Jurnal Manajemen Riset Inovasi (MRI)
Vol.1, No.3 Oktober 2023
e-ISSN : 2964-7800; p-ISSN : 2963-2307, Hal 93-106
DOI: https://doi.org/10.55606/mri.v1i3.1275

Penerapan Objek Vital, Pengamanan File, Dan Pengamanan *Cyber* Pada Bank JABAR

Edy Soesanto
Universitas Bhayangkara Jakarta Raya

Alifah Jiddal Masyruroh
Universitas Bhayangkara Jakarta Raya

Ganis Aliefiani Mulya Putri
Universitas Bhayangkara Jakarta Raya

Srirahayu Putri Maharani
Universitas Bhayangkara Jakarta Raya

Alamat: Jl. Perjuangan No.81, RT.003/RW.002, Marga Mulya, Kec. Bekasi Utara, Kota Bks, Jawa Barat 17143
Korespondensi penulis: edy.soesanto@dsn.ubharajaya.ac.id

ABSTRACT. *Information security and asset protection have become top priorities in the banking industry today. Bank JABAR (Jawa Barat), as one of the leading banks in the region, also recognizes the importance of effective security management. The objective of this research is to examine the implementation of vital objects, file security, and cyber security at Bank JABAR. This research uses a descriptive analysis method by studying the policies and practices implemented by Bank JABAR in information security. Data collection techniques include documentation study and interviews that cover security policies, guidelines, and procedures at Bank JABAR. The results of this research indicate that Bank JABAR has implemented vital objects by identifying critical assets or information and giving them appropriate protection priority. File security is implemented through strict access policies, data encryption, regular data backup and recovery, as well as secure data disposal. Cyber security is carried out through firewall policies, intrusion detection systems, continuous network monitoring, and regular system security updates. In conclusion, Bank JABAR has taken important steps in the implementation of vital objects, file security, and cyber security. However, there is a need for ongoing efforts to enhance security awareness, involve more intensive training, and adopt a proactive approach to information security.*

Keywords: *Cybersecurity, File Security, Vital Object Implementation*

ABSTRAK. Keamanan informasi dan perlindungan terhadap aset menjadi prioritas utama dalam industri perbankan saat ini. Bank JABAR (Jawa Barat) sebagai salah satu bank terkemuka di wilayah tersebut, juga menyadari pentingnya manajemen keamanan yang efektif. Tujuan dari penelitian ini adalah untuk mengkaji penerapan objek vital, pengamanan file, dan pengamanan *cyber* pada Bank JABAR. Penelitian ini menggunakan

Received April 07, 2023; Revised Mei 30, 2023; Accepted Juni 03, 2023
** Alifah Jiddal Masyruroh, edy.soesanto@dsn.ubharajaya.ac.id*

metode analisis deskriptif dengan mempelajari kebijakan dan praktik yang diterapkan oleh Bank JABAR dalam penerapan keamanan informasi. Tehnik pengumpulan data melalui studi dokumentasi dan wawancara yang mencakup kebijakan keamanan, pedoman, dan prosedur yang ada di Bank JABAR. Hasil penelitian ini menunjukkan bahwa Bank JABAR telah menerapkan objek vital dengan melakukan identifikasi aset atau informasi yang kritis dan memberikan prioritas perlindungan yang sesuai. Pengamanan file diimplementasikan melalui kebijakan akses yang ketat, enkripsi data, backup dan pemulihan data secara teratur, serta penghapusan data yang aman. Pengamanan *cyber* dilakukan melalui kebijakan penggunaan firewall, sistem deteksi intrusi, pemantauan jaringan secara terus-menerus, dan pembaruan keamanan sistem secara rutin. Dalam kesimpulan, Bank JABAR telah melakukan langkah-langkah yang penting dalam penerapan objek vital, pengamanan file, dan pengamanan *cyber*. Namun, perlu adanya upaya berkelanjutan dalam meningkatkan kesadaran keamanan, melibatkan pelatihan yang lebih intensif, serta mengadopsi pendekatan yang proaktif terhadap keamanan informasi.

Kata kunci : *Pengamanan Cyber, Pengamanan File, Penerapan Objek Vital*

LATAR BELAKANG

Dalam industri perbankan modern, keamanan informasi dan perlindungan terhadap aset menjadi hal yang sangat penting. Bank-bank harus menghadapi ancaman yang semakin kompleks dalam bentuk serangan *cyber* dan pelanggaran keamanan data. Oleh karena itu, bank-bank perlu menerapkan strategi dan langkah-langkah yang efektif untuk melindungi informasi vital dan mengamankan aset mereka.

Bank JABAR (Jawa Barat) merupakan salah satu bank terkemuka di wilayah tersebut. Sebagai lembaga keuangan yang mengelola informasi sensitif seperti data nasabah, transaksi keuangan, dan informasi bisnis, Bank JABAR memiliki tanggung jawab yang besar untuk menjaga kerahasiaan, integritas, dan ketersediaan data tersebut. Seperti dalam jurnal Prosiding Seminar Sosial Politik, Bisnis, Akuntansi dan Teknik Bandung yang meneliti pengamanan data pada Bank BJB KCP Pasteur Kota Bandung. Hasilnya didapatkan bahwa pada Bank BJB KCP Pasteur Kota Bandung mengimplementasikan pengamanan data nasabah dengan metode algoritma kriptografi AES (Jayana, 2022).

Penerapan objek vital, pengamanan file, dan pengamanan *cyber* menjadi aspek yang sangat penting dalam manajemen keamanan Bank JABAR. Objek vital, yang meliputi aset dan informasi yang kritis, harus diidentifikasi dengan baik dan diberikan perlindungan yang memadai. Pengamanan file, termasuk kebijakan akses yang ketat, enkripsi data, backup dan pemulihan data secara teratur, serta penghapusan data yang

aman, juga menjadi hal yang sangat penting dalam menjaga kerahasiaan dan integritas informasi. Selain itu, pengamanan *cyber* melibatkan kebijakan dan teknik untuk melindungi jaringan dan sistem bank dari serangan *cyber* seperti malware, serangan phishing, dan serangan DDoS.

Namun, implementasi penerapan objek vital, pengamanan file, dan pengamanan *cyber* di Bank JABAR mungkin masih menghadapi beberapa tantangan. Mungkin ada kebutuhan untuk meningkatkan kesadaran dan pemahaman karyawan terkait ancaman keamanan, mengadopsi teknologi keamanan yang lebih canggih, atau mengatur kebijakan yang lebih ketat untuk menghadapi serangan yang terus berkembang.

Dalam rangka memahami dan menganalisis penerapan objek vital, pengamanan file, dan pengamanan *cyber* pada Bank JABAR, penelitian ini dilakukan. Penelitian ini akan menganalisis kebijakan, praktik, dan infrastruktur yang ada di Bank JABAR untuk memberikan wawasan tentang sejauh mana bank ini telah berhasil mengimplementasikan langkah-langkah keamanan tersebut. Selain itu, penelitian ini juga akan mengidentifikasi area yang perlu diperbaiki atau ditingkatkan dalam rangka memperkuat keamanan informasi Bank JABAR.

Penelitian ini bertujuan untuk menganalisis serta penerapan objek vital, pengamanan *cyber*, serta pengamanan file terhadap Bank Jabar. Diharapkan bisa membagikan uraian yang mendalam tentang berartinya keamanan *cyber* serta pengamanan file untuk Bank Jabar, dan membagikan saran yang relevan dalam tingkatkan keamanan serta ketahanan system terhadap ancaman keamanan yang terus tumbuh di masa digital.

RUMUSAN MASALAH

Berdasarkan uraian dari latar belakang yang ada di atas, maka rumusan masalah yang akan dibahas dalam penelitian ini adalah :

Bagaimana penerapan objek vital, pengamanan file dan pengamanan *cyber* pada Bank Jabar ?

KAJIAN TEORITIS

2.1 Objek Vital pada Bank JABAR

Objek vital merupakan suatu komponen yang terdapat didalam perusahaan atau organisasi dan bersifat penting atau menyangkut keberlangsungan perusahaan atau

organisasi. Objek vital dapat bersifat crucial atau riskan, sehingga perlu diperhatikan dengan baik oleh perusahaan atau organisasi (Edy Soesanto, 2023). Setiap perusahaan atau organisasi perlu mengetahui dan memahami segala kekurangan yang ada pada objek vitalnya, agar dapat mengambil keputusan terhadap perusahaan dengan baik.

Bank JABAR, sebagai lembaga keuangan yang berperan dalam menyimpan, mengelola, dan mengalirkan dana masyarakat, memiliki beberapa objek vital yang harus dijaga keamanannya. Objek vital ini mencakup aset fisik, sistem informasi, dan proses bisnis yang krusial bagi operasional bank. Berikut adalah beberapa objek vital yang penting dalam konteks Bank JABAR diantaranya yaitu

1. Data Nasabah

   Informasi pribadi dan keuangan nasabah, seperti nama, alamat, nomor rekening, saldo, transaksi, dan dokumen identitas, merupakan salah satu objek vital yang harus dijaga kerahasiaannya dan keutuhannya. Bank JABAR harus memiliki kebijakan yang ketat dalam mengelola dan melindungi data nasabah.

2. Sistem Core Banking

   Sistem Core Banking adalah pusat dari operasional perbankan. Sistem ini mencakup basis data yang menyimpan informasi akun nasabah, transaksi, dan semua aktivitas perbankan. Keamanan dan ketersediaan sistem Core Banking sangat penting untuk menjaga kontinuitas operasional bank.

3. Infrastruktur IT

   Infrastruktur IT Bank JABAR, seperti server, jaringan komputer, dan perangkat penyimpanan data, juga merupakan objek vital yang harus dijaga keamanannya. Gangguan pada infrastruktur IT dapat menyebabkan gangguan operasional dan berpotensi merugikan nasabah.

4. Sistem Keamanan Fisik

   Keamanan fisik meliputi gedung bank, ruang server, ruang penyimpanan data, serta sistem pengamanan fisik seperti kamera pengawas, akses terbatas, dan sistem

kebakaran. Semua ini harus dijaga dengan baik untuk mencegah akses tidak sah, kerusakan, atau kehilangan data dan aset penting.

2.2 Pengamanan File pada Bank JABAR

Pengamanan file merupakan aspek penting dalam keamanan informasi di setiap organisasi, termasuk bank seperti Bank JABAR. Penerapan langkah-langkah keamanan file yang efektif memastikan kerahasiaan, integritas, dan ketersediaan data sensitif yang disimpan dalam sistem file bank. Beberapa kerangka teori dan praktik terbaik dapat memandu penerapan keamanan file dalam lingkungan perbankan. Berikut adalah beberapa teori dan konsep kunci terkait keamanan file:

1. Kontrol Akses

   Kontrol akses adalah prinsip dasar dalam keamanan file. Ini melibatkan pengendalian dan pengelolaan akses pengguna terhadap file serta memastikan bahwa hanya individu yang diizinkan yang dapat melihat, mengubah, atau menghapus informasi sensitif. Mekanisme kontrol akses meliputi autentikasi pengguna, otorisasi, dan manajemen hak akses.

2. Enkripsi

   Enkripsi adalah teknik yang digunakan untuk mengubah data menjadi format yang tidak terbaca, yang dikenal sebagai ciphertext, menggunakan algoritma enkripsi. Enkripsi memastikan bahwa meskipun individu yang tidak berwenang mendapatkan akses ke file, mereka tidak dapat memahami kontennya tanpa kunci dekripsi. Bank dapat menerapkan enkripsi pada berbagai tingkatan, seperti mengenkripsi file saat istirahat dan selama transmisi.

3. Integritas File

   Integritas file berkaitan dengan menjaga akurasi, konsistensi, dan kehandalan file. Bank dapat menggunakan teknik seperti checksum atau tanda tangan digital untuk memastikan file tetap tidak diubah dan tidak dapat dimanipulasi. Pemeriksaan integritas secara rutin dan mekanisme pemantauan membantu mengidentifikasi modifikasi atau kerusakan file yang tidak sah.

4. Cadangan dan Pemulihan

   Bank harus membentuk prosedur cadangan dan pemulihan yang kuat untuk melindungi file dari kehilangan atau penghancuran yang tidak sah. Cadangan rutin file-file kritis harus dilakukan, dan sistem penyimpanan cadangan yang dapat diandalkan harus dipelihara. Selain itu, pengujian proses pemulihan secara berkala memastikan bahwa file dapat dipulihkan dengan efektif dalam kejadian kehilangan data.

5. Retensi dan Pembuangan Data: Praktik retensi dan pembuangan data yang tepat sangat penting dalam keamanan file. Bank harus membentuk kebijakan dan prosedur untuk menyimpan file selama durasi yang diperlukan dan membuang file dengan aman ketika tidak lagi diperlukan. Teknik penghancuran atau penghapusan file yang aman harus digunakan untuk mencegah akses yang tidak sah ke informasi sensitif.

6. Pemantauan dan Audit File: Mengimplementasikan mekanisme pemantauan dan audit file memungkinkan bank untuk melacak akses file, modifikasi, dan aktivitas pengguna. Hal ini membantu mendeteksi aktivitas yang mencurigakan atau tidak sah dan memberikan jejak audit untuk tujuan investigasi. Pemantauan dapat mencakup kegiatan seperti log akses file, sistem deteksi intrusi, dan alat pemantauan

2.3 Pengamanan *cyber* pada Bank JABAR

Pengamanan *cyber* merupakan aspek penting dalam menjaga keamanan informasi dan melindungi aset dalam lingkungan perbankan. Dalam kajian teori, terdapat beberapa konsep dan teori yang relevan terkait pengamanan *cyber* pada bank. Berikut adalah beberapa di antaranya:

1. Keamanan Jaringan: Konsep keamanan jaringan melibatkan pengaturan dan perlindungan infrastruktur jaringan bank. Hal ini mencakup penggunaan firewall untuk mengatur lalu lintas jaringan, sistem deteksi intrusi untuk mendeteksi serangan

yang mencurigakan, dan pemantauan jaringan secara terus-menerus untuk mengidentifikasi aktivitas yang mencurigakan.

2. Keamanan Sistem: Keamanan sistem berkaitan dengan melindungi sistem operasi, perangkat keras, dan perangkat lunak yang digunakan dalam lingkungan perbankan. Konsep ini melibatkan penggunaan teknik dan alat keamanan seperti antivirus, antispyware, dan pembaruan perangkat lunak secara teratur untuk mengatasi kerentanan keamanan yang dapat dieksploitasi oleh penyerang.

3. Keamanan Aplikasi: Keamanan aplikasi mencakup praktik dan metode untuk melindungi aplikasi perbankan dari serangan seperti injeksi kode, cross-site scripting, dan serangan serupa. Upaya pengamanan aplikasi melibatkan pengkodean yang aman, pengujian keamanan aplikasi, dan penerapan praktik pengembangan perangkat lunak yang aman.

4. Kesadaran Keamanan: Kesadaran keamanan merupakan konsep yang penting dalam pengamanan *cyber*. Ini melibatkan pelatihan dan pendidikan kepada karyawan bank tentang praktik keamanan, ancaman *cyber* yang mungkin terjadi, dan tindakan pencegahan yang harus diambil. Dengan meningkatkan kesadaran keamanan, karyawan bank dapat menjadi lebih waspada terhadap serangan dan berkontribusi pada keamanan secara keseluruhan.

5. Manajemen Kejadian Keamanan: Manajemen kejadian keamanan melibatkan proses pengelolaan dan tanggapan terhadap insiden keamanan. Bank harus memiliki kebijakan dan prosedur yang jelas untuk mengatasi serangan *cyber*, termasuk identifikasi, penghentian, investigasi, dan pemulihan setelah serangan terjadi. Mekanisme pengumpulan dan analisis data juga dapat membantu dalam mendeteksi serangan dan merespons dengan cepat.

Penerapan teori-teori ini dalam pengamanan *cyber* pada bank, termasuk Bank JABAR, penting untuk menjaga keamanan informasi, melindungi data sensitif, dan mencegah serangan *cyber* yang dapat merugikan bank dan nasabahnya. Selain itu, bank juga harus mengikuti perkembangan dan tren terkini dalam keamanan *cyber* untuk terus meningkatkan pertahanan mereka dan mengatasi ancaman yang baru muncul.

METODE PENELITIAN

Menurut (Sugiyono, 2018) metode penelitian pada dasarnya merupakan cara ilmiah untuk mendapatkan data dengan tujuan dan kegunaan tertentu. Dalam penelitian ini peneliti menggunakan metode studi kasus (case study) dengan pendekatan kualitatif.

Metode penulisan artikel ilmiah ini yaitu dengan metode kualitatif dan kajian literatur (Library Research). Subjek penelitian pada topik "Penerapan Objek Vital, Pengamanan File, dan Pengamanan Cyber pada Bank JABAR" adalah Bank JABAR itu sendiri.

Penelitian akan fokus pada praktik dan kebijakan yang diterapkan oleh Bank JABAR dalam mengamankan objek vital mereka, melindungi file-file penting, dan menjaga keamanan cyber di dalam organisasi tersebut. Subjek penelitian ini akan mencakup aspek keamanan fisik, keamanan file, dan keamanan jaringan yang diterapkan oleh Bank JABAR dalam menjaga integritas, kerahasiaan, dan ketersediaan informasi serta melindungi sistem mereka dari ancaman keamanan.

Adapun sampel dalam penelitian ini yaitu staff Bank Jabar diantaranya manager keamanaan , Staff IT, staff analisis data internal, petugas keamanan serta nasabah Banjk Jabar. Pengumplan data dilakukan dengan menggunakan tehnik wawancara yang didahului dengan observasi pada Bank Jabar. Pada penelitian ini digunaka uji kredibilitas untuk menguji keabsahan data. Uji kredibilitas data dilakukan dengan triangulasi.

Dalam penelitian kualitatif, hasil temuan atau data yang telah diperoleh oleh peneliti dapat dinyatakan valid apabila hasil temuan atau data yang diperoleh dan dikemukakan peneliti sesuai dengan temuan atau data sebenarnya terjadi pada objek yang diteliti. Hasil pengumpulan data kemudian dianalisis dan disajikan dalam bentuk deskripsi.

HASIL DAN PEMBAHASAN

Penerapan objek vital, pengamanan file, dan pengamanan *cyber* pada bank-bank, termasuk Bank JABAR, sangat penting untuk menjaga keamanan data dan informasi nasabah serta mencegah serangan *cyber*. Pengamanan yang efektif melibatkan kombinasi dari pengamanan fisik, pengamanan file, dan pengamanan jaringan yang komprehensif.

A. Penerapan Objek Vital pada Bank JABAR

Dalam konteks penerapan objek vital, bank-bank biasanya mengidentifikasi data dan sistem yang dianggap vital dan memberikan perlindungan khusus terhadapnya. Hal ini melibatkan pemantauan dan pengendalian akses, penggunaan enkripsi data, dan pengamanan fisik terhadap infrastruktur yang penting.

Objek vital memiliki peran yang sangat penting dalam menjaga keamanan informasi dan kelangsungan operasional Bank JABAR. Berikut adalah beberapa peran objek vital pada Bank JABAR :

- Identifikasi Aset Penting: Objek vital membantu Bank JABAR dalam mengidentifikasi aset atau informasi yang kritis dan sangat penting dalam menjalankan operasional perbankan. Ini bisa meliputi data nasabah, informasi keuangan, sistem transaksi, infrastruktur jaringan, dan lain sebagainya.

- Prioritas Perlindungan: Objek vital memungkinkan Bank JABAR untuk memberikan prioritas perlindungan yang tinggi terhadap aset yang dianggap vital. Dalam hal ini, langkah-langkah keamanan yang lebih kuat dan solusi teknologi yang canggih dapat diterapkan untuk melindungi objek vital ini dari ancaman dan serangan.

- Manajemen Risiko: Objek vital juga memainkan peran penting dalam manajemen risiko Bank JABAR. Dengan mengidentifikasi dan fokus pada objek vital, bank dapat menentukan dan mengimplementasikan langkah-langkah pengamanan yang sesuai untuk mengurangi risiko keamanan dan menjaga kontinuitas bisnis.

- Pemulihan Bencana: Objek vital juga menjadi fokus utama dalam perencanaan pemulihan bencana. Bank JABAR perlu memiliki strategi dan prosedur pemulihan yang efektif untuk mengembalikan operasional normal setelah terjadinya bencana atau gangguan serius. Objek vital menjadi prioritas dalam proses pemulihan ini.

- Kepatuhan Peraturan: Objek vital juga memiliki peran penting dalam memastikan kepatuhan Bank JABAR terhadap peraturan dan standar keamanan yang berlaku.
  alam banyak kasus, regulasi perbankan mengharuskan bank untuk melindungi objek vital dan menerapkan langkah-langkah keamanan yang sesuai.

B. Penerapan Pengamanan File pada Bank JABAR

Sedangkan Pengamanan file melibatkan penggunaan teknik enkripsi data, pengendalian akses yang tepat, dan pemantauan aktivitas pengguna untuk mencegah akses tidak sah dan melindungi kerahasiaan data nasabah dan informasi keuangan dan ketersediaan data yang disimpan dalam sistem file bank. Beberapa aspek yang perlu dipertimbangkan dalam penerapan pengamanan file di Bank JABAR meliputi:

1. Kebijakan Akses:
   - Bank JABAR memiliki kebijakan akses yang ketat untuk mengatur hak akses pengguna terhadap file-file yang sensitif. Hal ini melibatkan pengaturan tingkat akses yang tepat berdasarkan peran dan tanggung jawab pengguna.
   - Mekanisme otentikasi, seperti penggunaan kata sandi yang kuat atau metode otentikasi ganda, dapat diterapkan untuk memastikan bahwa hanya pengguna yang sah yang dapat mengakses file tersebut.

2. Enkripsi Data:
   - Bank JABAR menerapkan teknik enkripsi untuk melindungi data yang disimpan dalam file. Enkripsi data melibatkan mengubah data menjadi format yang tidak dapat dibaca tanpa kunci dekripsi yang benar.
   - Enkripsi diterapkan baik saat data sedang berpindah (misalnya, saat mentransfer file melalui jaringan) maupun saat data berada dalam keadaan diam (misalnya, saat disimpan dalam penyimpanan fisik atau sistem penyimpanan).

3. Backup dan Pemulihan:
   - Bank JABAR memiliki kebijakan dan prosedur backup yang ketat untuk melindungi file dari kerusakan atau kehilangan yang tidak terduga. Backup

yang teratur harus dilakukan, dan salinan cadangan harus disimpan di lokasi yang aman dan terpisah dari sistem utama.

- Selain itu, prosedur pemulihan yang efektif harus disiapkan agar data dapat dipulihkan dengan cepat dalam situasi darurat atau kejadian tak terduga.

4. Penghapusan Data yang Aman:
   - Bank JABAR mengadopsi kebijakan dan prosedur penghapusan data yang aman untuk menghilangkan file yang tidak lagi diperlukan atau yang sudah mencapai batas retensi.
   - Penghapusan data dilakukan dengan menggunakan metode penghapusan permanen yang memastikan bahwa data tidak dapat dipulihkan oleh pihak yang tidak berwenang.

5. Audit dan Pemantauan:
   - Bank JABAR perlu melakukan pemantauan dan audit terhadap aktivitas file untuk mendeteksi aktivitas yang mencurigakan atau tidak sah. Pemantauan ini dapat dilakukan melalui penggunaan alat pemantauan keamanan, seperti sistem deteksi intrusi atau alat pemantauan integritas file.
   - Log akses file dan aktivitas pengguna juga menganalisis secara teratur untuk mengidentifikasi pola atau indikator kegiatan yang mencurigakan.

C. Penerapan Pengamanan *cyber* pada Bank JABAR

Pengamanan *cyber* melibatkan implementasi sistem pemantauan dan deteksi ancaman yang canggih, firewall, sistem deteksi intrusi, dan kebijakan keamanan yang ketat. Bank JABAR mungkin juga memiliki prosedur tanggap darurat dan rencana pemulihan untuk menghadapi serangan *cyber*. Penerapan pengamanan cyber pada Bank JABAR sangat penting untuk melindungi sistem dan data dari serangan dan ancaman siber. Beberapa langkah yang dapat diambil dalam penerapan pengamanan cyber pada Bank JABAR meliputi:

- Kebijakan Keamanan:

Bank JABAR memiliki kebijakan keamanan yang jelas dan komprehensif yang mencakup aspek-aspek seperti penggunaan sandi yang kuat, penggunaan perangkat lunak yang terbaru, kebijakan akses jaringan, dan pengelolaan izin pengguna.
Kebijakan ini harus diperbarui secara teratur sesuai dengan perkembangan terbaru dalam ancaman keamanan dan perubahan regulasi.

- Firewall:
  Bank JABAR mengimplementasikan firewall yang kuat untuk melindungi jaringan dari serangan eksternal yang tidak sah. Firewall ini dikonfigurasi dengan benar untuk mengontrol lalu lintas masuk dan keluar serta menerapkan kebijakan akses yang sesuai.

- Sistem Deteksi Intrusi (IDS) dan Sistem Pencegahan Intrusi (IPS):
  Bank JABAR menggunakan sistem deteksi intrusi dan sistem pencegahan intrusi untuk mendeteksi dan mencegah serangan siber yang mencurigakan. Sistem ini diperbarui secara berkala dan dikonfigurasi dengan aturan dan kebijakan yang relevan untuk mengidentifikasi dan merespons serangan potensial.

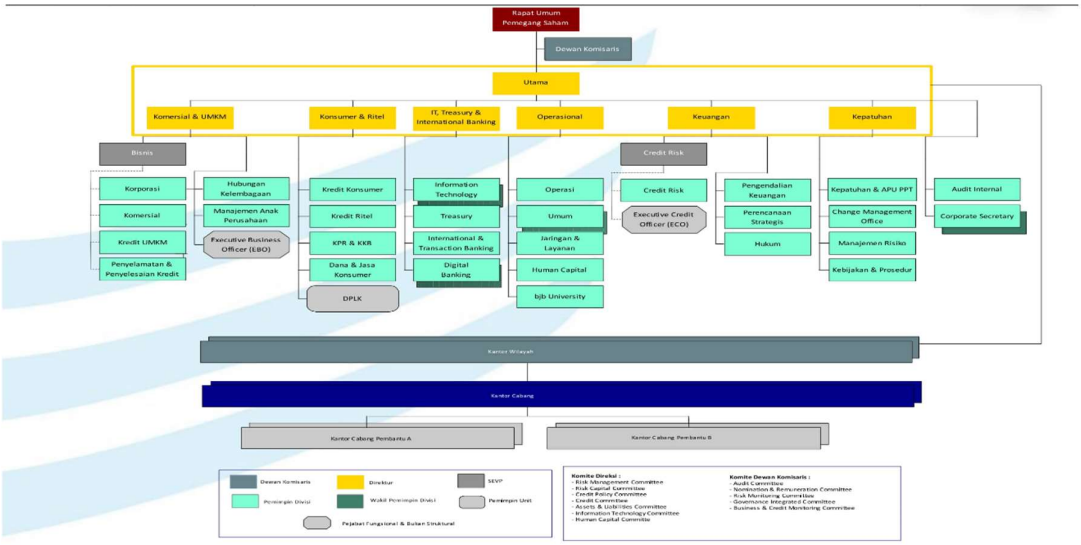
- Pemantauan Jaringan:
  Bank JABAR melakukan pemantauan jaringan secara terus-menerus untuk mendeteksi aktivitas yang mencurigakan atau tidak sah. Pemantauan ini dapat melibatkan penggunaan alat pemantauan jaringan yang canggih untuk menganalisis lalu lintas jaringan dan mengidentifikasi ancaman yang mungkin terjadi.

- Pembaruan Keamanan:
  Bank JABAR secara teratur memperbarui perangkat lunak, sistem operasi, dan aplikasi mereka dengan patch keamanan terbaru. Pembaruan ini diperlukan untuk memperbaiki kerentanan yang diketahui dan melindungi sistem dari serangan yang memanfaatkannya.

- Kesadaran dan Pelatihan Karyawan:

Bank JABAR memberikan pelatihan keamanan yang teratur kepada karyawan untuk meningkatkan kesadaran mereka tentang ancaman keamanan cyber dan praktik terbaik dalam penggunaan teknologi. Karyawan juga diberi tahu tentang tindakan pencegahan yang harus diambil, seperti menghindari mengklik tautan atau lampiran yang mencurigakan dan melaporkan aktivitas yang mencurigakan.

Berikut adalah struktur organisasi pada Bank JABAR:



Gambar 1: Struktur Organisasi Bank JABAR

Sumber: Website Resmi Bank Jabar (https://www.bankbjb.co.id/: 2023)

KESIMPULAN

Berdasarkan uraian yang didapatkan dapat disimpulkan bahwa dalam suatu organisasi yang memuat banyak data public seperti Bank misalnya diperlukan adanya pengamanan dalam objek vital, file maupun cyber. Bank JABAR menerapakan ketiga poin tersebt guna melindungi data nasabah dan berbagai komponen penting yang terdapat didalamnya. Adapun dalam penerapan objek vital melibatkan pemantauan dan pengendalian akses, penggunaan enkripsi data, dan pengamanan fisik terhadap infrastruktur yang penting. Sedangkan pengamanan file menggunakan enkripsi data dan pada pengamanan cyber sangat penting diperkuat guna melindungi system dari serangan.

DAFTAR REFERENSI

Edy Soesanto, D. (2023). Determinasi Sistem Manajemen Sekuriti: Analisis Objek Vital, Pengamanan File Dan Pengamanan Cyber Pada Yayasan Publisher. Jurnal Ilmu Multi Disiplin.

Jayana, M. A. (2022). Implementasi Pengamanan Data Pengarsipan Dengan Metode Algoritma Kriptografi Aes Studi Kasus Pada Bank Bjb Kcp Pasteur Bandng. Prosiding Seminar Sosial Politik, Bisnis, Akuntansi Dan Teknik (Sobat) Ke-4 Bandung.

https://www.bankbjb.co.id

Sugiyono. (2018). Metode Penelitian Kombinasi (Mixed Methods). Jakarta: Cv Alfabeta.

Vickky Tandaju, D. (2021). Implementasi Pengamanan Objek Vital Oleh Kepolisian Daerah Sulawesi Utara Di Kota Manado. Agrisosioekonomi.