Journal of Information and Information Security (JIFORTY)
Vol. 5, No. 2, Desember 2024, 281-292
e-ISSN : 2722-4058
Available Online at http://ejurnal.ubharajaya.ac.id/index.php/jiforty

Keamanan File dalam Sistem Manajemen pada Mahasiswa Universitas Bhayangkara Jakarta Raya

Eka Dharma Putra [1,*], Ezra Hafiz Zachary [1], M Thariq Izaz [1], Nauval Arif Fadilah [1]

[1] Informatika; Universitas Bhayangkara Jakarta Raya; Jl. Raya Perjuangan No. 81 Marga Mulya, Bekasi Utara Jawa Barat, 17143, (021) 88955882,
202210715190@mhs.ubharajaya.ac.id, 202210715187@mhs.ubharajaya.ac.id,
202210715226@mhs.ubharajaya.ac.id, 202210715182@mhs.ubharajaya.ac.id

* Korespondensi: e-mail: 202210715190@mhs.ubharajaya.ac.id

Diterima: 8 Jan 25; Review: 8 Jan 25; Disetujui: 12 Jan 25; Diterbitkan: 12 Jan 25

Abstract

File security in information management systems is crucial to prevent data leakage, theft, and manipulation. Bhayangkara University, as an educational institution, stores essential data such as academic, financial, and administrative information that is vulnerable to security threats. This study aims to identify security risks in the university's management system and propose strategic solutions. Using a descriptive method and a case study approach, the research identifies major risks, including unauthorized access, malware attacks, and user negligence. Proposed solutions include data encryption, multi-layered authentication, and user training to enhance security awareness. Implementing these strategies is expected to significantly improve the overall system security.
***Keywords**: file security, information management system, security risks, data encryption, multi-layered authentication, user training, cyberattacks.*

Abstrak

Keamanan file dalam sistem manajemen informasi sangat penting untuk melindungi data dari risiko kebocoran, pencurian, atau manipulasi. Universitas Bhayangkara sebagai institusi pendidikan memiliki sistem manajemen yang menyimpan data akademik, keuangan, dan administrasi lainnya. Penelitian ini bertujuan untuk mengidentifikasi risiko keamanan file pada sistem manajemen Universitas Bhayangkara serta menawarkan solusi yang tepat. Dengan menggunakan metode deskriptif dan pendekatan studi kasus, penelitian ini menemukan beberapa risiko utama seperti akses tidak sah, serangan malware, dan kelalaian pengguna. Solusi yang diusulkan meliputi penerapan enkripsi data, sistem otentikasi berlapis, serta pelatihan pengguna. Implementasi strategi ini diharapkan dapat meningkatkan keamanan sistem secara keseluruhan.
***Kata kunci**: Keamanan file, sistem manajemen informasi, Universitas Bhayangkara, risiko keamanan, enkripsi data, otentikasi berlapis, pelatihan pengguna, serangan siber.*

1. Pendahuluan

Dalam era digital, sistem manajemen informasi telah menjadi tulang punggung operasional di berbagai sektor, termasuk dunia pendidikan. Perguruan tinggi, seperti Universitas Bhayangkara, mengandalkan sistem manajemen untuk mengelola data akademik, administrasi, keuangan, dan sumber daya manusia. Sistem ini tidak hanya membantu meningkatkan efisiensi,

tetapi juga memberikan kemudahan dalam penyimpanan, pengelolaan, dan akses data. Namun, di balik manfaat tersebut. keamanan data menjadi tantangan besar yang harus dihadapi (Sulaeman et al., 2023).

Keamanan file dalam sistem manajemen informasi menjadi isu yang semakin mendesak mengingat meningkatnya ancaman siber, seperti pencurian data, serangan malware, dan akses tidak sah. Data-data yang tersimpan di dalam sistem, seperti informasi pribadi mahasiswa, nilai akademik, laporan keuangan, hingga penelitian dosen, bersifat sensitif dan harus dijaga kerahasiaannya. Jika sistem ini tidak dilindungi dengan baik, konsekuensinya bisa sangat merugikan, baik bagi institusi maupun individu terkait (Edy Susanto et al., 2023).

Universitas Bhayangkara, sebagai salah satu institusi pendidikan tinggi, menghadapi tantangan serupa. Sistem manajemen yang digunakan universitas ini menyimpan data dalam jumlah besar dengan tingkat sensitivitas yang tinggi. Dalam beberapa kasus, institusi pendidikan menjadi target serangan karena seringkali memiliki celah keamanan yang belum sepenuhnya ditangani. Misalnya, kelalaian pengguna dalam menjaga kerahasiaan kata sandi atau kurangnya pembaruan pada sistem keamanan dapat membuka peluang bagi pihak tidak bertanggung jawab untuk mengakses atau merusak data (Novita Setyaningrum & Maria, 2024).

Seiring dengan berkembangnya teknologi, ancaman terhadap keamanan file semakin canggih. Oleh karena itu, Universitas Bhayangkara perlu mengidentifikasi risiko yang ada dan menerapkan solusi keamanan yang efektif untuk melindungi data dalam sistem manajemen mereka. Penelitian ini bertujuan untuk memberikan gambaran menyeluruh tentang risiko keamanan file dalam sistem manajemen Universitas Bhayangkara serta menawarkan rekomendasi solusi yang dapat diimplementasikan (Darmawan, 2024).

Penelitian ini memiliki urgensi yang tinggi, mengingat potensi kerugian yang dapat ditimbulkan jika keamanan data tidak dikelola dengan baik. Dengan pemahaman yang mendalam tentang ancaman yang ada dan penerapan langkah-langkah preventif yang memadai, Universitas Bhayangkara dapat memastikan bahwa data mereka tetap aman, sehingga mendukung keberlangsungan operasional universitas secara efektif dan efisien (Novianto et al., 2023).

Melalui penelitian ini, diharapkan dapat memberikan kontribusi dalam memperbaiki sistem keamanan file pada institusi pendidikan serta meningkatkan kesadaran akan pentingnya keamanan data bagi seluruh pihak yang terlibat, baik staf, mahasiswa, maupun pengelola system (Anggara, 2024).

2. Metode Penelitian

Penelitian ini menggunakan metode deskriptif kualitatif dengan pendekatan studi literatur dan survei. Tahapan penelitian yang dilakukan adalah sebagai berikut:

- **Pengumpulan Data:** Survei dilakukan melalui kuesioner yang diberikan kepada responden yang terdiri dari mahasiswa Universitas Bhayangkara.

- **Analisis Data:** Data dari studi literatur dianalisis untuk mengidentifikasi teori-teori pendukung dan praktik terbaik dalam keamanan file. Data survei dianalisis secara kualitatif dengan menggunakan metode tematik untuk menemukan pola, persepsi, dan potensi kelemahan dari sistem manajemen Universitas Bhayangkara.
- **Penyusunan Solusi:** Berdasarkan hasil studi literatur dan survei, solusi yang dirumuskan mencakup rekomendasi teknologi (seperti enkripsi dan otentikasi), kebijakan manajemen, serta program pelatihan untuk meningkatkan kesadaran pengguna.

3. Hasil dan Pembahasan

Identifikasi Risiko Keamanan Data

I. Identifikasi Risiko Keamanan

- **Ancaman Internal:** Mayoritas risiko berasal dari kelalaian pengguna, seperti penggunaan kata sandi yang lemah dan pengunduhan file dari sumber tidak terpercaya.
- **Ancaman Eksternal:** Serangan siber, termasuk malware dan ransomware, menjadi risiko utama yang dapat mengancam integritas dan kerahasiaan data.

II. Kesiapan Sistem

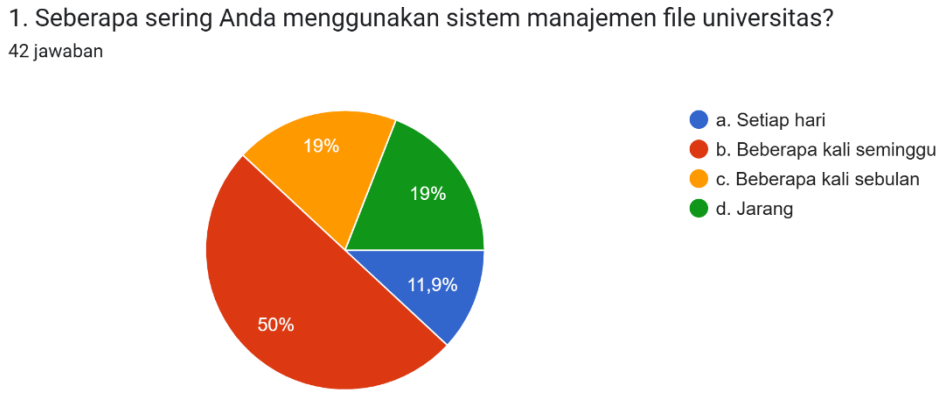
- Sistem manajemen informasi Universitas Bhayangkara memiliki perlindungan dasar seperti firewall dan antivirus. Namun, pembaruan perangkat lunak belum dilakukan secara rutin, sehingga masih ada kerentanan terhadap serangan terbaru.
- Proses backup data belum terintegrasi secara otomatis, sehingga berisiko kehilangan data dalam insiden tertentu.

III. Kesadaran Pengguna

- Hasil survei menunjukkan tingkat kesadaran pengguna terhadap keamanan data masih rendah. Pengguna cenderung abai terhadap risiko akibat tindakan mereka sendiri, seperti berbagi akses atau tidak memperhatikan protokol keamanan.

3.1. Penggunaan Manajemen File

Hasil ini menunjukkan bahwa sistem tersebut cukup sering digunakan oleh mayoritas responden. Namun, persentase pengguna yang jarang memanfaatkannya mengindikasikan perlunya evaluasi lebih lanjut untuk memahami hambatan penggunaan dan meningkatkan aksesibilitas system (Deva & Jayadi, 2022)



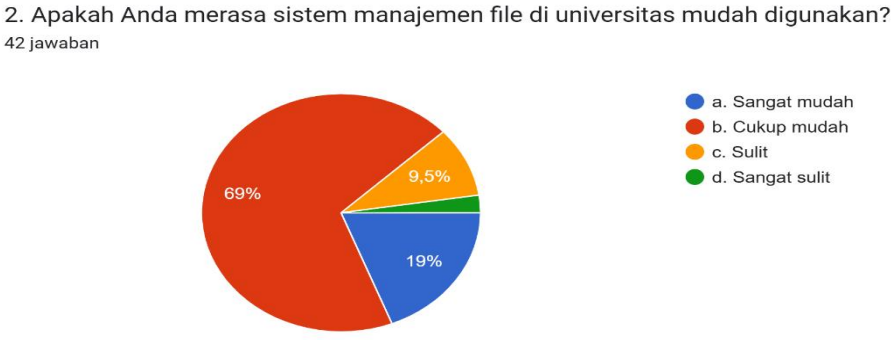
Sumber Hasil : Penelitian (2024)

Gambar 1. Pertanyaan No 1

Pada gambar 1 menunjukan Survei terhadap 42 responden menunjukkan bahwa **50% responden** menggunakan sistem manajemen file universitas **beberapa kali seminggu**, sedangkan **11,9%** menggunakannya **setiap hari**. Sebanyak **19%** responden menggunakan sistem ini **beberapa kali sebulan**, dan **19% lainnya** jarang menggunakannya.

3.2. Sistem Manajemen File

Hasil ini menunjukkan bahwa secara umum, sistem manajemen file universitas dianggap mudah digunakan oleh mayoritas responden. Namun, keberadaan responden yang mengalami kesulitan (sekitar 12%) mengindikasikan perlunya peningkatan antarmuka pengguna, panduan penggunaan, atau dukungan teknis untuk memastikan semua pengguna dapat memanfaatkan system secara optimal.



Sumber : Hasil Penelitian (2024)

Gambar 2. Pertanyaan No 2

Pada gambar 2 menunjukkan survei terhadap 42 responden mengenai kemudahan penggunaan sistem manajemen file universitas, mayoritas responden, yaitu 69%, menilai sistem

tersebut cukup mudah digunakan (opsi b). Sebanyak 19% responden merasa sistem ini sangat mudah digunakan (opsi a), sementara 9,5% menyatakan sistem ini sulit digunakan (opsi c), dan hanya 2,5% menilai sistem ini sangat sulit digunakan (opsi d).

3.3. kendala dalam megakses sistem file

Hasil ini mengindikasikan bahwa mayoritas responden menghadapi tantangan dalam menggunakan sistem tersebut. Hal ini bisa disebabkan oleh berbagai faktor, seperti gangguan teknis, keterbatasan akses, atau kurangnya panduan penggunaan. Sementara itu, responden yang tidak mengalami kendala menunjukkan bahwa sistem ini sudah cukup stabil dan mudah digunakan bagi sebagian pengguna.

Diperlukan evaluasi lebih lanjut untuk mengidentifikasi jenis kendala yang paling sering dialami dan memberikan solusi, seperti peningkatan infrastruktur atau layanan bantuan teknis, guna meningkatkan pengalaman pengguna secara keseluruhan**.**

Sumber : Hasil Penelitian (2024)

Gambar 3. Pertanyaan No 3

Pada gambar 3 menunjukan survei terhadap 42 responden menunjukkan bahwa **61,9% responden** pernah mengalami kendala dalam mengakses file di sistem manajemen universitas, sedangkan **38,1%** menyatakan tidak pernah mengalami kendala(Nikmat, 2024)

3.4. Resiko Keamanan Sistem Manajeman File

Hasil ini menunjukkan bahwa sebagian besar responden memiliki kesadaran akan pentingnya keamanan dalam pengelolaan file. Namun, persentase yang cukup signifikan (lebih dari sepertiga) yang belum menyadari risiko ini mengindikasikan adanya kebutuhan untuk meningkatkan pemahaman dan edukasi tentang topik tersebut (Febriani et al., 2024).

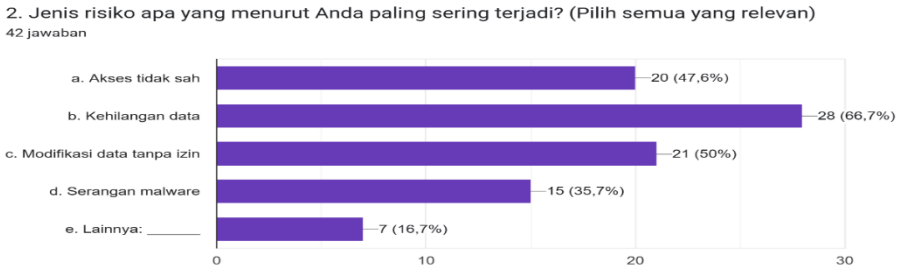
Sumber : Hasil Penelitian (2024)

Gambar 4. Pertanyaan No 1

. Pada gambar 4 menunjukan hasil survei yang melibatkan 42 responden, mayoritas peserta (64,3%) menyatakan bahwa mereka mengetahui risiko keamanan yang dapat terjadi pada sistem manajemen file. Sementara itu, sebanyak 35,7% responden mengaku belum memiliki pengetahuan terkait risiko tersebut (Soesanto et al., 2023).

3.5. Jenis Resiko Sistem Manajemen File

Hasil ini menunjukkan bahwa kehilangan data merupakan ancaman utama yang paling dikhawatirkan, diikuti oleh risiko terkait integritas dan akses data. Tingginya kekhawatiran ini menggarisbawahi pentingnya implementasi langkah-langkah keamanan seperti pencadangan data, pengendalian akses, dan perlindungan dari malware.



Sumber : Hasil Penelitian (2024)

Gambar 5. Pertanyaan 2

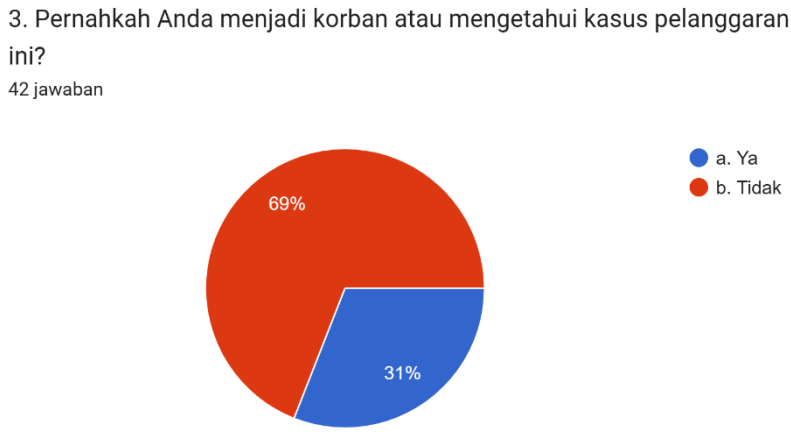
Pada gambar 5 menunjukan Survei mengenai jenis risiko keamanan pada sistem manajemen file menunjukkan hasil sebagai berikut:

1. Kehilangan data menjadi risiko paling sering terjadi, dipilih oleh 66,7% responden (28 orang).

2. Modifikasi data tanpa izin berada di urutan kedua, dengan 50% responden (21 orang) memilihnya.
3. Akses tidak sah juga menjadi perhatian signifikan, dipilih oleh 47,6% responden (20 orang).
4. Serangan malware mendapatkan perhatian dari 35,7% responden (15 orang).
5. Responden lainnya (16,7% atau 7 orang) menyebutkan risiko lain yang relevan.

3.6. Kasus Pelanggaran Keamanan Data sistem Manajemen File

Kasus-kasus pelanggaran ini dapat terjadi akibat akses tidak sah, kehilangan data, atau serangan malware, seperti yang juga diidentifikasi dalam survei sebelumnya. Oleh karena itu, penerapan langkah-langkah pencegahan seperti penggunaan enkripsi, sistem autentikasi yang kuat, dan edukasi pengguna menjadi krusial untuk meminimalkan risiko tersebut.
Temuan ini menggarisbawahi pentingnya upaya proaktif untuk meningkatkan keamanan data dan mencegah pelanggaran yang lebih luas di masa depan.



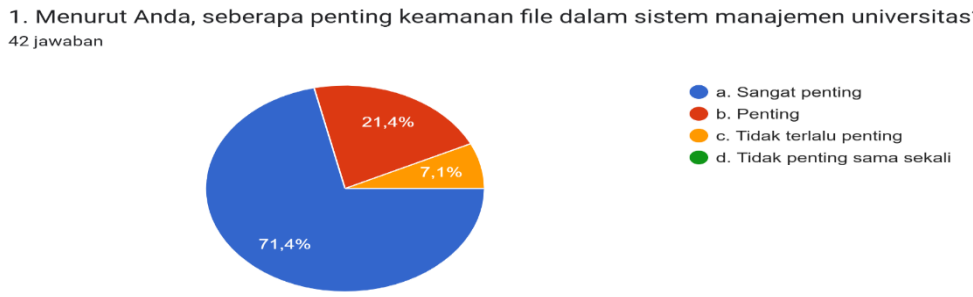
Sumber : Hasil Penelitian (2024)

Gambar 6. Pertanyaan No 3

Pada gambar 6 menunjukan hasil survei bahwa 31% responden pernah menjadi korban atau mengetahui kasus pelanggaran keamanan data pada sistem manajemen file. Sementara itu, 69% responden menyatakan tidak pernah mengalami atau mengetahui kasus tersebut.
Hasil ini menunjukkan bahwa meskipun mayoritas responden belum mengalami langsung atau mengetahui pelanggaran keamanan, persentase yang mengalami (31%) tetap signifikan. Ini menandakan bahwa risiko pelanggaran keamanan data adalah ancaman nyata yang memerlukan perhatian serius.

3.7. Pentingnya Manajemen File

Hasil survei ini mencerminkan urgensi penerapan sistem keamanan data yang kuat dalam lingkungan universitas. Sebagai institusi yang mengelola data pribadi mahasiswa, staf, dan dokumen akademik penting lainnya, universitas harus memastikan bahwa sistem manajemennya dilengkapi dengan langkah-langkah keamanan yang memadai. Implementasi seperti enkripsi data, sistem autentikasi yang kuat, dan pelatihan kesadaran keamanan bagi pengguna dapat menjadi langkah konkret untuk meningkatkan keamanan file.



Sumber : Hasil Penelitian (2024)

Gambar 7. Pertanyaan No 1

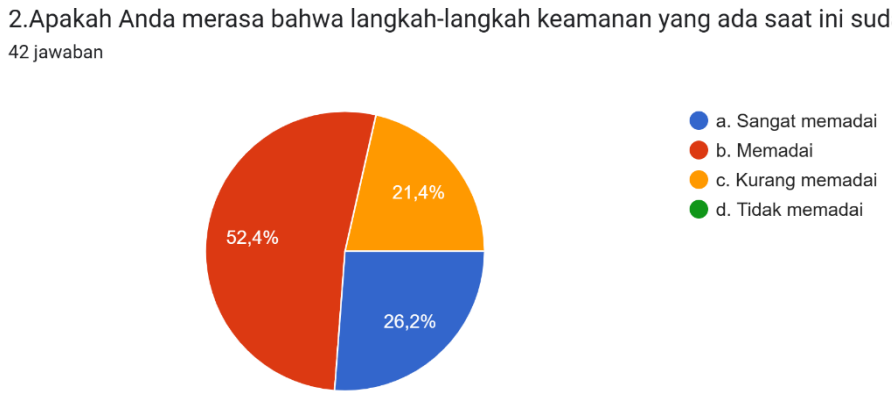
Pada gambar 7 menunjukan survei yang dilakukan terhadap 42 responden mengenai pentingnya keamanan file dalam sistem manajemen universitas, hasil yang diperoleh menunjukkan bahwa sebagian besar responden menganggap keamanan file sebagai aspek yang sangat penting. Berikut rincian hasilnya:

1. Sangat Penting (71,4%): Mayoritas responden menyatakan bahwa keamanan file dalam sistem manajemen universitas adalah hal yang sangat krusial. Hal ini menunjukkan kesadaran yang tinggi akan pentingnya menjaga kerahasiaan dan integritas data.
2. Penting (21,4%): Sebagian responden juga setuju bahwa keamanan file penting, meskipun tidak sampai menempatkannya dalam kategori yang sangat mendesak.
3. Tidak Terlalu Penting (7,1%): Sebagian kecil responden merasa bahwa keamanan file bukan prioritas utama, namun tetap perlu diperhatikan.
4. Tidak Penting Sama Sekali (0%): Tidak ada responden yang memilih opsi ini, yang mengindikasikan bahwa keamanan file tetap memiliki nilai penting dalam konteks manajemen universitas.

3.8. Langkah Langkah Keamanan

Mayoritas responden yang menilai langkah keamanan sebagai "Memadai" dan "Sangat Memadai" menunjukkan bahwa sistem keamanan yang diterapkan telah memenuhi kebutuhan dasar perlindungan data. Namun, responden yang memilih "Kurang Memadai" memberikan

indikasi adanya area perbaikan, seperti peningkatan teknologi keamanan, audit berkala, atau pelatihan kepada pengguna sistem.



Sumber : Hasil Penelitian (2024)

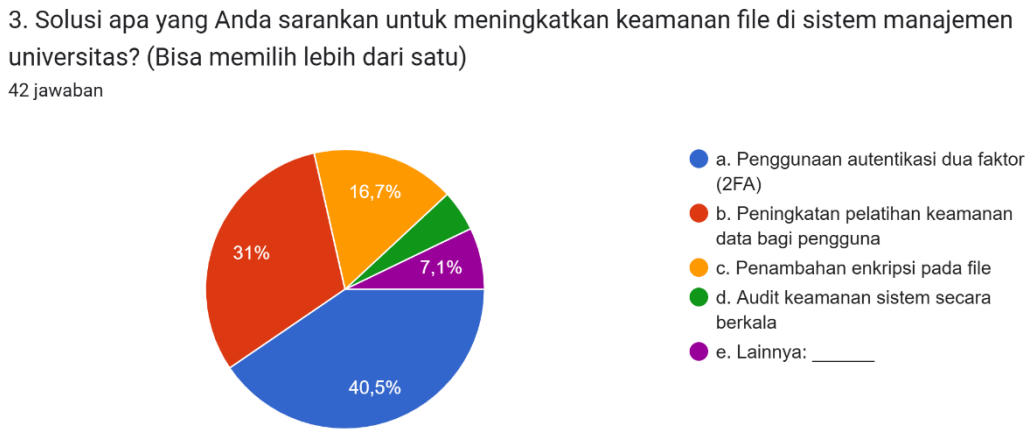
Gambar 8. Pertanyaan No 2

Pada gambar 8 menunjukan hasil survei mengenai pandangan responden terhadap langkah-langkah keamanan yang ada dalam sistem manajemen universitas menunjukkan variasi dalam tingkat kepuasan. Survei ini dilakukan terhadap 42 responden, dan berikut adalah hasilnya:

1. **Sangat Memadai** (26,2%): Sebagian responden merasa bahwa langkah-langkah keamanan yang ada saat ini sudah sangat memadai. Hal ini mencerminkan adanya kepercayaan terhadap sistem keamanan yang diterapkan.
2. **Memadai** (52,4%): Mayoritas responden berpendapat bahwa langkah-langkah keamanan sudah cukup memadai. Meski demikian, kategori ini mungkin mencerminkan kebutuhan akan perbaikan lebih lanjut agar sistem menjadi lebih optimal.
3. **Kurang Memadai** (21,4%): Sejumlah responden menganggap bahwa langkah-langkah keamanan saat ini masih kurang memadai. Hal ini menunjukkan adanya potensi risiko yang memerlukan perhatian khusus.
4. **Tidak Memadai** (0%): Tidak ada responden yang menyatakan langkah-langkah keamanan benar-benar tidak memadai, yang menunjukkan bahwa tidak ada ketidakpuasan ekstrem terhadap sistem keamanan saat ini.

3.9. Solusi untuk Meningkatkan Keamanan File

Hasil survei ini mengindikasikan bahwa kombinasi pendekatan teknis dan edukasi sangat diperlukan untuk meningkatkan keamanan sistem manajemen universitas. Penggunaan autentikasi dua faktor menjadi prioritas utama, karena memberikan perlindungan ganda terhadap akses sistem. Selain itu, pelatihan pengguna penting untuk meningkatkan kesadaran dan keterampilan dalam mengelola data dengan aman.



Sumber : Hasil Penelitian (2024)

Gambar 9. Pertanyaan No 3

Pada gambar 9 menunjukan survei terkait solusi untuk meningkatkan keamanan file dalam sistem manajemen universitas menghasilkan beberapa rekomendasi utama yang diusulkan oleh responden. Dari 42 jawaban yang diberikan, solusi-solusi berikut menjadi pilihan:

1. Penggunaan autentikasi dua faktor (2FA) (40,5%): Sebagian besar responden merekomendasikan implementasi autentikasi dua faktor sebagai langkah utama untuk meningkatkan keamanan. Hal ini menunjukkan bahwa responden menyadari pentingnya lapisan perlindungan tambahan dalam proses otentikasi.
2. Peningkatan pelatihan keamanan data bagi pengguna (31%): Banyak responden menganggap edukasi dan pelatihan bagi pengguna sebagai solusi yang penting. Langkah ini diharapkan dapat mengurangi risiko human error yang sering menjadi penyebab pelanggaran keamanan.
3. Penambahan enkripsi pada file (16,7%): Sebagian responden menyarankan penggunaan teknologi enkripsi untuk melindungi data dari akses tidak sah. Solusi ini relevan untuk meningkatkan kerahasiaan dan integritas data.
4. Audit keamanan sistem secara berkala (7,1%): Responden yang memilih opsi ini menunjukkan pentingnya evaluasi dan pemantauan rutin terhadap sistem keamanan. Dengan melakukan audit berkala, potensi celah keamanan dapat diidentifikasi dan diperbaiki lebih cepat.
5. Lainnya (7,1%): Sebagian kecil responden memberikan usulan tambahan yang belum tercakup dalam pilihan di atas. Usulan ini dapat mencakup teknologi atau pendekatan keamanan lain yang lebih spesifik.

Kesimpulan

Keamanan file dalam sistem manajemen informasi Universitas Bhayangkara Jakarta Raya merupakan aspek yang sangat penting mengingat data akademik, administrasi, dan keuangan yang tersimpan memiliki tingkat sensitivitas yang tinggi. Penelitian ini mengidentifikasi bahwa sistem saat ini menghadapi berbagai risiko keamanan, baik dari ancaman internal seperti kelalaian pengguna maupun ancaman eksternal seperti serangan malware, ransomware, dan akses tidak sah.

Daftar Pustaka

Anggara, Y. (2024). *IMPLEMENTASI ALGORITMA AES 128 BERBASIS WEB UNTUK KEAMANAN FILE PT . TUMBAKMAS NIAGA SAKTI WEB-BASED AES 128 ALGORITHM IMPLEMENTATION FOR FILE SECURITY PT . TUMBAKMAS NIAGA SAKTI*. *3*(September), 480–489.

Darmawan, D. (2024). Nextcloud: Keamanan Data Terbaik Dengan Manajemen File dan Pengguna yang Cerdas. *Jurnal Sosial Teknologi*, *4*(1), 80–89. https://doi.org/10.59188/jurnalsostech.v4i1.1130

Deva, B. S., & Jayadi, R. (2022). Analisis Risiko dan Keamanan Informasi pada Sebuah Perusahaan System Integrator Menggunakan Metode Octave Allegro. *Jurnal Teknologi Dan Informasi*, *12*(2), 106–117. https://doi.org/10.34010/jati.v12i2.6829

Edy Susanto, DenyaSaputri, Devan Adika Prasetya, Ian Arbatona, Joshua Christian Marpaung5, & Syuhada Hikmatyar Rahadian. (2023). Pengamanan Objek Vital, Keamanan File, Dan Keamanan Cyber Pada Pt Pos Indonesia. *Jurnal Mutiara Ilmu Akuntansi*, *1*(3), 163–174. https://doi.org/10.55606/jumia.v1i3.1516

Febriani, S. A., Muni, A., Rianto, B., Jalil, M., & Chrismondari. (2024). Analisis Kerentanan Keamanan Sistem Informasi Akademik Menggunakan Owasp-Zap Di Universitas Islam Indragiri. *Jurnal Sistem Informasi (TEKNOFILE)*, *2*(6), 409–420.

Nikmat, A. (2024). Analisis Manajemen Risiko Teknologi Informasi Pada Sistem Informasi Akademik (Siak) Universitas Muhammadiyah Sukabumi (Umm) Menggunakan Iso 31000. *Jurnal Manajemen Dan Teknologi Informasi*, *14*(1), 49–58. https://doi.org/10.59819/jmti.v14i1.3321

Novianto, E., Heri Ujianto, E. I., & Rianto, R. (2023). Keamanan Informasi (Information Security) Pada Aplikasi Sistem Informasi Manajemen Kepegawaian Dengan Defense in Depth. *Jurnal Komputer Dan Informatika*, *11*(1), 1–6. https://doi.org/10.35508/jicon.v11i1.9139

Novita Setyaningrum, N., & Maria, E. (2024). Penerapan Iso 31000:2018 Untuk Manajemen Risiko Pada Sistem Informasi Sekolah Terpadu. *Jurnal Pendidikan Teknologi Informasi (JUKANTI)*, *7*(1), 31–44. https://doi.org/10.37792/jukanti.v7i1.1164

Soesanto, E., Romadhon, A., Dwi Mardika, B., & Fahmi Setiawan, M. (2023). Analisis dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital Untuk Mengamankan Objek Vital dan File. *SAMMAJIVA : Jurnal Penelitian Bisnisdan*

Manajemen, *1*(2), 186.

Sulaeman, H., Utomo, H. P., & Suryana, A. I. (2023). Penilaian Risiko Keamanan Informasi Pada Sistem Informasi Akademik (Siakad) Dengan Menggunakan Framework Nist-Sp 800 30. *Naratif : Jurnal Nasional Riset, Aplikasi Dan Teknik Informatika*, *5*(2), 171–185. https://doi.org/10.53580/naratif.v5i2.254