Journal of Information and Information Security (JIFORTY)
Vol. 5, No. 2, Desember 2024, 269-280
e-ISSN : 2722-4058
Available Online at http://ejurnal.ubharajaya.ac.id/index.php/jiforty

Strategi Dan Praktik Terbaik Untuk Melindungi Data Di Universitas Bhayangkara Jakarta Raya

Arya Radithya [1,*], Iqbal Mahdi Bisyafaa [1], Gilang Gs Putra [1]

Informatika Universitas Bhayangkara Jakarta Raya. Jalan Raya Perjuangan No 81 Marga Mulya, Bekasi Utara Jawa Barat, 17143, (021) 88955882,
202210715195@mhs.ubharajaya.ac.id, 202210715212@mhs.ubharajaya.ac.id,
202210715202@mhs.ubharajaya.ac.id

* Korespondensi: e-mail: 202210715195@mhs.ubharajaya.ac.id

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

Abstract

Cybersecurity is a crucial aspect in protecting important data at universities, including Universitas Bhayangkara Jakarta Raya, which handles student, staff, and financial data. This article discusses strategies as well as best techniques that can be employed to strengthen the university's data security. The research covers risk assessment, security training, secure authentication, data backup, system maintenance, network security, security policies, threat monitoring, encryption, and external collaboration. By adopting these strategies, Universitas Bhayangkara Jakarta Raya can minimize risks and enhance the security of their digital information. The research findings indicate that implementing a layered security system can improve the effectiveness of data protection at the university.
Keywords*: Cybersecurty, Data, college student, University Bhayangkara Jakarta Raya.*

Abstrak

Keamanan siber menjadi aspek krusial dalam melindungi data penting di perguruan tinggi, termasuk Universitas Bhayangkara Jakarta Raya, yang menangani data mahasiswa, staf, dan keuangan. Artikel ini membahas strategi dan praktik terbaik yang dapat diimplementasikan untuk memperkuat keamanan data universitas. Penelitian ini mencakup penilaian risiko, pelatihan keamanan, otentikasi aman, pencadangan data, pemeliharaan sistem, keamanan jaringan, kebijakan keamanan, pemantauan ancaman, enkripsi, dan kolaborasi eksternal. Dengan menerapkan strategi ini, Universitas Bhayangkara Jakarta Raya dapat meminimalkan risiko dan meningkatkan keamanan informasi digital mereka. Hasil penelitian menunjukkan bahwa implementasi sistem keamanan berlapis dapat meningkatkan efektivitas perlindungan data di universitas.
Kata Kunci : Keamanan Siber, Data, Mahasiswa, Universitas Bhayangkara Jakarta Raya.

1. Pendahuluan

Keamanan siber kini menjadi isu yang semakin penting seiring dengan kemajuan teknologi informasi dan komunikasi. Di era digital saat ini, hampir semua aspek kehidupan, termasuk pendidikan, sangat tergantung pada teknologi. Universitas, sebagai lembaga pendidikan tinggi, tidak hanya menyimpan data pribadi mahasiswa, dosen, dan staf, tetapi juga menyimpan informasi akademik serta hasil penelitian yang bernilai tinggi. Dengan meningkatnya ketergantungan pada sistem informasi digital, risiko terkait ancaman siber pun semakin besar.

Keamanan siber adalah elemen penting dalam keamanan informasi, yang bertujuan untuk melindungi sistem yang terhubung ke internet, seperti perangkat keras, perangkat lunak, aplikasi, dan data, dari ancaman serangan siber. (Harahap, 2024). Universitas Bhayangkara Jakarta Raya (UBJ), sebagai institusi pendidikan yang berkomitmen menyediakan layanan pendidikan berkualitas, harus memberikan perhatian serius terhadap aspek keamanan siber. Data yang disimpan di server universitas termasuk informasi akademik, data keuangan, dan hasil penelitian sangat rentan terhadap potensi serangan.

Kejahatan siber semakin meningkat di Indonesia, yang menjadi ancaman serius terhadap pertahanan dan keamanan negara. Dampak dari masalah ini adalah kebocoran data pribadi, data perusahaan, hingga data negara yang bisa dengan mudah diakses oleh pihak-pihak yang tidak bertanggung jawab. Menyadari pentingnya isu ini, kelompok kami berencana untuk melakukan penelitian terkait pertahanan dan keamanan siber di era digital, dengan melibatkan mahasiswa dalam prosesnya. (Azzahrah et al. , 2024).

Pelanggaran terhadap data ini tidak hanya mengganggu proses pembelajaran, tetapi juga dapat merugikan individu yang datanya dicuri. Oleh karena itu, penting bagi mahasiswa sebagai pengguna utama sistem untuk memiliki pemahaman yang mendalam tentang keamanan siber serta cara berkontribusi dalam melindungi data yang ada. Perkembangan teknologi komputer terus berlangsung, namun para peretas dan pelaku kejahatan siber juga terus meningkatkan kemampuan mereka, sehingga kita harus terus memperbarui pengetahuan tentang perkembangan jaringan komputer dan teknologi keamanan. Teknologi perlindungan harus dapat mengimbangi kecepatan para penjahat dunia maya dalam mempelajari virus. Salah satu masalah yang sering dibahas dalam keamanan jaringan komputer adalah adanya celah keamanan informasi. Dengan memanfaatkan teknologi enkripsi data, informasi pengguna dapat lebih terlindungi dari ancaman pencurian. (Saputra, 2023).

Pentingnya pendidikan terkait keamanan siber di lingkungan universitas tidak dapat dianggap remeh. Masyarakat yang semakin terhubung secara digital memerlukan individu yang tidak hanya memiliki keterampilan teknis, tetapi juga kesadaran etis mengenai penggunaan dan perlindungan teknologi. Melalui pelatihan dan sosialisasi tentang keamanan siber, UBJ dapat menyiapkan mahasiswa untuk menjadi pengguna teknologi yang bijak dan bertanggung jawab.

Artikel ini bertujuan untuk menjelajahi berbagai regulasi dan peraturan keamanan siber yang ada di era digital, mengidentifikasi praktik terbaik, serta menganalisis tantangan yang dihadapi dalam implementasinya. Dengan memahami dinamika regulasi keamanan siber, penelitian ini diharapkan dapat memberikan wawasan dan rekomendasi yang bermanfaat bagi pembuat kebijakan, penegak hukum, dan praktisi keamanan siber (Kristianti et al. , 2024).

2. Metode Penelitian

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

1. Pengumpulan Data: Data diperoleh melalui studi pustaka yang melibatkan berbagai referensi mengenai keamanan siber di institusi pendidikan dan melalui survei yang dilakukan terhadap staf dan mahasiswa UBJ, berkaitan dengan pengetahuan serta perilaku mereka terkait keamanan siber.
2. Analisis Risiko: Tahap ini mencakup analisis risiko yang bertujuan untuk mengidentifikasi potensi ancaman terhadap infrastruktur teknologi informasi di UBJ.
3. Penyusunan Strategi dan Praktik Terbaik: Berdasarkan hasil analisis risiko, peneliti merancang strategi keamanan yang mencakup pelatihan keamanan, penguatan akses, penerapan enkripsi, serta penyusunan kebijakan keamanan yang tepat.
4. Evaluasi: Evaluasi dilakukan melalui simulasi serangan siber, yang dirancang untuk menguji efektivitas strategi keamanan yang telah diterapkan.
5. Dasar Teoritis: Menurut Creswell (2019), penelitian yang baik adalah sebuah model penelitian yang mengedepankan desain yang tersusun berdasarkan strategi yang jelas. Dalam hal ini, teknik pengumpulan data yang digunakan adalah studi kepustakaan. Setelah informasi terkumpul, peneliti menggunakan data tersebut untuk menganalisis peran negara sesuai dengan konsep yang diusulkan oleh K. J. Holsti, yang berfokus pada pemahaman peran sebuah negara bangsa dari berbagai sudut.
6. Metode Penelitian: Penelitian ini menggunakan metode kualitatif dengan mengutamakan studi literatur yang berfokus pada sistem informasi manajemen dan sistem manajemen keamanan di perusahaan. Peneliti mengevaluasi berbagai dokumen, buku, dan jurnal terkait untuk memahami bagaimana perusahaan dapat meningkatkan perlindungan data dan privasi pengguna melalui pengelolaan data yang efektif. Hasil peninjauan dokumen ini akan dianalisis untuk mengidentifikasi titik-titik lemah dalam keamanan data perusahaan. Pendekatan ini memberikan wawasan komprehensif tentang kerentanan yang mungkin muncul serta solusi yang relevan dan efektif (Hapsah dan Nasution, 2023).

3. Hasil dan Pembahasan

3. 1. Peningkatan Keamanan Siber di Kampus

Keamanan siber berfungsi sebagai perlindungan terhadap infrastruktur digital dari berbagai ancaman yang mungkin muncul. Oleh karena itu, keamanan siber memainkan peran penting dalam melindungi informasi dan data, memastikan bahwa informasi yang dikirimkan tetap aman (E-commerce et al. , 2024).

Temuan penelitian ini menunjukkan bahwa isu keamanan siber telah menjadi perhatian serius di masyarakat, dengan sebagian besar responden menunjukkan tingkat pemahaman yang baik tentang topik ini. Namun, masih terdapat kesempatan untuk meningkatkan edukasi dan kampanye kesadaran, terutama dalam mendalami pemahaman yang lebih komprehensif daripada sekadar pengetahuan superficial.(Wiratama,2023)

Responden yang menyatakan mereka "cukup sering" mendengar tentang keamanan siber menunjukkan adanya peluang untuk mengubah kesadaran ini menjadi tindakan konkret, seperti

penerapan praktik keamanan digital yang lebih baik. Berbagai pendekatan, seperti pelatihan, seminar, atau kampanye sosialisasi mengenai keamanan siber, dapat dilaksanakan untuk meningkatkan pemahaman penerima tentang pentingnya perlindungan data dan privasi.
Penelitian sebelumnya juga mencatat pentingnya bagi organisasi untuk mengadopsi mekanisme audit manajemen keamanan informasi yang sesuai dengan peraturan yang berlaku (Fachrudin et al.2024).

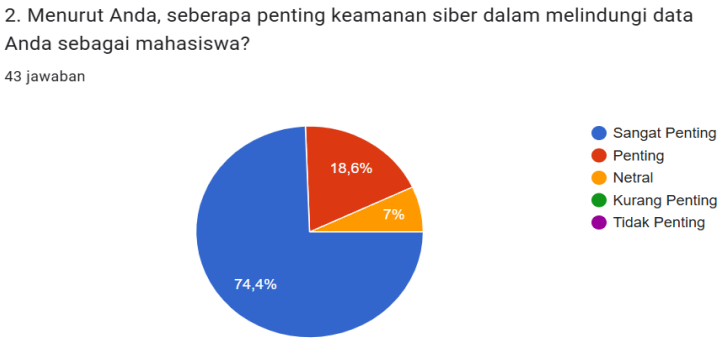
.

Sumber: Hasil Penelitian (2024)

Gambar 1. Pertanyaan 1

Pada gambar 1 menunjukan bahwa mayoritas responden telah terpapar topik keamanan siber. Sebanyak 51,2% mendengar topik ini "Cukup Sering," dan 41,9% "Sangat Sering," menunjukkan tingkat kesadaran yang cukup baik. Hanya 7% yang mengaku jarang mendengar, dan tidak ada yang memilih "Tidak Pernah."

Hasil ini menandakan bahwa keamanan siber sudah menjadi perhatian utama. Namun, perlu ditingkatkan edukasi dan kampanye untuk mendorong pemahaman yang lebih mendalam, sehingga kesadaran dapat diubah menjadi tindakan nyata dalam menjaga keamanan digital.



Sumber: Hasil Penelitian (2024)

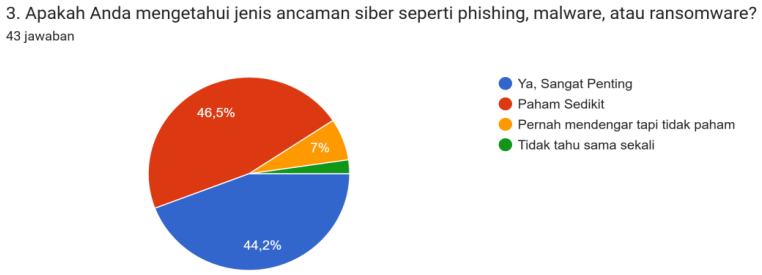
Gambar 2. Pertanyaan 2

Pada gambar 2 menunjukan bahwa mayoritas responden menganggap keamanan siber sangat penting dalam melindungi data sebagai mahasiswa. Sebanyak 74,4% responden memilih kategori **"Sangat Penting"**, diikuti oleh 18,6% yang memilih **"Penting"**, dan 7% yang bersikap

"Netral". Tidak ada responden yang menganggap keamanan siber kurang penting atau tidak penting.

Hasil ini mencerminkan kesadaran yang tinggi di kalangan mahasiswa terhadap pentingnya keamanan siber. Mayoritas responden menyadari bahwa melindungi data pribadi merupakan prioritas utama di era digital. Namun, masih ada sebagian kecil yang netral, menunjukkan perlunya kampanye edukasi yang lebih luas untuk menjangkau kelompok ini. Edukasi dapat difokuskan pada dampak nyata ancaman siber dan pentingnya langkah-langkah perlindungan data untuk meningkatkan kesadaran dan tindakan proaktif.

3.2 Ancaman Siber



Sumber: Hasil Penelitian (2024)

Gambar 3. Pertanyaan 3

Pada gambar 3 menunjukan dari 43 responden, **44,2%** memahami ancaman siber seperti phishing, malware, atau ransomware dengan baik, sementara **46,5%** hanya memahami sedikit. Sebanyak **7%** pernah mendengar istilah tersebut tetapi tidak memahaminya, dan **2,3%** tidak tahu sama sekali.

Hasil ini menunjukkan perlunya peningkatan literasi keamanan digital, terutama melalui edukasi sederhana dan kampanye yang relevan. Langkah-langkah seperti pelatihan, sosialisasi, dan kolaborasi berbagai pihak diharapkan mampu meningkatkan kesadaran masyarakat terhadap ancaman siber.

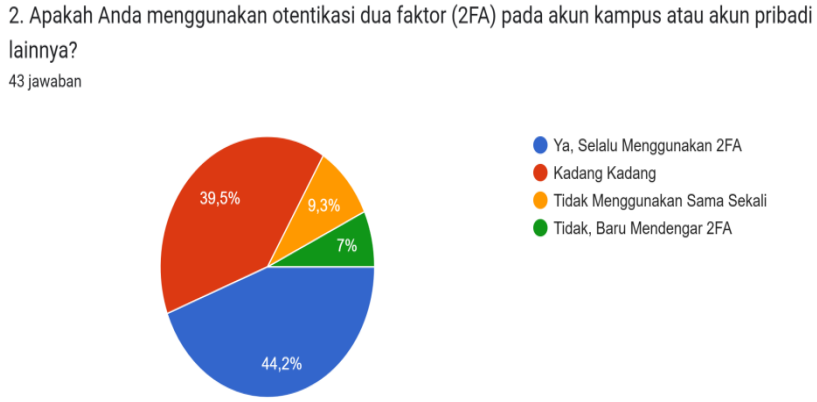
3.3 Otentikasi dua faktor (2FA)

Sumber: Hasil Penelitian (2024)

Gambar 4. Pertanyaan 1

Pada gambar 4 menunjukan dari 43 responden, **53,5%** sangat sering menggunakan kata sandi yang kuat dan unik, sementara **37,2%** sering melakukannya. Sebanyak **9,3%** jarang menggunakan kata sandi yang kuat, dan tidak ada responden yang tidak pernah melakukannya.

Hasil ini menunjukkan bahwa sebagian besar responden sudah memahami pentingnya keamanan kata sandi, meskipun masih ada kelompok kecil yang perlu diedukasi lebih lanjut tentang risiko penggunaan kata sandi yang lemah. Edukasi tentang kriteria kata sandi aman dan penggunaan pengelola kata sandi dapat membantu meningkatkan praktik keamanan digital.

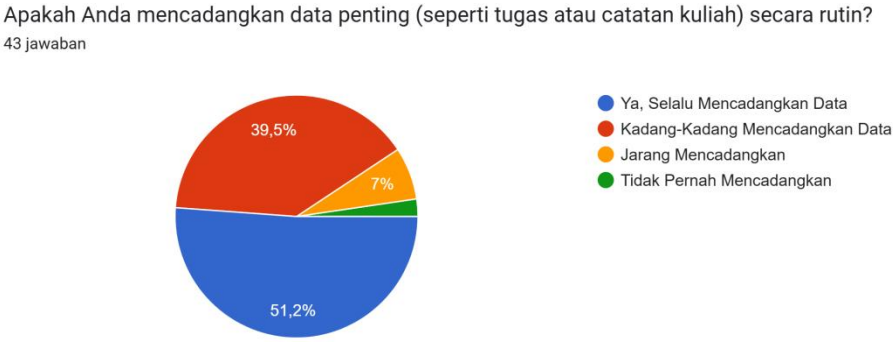


Sumber: Hasil Penelitian (2024)

Gambar 5. Pertanyaan 2

Pada gambar 5 menunjukan dari 43 responden, **44,2%** selalu menggunakan 2FA, **39,5%** kadang-kadang menggunakannya, **9,3%** tidak pernah menggunakan, dan **7%** baru mendengar tentang 2FA.

Hasil ini menunjukkan sebagian besar responden sudah memahami pentingnya 2FA, meskipun ada kelompok kecil yang memerlukan edukasi lebih lanjut untuk meningkatkan kesadaran dan penggunaan fitur keamanan ini.



Sumber: Hasil Penelitian (2024)

Gambar 6. Pertanyaan 6

Pada gambar 6 menunjukan dari survei terhadap 43 responden, 51,2% selalu mencadangkan data, menunjukkan kesadaran tinggi akan pentingnya menjaga data. Sebanyak 39,5% kadang-kadang mencadangkan, sementara 7% jarang, dan 2,3% tidak pernah mencadangkan data.

Hasil ini menunjukkan perlunya meningkatkan kesadaran di kalangan yang jarang atau tidak mencadangkan data. Edukasi tentang risiko kehilangan data dan penggunaan alat pencadangan, seperti cloud storage, dapat membantu membangun kebiasaan mencadangkan secara rutin.

3.4 Pemahaman Keamanan Siber

Sumber: Hasil Penelitian (2024)

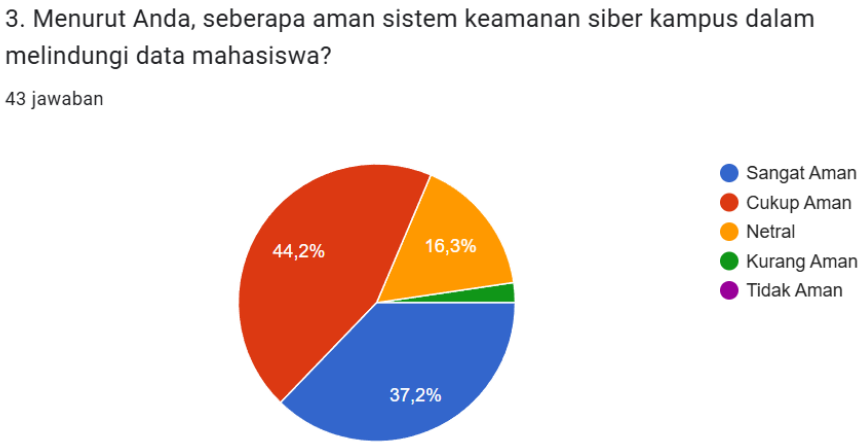
Gambar 7. Pertanyaan 1

Pada gambar 7 menunjukan dari survei, 67,4% responden telah menerima pelatihan atau sosialisasi keamanan siber dari kampus, sedangkan 32,6% belum. Hal ini menunjukkan mayoritas sudah mendapatkan edukasi, tetapi perlu upaya lebih untuk menjangkau semua mahasiswa agar kesadaran keamanan siber merata.

Sumber: Hasil Penelitian (2024)

Gambar 8. Pertanyaan 2

Pada gambar 8 menunjukan mayoritas responden (69,8%) merasa pelatihan keamanan siber **sangat diperlukan**, dan 27,9% menyatakan **diperlukan**. Hanya sedikit yang menganggapnya **kurang diperlukan** (2,3%). Hasil ini menunjukkan kebutuhan mendesak akan pelatihan untuk meningkatkan kesadaran mahasiswa terhadap ancaman siber.

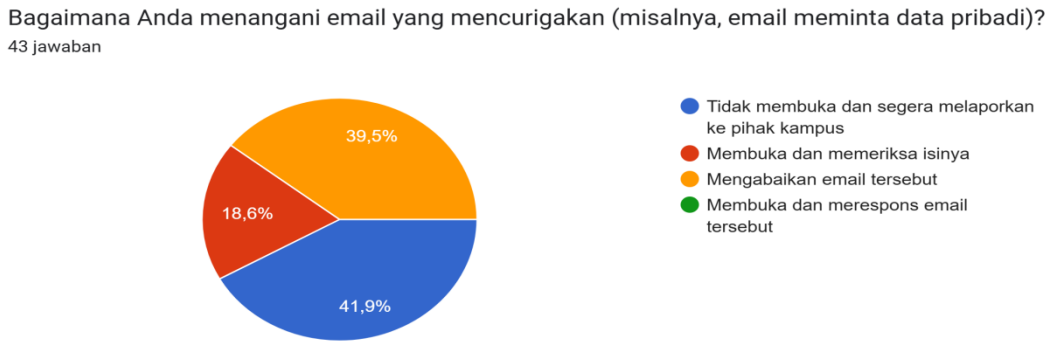


Sumber: Hasil Penelitian (2024)

Gambar 9. Pertanyaan 3

Pada gambar 9 menunjukan banyak 37,2% responden menilai sistem keamanan siber kampus **cukup aman**, sementara 44,2% bersikap **netral**. Sisanya, 16,3%, menganggapnya **kurang aman**. Hasil ini menunjukkan perlunya peningkatan keamanan dan transparansi untuk meningkatkan kepercayaan mahasiswa terhadap perlindungan data.

3.5 Pencegahan dari ancaman berupa email

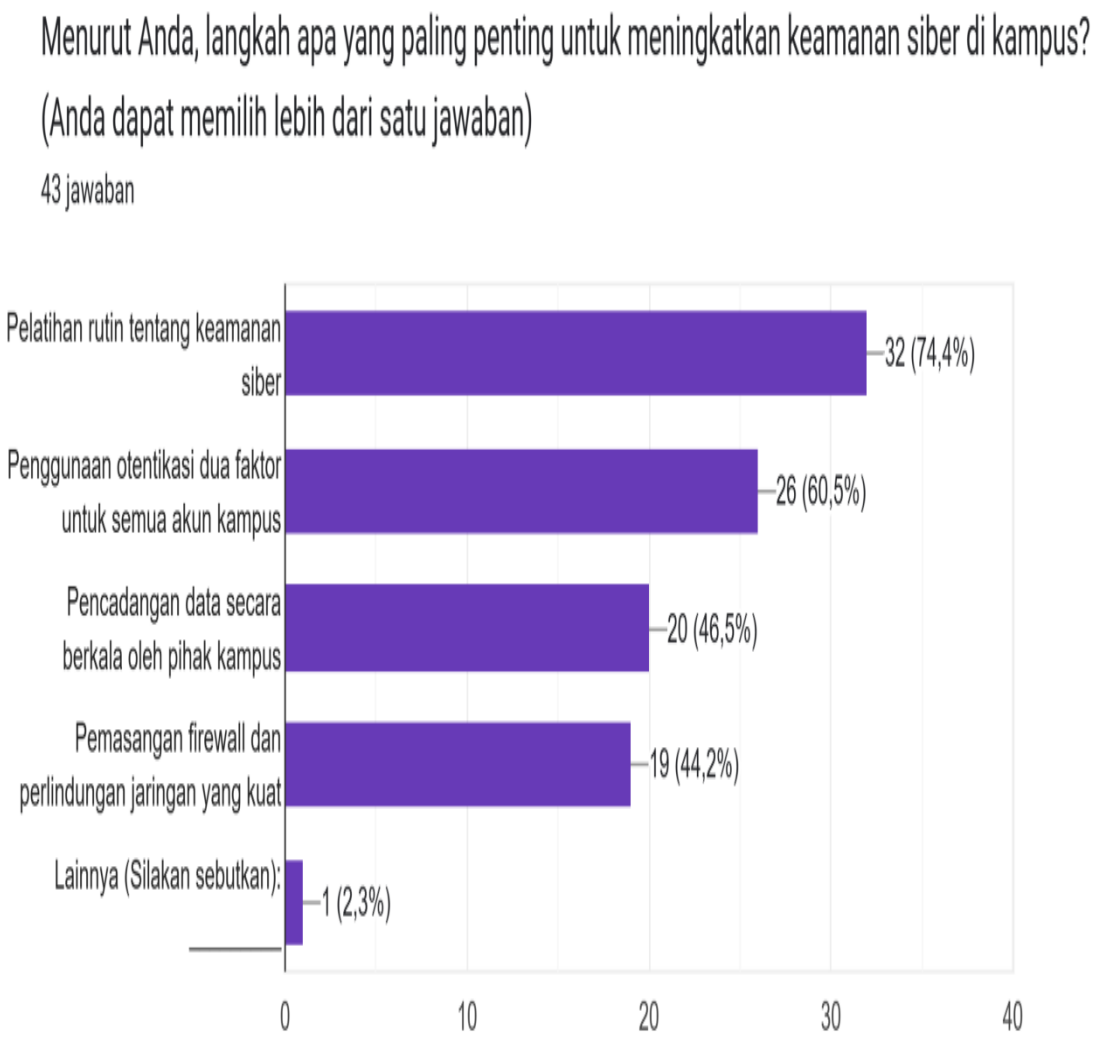


Sumber: Hasil Penelitian (2024)

Gambar 10. Pertanyaan 4

Pada gambar 10 menunjukan 41,9% responden memilih untuk **tidak membuka dan segera melaporkan** email mencurigakan ke pihak kampus. Namun, 39,5% justru **membuka dan memeriksa isinya**, dan 18,6% **mengabaikan email tersebut**.

Hasil ini menunjukkan perlunya edukasi lebih lanjut untuk memastikan mahasiswa dapat menangani ancaman phishing dengan benar dan meningkatkan kebiasaan melapor.

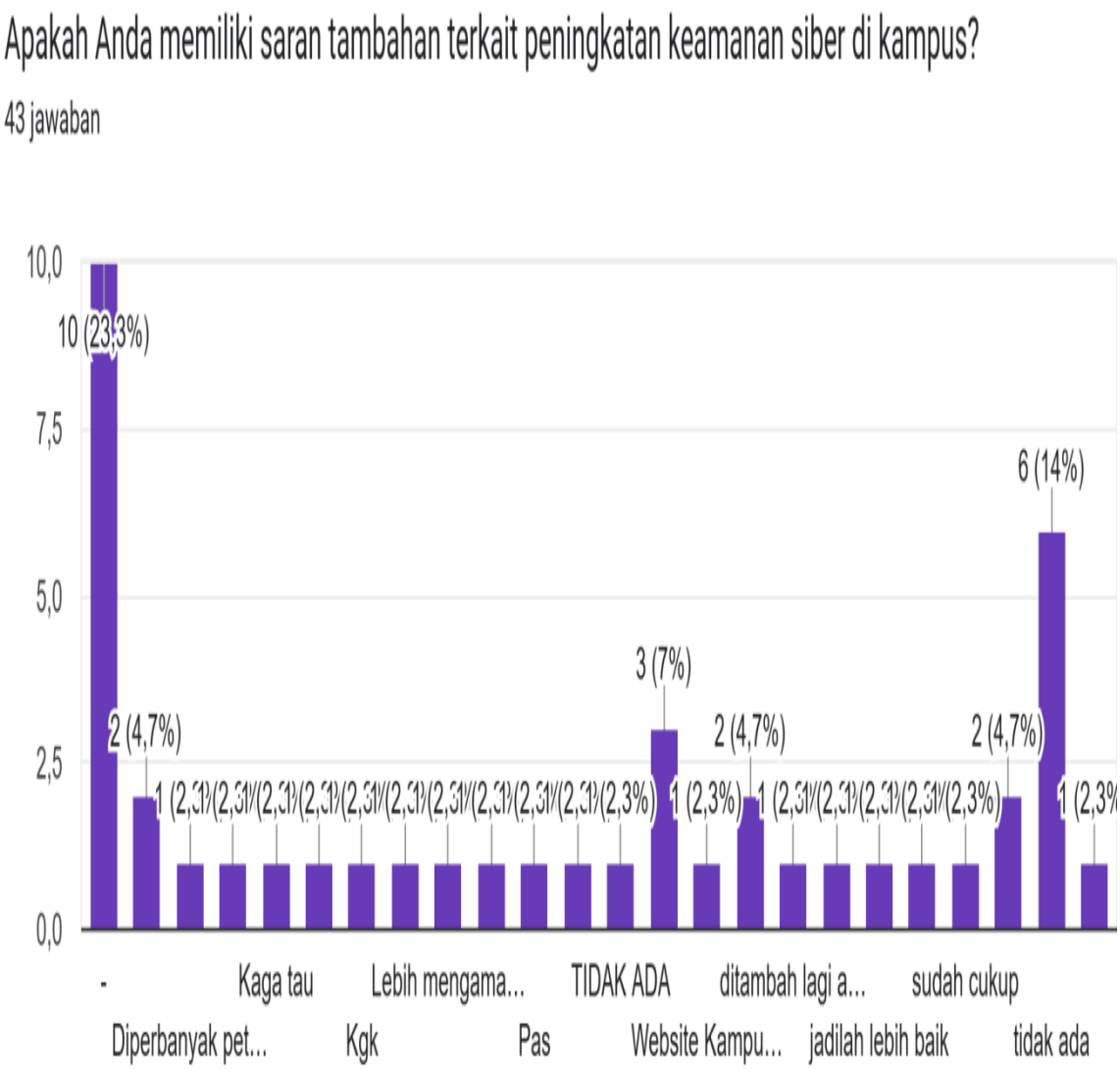


Sumber: Hasil Penelitian (2024)

Gambar 11. Grafik Langkah Penting untuk peningkatan KeamananSiber di kampus

Pada gambar 11 menunjukan sebanyak 74,4% responden menyarankan **pelatihan rutin tentang keamanan siber** sebagai langkah penting. Selain itu, 60,5% mengutamakan **penggunaan autentikasi dua faktor**, 46,5% mendukung **pencadangan data berkala**, dan 44,2% memilih **pemasangan firewall serta perlindungan jaringan**.

Hasil ini menunjukkan bahwa pelatihan dan penguatan sistem keamanan menjadi prioritas utama untuk meningkatkan keamanan siber di kampus.



Sumber: Hasil Penelitian (2024)

Gambar 12. Grafik Saran Tambahan untuk peningkatan KeamananSiber di kampus

Pada gambar 12 menunjukan sebanyak 23,3% responden tidak memberikan saran tambahan, sementara 14% merasa langkah yang ada sudah cukup. Saran utama lainnya mencakup **memperbanyak pelatihan** (4,7%), **meningkatkan keamanan website kampus** (7%), dan **pengelolaan sistem yang lebih baik**.

Hasil ini menunjukkan perlunya kampus mengedepankan pelatihan dan peningkatan sistem keamanan sesuai kebutuhan mahasiswa.

4. Kesimpulan

Untuk menghadapi berbagai ancaman, seperti email mencurigakan, sangat penting bagi kampus untuk memberikan edukasi yang lebih mendalam kepada mahasiswa agar mereka dapat mengenali dan mengambil langkah-langkah yang tepat dalam menangani potensi risiko tersebut. Salah satu langkah yang perlu ditekankan adalah pentingnya melaporkan ancaman yang diterima kepada pihak kampus agar dapat segera ditindaklanjuti.

Selain itu, sejumlah rekomendasi utama yang disarankan meliputi pelaksanaan pelatihan keamanan siber secara rutin bagi mahasiswa dan staf kampus, penerapan sistem autentikasi dua faktor untuk memperkuat perlindungan akun, pencadangan data secara berkala agar data yang penting tetap aman, serta pemasangan firewall untuk mencegah akses tidak sah yang dapat membahayakan sistem kampus.

Dengan menerapkan langkah-langkah tersebut secara konsisten, diharapkan kampus dapat menciptakan lingkungan digital yang lebih aman dan terlindungi, sehingga meningkatkan rasa aman dan kepercayaan mahasiswa terhadap perlindungan data pribadi mereka, sekaligus meminimalkan potensi risiko terhadap sistem keamanan siber kampus secara keseluruhan.

Daftar Pustaka

Azzahrah, B. T., Naufal, M., Hamdi, R., Raynee, R., & Layla, Z. (2024). Tantangan Pertahanan dan Keamanan Data Cyber dalam Era Digital : Studi Kasus dan Implementasi. *Jurnal Pendidikan Tambusai*, *8*(2), 23934–23943.

E-commerce, P., Kurnia, E., Rahmadani, T., & Saven, R. F. (2024). *Menghadapi Ancaman Cyber : Strategi Keamanan Untuk Sistem Program Studi Ekonomi Syariah , Sekolah Tinggi Agama Islam Negeri (STAIN) Bengkalis Email : Titinijal@gmail.com Kurniaeni780@gmail.com*. *1*, 15–27.

Fachrudin, R., Respaty, E., Adilah, I. S., & Sinlae, F. (2024). Peranan Penting Manajemen Sekuriti di Era Digitalisasi. *Nusantara Journal of Multidisciplinary Science*, *2*(1), 94–102. https://www.researchgate.net/publication/377219065_Peranan_Penting_Manajemen_Sekuriti_di_Era_Digitalisasi

Hapsah, Z. F., & Nasution, M. I. P. (2023). Analisis Tingkat Keamanan Data Perusahaan Yang Rentan Terhadap Serangan Cyber Dalam Sistem Informasi Manajemen. *Jurnal Manajemen Dan Akuntansi*, *1*(2), 338–343.

Harahap, F. F. (2024). Penerapan Pengamanan Objek Vital, Pengamanan Manajemen File, Dan Pengamanan Cyber Pada Rumah Sakit. *Jurnal Ilmu Pendidikan*, *2*(2), 102–111.

Kristianti, N., Kurniasi, R., Raya, U. P., & Jurnal, R. (2024). Peraturan dan Regulasi Keamanan Siber di Era Digital. *Satya Dharma: Jurnal Ilmu Hukum*, *6055*(1), 297–310. https://ejournal.iahntp.ac.id/index.php/satya-dhamat

Rai, I. N. A. S., Heryadi, D., & Kamaluddin N., A. (2022). The Role of Indonesia to Create Security and Resilience in Cyber Spaces [Peran Indonesia dalam Membentuk Keamanan dan

Ketahanan di Ruang Siber]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *13*(1), 43–66. https://doi.org/10.22212/jp.v13i1.2641

Ramadhan, Y. A., & Renaldy, R. (2024). *IN-FEST 2024 Analisis Ancaman , Metode dan Mitigasi dalam Keamanan Privasi Data di Internet IN-FEST 2024*. *2*, 607–614.

Saputra, M. I. (2023). Literature Review Network Security. *Jurnal Jaringan Komputer Dan Keamanan*, *04*(03), 30–34.

Wiratama, A. D. (2023). Cyber Security In 2023: The Latest Challenges And Solutions. *Jurnal Komputer Indonesia*, *2*(1), 47–54. https://doi.org/10.37676/jki.v2i1.569