

Tanggal: 10 Mei 2024

1. Bagaimana Anda menilai keamanan jaringan perusahaan saat ini? Apakah Anda merasa data dan informasi terlindungi dengan baik?

Jane: "Saya rasa keamanan jaringan kita cukup baik, tetapi ada beberapa area yang masih perlu diperbaiki. Misalnya, ada kalanya saya merasa ada risiko kebocoran data, terutama saat menggunakan sistem lama."

2. Apakah Anda pernah mengalami atau mengetahui insiden keamanan jaringan (seperti serangan malware, kebocoran data) di perusahaan ini? Jika ya, bisakah Anda menceritakan pengalaman tersebut?

Jane: "Beberapa bulan yang lalu, departemen kami mengalami serangan malware yang menginfeksi beberapa komputer. Tim IT berhasil mengatasinya, tetapi butuh beberapa hari untuk pulih sepenuhnya, dan itu sangat mengganggu operasional kami."

3. Fitur keamanan apa yang menurut Anda paling penting untuk ditingkatkan dalam sistem jaringan kita? Mengapa?

Jane: "Menurut saya, kita perlu meningkatkan sistem enkripsi data dan firewall. Enkripsi data penting untuk melindungi informasi sensitif, sedangkan firewall yang kuat bisa mencegah serangan dari luar."

4. Seberapa puas Anda dengan dukungan yang diberikan oleh tim IT terkait masalah keamanan jaringan? Apa yang bisa ditingkatkan?

Jane: "Saya cukup puas dengan dukungan tim IT. Mereka responsif, tetapi kadang-kadang butuh waktu lama untuk menyelesaikan masalah. Mungkin mereka perlu lebih banyak sumber daya atau pelatihan tambahan."

5. Apakah Anda merasa perlu adanya pelatihan tambahan tentang keamanan jaringan? Jika ya, pelatihan apa yang menurut Anda paling bermanfaat?

Jane: "Ya, pelatihan tentang bagaimana mengenali dan menghindari serangan phishing akan sangat berguna. Banyak karyawan yang masih belum sadar bagaimana cara mengenali email atau link yang mencurigakan."

6. Bagaimana menurut Anda dampak dari peningkatan sistem keamanan jaringan terhadap pekerjaan sehari-hari Anda?

Jane: "Peningkatan sistem keamanan pasti akan membantu dalam jangka panjang. Mungkin awalnya akan ada penyesuaian, tetapi jika sistem lebih aman, kita akan bekerja dengan lebih tenang dan efisien."

7. Adakah saran atau rekomendasi lain yang ingin Anda berikan terkait peningkatan keamanan jaringan perusahaan?

Jane: "Saya pikir kita harus mempertimbangkan untuk menerapkan autentikasi multi-faktor. Ini akan menambah lapisan keamanan tambahan dan membuat akses data lebih aman."

Observasi Keamanan Jaringan

Metode Observasi

Lokasi: Kantor Pusat Organisasi ABC

Waktu Observasi: 2 Hari (12-13 Mei 2024)

Tim Observasi: [Nama Tim Observasi]

Tujuan Observasi:

1. Mengamati perilaku pengguna terkait penggunaan jaringan.

2. Mengevaluasi prosedur keamanan yang ada.

3. Mengidentifikasi kelemahan atau celah keamanan dalam praktik sehari-hari.

Hasil Observasi

Hari 1: 12 Mei 2024

Lokasi: Departemen IT dan Keuangan

Pengamatan:

1. **Penggunaan Password:**

- Banyak pengguna tidak mengganti password secara berkala.
- Beberapa pengguna mencatat password di tempat yang mudah diakses (misalnya, tempel di monitor).

2. **Akses Fisik ke Perangkat:**

- Ruang server tidak selalu terkunci.
- Ada beberapa kasus di mana karyawan meninggalkan komputer dalam keadaan menyala tanpa logout saat meninggalkan meja kerja.

3. **Prosedur Penanganan Insiden:**

- Tim IT responsif terhadap laporan masalah, namun dokumentasi dan pelaporan insiden tidak selalu lengkap.
- Tidak ada simulasi rutin untuk menghadapi insiden keamanan seperti serangan siber.

4. **Penggunaan Perangkat Pribadi:**

- Beberapa karyawan menggunakan perangkat pribadi untuk mengakses jaringan perusahaan tanpa protokol keamanan yang memadai.

Catatan Tambahan:

- Terlihat adanya ketergantungan yang tinggi pada tim IT untuk mengatasi masalah keamanan. Pengguna kurang dilibatkan dalam menjaga keamanan data.

Hari 2: 13 Mei 2024

Lokasi: Departemen Pemasaran dan Operasional

Pengamatan:

1. **Pelatihan dan Kesadaran Keamanan:**

- Sebagian besar karyawan belum pernah mengikuti pelatihan keamanan jaringan.
- Kesadaran mengenai ancaman phishing dan malware masih rendah.

2. **Keamanan Data dan Enkripsi:**

- Data sensitif terkadang disimpan di tempat yang kurang aman, seperti hard drive eksternal tanpa enkripsi.
- Enkripsi data pada email penting tidak diterapkan secara konsisten.

3. **Akses Jaringan dan VPN:**

- Akses jaringan jarak jauh (VPN) digunakan oleh beberapa karyawan, namun beberapa koneksi tidak terenkripsi dengan baik.
- Tidak ada kebijakan yang jelas mengenai penggunaan VPN.

4. **Pemantauan dan Logging:**

- Sistem pemantauan jaringan real-time belum sepenuhnya diimplementasikan.
- Log aktivitas jaringan tidak diperiksa secara rutin untuk mendeteksi aktivitas mencurigakan.

Catatan Tambahan:

- Perlu adanya peningkatan dalam prosedur enkripsi dan penggunaan VPN untuk mengamankan akses jarak jauh.
- Kesadaran karyawan terhadap praktik keamanan perlu ditingkatkan melalui pelatihan berkala.

Kesimpulan Observasi

Hasil observasi menunjukkan bahwa meskipun ada beberapa prosedur keamanan yang sudah diterapkan, masih terdapat banyak celah dan kelemahan yang perlu diperbaiki. Beberapa area yang perlu diperhatikan adalah:

1. Pengelolaan Password: Implementasi kebijakan pergantian password secara berkala dan pelatihan tentang cara menyimpan password dengan aman.

2. Keamanan Fisik dan Akses: Pengawasan yang lebih ketat terhadap akses fisik ke perangkat dan ruang server.

3. Pelatihan dan Kesadaran: Pelatihan rutin untuk meningkatkan kesadaran keamanan siber di kalangan karyawan.

4. Prosedur Enkripsi: Penggunaan enkripsi data yang konsisten untuk melindungi informasi sensitif.

5. Pemantauan Jaringan: Peningkatan sistem pemantauan jaringan real-time dan pemeriksaan log secara rutin.

Analisis dan Kesimpulan Permasalahan Sistem yang Sedang Berjalan

Analisis Permasalahan

1. Penggunaan Password:

- **Masalah:** Banyak pengguna tidak mengganti password secara berkala dan mencatatnya di tempat yang mudah diakses.
- **Dampak:** Risiko tinggi terhadap pencurian identitas dan akses tidak sah ke sistem jaringan.

2. Akses Fisik ke Perangkat:

- **Masalah:** Ruang server sering tidak terkunci dan komputer sering ditinggalkan dalam keadaan menyala tanpa logout.
- **Dampak:** Meningkatkan risiko akses fisik tidak sah dan potensi sabotase atau pencurian data.

3. Prosedur Penanganan Insiden:

- **Masalah:** Dokumentasi dan pelaporan insiden tidak selalu lengkap, dan tidak ada simulasi rutin untuk menghadapi serangan siber.
- **Dampak:** Respon terhadap insiden bisa tidak optimal, mengurangi efektivitas dalam menangani dan mencegah insiden keamanan di masa depan.

4. Penggunaan Perangkat Pribadi:

- **Masalah:** Penggunaan perangkat pribadi tanpa protokol keamanan yang memadai untuk mengakses jaringan perusahaan.
- **Dampak:** Meningkatkan risiko malware dan kebocoran data melalui perangkat yang tidak aman.

5. Pelatihan dan Kesadaran Keamanan:

- **Masalah:** Rendahnya kesadaran dan pelatihan tentang keamanan jaringan di kalangan karyawan.
- **Dampak:** Karyawan kurang waspada terhadap ancaman keamanan seperti phishing dan malware, yang dapat mengakibatkan insiden keamanan.

6. Keamanan Data dan Enkripsi:

- **Masalah:** Data sensitif sering disimpan tanpa enkripsi yang memadai, dan email penting tidak selalu dienkripsi.
- **Dampak:** Data sensitif menjadi rentan terhadap akses tidak sah dan kebocoran.

7. Akses Jaringan dan VPN:

- **Masalah:** Beberapa koneksi VPN tidak terenkripsi dengan baik, dan tidak ada kebijakan yang jelas mengenai penggunaan VPN.
- **Dampak:** Akses jarak jauh menjadi rentan terhadap penyadapan dan serangan man-in-the-middle.

8. Pemantauan dan Logging:

- **Masalah:** Sistem pemantauan jaringan real-time belum sepenuhnya diimplementasikan, dan log aktivitas tidak diperiksa secara rutin.
- **Dampak:** Aktivitas mencurigakan mungkin tidak terdeteksi dengan cepat, memungkinkan ancaman berlanjut tanpa penanganan.

Kesimpulan Permasalahan

1. Rendahnya Kesadaran dan Pelatihan Keamanan:

- Kesadaran dan pelatihan karyawan tentang keamanan jaringan perlu ditingkatkan melalui program pelatihan rutin dan kampanye kesadaran.

2. Prosedur Keamanan yang Tidak Konsisten:

- Kebijakan dan prosedur keamanan, termasuk manajemen password, akses fisik, dan penggunaan perangkat pribadi, perlu diperketat dan disosialisasikan dengan jelas.

3. Kurangnya Penggunaan Enkripsi:

- Implementasi enkripsi data yang lebih konsisten dan komprehensif diperlukan untuk melindungi informasi sensitif baik dalam penyimpanan maupun dalam transmisi.

4. Kelemahan dalam Pemantauan dan Respon Insiden:

- Sistem pemantauan jaringan real-time perlu diimplementasikan dan diperbarui, dan prosedur penanganan insiden harus ditingkatkan untuk memastikan respon yang cepat dan efektif.

5. Akses Jarak Jauh yang Tidak Aman:

- Kebijakan penggunaan VPN harus diperjelas dan diterapkan dengan enkripsi yang memadai untuk memastikan keamanan akses jarak jauh.

Visi, Misi, dan Strategi Perusahaan dalam Mencapai Tujuan Perusahaan

Visi Perusahaan

"Menjadi penyedia layanan finansial terdepan yang inovatif dan terpercaya, dengan fokus pada keamanan data dan kepuasan pelanggan."

Misi Perusahaan

1. Menyediakan Layanan Berkualitas Tinggi:

- Menawarkan produk dan layanan finansial yang unggul dengan mengutamakan kepuasan pelanggan.

2. Keamanan dan Privasi:

- Melindungi data dan informasi pelanggan dengan teknologi keamanan terkini dan kebijakan privasi yang ketat.

3. Inovasi Berkelanjutan:

- Terus berinovasi dalam pengembangan produk dan layanan untuk memenuhi kebutuhan pasar yang selalu berubah.

4. Kepuasan Pelanggan:

- Memberikan layanan pelanggan yang responsif dan solutif untuk menciptakan pengalaman positif bagi pelanggan.

5. Pengembangan Sumber Daya Manusia:

- Meningkatkan kompetensi karyawan melalui pelatihan dan pengembangan berkelanjutan.

Strategi Perusahaan

1. Strategi Keamanan Informasi:

- **Implementasi Teknologi Terbaru:**
  - Mengadopsi teknologi keamanan terbaru, seperti enkripsi data, firewall canggih, dan sistem deteksi intrusi.

- **Pengawasan dan Pemantauan:**
  - Menerapkan sistem pemantauan jaringan real-time untuk mendeteksi dan merespons ancaman secara proaktif.

- **Kebijakan Keamanan yang Kuat:**
  - Mengembangkan dan menerapkan kebijakan keamanan yang ketat untuk melindungi data pelanggan dan aset perusahaan.

2. Strategi Peningkatan Layanan:

- **Pengembangan Produk:**
  - Terus mengembangkan produk dan layanan baru yang sesuai dengan kebutuhan pelanggan.

- **Peningkatan Kualitas Layanan:**
  - Menyediakan pelatihan bagi staf layanan pelanggan untuk memastikan pelayanan yang cepat dan efektif.

3. Strategi Inovasi:

- **Investasi dalam R&D:**
  - Mengalokasikan anggaran untuk penelitian dan pengembangan guna menciptakan solusi finansial yang inovatif.

- **Kemitraan Strategis:**
  - Menjalin kemitraan dengan perusahaan teknologi dan institusi keuangan untuk mempercepat inovasi.

4. Strategi Kepuasan Pelanggan:

- **Penyelesaian Cepat Keluhan:**
  - Membangun sistem manajemen keluhan yang efisien untuk menangani masalah pelanggan dengan cepat.

- **Survei Kepuasan Pelanggan:**
  - Melakukan survei rutin untuk mengukur kepuasan pelanggan dan mengidentifikasi area yang perlu perbaikan.

5. Strategi Pengembangan Sumber Daya Manusia:

- **Pelatihan Rutin:**
  - Mengadakan program pelatihan berkala tentang keamanan informasi dan teknologi terbaru.

- **Pengembangan Karir:**
  - Menyediakan jalur pengembangan karir yang jelas dan kesempatan bagi karyawan untuk berkembang.

Analisis SWOT Perusahaan

Strengths (Kekuatan)

1. Reputasi dan Kepercayaan:

- Organisasi ABC memiliki reputasi yang baik dan kepercayaan tinggi dari pelanggan berkat layanan yang andal dan aman.

2. Teknologi Canggih:

- Penggunaan teknologi terkini dalam layanan finansial dan sistem keamanan yang kuat.

3. Layanan Pelanggan yang Responsif:

- Tim layanan pelanggan yang responsif dan efektif dalam menangani keluhan dan kebutuhan pelanggan.

4. Inovasi Berkelanjutan:

- Budaya perusahaan yang mendukung inovasi berkelanjutan dan pengembangan produk baru.

5. Sumber Daya Manusia yang Kompeten:

- Karyawan yang terlatih dan berkompeten dalam bidang teknologi dan keuangan.

Weaknesses (Kelemahan)

1. Keamanan Jaringan yang Belum Optimal:

- Masih terdapat kelemahan dalam sistem keamanan jaringan yang perlu diperbaiki, seperti manajemen password dan enkripsi data.

2. Prosedur Penanganan Insiden:

- Prosedur penanganan insiden belum sepenuhnya terdokumentasi dan dilaksanakan dengan baik.

3. Penggunaan Perangkat Pribadi:

- Kurangnya kebijakan yang ketat mengenai penggunaan perangkat pribadi untuk mengakses jaringan perusahaan.

4. Kesadaran Keamanan yang Rendah:

- Kesadaran karyawan tentang ancaman keamanan siber masih rendah, membutuhkan pelatihan tambahan.

5. Ketergantungan pada Tim IT:

- Ketergantungan yang tinggi pada tim IT untuk mengatasi masalah keamanan, dengan keterlibatan pengguna yang minimal.

Opportunities (Peluang)

1. Pertumbuhan Pasar Digital:

- Pertumbuhan pesat dalam penggunaan layanan finansial digital memberikan peluang besar untuk ekspansi dan inovasi.

2. Regulasi Keamanan yang Meningkat:

- Peningkatan regulasi keamanan siber dapat memperkuat kepercayaan pelanggan jika perusahaan mampu mematuhi dan melampaui standar tersebut.

3. Teknologi Baru:

- Adopsi teknologi baru seperti AI dan blockchain untuk meningkatkan keamanan dan efisiensi layanan.

4. Kolaborasi dan Kemitraan:

- Peluang untuk menjalin kemitraan dengan perusahaan teknologi lain dan institusi keuangan untuk memperkuat posisi di pasar.

5. Kebutuhan Akan Pelatihan Keamanan:

- Meningkatkan pelatihan keamanan bagi karyawan dapat mengurangi risiko keamanan dan meningkatkan kinerja keseluruhan.

Threats (Ancaman)

1. Serangan Siber:

- Ancaman serangan siber yang terus berkembang dan semakin canggih dapat mengancam keamanan data dan operasional perusahaan.

2. Persaingan yang Ketat:

- Persaingan yang semakin ketat dari perusahaan teknologi dan layanan finansial lain dapat mengurangi pangsa pasar.

3. Perubahan Regulasi:

- Perubahan regulasi yang cepat dapat menimbulkan tantangan bagi kepatuhan dan operasional perusahaan.

4. Kehilangan Data dan Kebocoran:

- Risiko kehilangan atau kebocoran data dapat merusak reputasi dan mengakibatkan kerugian finansial yang signifikan.

5. Ketidakpastian Ekonomi:

- Ketidakpastian ekonomi global dapat mempengaruhi kemampuan pelanggan untuk menggunakan layanan finansial, mengurangi pendapatan perusahaan.

2. Analisis Kebutuhan Sistem Keamanan Jaringan

A. Masukkan Visi, Misi, Strategi, dan Analisis SWOT Perusahaan ke dalam Analisis Kebutuhan Sistem

Visi Perusahaan:

"Menjadi penyedia layanan finansial terdepan yang inovatif dan terpercaya, dengan fokus pada keamanan data dan kepuasan pelanggan."

Misi Perusahaan:

1. Menyediakan produk dan layanan finansial yang unggul dengan mengutamakan kepuasan pelanggan.

2. Melindungi data dan informasi pelanggan dengan teknologi keamanan terkini dan kebijakan privasi yang ketat.

3. Terus berinovasi dalam pengembangan produk dan layanan untuk memenuhi kebutuhan pasar yang selalu berubah.

4. Memberikan layanan pelanggan yang responsif dan solutif untuk menciptakan pengalaman positif bagi pelanggan.

5. Meningkatkan kompetensi karyawan melalui pelatihan dan pengembangan berkelanjutan.

Strategi Perusahaan:

1. Mengadopsi teknologi keamanan terbaru, seperti enkripsi data, firewall canggih, dan sistem deteksi intrusi.

2. Menerapkan sistem pemantauan jaringan real-time untuk mendeteksi dan merespons ancaman secara proaktif.

3. Mengembangkan dan menerapkan kebijakan keamanan yang ketat untuk melindungi data pelanggan dan aset perusahaan.

4. Menyediakan pelatihan bagi staf layanan pelanggan untuk memastikan pelayanan yang cepat dan efektif.

5. Mengalokasikan anggaran untuk penelitian dan pengembangan guna menciptakan solusi finansial yang inovatif.

Analisis SWOT:

- **Strengths:** Reputasi baik, teknologi canggih, layanan pelanggan yang responsif, inovasi berkelanjutan, SDM kompeten.
- **Weaknesses:** Keamanan jaringan belum optimal, prosedur penanganan insiden belum memadai, penggunaan perangkat pribadi tanpa protokol keamanan yang baik, kesadaran keamanan rendah, ketergantungan pada tim IT.
- **Opportunities:** Pertumbuhan pasar digital, peningkatan regulasi keamanan, adopsi teknologi baru, kolaborasi dan kemitraan, kebutuhan akan pelatihan keamanan.
- **Threats:** Serangan siber, persaingan ketat, perubahan regulasi, kehilangan data dan kebocoran, ketidakpastian ekonomi.

B. Kebutuhan Fungsional

1. Fitur:

- Sistem enkripsi data untuk melindungi informasi sensitif.
- Firewall dan sistem deteksi intrusi untuk mencegah akses tidak sah.
- Autentikasi multi-faktor untuk mengamankan akses pengguna.

2. Menu:

- Dashboard keamanan yang menampilkan status keamanan jaringan secara real-time.
- Menu manajemen pengguna untuk mengatur hak akses dan autentikasi.
- Menu pelaporan insiden untuk mendokumentasikan dan melacak insiden keamanan.
- Menu pelatihan dan edukasi untuk menyediakan materi pelatihan tentang keamanan siber.

3. Proses:

- Proses enkripsi dan dekripsi data.
- Proses deteksi dan respon terhadap ancaman siber.
- Proses manajemen insiden keamanan.
- Proses pembaruan dan pemeliharaan sistem keamanan.

4. Output:

- Laporan keamanan harian, mingguan, dan bulanan.
- Notifikasi dan peringatan jika terdeteksi adanya ancaman.
- Laporan audit akses pengguna.
- Materi pelatihan dan edukasi yang dapat diakses karyawan.

5.Input:

- Data pengguna untuk autentikasi.
- Data insiden keamanan untuk pelaporan.
- Data jaringan untuk pemantauan dan deteksi ancaman.
- Feedback dan hasil evaluasi dari pelatihan keamanan.

C. Kebutuhan Non-Fungsional

1. Kinerja:

- Sistem harus mampu memproses data enkripsi dan dekripsi dengan cepat tanpa mengganggu performa jaringan.
- Pemantauan real-time harus responsif dan tidak menyebabkan latency yang signifikan.

2. Keamanan (Fisik & Non-Fisik):

- Fisik: Pengamanan akses fisik ke ruang server dan perangkat keras dengan kontrol akses yang ketat.
- Non-Fisik: Implementasi protokol keamanan siber seperti SSL/TLS untuk komunikasi data, serta backup dan pemulihan data secara rutin.

3. Kehandalan:

- Sistem harus memiliki uptime yang tinggi dengan toleransi kesalahan minimal.
- Prosedur backup dan pemulihan data harus diterapkan untuk memastikan data dapat dipulihkan dengan cepat jika terjadi kegagalan sistem.
- Dukungan teknis yang tersedia 24/7 untuk menangani masalah dan insiden keamanan.

3. Analisis Mitigasi Risiko Sistem

Identifikasi Risiko

1. Serangan Malware dan Virus

2. Serangan Phishing

3. Serangan DDoS (Distributed Denial of Service)

4. Kebocoran Data

5. Kegagalan Sistem atau Perangkat Keras

6. Akses Tidak Sah

7. Kegagalan Pemulihan Data

8. Human Error

Evaluasi Risiko

- **Serangan Malware dan Virus:** Tinggi
- **Serangan Phishing:** Menengah
- **Serangan DDoS:** Tinggi
- **Kebocoran Data:** Tinggi
- **Kegagalan Sistem atau Perangkat Keras:** Menengah

- **Akses Tidak Sah:** Tinggi
- **Kegagalan Pemulihan Data:** Menengah
- **Human Error:** Menengah

Mitigasi Risiko

1. Serangan Malware dan Virus

- **Tindakan Mitigasi:**
  - Instalasi dan pembaruan rutin perangkat lunak antivirus dan anti-malware.
  - Penerapan kebijakan penggunaan perangkat lunak yang ketat.
  - Pelatihan karyawan tentang pengenalan dan pencegahan malware.

- **Respons Saat Risiko Terjadi:**
  - Isolasi perangkat yang terinfeksi.
  - Pembersihan malware dan pemulihan sistem.

2. Serangan Phishing

- **Tindakan Mitigasi:**
  - Pelatihan karyawan tentang pengenalan email phishing.
  - Implementasi filter email untuk mendeteksi dan memblokir email phishing.

- **Respons Saat Risiko Terjadi:**
  - Informasikan karyawan dan lakukan pemulihan terhadap akun yang terdampak.
  - Peninjauan dan perbaikan kebijakan keamanan email.

3. Serangan DDoS

- **Tindakan Mitigasi:**
  - Implementasi solusi mitigasi DDoS seperti Web Application Firewall (WAF) dan layanan CDN (Content Delivery Network).
  - Monitoring jaringan secara real-time.

- **Respons Saat Risiko Terjadi:**
  - Aktivasi protokol mitigasi DDoS.
  - Komunikasi dengan penyedia layanan untuk mempercepat pemulihan.

4. Kebocoran Data

- **Tindakan Mitigasi:**
  - Implementasi enkripsi data baik saat transit maupun saat penyimpanan.
  - Pembatasan akses data berdasarkan kebutuhan.

- **Respons Saat Risiko Terjadi:**
  - Identifikasi sumber kebocoran.
  - Komunikasi dan peringatan kepada pihak yang terdampak.
  - Evaluasi dan perbaikan kebijakan keamanan data.

5. Kegagalan Sistem atau Perangkat Keras

- **Tindakan Mitigasi:**
  - Redundansi sistem dan perangkat keras.
  - Pemeliharaan dan pengujian rutin perangkat keras.

- **Respons Saat Risiko Terjadi:**
  - Aktivasi sistem cadangan.
  - Pemulihan data dari backup.

6. Akses Tidak Sah

- **Tindakan Mitigasi:**
  - Implementasi autentikasi multi-faktor (MFA).
  - Penerapan kebijakan manajemen akses yang ketat.

- **Respons Saat Risiko Terjadi:**
  - Penguncian akun yang dicurigai.
  - Peninjauan log akses untuk menentukan sumber dan tujuan akses tidak sah.

7. Kegagalan Pemulihan Data

- **Tindakan Mitigasi:**
  - Backup data secara rutin dan penyimpanan di lokasi terpisah.
  - Pengujian rutin prosedur pemulihan data.

- **Respons Saat Risiko Terjadi:**
  - Aktivasi prosedur pemulihan data.
  - Evaluasi dan perbaikan prosedur backup dan pemulihan.

8. Human Error

- **Tindakan Mitigasi:**
  - Pelatihan rutin bagi karyawan tentang praktik keamanan yang baik.
  - Implementasi prosedur operasi standar yang jelas dan mudah diikuti.

- **Respons Saat Risiko Terjadi:**
  - Identifikasi dan koreksi kesalahan.
  - Pengembangan lebih lanjut dalam pelatihan untuk mencegah pengulangan kesalahan.

4. Analisis Manajemen Perubahan Sistem

Tujuan Manajemen Perubahan Sistem

1. Memastikan Keamanan dan Keberlanjutan:

- Melindungi sistem dari risiko yang mungkin timbul akibat perubahan.

2. Meningkatkan Efisiensi dan Efektivitas:

- Mengoptimalkan penggunaan sumber daya dan memastikan bahwa perubahan memberikan manfaat yang diharapkan.

3. Mengurangi Gangguan Operasional:

- Meminimalkan gangguan terhadap operasional sehari-hari dan layanan kepada pelanggan.

4. Meningkatkan Kepatuhan:

- Memastikan bahwa perubahan mematuhi regulasi dan kebijakan internal perusahaan.

Proses Manajemen Perubahan

1. Identifikasi Kebutuhan Perubahan

- **Contoh:**
  - Adanya kebutuhan untuk meningkatkan sistem enkripsi data setelah analisis risiko menunjukkan kelemahan dalam metode enkripsi saat ini.

2. Permintaan Perubahan

- **Contoh:**
  - Tim IT mengajukan permintaan perubahan untuk mengimplementasikan enkripsi AES-256 yang lebih kuat.
  - Dokumen permintaan perubahan mencakup deskripsi perubahan, alasan, dampak, dan sumber daya yang dibutuhkan.

3. Analisis Dampak

- **Contoh:**
  - Analisis dampak dilakukan untuk memahami efek perubahan pada sistem saat ini, termasuk:
    - Dampak pada kinerja sistem.
    - Potensi gangguan layanan.
    - Kebutuhan pelatihan bagi staf.

4. Persetujuan Perubahan

- **Contoh:**
  - Dewan perubahan (Change Advisory Board) meninjau permintaan perubahan dan hasil analisis dampak.
  - Persetujuan diberikan berdasarkan manfaat, risiko, dan kesiapan organisasi untuk menerapkan perubahan.

5. Perencanaan dan Pelaksanaan Perubahan

- **Contoh:**
  - Pengembangan rencana pelaksanaan yang rinci, termasuk jadwal, tim yang terlibat, dan langkah-langkah implementasi.
  - Implementasi perubahan dilakukan di luar jam operasional utama untuk meminimalkan gangguan.

6. Pengujian dan Verifikasi

- **Contoh:**
  - Pengujian dilakukan untuk memastikan bahwa enkripsi baru berfungsi dengan benar dan tidak menyebabkan masalah pada sistem.
  - Uji coba dilakukan dalam lingkungan yang terisolasi sebelum diterapkan di seluruh jaringan.

7. Komunikasi Perubahan

- **Contoh:**
  - Komunikasi kepada semua pihak terkait mengenai perubahan yang akan dilakukan, jadwal, dan dampaknya.
  - Termasuk pengumuman kepada karyawan tentang pelatihan terkait perubahan enkripsi.

8. Implementasi Perubahan

- **Contoh:**
  - Implementasi enkripsi AES-256 pada sistem produksi sesuai rencana.
  - Pemantauan secara real-time untuk mendeteksi dan menangani masalah yang mungkin timbul selama dan setelah perubahan.

9. Pemantauan dan Evaluasi

- **Contoh:**
  - Pemantauan sistem secara intensif selama periode pasca-implementasi untuk memastikan stabilitas dan kinerja.
  - Evaluasi efektivitas perubahan dan dokumentasi hasil.

10. Review Pasca-Implementasi

- **Contoh:**
  - Melakukan review pasca-implementasi untuk menilai keberhasilan perubahan dan mengidentifikasi area untuk perbaikan.
  - Review melibatkan evaluasi dari tim IT, manajemen, dan pengguna akhir.