Journal of Information and Information Security (JIFORTY)
Vol. 5, No. 2, Desember 2024, 213-222
e-ISSN : 2722-4058
Available Online at http://ejurnal.ubharajaya.ac.id/index.php/jiforty

Analisis Ancaman Keamanan Informasi Pada Insfrastruktur Teknologi di Universitas Bhayangkara Jakarta Raya

Farhan Maulana [1,*], Khalil Putra Pratama [1], Muhammad Fadillah [1]
Muhammad Irfan Adji Wicaksono [1], Raka Kristianto [1]

[1] Informatika; Universitas Bhayangkara Jakarta Raya; Jl. Perjuangan No. 81 Bekasi Utara, (021) 889558822; e-mail: 202310715270@mhs.ubharajaya.ac.id, 202310715244@mhs.ubharajaya.ac.id, 202310715153@mhs.ubharajaya.ac.id, 202310715213@mhs.ubharajaya.ac.id, 202310715076@mhs.ubharajaya.ac.id

* Korespondensi: e-mail: 202310715270@mhs.ubharajaya.ac.id

Diterima: 4 Jan 25; Review: 4 Jan 25; Disetujui: 9 Jan 25; Diterbitkan: 9 Jan 25

Abstract

information security is a critical aspect in the digital era, especially for higher education institutions such as Universitas Bhayangkara Jakarta Raya. With the increasing use of information technology in learning and administrative processes, the potential for information security threats has also grown, ranging from cyberattacks to system vulnerabilities. This study aims to analyze various information security threats faced by the university's technological infrastructure and evaluate the effectiveness of the implemented mitigation measures. The methodology used is a quantitative survey with respondents consisting of university students, collected through online questionnaires.The findings of this research indicate that the majority of respondents consider information security to be very important, with many reporting experiences of threats such as malware and phishing. Furthermore, the study found that although the university has a dedicated team to handle security incidents, there is still a need to improve infrastructure and awareness regarding information security. Recommendations include implementing machine learning technology for threat detection and enhancing training for the information security team to improve responses to evolving threats.
***Keywords**: information security, cyber threats, risk mitigation, Universitas Bhayangkara Jakarta Raya, machine learning.*

Abstrak

Keamanan informasi merupakan aspek yang krusial di era digital, terutama untuk institusi pendidikan tinggi seperti Universitas Bhayangkara Jakarta Raya. Penelitian ini bertujuan untuk menganalisis ancaman keamanan informasi yang dihadapi oleh infrastruktur teknologi universitas dan mengevaluasi efektivitas langkah mitigasi yang telah diterapkan. Metodologi yang digunakan adalah survei kuantitatif dengan responden mahasiswa, yang datanya dikumpulkan melalui kuesioner daring.Hasil penelitian menunjukkan bahwa mayoritas responden menganggap keamanan informasi sangat penting, dengan banyak yang melaporkan pengalaman terhadap ancaman seperti malware dan phishing. Selain itu, penelitian ini juga menemukan bahwa meskipun universitas memiliki tim khusus untuk menangani insiden keamanan, masih ada kebutuhan untuk meningkatkan infrastruktur dan kesadaran akan keamanan informasi. Rekomendasi yang diberikan mencakup penerapan teknologi machine learning untuk deteksi ancaman dan peningkatan pelatihan bagi tim keamanan informasi, guna meningkatkan respons terhadap ancaman yang terus berkembang.
Kata kunci: keamanan informasi, ancaman siber, mitigasi risiko, Universitas Bhayangkara Jakarta Raya, machine learning.

1. Pendahuluan

Keamanan informasi merupakan aspek yang sangat penting dalam era digital saat ini, terutama di lingkungan pendidikan tinggi seperti Universitas Bhayangkara Jakarta Raya. Dengan semakin banyaknya penggunaan teknologi informasi dalam proses pembelajaran dan administrasi, ancaman terhadap keamanan informasi juga meningkat. Ancaman ini tidak hanya berasal dari individu jahat, tetapi juga dapat muncul dari kerentanan sistem dan bencana alam yang tidak terduga.

Seiring dengan meningkatnya jumlah pengguna internet di Indonesia, yang mencapai lebih dari setengah populasi, risiko terhadap data dan informasi semakin tinggi. Penggunaan alat elektronik sebagai media pertukaran informasi membuat institusi pendidikan rentan terhadap serangan siber, seperti malware, phishing, dan serangan DDoS. Oleh karena itu, penting bagi universitas untuk menerapkan langkah-langkah keamanan yang efektif untuk melindungi data sensitif dan menjaga integritas sistem.

Universitas Bhayangkara Jakarta Raya memiliki tanggung jawab untuk melindungi informasi akademik dan administratif yang dikelola. Dalam konteks ini, analisis ancaman keamanan informasi menjadi krusial untuk memahami potensi risiko yang ada dan mengembangkan strategi mitigasi yang tepat. Penelitian ini bertujuan untuk menganalisis berbagai ancaman yang mungkin dihadapi oleh infrastruktur teknologi di universitas serta mengevaluasi efektivitas langkah-langkah keamanan yang telah diterapkan.

Dalam upaya meningkatkan keamanan informasi, penerapan teknologi seperti machine learning dan algoritma analisis data dapat membantu dalam mendeteksi dan merespons ancaman secara lebih cepat dan akurat. Dengan demikian, penelitian ini tidak hanya akan memberikan wawasan tentang kondisi keamanan informasi saat ini di Universitas Bhayangkara Jakarta Raya, tetapi juga menawarkan rekomendasi untuk perbaikan sistem keamanan di masa depan. Melalui pemahaman yang lebih baik mengenai ancaman-ancaman ini, diharapkan pihak universitas dapat mengambil langkah-langkah yang diperlukan untuk meningkatkan kesiapan mereka dalam menghadapi tantangan keamanan informasi yang terus berkembang.

2. Metode Penelitian

2.1. Kerangka Penelitian

Penelitian ini dilakukan untuk mengeksplorasi Ancaman keamanan informasi pada insfrastruktur teknologi di Universitas Bhayangkara Jakarta Raya. Pendekatan penelitian yang digunakan adalah pendekatan kuantitatif dengan metode survei, yang bertujuan untuk mengumpulkan data dari mahasiswa/i melalui kuesioner.(Gomm, 2008)

2.2. Pendekatan penelitian

Penelitian ini dilakukan dengan menggunakan metode kuantitatif, yang bertujuan untuk mengukur variabel-variabel spesifik, seperti tingkat ancaman serangan siber terhadap insfrastruktur di Universitas Bhayangkara Jakarta Raya. Pemilihan metode ini terjadi karena mampu memberikan data dengan cara yang terstruktur dan dapat diukur

2.3. Populasi dan Sampel

Pada penelitian ini kami berfokus kepada mahasiswa/i Universitas Bhayangkara Jakarta Raya yang sebsagai bahan penelitian kami. Sampel penelitian diambil dengan teknik random sampling untuk memastikan representasi yang adil dari populasi. Jumlah sampel yang diambil adalah 42 mahasisaw/i.

2.4. Prosedur Penelitian

Penelitian ini dilakukan melalui langkah-langkah berikut:

1. **Persiapan :** Menyusun kuisoner berdasarkan study literatur terkait ancaman keamanan insfrastruktud di Universitas Bhayangkara Jakarta Raya dan uji coba kecil untuk memastikan validitas pertanyaan
2. **Pengumpulan Data :** Kuesioner dibagikan secara daring menggunakan Google Forms untuk mengambil data responden.
3. **Analisis Data :** Data yang diperoleh dianalisis menggunakan teknik statistik deskriptif, seperti distribusi frekuensi dan persentase, untuk menjelaskan temuan utama (Mackiewicz, 2018).

3. Hasil dan Pembahasan

Pada bagian ini, hasil penelitian disajikan dalam bentuk gambar untuk memberikan gambaran yang lebih jelas dan terstruktur. Penyajian ini mencakup analisis kebutuhan hingga pengolahan data, disusun secara sistematis sesuai dengan tujuan penelitian.

3.1. Hasil Penelitian

Penelitian ini dilakukan untuk mengidentifikasi tingkat keamanan informasi di Universitas Bhayangkara Jakarta Raya terhadap kejahatan siber, dan juga mengidentifikasi tingkat pemahaman dan kesadaran Mahasiswa/Mahasiswi terhadap ancaman keamanan siber (Sholikhatin et al., 2019). Berdasarkan survei yang telah dilakukan bersama dengan total 42 Mahasiswa/Mahasiswi sebagai responden, berikut adalah beberapa hasil table pada setiap pertanyaan yang sudah di berikan :

3.1.1. Infrastruktur teknologi

a. Pertanyaan Nomor 1 : Menurut kamu Infrastruktur teknologi apa yang digunakan di kampus ?

Tabel 1. Hasil Pertanyaan nomor 1

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	4	9.5	9.5	9.5
	2	6	14.3	14.3	23.8
	3	8	19.0	19.0	42.9
	4	24	57.1	57.1	100.0
	Total	42	100.0	100.0	

Sumber : Hasil Penelitian (2024)

Pada tabel 1 menjelaskan data survei, Hasil analisis menunjukkan bahwa pada Pertanyaan 1, mayoritas responden (57.1%) memilih kategori 4, yang menunjukkan preferensi tertinggi dalam variabel ini. Sedangkan kategori 3 dipilih oleh 19.0% responden, diikuti oleh kategori 2 (14.3%) dan kategori 1 (9.5%). Responden menunjukkan bahwa mayoritas memilih jaringan (LAN/WAN) sebagai infrastruktur yang digunakan, dengan Data Center dan Cloud Computing juga mendapatkan persentase signifikan (Hoshmand et al., 2023).

3.1.2. Pentingnya dan Kesiapan Keamanan Informasi

b. Pertanyaan nomor 2 : Seberapa penting keamanan informasi bagi kampus ?

Tabel 2. Hasil Pertanyaan nomor 2

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	3	7	16.7	16.7	16.7
	4	35	83.3	83.3	100.0
	Total	42	100.0	100.0	

Sumber : Hasil Penelitian (2024)

Pada tabel 2 menjelaskan data survei, Hasil analisis menunjukkan bahwa pada Pertanyaan 2, menunjukkan dominasi kategori 4 dengan persentase sebesar 83.3%, sementara kategori 3 dipilih oleh 16.7% responden. Variabel ini memperlihatkan tingkat keseragaman opini yang tinggi. Sebagian besar responden menilai keamanan informasi sangat penting. Hanya sedikit yang memberikan penilaian cukup penting, dan tidak ada responden yang memilih tidak penting.

c. Peranyaan nomor 3 : Apa saja jenis ancaman keamanan informasi yang pernah dialami oleh kampus menurut anda ?

Tabel 3. Hasil Pertanyaan nomor 3

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	21	50.0	50.0	50.0
	2	13	31.0	31.0	81.0
	3	1	2.4	2.4	83.3
	4	2	4.8	4.8	88.1
	5	4	9.5	9.5	97.6
	6	1	2.4	2.4	100.0
	Total	42	100.0	100.0	

Sumber : Hasil Penelitian (2024)

Pada tabel 3 menjelaskan data survei, Hasil analisis menunjukkan bahwa pada Pertanyaan 3, setengah dari total responden (50.0%) memilih kategori 1, sementara kategori 2 dipilih oleh 31.0%. Kategori 4, 5, dan 6 masing-masing dipilih oleh sejumlah kecil responden, yaitu 4.8%, 9.5%, dan 2.4%. Malware, phishing, dan serangan DDoS mendominasi jenis ancaman yang disebutkan, diikuti oleh insider threats dan pencurian data. Beberapa responden juga menambahkan kategori lain yang tidak disebutkan.

3.1.3. Ancaman Keamanan Informasi

d. Pertanyaan nomor 4 : Seberapa sering kampus menghadapi ancaman keamanan informasi ?

Tabel 4. Hasil Pertanyaan nomor 4

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	2	4.8	4.8	4.8
	2	25	59.5	59.5	64.3
	3	15	35.7	35.7	100.0
	Total	42	100.0	100.0	

Sumber : Hasil Penelitian (2024)

Pada tabel 4, menjelaskan bahwa pada Pertanyaan 4, berdasarkan data survei, menunjukkan bahwa sebagian besar responden (59.5%) memilih kategori 2, sedangkan kategori 3 dipilih oleh 35.7%. Kategori 1 hanya dipilih oleh 4.8% responden. Responden melaporkan bahwa kampus sering menghadapi ancaman keamanan informasi. Namun, sebagian kecil menyatakan jarang mengalami ancaman.

3.1.4. Perlindungan dan Respons Keamanan Informasi

e. Pertanyaan nomor 5 : Bagaimana Anda menilai tingkat kesiapan kampus dalam menghadapi ancaman keamanan informasi ?

Tabel 5. Hasil Pertanyaan nomor 5

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	2	4.8	4.8	4.8
	2	16	38.1	38.1	42.9
	3	20	47.6	47.6	90.5
	4	4	9.5	9.5	100.0
	Total	42	100.0	100.0	

Sumber : Hasil Penelitian (2024)

Pada tabel 5 menjelaskan bahwa pada Pertanyaan 5, berdasarkan data survei, distribusi terlihat lebih merata dibandingkan dengan variabel lainnya. Kategori 3 dipilih oleh hampir separuh responden (47.6%), diikuti oleh kategori 2 dengan persentase sebesar 38.1%. Sementara kategori 4 dan 1 masing-masing mendapatkan 9.5% dan 4.8%. Sebagian besar responden menilai kampus cukup siap, namun ada juga yang menilai kampus sangat siap.

f. Pertanyaan nomor 6 : Apa penyebab utama kerentanan keamanan informasi di kampus ?

Tabel 6. Hasil Pertanyaan nomor 6

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	10	23.8	23.8	23.8
	2	7	16.7	16.7	40.5
	3	16	38.1	38.1	78.6
	4	9	21.4	21.4	100.0
	Total	42	100.0	100.0	

Sumber : Hasil Penelitian (2024)

Pada tabel 6 menjelaskan bahwa pada Pertanyaan 6, berdasarkan data survei, mencatat bahwa kategori 3 merupakan yang paling banyak dipilih (38.1%), disusul oleh kategori 1 (23.8%), kategori 4 (21.4%), dan kategori 2 (16.7%). Faktor utama yang diidentifikasi adalah kelemahan pada perangkat lunak/sistem, diikuti oleh kurangnya kesadaran/kepedulian karyawan dan infrastruktur yang usang.

g. Pertanyaan nomor 7 : Seberapa besar Anda percaya bahwa pihak universitas telah menyediakan perlindungan yang memadai terhadap data mahasiswa ?

Tabel 7. Hasil Pertanyaan nomor 7

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	3	7.1	7.1	7.1
	2	18	42.9	42.9	50.0
	3	15	35.7	35.7	85.7
	4	6	14.3	14.3	100.0
	Total	42	100.0	100.0	

Sumber : Hasil Penelitian (2024)

Pada tabel 7 menjelaskan bahwa pada Pertanyaan 7, berdasarkan data survei, mayoritas responden memilih kategori 2 (42.9%), diikuti oleh kategori 3 (35.7%). Kategori 1 dan 4 masing-masing mendapatkan 7.1% dan 14.3%. Sebagian besar responden menyatakan cukup percaya atau percaya bahwa universitas menyediakan perlindungan yang memadai terhadap data mahasiswa.

3.1.5. Penyebab Kerentanan dan Metode Perlindungan

h. Pertanyaan nomor 8 : Metode apa yang digunakan oleh kampus untuk melindungi data sensitif ?

Tabel 8. Hasil Pertanyaan nomor 8

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	14	33.3	33.3	33.3
	2	11	26.2	26.2	59.5
	3	15	35.7	35.7	95.2
	4	2	4.8	4.8	100.0
	Total	42	100.0	100.0	

Sumber : Hasil Penelitian (2024)

Pada tabel 8 menjelaskan bahwa pada Pertanyaan 8, berdasarkan data survei, kategori 1 mendominasi dengan persentase sebesar 33.3%, diikuti oleh kategori 3 (35.7%) dan kategori

2 (26.2%). Kategori 4 dipilih oleh 4.8% responden. Firewall, sistem deteksi intrusi, dan antivirus/malware protection adalah metode yang paling sering disebutkan oleh responden.

i. Pertanyaan nomor 9 : Seberapa cepat kampus merespons insiden keamanan informasi ?

Tabel 9. Hasil Pertanyaan nomor *9*

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	6	14.3	14.3	14.3
	2	23	54.8	54.8	69.0
	3	8	19.0	19.0	88.1
	4	5	11.9	11.9	100.0
	Total	42	100.0	100.0	

Sumber : Hasil Penelitian (2024)

Pada tabel 9 menjelaskan bahwa pada Pertanyaan 9, berdasarkan data survei, menunjukkan bahwa lebih dari separuh responden (54.8%) memilih kategori 2. Kategori 3 dan 1 masing-masing dipilih oleh 19.0% dan 14.3% responden, sementara kategori 4 mendapatkan 11.9%. Responden mayoritas menilai kampus merespons dengan cepat, meskipun ada yang menyatakan cukup cepat.(Hobbs, 2023).

j. Pertanyaan nomor 10 : Apakah kampus memiliki tim khusus untuk menangani insiden keamanan informasi ?

Tabel 10. Hasil Pertanyaan nomor 10

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	8	19.0	19.0	19.0
	2	34	81.0	81.0	100.0
	Total	42	100.0	100.0	

Sumber : Hasil Penelitian (2024)

Pada tabel 10 menjelaskan bahwa pada Pertanyaan 10 ,berdasarkan data survei, menunjukkan bahwa mayoritas responden (81.0%) memilih kategori 2, sedangkan kategori 1 dipilih oleh 19.0% responden. Mayoritas responden menyatakan bahwa kampus memiliki tim

khusus untuk menangani insiden keamanan informasi, meskipun ada responden yang menyatakan sebaliknya.

3.2. Pembahasan

Secara keseluruhan, hasil penelitian ini menunjukkan kecenderungan kuat dalam beberapa variabel, seperti Pertanyaan ke-2 dan Pertanyaan ke-10, yang memiliki dominasi kategori tertentu. Hal ini mengindikasikan bahwa mayoritas responden memiliki pandangan yang konsisten terhadap pentingnya keamanan informasi di kampus dan keberadaan tim khusus untuk menangani insiden keamanan informasi.(Stallings et al., 2013) Sementara itu, variabel lainnya, seperti Pertanyaan ke-5 dan Pertanyaan ke-6, menunjukkan distribusi yang lebih merata, mencerminkan beragamnya pendapat responden mengenai kesiapan kampus dalam menghadapi ancaman dan faktor utama kerentanan keamanan informasi.(Ross J. Anderson, 2018)

Implikasi dari hasil survei ini adalah bahwa universitas perlu memperhatikan dua hal utama:

A. Peningkatan Infrastruktur Keamanan Informasi:

- Berdasarkan respon mayoritas, penting bagi universitas untuk memperkuat keberadaan tim khusus dengan memberikan pelatihan lebih lanjut, memastikan tim memiliki kompetensi dalam mengidentifikasi dan menangani ancaman terbaru.(Whitman & Mattord, 2011)
- Penerapan teknologi seperti machine learning untuk deteksi dini dan respons terhadap ancaman harus diprioritaskan. Hal ini dapat mempercepat waktu respons sekaligus meningkatkan akurasi dalam mengidentifikasi ancaman potensial.(Kingsley David Onyewuchi Ofoegbu et al., 2023)

B. Meningkatkan Kesadaran dan Kepedulian:

Hasil distribusi variabel terkait kesiapan kampus dan penyebab kerentanan menunjukkan perlunya kampus melakukan pelatihan rutin kepada staf dan mahasiswa mengenai pentingnya keamanan informasi. Misalnya, kampus dapat mengadakan seminar atau workshop berkala tentang praktik keamanan digital.

C. Penguatan Sistem Teknologi:

Mengingat adanya distribusi variabel yang menunjukkan kerentanan pada perangkat lunak usang dan infrastruktur lama, universitas perlu mengevaluasi ulang sistem yang digunakan. (Torres & Olipas, 2024)

Upgrade sistem menjadi versi yang lebih aman dan efisien dapat membantu menurunkan risiko ancaman.

- Melalui langkah-langkah di atas, hasil penelitian ini dapat menjadi pijakan untuk pengambilan keputusan strategis yang tidak hanya meningkatkan keamanan

informasi tetapi juga kepercayaan civitas akademika terhadap perlindungan data yang dilakukan oleh universitas.

4. Kesimpulan

Berdasarkan hasil penelitian, ancaman keamanan informasi di Universitas Bhayangkara Jakarta Raya mencakup serangan malware, phishing, DDoS, insider threats, dan pencurian data. Hasil survei menunjukkan bahwa sebagian besar responden menilai keamanan informasi sangat penting, meskipun kesiapan universitas dalam menghadapi ancaman masih dianggap cukup siap. Analisis menunjukkan faktor utama kerentanan adalah kelemahan perangkat lunak, kurangnya kesadaran karyawan, dan infrastruktur yang usang. Solusi yang dapat diterapkan meliputi penggunaan teknologi modern seperti machine learning untuk deteksi dan respons ancaman yang lebih cepat dan akurat. Penting pula untuk meningkatkan pelatihan kesadaran keamanan informasi di kalangan staf dan mahasiswa.

Daftar Pustaka

Gomm, R. (2008). Social Research Methodology. *Social Research Methodology*. https://doi.org/10.1007/978-0-230-22911-2

Hobbs, J. (2023). Cybersecurity awareness in higher education: a comparative analysis of faculty and staff. *Issues in Information Systems*, *24*(1), 159–169. https://doi.org/10.48009/1_iis_2023_114

Hoshmand, M. O., Ratnawati, S., & Korespondensi, E. P. (2023). Analisis Keamanan Infrastruktur Teknologi Informasi dalam Menghadapi Ancaman Cybersecurity. *Jurnal Sains Dan Teknologi*, *5*(2), 679–686. https://doi.org/10.55338/saintek.v5i2.2347

Kingsley David Onyewuchi Ofoegbu, Olajide Soji Osundare, Chidiebere Somadina Ike, Ololade Gilbert Fakeyede, & Adebimpe Bolatito Ige. (2023). Empowering users through AI-driven cybersecurity solutions: enhancing awareness and response capabilities. *Engineering Science & Technology Journal*, *4*(6), 707–727. https://doi.org/10.51594/estj.v4i6.1528

Mackiewicz, J. (2018). A Mixed-Method Approach. In *Writing Center Talk over Time*. https://doi.org/10.4324/9780429469237-3

Ross J. Anderson. (2018). Security Engineering - A Guide to Building Dependable Distributed Systems. In *Paper Knowledge . Toward a Media History of Documents*.

Sholikhatin, S. A., Setyanto, A., & Luthfi, E. T. (2019). Analisis Keamanan Sistem Informasi Dengan ISO 27001 (Studi Kasus: Sistem Informasi Akademik Universitas Muhammadiyah Purwokerto). *Jurnal Ilmiah IT CIDA*, *4*(1), 1–9. https://doi.org/10.55635/jic.v4i1.75

Stallings, W., Bauer, M., & Hirsch, E. M. (2013). *C OMPUTER S ECURITY Second Edition*.

Torres, R. A. G., & Olipas, C. N. P. (2024). *Analyzing Student Academic Performance and Cybersecurity Awareness Levels : Basis for Enhancing Instruction*. *45*(1), 304–314.

Whitman, M. E., & Mattord, H. J. (2011). Principles of Information Security Fourth Edition. *Learning*, 269, 289.