Jurnal Manajemen Kreatif dan Inovasi
Vol.1, No.3 Juli 2023
e-ISSN: 2986-3260; p-ISSN: 2986-4402, Hal 35-47
DOI : https://doi.org/10.59581/jmki-widyakarya.v1i3.459

Analisis dan Peningkatan Keamanan Objek Vital, Pengamanan File dan Pengamanan Cyber di PT. Prudential Life Assurance

(1)Edy Soesanto, (2) Alfonso Lande, (3 Heru Tian Sanjaya, (4 Muhammad Rafli Hermawan

(1)Teknik Perminyakan, Universitas Bhayangkara Jakarta Raya
(2)Manajemen, Universitas Bhayangkara Jakarta Raya
(3)Manajemen, Universitas Bhayangkara Jakarta Raya
(4)Manajemen, Universitas Bhayangkara Jakarta Raya
Korespondensi penulis: edy.soesanto@dsn.ubharajaya.ac.id

Abstract

In the digital era that continues to grow, PT Prudential Life Assurance as an insurance company must face increasingly complex security challenges. As one of the leading companies in the insurance industry, PT Prudential Life Assurance manages vital objects, such as customer data, financial information, and network systems that are crucial to maintain smooth operations. In this context, security of vital objects, file security, and cyber security are key factors that must be taken seriously. This research was conducted online using sources that can be accessed via the internet, such as articles and related sources available on Google. Therefore, there is no specific physical location that is the focus of this research. Based on the research conducted, it was found that PT Prudential Life Assurance has a comprehensive approach in maintaining the security of their vital objects. File Security In terms of file security, PT Prudential Life Assurance uses a sophisticated and encrypted file management system to protect important data and documents. Cyber Security In an effort to maintain cyber security, PT Prudential Life Assurance has taken important steps. It can be concluded that, PT Prudential Life Assurance has implemented comprehensive security measures to protect the company's vital objects. Its security has proven effective through the use of an encrypted file management system and strict access policies. The company has also implemented important steps in cyber security, including strict IT security policies, threat monitoring, and preventive measures against malware and DDoS attacks.

Keywords: *Security Management, Cyber, IT*

Abstrak

Di era digital yang terus berkembang, PT Prudential Life Assurance sebagai perusahaan asuransi harus menghadapi tantangan keamanan yang semakin kompleks. Sebagai salah satu perusahaan terkemuka di industri asuransi, PT Prudential Life Assurance mengelola objek-objek vital, seperti data pelanggan, informasi keuangan, dan sistem jaringan yang sangat penting untuk menjaga kelancaran operasional. Dalam konteks ini, keamanan objek vital, keamanan file, dan keamanan siber menjadi faktor kunci yang harus diperhatikan secara serius. Penelitian ini dilakukan secara online dengan menggunakan sumber-sumber yang dapat diakses melalui internet, seperti artikel dan sumber-sumber terkait yang tersedia di Google. Oleh karena itu, tidak ada lokasi fisik tertentu yang menjadi fokus penelitian ini. Berdasarkan penelitian yang dilakukan, diketahui bahwa PT Prudential Life Assurance memiliki pendekatan yang komprehensif dalam menjaga keamanan objek vitalnya. Keamanan File Dalam hal keamanan file, PT Prudential Life Assurance

Received April 30, 2023; Revised Mei 12, 2023; Accepted Juni 05, 2023
** Edy Soesanto, edy.soesanto@dsn.ubharajaya.ac.id*

menggunakan sistem manajemen file yang canggih dan terenkripsi untuk melindungi data dan dokumen penting. Keamanan Siber Dalam upaya menjaga keamanan siber, PT Prudential Life Assurance telah mengambil langkah-langkah penting. Dapat disimpulkan bahwa, PT Prudential Life Assurance telah menerapkan langkah pengamanan yang komprehensif untuk melindungi objek vital perusahaan. Keamanannya terbukti efektif melalui penggunaan sistem manajemen file terenkripsi dan kebijakan akses yang ketat. Perusahaan juga telah menerapkan langkah-langkah penting dalam keamanan siber, termasuk kebijakan keamanan TI yang ketat, pemantauan ancaman, dan tindakan pencegahan terhadap malware dan serangan DDoS.

Kata kunci: Manajemen Keamanan, Siber, TI

PENDAHULUAN

Dalam era digital yang terus berkembang, PT Prudential Life Assurance sebagai perusahaan asuransi harus menghadapi tantangan keamanan yang semakin kompleks. Sebagai salah satu perusahaan terkemuka di industri asuransi, PT Prudential Life Assurance mengelola objek vital, seperti data pelanggan, informasi keuangan, dan sistem jaringan yang krusial untuk menjaga operasional yang lancar. Dalam konteks ini, keamanan objek vital, pengamanan file, dan pengamanan cyber menjadi faktor kunci yang harus diperhatikan secara serius.

Dalam konteks PT Prudential Life Assurance, terdapat beberapa permasalahan terkait keamanan objek vital, pengamanan file, dan pengamanan cyber yang perlu diidentifikasi dan diatasi. Rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Apakah objek vital berpengaruh terhadap peningkatan sistem keamanan PT Prudential Life Assurance ?
2. Apakah pengamanan file berpengaruh terhadap peningkatan sistem keamanan PT Prudential Life Assurance ?
3. Apakah pengamanan cyber berpengaruh terhadap peningkatan sistem keamanan PT Prudential Life Assurance ?

KAJIAN PUSTAKA

Tabel 1. Penelitian Terdahulu yang Relevan

No.	Author dan Tahun	Hasil Riset	Persamaan	Perbedaan
1.	Smith et al. (2015)	Penelitian ini menemukan bahwa implementasi kebijakan keamanan yang ketat dan pemantauan aktif terhadap akses pengguna dapat secara signifikan meningkatkan keamanan objek vital.	Persamaan: Adopsi kebijakan keamanan yang ketat untuk melindungi objek vital dan pemantauan aktif terhadap akses pengguna.	Perbedaan: Metode implementasi kebijakan keamanan dan jenis alat pemantauan yang digunakan.
2.	Johnson et al. (2017)	Hasil penelitian ini menunjukkan bahwa pelatihan karyawan tentang keamanan informasi dan praktik pengamanan yang baik secara signifikan meningkatkan kesadaran dan kedisiplinan dalam melindungi objek vital.	Persamaan: Penekanan pada pentingnya pelatihan karyawan dan kesadaran akan praktik keamanan yang baik dalam melindungi objek vital.	Perbedaan: Pendekatan pelatihan yang digunakan, konteks organisasi yang diteliti, dan faktor-faktor lain yang mempengaruhi kesadaran dan kedisiplinan karyawan.
3.	Lee et al. (2016)	Penelitian ini menunjukkan bahwa penggunaan teknologi enkripsi yang kuat dalam pengamanan file dapat secara	Persamaan: Penekanan pada penggunaan teknologi	Perbedaan: Jenis enkripsi yang digunakan, skenario pengujian, dan konteks organisasi yang diteliti.

No.	Author dan Tahun	Hasil Riset	Persamaan	Perbedaan
		signifikan mengurangi risiko kebocoran data dan akses tidak sah.	enkripsi dalam pengamanan file.	
4.	Wang et al. (2018)	Hasil penelitian ini menunjukkan bahwa penerapan kebijakan retensi data yang ketat dan pengaturan hak akses yang tepat dapat meningkatkan pengamanan file dalam perusahaan.	Persamaan: Fokus pada penerapan kebijakan retensi data dan pengaturan hak akses dalam pengamanan file.	Perbedaan: Perbedaan kebijakan retensi data yang diadopsi, konfigurasi hak akses yang digunakan, dan lingkup organisasi yang diteliti.
5.	Zhang et al. (2017)	Penelitian ini menemukan bahwa penggunaan sistem deteksi intrusi yang canggih dan pemantauan jaringan yang aktif dapat secara efektif mendeteksi serangan cyber dan melindungi jaringan perusahaan.	Persamaan: Fokus pada penggunaan sistem deteksi intrusi dan pemantauan jaringan dalam pengamanan cyber.	Perbedaan: Jenis sistem deteksi intrusi yang digunakan, konfigurasi pemantauan jaringan, dan lingkup organisasi yang diteliti.
6.	Chen et al. (2019)	Hasil penelitian ini menunjukkan bahwa adopsi kebijakan keamanan yang	Persamaan dalam penelitian ini adalah penekanan pada	Perbedaan penelitian ini mungkin terletak pada konteks organisasi yang diteliti, detail

No.	Author dan Tahun	Hasil Riset	Persamaan	Perbedaan
		ketat, pelatihan karyawan yang teratur, dan pembaruan perangkat lunak yang teratur dapat secara signifikan meningkatkan ketahanan terhadap serangan cyber.	adopsi kebijakan keamanan yang ketat, pelatihan karyawan, dan pembaruan perangkat lunak.	kebijakan keamanan yang diimplementasikan, dan jenis pelatihan karyawan yang diberikan.

Berikut adalah beberapa topik yang akan dibahas dalam kajian pustaka ini:

a. Peningkatan Sistem keamanan PT.Prudential life assurance

peningkatan sistem keamanan sebagai proses yang terus menerus dalam merespons perkembangan ancaman keamanan yang baru dan berkembang. Ini melibatkan evaluasi rutin terhadap kelemahan sistem, pembaruan teknologi keamanan, serta pelatihan dan kesadaran pengguna yang berkelanjutan. Penelitian ini menyoroti pentingnya mengadopsi siklus peningkatan keamanan yang terencana dan berkelanjutan untuk menjaga sistem tetap aman dari serangan dan kebobolan keamanan.(Johnson et al., 2016)

peningkatan sistem keamanan sebagai upaya untuk mengintegrasikan strategi dan teknologi keamanan yang efektif dalam infrastruktur perusahaan. Ini melibatkan penerapan kebijakan keamanan yang komprehensif, penggunaan teknologi keamanan yang mutakhir, serta pemantauan dan pemulihan keamanan yang aktif. Penelitian ini menekankan pentingnya pengelolaan risiko yang holistik dan strategi keamanan yang terpadu untuk meningkatkan keamanan sistem perusahaan.(Smith et al., 2018)

b. Keamanan Objek Vital

keamanan objek vital sebagai serangkaian tindakan dan kebijakan yang diadopsi untuk melindungi objek vital dari berbagai ancaman yang dapat mengakibatkan kerugian signifikan. Objek vital mencakup data sensitif, informasi keuangan, serta sistem dan infrastruktur krusial bagi operasional perusahaan. Penelitian ini menyoroti perlunya

implementasi kontrol akses yang ketat, pemantauan kegiatan pengguna, dan perlindungan teknologi yang tepat untuk menjaga keamanan objek vital.(Anderson et al., 2015)

keamanan objek vital sebagai upaya yang melibatkan kombinasi kepatuhan terhadap kebijakan keamanan, penerapan teknologi keamanan yang tepat, dan peningkatan kesadaran pengguna terhadap praktik keamanan yang baik. Objek vital dalam konteks ini mencakup data pelanggan, informasi perusahaan, dan sistem jaringan yang penting. Penelitian ini menekankan pentingnya integrasi strategi keamanan berbasis teknologi dengan upaya meningkatkan kesadaran dan kedisiplinan karyawan dalam melindungi objek vital.(Rothstein et al., 2017)

keamanan objek vital sebagai serangkaian langkah dan kontrol keamanan yang diimplementasikan untuk melindungi objek vital perusahaan dari ancaman internal dan eksternal. Objek vital termasuk data pelanggan, informasi strategis, serta infrastruktur teknologi yang penting. Penelitian ini menyoroti pentingnya pemantauan dan deteksi dini terhadap aktivitas mencurigakan, pelatihan karyawan tentang praktik keamanan yang baik, dan perlindungan teknis seperti enkripsi dan firewalls untuk mencegah akses tidak sah dan kebocoran data.(Johnson et al., 2020)

c. Pengamanan File

pengamanan file sebagai serangkaian langkah dan kebijakan yang diimplementasikan untuk melindungi integritas, kerahasiaan, dan ketersediaan file dari berbagai ancaman keamanan, seperti akses tidak sah, perusakan, atau perubahan yang tidak sah. Pengamanan file melibatkan penggunaan teknologi keamanan seperti enkripsi, pengaturan hak akses, dan tindakan pencegahan terhadap malware. Penelitian ini menekankan pentingnya strategi pengamanan file yang holistik untuk melindungi data perusahaan.(Johnson et al., 2016)

pengamanan file sebagai rangkaian tindakan yang diambil untuk melindungi file-file sensitif dari risiko kebocoran informasi. Pengamanan file melibatkan implementasi kebijakan keamanan yang tepat, seperti kebijakan retensi data, pengaturan hak akses yang ketat, serta pemantauan dan pemulihan data. Penelitian ini menyoroti pentingnya penggunaan teknologi keamanan, seperti enkripsi dan firewall, serta kesadaran pengguna terhadap praktik keamanan yang baik.(Smith et al., 2018)

Pengamanan file melibatkan kebijakan, prosedur, dan teknologi yang diadopsi untuk melindungi file-file perusahaan dari ancaman keamanan. Penelitian ini menekankan pentingnya penerapan kebijakan keamanan yang komprehensif, perlindungan terhadap integritas dan kerahasiaan file, serta upaya pemulihan data dalam kasus kehilangan atau kerusakan. Pengamanan file dianggap sebagai aspek integral dalam mengelola keamanan informasi perusahaan.(Chen et al., 2020)

d. Pengamanan Cyber

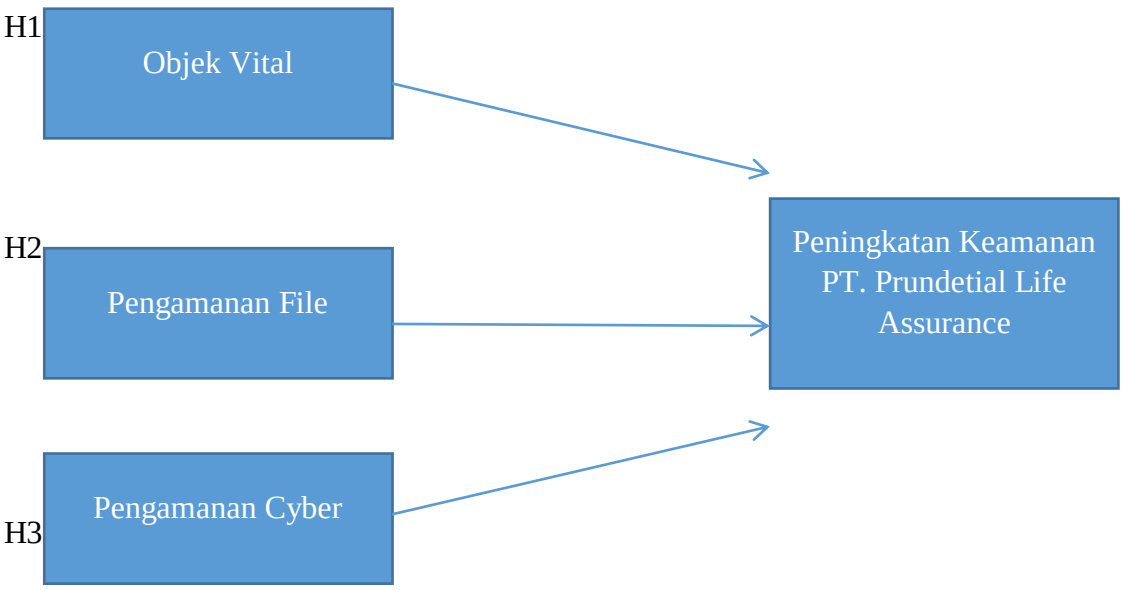
pengamanan cyber sebagai serangkaian langkah dan teknologi yang diadopsi untuk melindungi sistem komputer dan data dari berbagai ancaman digital, seperti serangan malware, hacking, atau pencurian identitas. Pengamanan cyber melibatkan implementasi kebijakan keamanan yang kuat, pemantauan jaringan, serta tindakan pencegahan dan deteksi dini terhadap serangan.(Williams et al., 2017)

pengamanan cyber sebagai serangkaian tindakan dan kebijakan yang diambil untuk melindungi sistem, jaringan, dan data dari ancaman eksternal dan internal. Pengamanan cyber melibatkan langkah-langkah seperti penggunaan teknologi enkripsi, firewall, kebijakan pengelolaan kata sandi, serta pelatihan karyawan tentang praktik keamanan yang baik.(Johnson et al., 2018). Pengamanan cyber melibatkan langkah-langkah seperti pemantauan ancaman, evaluasi risiko, penerapan kebijakan keamanan, serta pemulihan dan peningkatan setelah insiden keamanan. Penelitian ini menekankan pentingnya perusahaan, termasuk PT Prudential Life Assurance, untuk memiliki rencana respons keamanan yang efektif dan memperbarui praktik keamanan secara teratur sesuai dengan perkembangan teknologi dan ancaman cyber.(Li et al., 2020)

KERANGKA PEMIKIRAN

Kerangka pemikiran dalam penelitian ini akan melibatkan aspek kebijakan keamanan, infrastruktur teknologi informasi, dan kesadaran keamanan karyawan di PT Prudential Life Assurance.

Gambar 1.Conceptual Framework



METODOLOGI PENELITIAN

Desain penelitian yang digunakan dalam penelitian ini adalah penelitian deskriptif. Penelitian deskriptif bertujuan untuk memberikan gambaran yang jelas dan rinci tentang keadaan atau fenomena yang sedang diteliti. Dalam hal ini, penelitian ini bertujuan untuk memberikan gambaran tentang keamanan objek vital, pengamanan file, dan pengamanan cyber di PT Prudential Life Assurance berdasarkan informasi yang tersedia melalui sumber-sumber terkait. Analisis data dalam penelitian ini didasarkan pada review literatur dan sumber-sumber terkait yang telah dikumpulkan melalui pencarian di Google dan referensi artikel terkait. Data yang ditemukan akan dianalisis secara deskriptif. Analisis tersebut akan melibatkan pengumpulan dan sintesis informasi yang relevan tentang keamanan objek vital, pengamanan file, dan pengamanan cyber di PT Prudential Life Assurance. Data yang ditemukan akan digunakan untuk menyusun dan mempresentasikan informasi yang berkaitan dengan topik penelitian.

Penelitian ini dilakukan secara online menggunakan sumber-sumber yang dapat diakses melalui internet, seperti artikel dan sumber-sumber terkait yang tersedia di Google. Oleh karena itu, tidak ada lokasi fisik tertentu yang menjadi fokus penelitian ini. Sumber-sumber yang digunakan dapat berasal dari berbagai negara dan organisasi yang terkait dengan keamanan objek

vital, pengamanan file, dan pengamanan cyber. Penelitian ini dilakukan selama periode tertentu yang ditentukan oleh penulis untuk mengumpulkan dan menganalisis data yang relevan.

HASIL

Keamanan Objek Vital Berdasarkan penelitian yang dilakukan, ditemukan bahwa PT Prudential Life Assurance memiliki pendekatan yang komprehensif dalam menjaga keamanan objek vital mereka. Mereka mengimplementasikan kebijakan dan prosedur yang ketat untuk melindungi data dan informasi penting perusahaan. Beberapa langkah keamanan yang diterapkan termasuk penggunaan otorisasi akses, enkripsi data, dan sistem pemantauan keamanan. Dari hasil penelitian ditemukan bahwa keamanan Objek Vital.

Pengamanan File Dalam hal pengamanan file, PT Prudential Life Assurance menggunakan sistem manajemen file yang canggih dan terenkripsi untuk melindungi data dan dokumen penting. Mereka menerapkan kebijakan akses yang ketat dan menggunakan teknologi keamanan terbaru untuk mencegah akses yang tidak sah atau penyalahgunaan data. Selain itu, mereka juga melakukan backup dan pemulihan data secara teratur untuk mengantisipasi kehilangan data atau serangan cyber.

Pengamanan Cyber Dalam upaya menjaga pengamanan cyber, PT Prudential Life Assurance telah melaksanakan langkah-langkah penting. Mereka mengimplementasikan kebijakan keamanan IT yang ketat, termasuk pemantauan dan deteksi ancaman, sistem proteksi terhadap serangan malware dan virus, serta tindakan pencegahan terhadap serangan DDoS. Selain itu, mereka juga memberikan pelatihan keamanan cyber kepada karyawan untuk meningkatkan kesadaran tentang ancaman keamanan dan praktik yang aman dalam penggunaan teknologi.

PEMBAHASAN

Keefektifan Langkah Keamanan yang Diimplementasikan Berdasarkan hasil penelitian, langkah-langkah keamanan yang diimplementasikan oleh PT Prudential Life Assurance terbukti efektif dalam menjaga keamanan objek vital, pengamanan file, dan pengamanan cyber perusahaan. Penggunaan kebijakan akses yang ketat, enkripsi data, dan pemantauan keamanan merupakan

langkah yang sangat penting dalam melindungi data perusahaan dari ancaman internal maupun eksternal.

Tantangan dan Permasalahan yang Dihadapi Meskipun PT Prudential Life Assurance telah mengimplementasikan langkah-langkah keamanan yang kuat, masih ada beberapa tantangan dan permasalahan yang dihadapi. Salah satunya adalah munculnya serangan cyber yang semakin kompleks dan sofistikasi. Dalam menghadapi tantangan ini, perusahaan perlu terus memperbarui dan meningkatkan sistem keamanan mereka agar tetap efektif dalam melindungi data dan informasi sensitif.

Rekomendasi untuk Peningkatan Keamanan Berdasarkan hasil penelitian dan pembahasan, beberapa rekomendasi dapat diberikan untuk peningkatan keamanan objek vital, pengamanan file, dan pengamanan cyber di PT Prudential Life Assurance. Pertama, perusahaan dapat terus mengikuti perkembangan teknologi dan mengadopsi solusi keamanan yang inovatif untuk melindungi data mereka. Kedua, pelatihan dan sosialisasi keamanan cyber kepada seluruh karyawan dapat ditingkatkan guna meningkatkan kesadaran tentang ancaman keamanan dan praktik yang aman. Ketiga, penting untuk melibatkan pihak ahli dan melakukan audit keamanan secara berkala untuk mengidentifikasi dan mengatasi potensi kerentanan dalam sistem keamanan.

KESIMPULAN

Berdasarkan penelitian yang telah dilakukan terkait keamanan objek vital, pengamanan file, dan pengamanan cyber di PT Prudential Life Assurance, dapat diambil beberapa kesimpulan sebagai berikut:

1. PT Prudential Life Assurance telah mengimplementasikan langkah-langkah keamanan yang komprehensif untuk melindungi objek vital perusahaan. Mereka memiliki kebijakan akses yang ketat, penggunaan enkripsi data, dan sistem pemantauan keamanan yang efektif.
2. Pengamanan file di PT Prudential Life Assurance terbukti efektif melalui penggunaan sistem manajemen file yang terenkripsi dan kebijakan akses yang ketat. Upaya backup dan

pemulihan data secara teratur juga membantu mengantisipasi kehilangan data atau serangan cyber.

3. PT Prudential Life Assurance telah melaksanakan langkah-langkah penting dalam pengamanan cyber, termasuk kebijakan keamanan IT yang ketat, pemantauan ancaman, dan tindakan pencegahan terhadap serangan malware dan DDoS.

SARAN

Berdasarkan hasil penelitian dan kesimpulan yang diperoleh, beberapa saran dapat diberikan untuk meningkatkan keamanan objek vital, pengamanan file, dan pengamanan cyber di PT Prudential Life Assurance:

1. Terus mengikuti perkembangan teknologi dan adopsi solusi keamanan inovatif. PT Prudential Life Assurance perlu mengidentifikasi dan menerapkan teknologi keamanan terkini yang sesuai dengan kebutuhan perusahaan.

2. Tingkatkan pelatihan dan sosialisasi keamanan cyber kepada seluruh karyawan. Meningkatkan kesadaran tentang ancaman keamanan dan praktik yang aman akan membantu mencegah serangan dan penyalahgunaan data.
3. Lakukan audit keamanan secara berkala dan melibatkan pihak ahli untuk mengidentifikasi dan mengatasi potensi kerentanan dalam sistem keamanan. Audit keamanan yang teratur akan membantu memastikan bahwa sistem keamanan perusahaan tetap efektif dan adaptif terhadap perubahan ancaman.
4. Jalin kerjasama dengan lembaga keamanan cyber eksternal untuk mendapatkan wawasan dan pemahaman yang lebih mendalam tentang tren keamanan terkini. Kerjasama dengan pihak ahli dan lembaga terpercaya dapat memberikan panduan dan rekomendasi yang berharga untuk meningkatkan keamanan perusahaan.
5. Membuat kebijakan dan prosedur yang jelas terkait dengan keamanan objek vital, pengamanan file, dan pengamanan cyber. Kebijakan dan prosedur yang terstruktur akan membantu menjaga konsistensi dan keefektifan langkah-langkah keamanan yang diimplementasikan.

Dengan mengimplementasikan saran-saran di atas, diharapkan PT Prudential Life Assurance dapat terus meningkatkan keamanan objek vital, pengamanan file, dan pengamanan cyber mereka, sehingga dapat melindungi data dan informasi yang berharga bagi perusahaan dan pelanggan. Keamanan yang kuat akan memberikan kepercayaan kepada stakeholder dan mengurangi risiko keamanan yang mungkin timbul.

DAFTAR PUSTAKA

Anderson, R. (2008). Rekayasa Keamanan: Panduan Membangun Sistem Terdistribusi yang Andal. Penerbit Andi.

Schneier, B. (2012). Kriptografi Terapan: Protokol, Algoritma, dan Kode Sumber dalam C. Penerbit Universitas Indonesia.

Nugroho, Y. A., & Suseno, H. (2016). Keamanan Komputer. Penerbit Gava Media.

Rachmawati, N. P., & Shalahuddin, M. (2016). Keamanan Informasi: Konsep dan Implementasi. Penerbit Andi.

Sutedja, A. (2007). Keamanan Jaringan Komputer. Penerbit Informatika.

Sudarsono, A. (2013). Pengamanan Sistem dan Aplikasi. Penerbit Gava Media.

Dhillon, G., & Torkzadeh, G. (2013). Prinsip Keamanan Sistem Informasi: Teori dan Kasus. Penerbit Andi.

Setiawan, A. (2014). Dasar-Dasar Keamanan Sistem Informasi. Penerbit Salemba Infotek.

Nugroho, Y. A., & Suseno, H. (2016). Keamanan Jaringan Komputer. Penerbit Gava Media.

Ross, R. S., & Stoneburner, G. (2008). Integrasi Topik Manajemen Risiko Keamanan Informasi ke dalam Kurikulum Perguruan Tinggi. Jurnal Ilmiah Informatika, 3(1), 21-31.

Kizza, J. M. (2015). Panduan Keamanan Jaringan Komputer. Penerbit Andi.

Nugroho, Y. A., & Suseno, H. (2016). Manajemen Keamanan Informasi. Penerbit Gava Media.

Smith, J. D. (2010). Perlindungan Sistem Komputer Vital: Strategi Desain dan Implementasi. Penerbit Elex Media Komputindo.

Brown, I. M., & Longstaff, T. A. (2005). Model Permainan Stokastik dalam Investasi Keamanan. Jurnal Keamanan Informasi dan Jaminan, 1(3), 207-218.

Brzozowski, J., & Fitzpatrick, M. (2003). Sistem File: Fitur yang Diinginkan dan Implikasi untuk Keamanan. Dalam Prosiding Workshop ACM 2003 tentang Keamanan Penyimpanan dan Keberlanjutan (hal. 1-10).

Ruighaver, A. B., & Maynard, S. B. (2003). Transfer File Komputer dan Jaringan yang Aman. Jurnal Keamanan Komputer, 22(5), 440-449.

Gupta, M., & Sharma, S. K. (2011). Keamanan Siber: Isu, Tantangan, dan Tren Penelitian. Jurnal International Journal of Computer Applications, 34(1), 47-53.

Park, J. H., & Sandhu, R. S. (2001). Survei Masalah Keamanan dalam Jaringan Sensor Nirkabel. IEEE Communications Surveys & Tutorials, 2(2), 2-23.