Volume 6 No.1 Maret 2026
E-ISSN : 2808-2478
Website : https://journal.aiska-university.ac.id/index.php/empowerment
E-mail : empowerment@aiska-university.ac.id
Doi : https://doi.org/10.30787/empowerment.v6i1.2395

EMPOWERMENT JOURNAL
Universitas 'Aisyiyah Surakarta

PENGETAHUAN MAHASISWA MENGENAI ISU KEAMANAN SEKURITI PADA PUSAT DATA NASIONAL: RANSOMWARE

Latifah Iriani[1], Ridho Surya Kusuma[2], Muhammad Immawan[3], Rakhmat Prasetyo Agung Nugroho[4], Joko Supriyanto[5], Andi Sugandi[6]

[1] Program Studi PJJ Informatika, Universitas Siber Muhammadiyah, DI Yogyakarta, Indonesia
[2] Program Studi Informatika, Universitas Islam Mulia, DI Yogyakarta, Indonesia
email: latifahiriani@sibermu.ac.id

ABSTRAK

Pusat Data Nasional (PDN) merupakan infrastruktur vital yang rentan terhadap berbagai ancaman keamanan siber, termasuk ransomware. Penelitian ini bertujuan untuk mengukur peningkatan pengetahuan mahasiswa terkait keamanan siber setelah mengikuti kegiatan edukatif berbasis webinar. Metode yang digunakan adalah kuasi-eksperimen dengan desain one-group pre-test–post-test terhadap 50 mahasiswa dari dua perguruan tinggi. Instrumen penelitian berupa soal pre-test dan post-test yang diberikan sebelum dan sesudah webinar. Hasil penelitian menunjukkan adanya peningkatan signifikan, dengan nilai rata-rata pre-test sebesar 52,5 meningkat menjadi 85,3 pada post-test atau naik sebesar 32,8 poin. Selain itu, jumlah peserta dengan nilai sempurna meningkat dari 3 menjadi 11 orang, dan hampir seluruh peserta mengalami peningkatan skor. Hasil ini menunjukkan bahwa webinar efektif dalam meningkatkan pengetahuan mahasiswa mengenai keamanan siber, khususnya ancaman ransomware pada PDN.

Kata Kunci: Pusat Data Nasional (PDN), Ransomware, Kesadaran Keamanan Siber

ABSTRACT

The National Data Center (PDN) is a vital infrastructure that is vulnerable to various cybersecurity threats, including ransomware. This study aims to measure the improvement of students' knowledge regarding cybersecurity after participating in a webinar-based educational activity. The research employed a quasi-experimental method with a one-group pre-test–post-test design involving 50 students from two universities. The research instrument consisted of pre-test and post-test questions administered before and after the webinar. The results showed a significant improvement, with the average pre-test score of 52.5 increasing to 85.3 in the post-test, indicating a gain of 32.8 points. In addition, the number of participants achieving perfect scores increased from 3 to 11, and almost all participants experienced score improvements. These findings indicate that webinars are effective in enhancing students' knowledge of cybersecurity, particularly ransomware threats to the PDN.

***Keywords**: National Data Center (PDN), Ransomware, Cybersecurity Awareness*

PENDAHULUAN

Perkembangan teknologi digital yang pesat telah mengubah lanskap ancaman keamanan nasional secara signifikan. Serangan siber yang semakin canggih dan terorganisir telah menjadi ancaman nyata bagi kedaulatan negara, infrastruktur kritis, dan kepentingan nasional. Dalam konteks ini, pembentukan angkatan siber menjadi semakin mendesak. Keberadaan angkatan siber yang profesional dan terlatih akan memungkinkan suatu negara untuk membangun pertahanan siber yang kuat, menangkal serangan siber, dan melakukan operasi siber defensif secara proaktif (Kementerian Komunikasi dan Informatika, 2024).

Perkembangan teknologi digital telah meningkatkan kompleksitas ancaman keamanan siber, terutama pada infrastruktur kritis seperti Pusat Data Nasional (PDN). PDN berperan penting dalam

pengelolaan data pemerintah dan publik, sehingga menjadi target strategis berbagai serangan siber, termasuk ransomware. Serangan ini dapat menyebabkan gangguan operasional, kerugian finansial, serta menurunkan kepercayaan publik terhadap sistem informasi (Von Solms and Van Niekerk, 2013). Selain itu, meningkatnya kasus kebocoran data dan kejahatan siber menunjukkan bahwa keamanan data menjadi isu yang semakin mendesak untuk ditangani (Fikri Irfan Adristi and Erika Ramadhani, 2024)(Sahatatua et.al, 2024).

Ransomware merupakan salah satu ancaman paling berbahaya dalam keamanan siber karena mampu mengenkripsi data dan menahan akses hingga tebusan dibayarkan (Caroscio *et al.*, 2022)(Kumar, 2023). Perkembangannya yang semakin kompleks telah berdampak luas pada berbagai sektor, termasuk pemerintahan dan infrastruktur publik (Ansori, 2024). Dalam konteks ini, faktor manusia menjadi salah satu titik lemah utama dalam sistem keamanan siber, sehingga peningkatan pengetahuan dan kesadaran pengguna menjadi aspek penting dalam upaya mitigasi risiko (Chandarman and Niekerk, 2017)(Moallem, 2019).

Sejumlah penelitian sebelumnya telah membahas keamanan siber, deteksi ransomware, serta pentingnya cybersecurity awareness melalui pendekatan teknis maupun edukatif (Arbanas and Hrustek, 2019)(Alraizza and Algarni, 2023). Namun, sebagian besar penelitian masih berfokus pada aspek teknis atau konseptual, dan belum banyak yang mengkaji efektivitas intervensi edukatif secara langsung terhadap peningkatan pengetahuan pengguna. Selain itu, penelitian yang secara spesifik mengukur peningkatan pemahaman mahasiswa melalui pendekatan kuantitatif dengan desain pre-test dan post-test, khususnya pada konteks keamanan PDN, masih terbatas.

Berdasarkan gap tersebut, penelitian ini bertujuan untuk menganalisis peningkatan pengetahuan mahasiswa mengenai isu keamanan sekuriti pada PDN, khususnya ancaman ransomware, melalui kegiatan webinar. Penelitian ini menggunakan pendekatan pre-test dan post-test untuk mengukur efektivitas intervensi edukatif dalam meningkatkan literasi keamanan siber di kalangan mahasiswa.

METODE

Penelitian ini bertujuan untuk mengevaluasi pengetahuan mahasiswa mengenai isu keamanan sekuriti pada Pusat Data Nasional, khususnya mengenai ancaman ransomware, melalui pendekatan edukatif berbasis webinar. Metode yang digunakan adalah kuasi-eksperimen dengan desain one-group pre-test–post-test. Penelitian ini dilaksanakan secara daring dengan melibatkan mahasiswa dari Universitas Siber Muhammadiyah dan Universitas Islam Mulia, yang berlokasi di Daerah Istimewa Yogyakarta, pada bulan 20 Juli 2024, dengan durasi kegiatan webinar selama 2 jam dalam satu sesi. Metode penelitian ini meliputi beberapa tahapan, yaitu:

1. Webinar Series
   Webinar series dirancang untuk memberikan pemahaman mendalam tentang isu keamanan sekuriti pada Pusat Data Nasional. Materi webinar mencakup topik-topik seperti pengenalan dasar keamanan siber, teknik perlindungan terhadap ransomware, dan studi kasus serangan ransomware pada infrastruktur penting. Webinar dilakukan secara daring selama 2 jam. Setiap sesi diisi oleh pakar di bidang cybersecurity dan diikuti dengan sesi tanya jawab untuk memperdalam pemahaman peserta.
2. Pre-Test
   Sebelum dimulainya webinar series, mahasiswa yang menjadi peserta diminta untuk mengikuti pre-test. Pre-test ini bertujuan untuk mengukur tingkat pemahaman awal mahasiswa tentang isu keamanan siber, khususnya mengenai ancaman ransomware. Soal pre-test dirancang untuk

mengevaluasi pengetahuan konseptual dan praktis mengenai teknik-teknik dasar keamanan siber. Pengambilan pre-test dengan menggunakan media quizzes.

3. Post-Test
   Setelah mengikuti seluruh rangkaian webinar, mahasiswa diwajibkan mengikuti post-test yang sama dengan pre-test. Post-test ini bertujuan untuk mengukur peningkatan pengetahuan dan pemahaman mahasiswa setelah mengikuti webinar series. Hasil dari pre-test dan post-test akan dibandingkan untuk menilai efektivitas dari webinar dalam meningkatkan pengetahuan mahasiswa mengenai keamanan siber. Pengambilan pre-test dengan menggunakan media quizzes.
4. Sampel Penelitian
   Sampel penelitian ini terdiri dari mahasiswa program studi informatika dari Universitas Islam Mulia (UIM) dan Universitas Siber Muhammadiyah (Sibermu). Pemilihan sampel dilakukan secara acak dari mahasiswa yang telah menyatakan minat untuk berpartisipasi dalam webinar series. Total peserta yang terlibat dalam penelitian ini adalah 50 mahasiswa, dengan distribusi yang seimbang dari kedua universitas.
5. Teknik Analisis Data
   Data dianalisis secara kuantitatif menggunakan statistik deskriptif untuk mengetahui nilai rata-rata *pre-test* dan *post-test* serta peningkatan yang terjadi. Selain itu, perhitungan N-Gain digunakan untuk mengukur tingkat efektivitas kegiatan dalam meningkatkan pengetahuan mahasiswa. Hasil analisis ini digunakan untuk mengevaluasi keberhasilan program webinar dalam meningkatkan literasi keamanan siber.

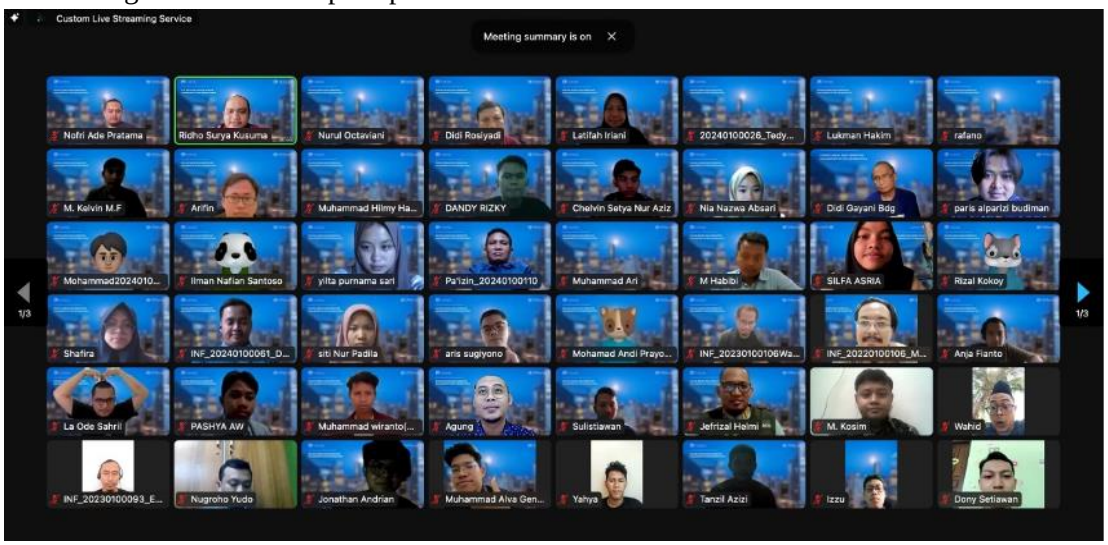
Data yang diperoleh dari pre-test dan post-test dianalisis secara kuantitatif untuk mengidentifikasi perubahan signifikan dalam pengetahuan mahasiswa. Analisis statistik digunakan untuk menilai efektivitas webinar sebagai metode edukasi dalam meningkatkan kesadaran dan pemahaman mahasiswa tentang ancaman siber, khususnya ransomware. Hasil analisis ini diharapkan dapat memberikan gambaran mengenai strategi edukasi yang efektif dalam meningkatkan literasi keamanan siber di kalangan mahasiswa.

HASIL PEMBAHASAN

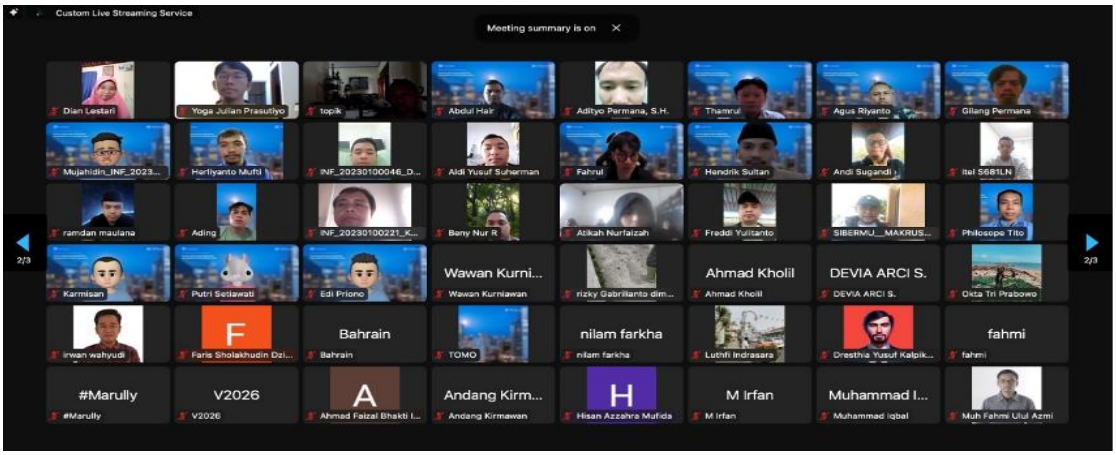
Penelitian ini melibatkan 50 koresponden dari mahasiswa program studi informatika yang mengikuti webinar series mengenai keamanan siber dan ancaman ransomware. Berikut undangan terbuka secara umum untuk mahasiswa melalui konten gambar yang dapat diakses melalui platform Instagram seperti pada Gambar 1.

Gambar 1. Konten Webinar di Instagram

Gambar 1 merupakan ajakan kepada mahasiswa umum, khususnya mahasiswa yang memiliki latar belakang keilmuan informatika atau informasi untuk bersama-sama membahas tentang "Trust Issue dan Serangan Ransomware ke PDN". Pembahasan ini tentunya menjadi tantangan dan solusi untuk keamanan siber yang lebih baik. Oleh karena itu, penting bagi generasi muda untuk lebih memahami faktor-faktor keamanan khususnya serangan Ransomware. Beriku foto para peserta yang hadir dalam kegiatan tersebut seperti pada Gambar 2 dan 3.

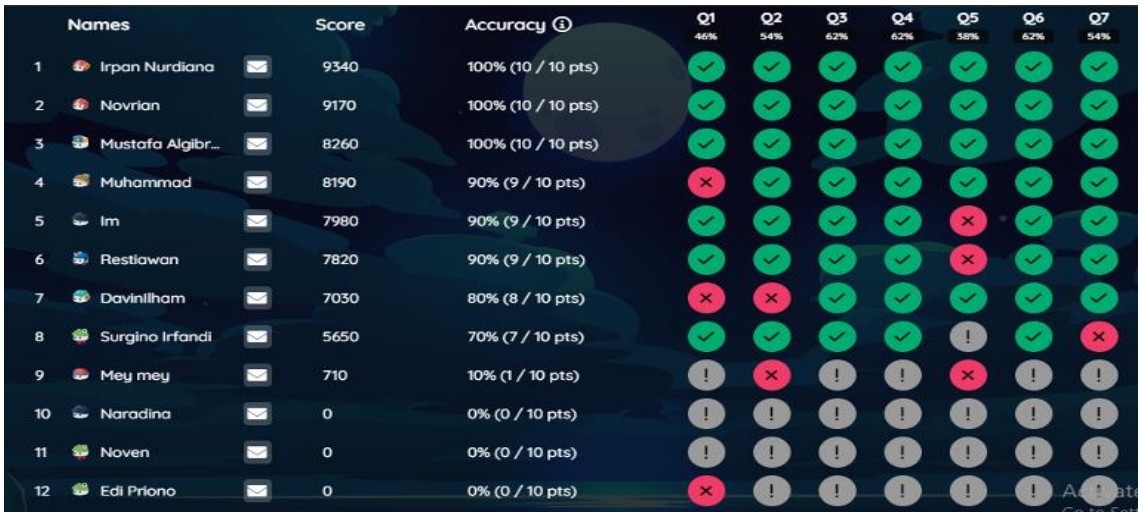


Gambar 2. Para peserta webinar di layar pertama



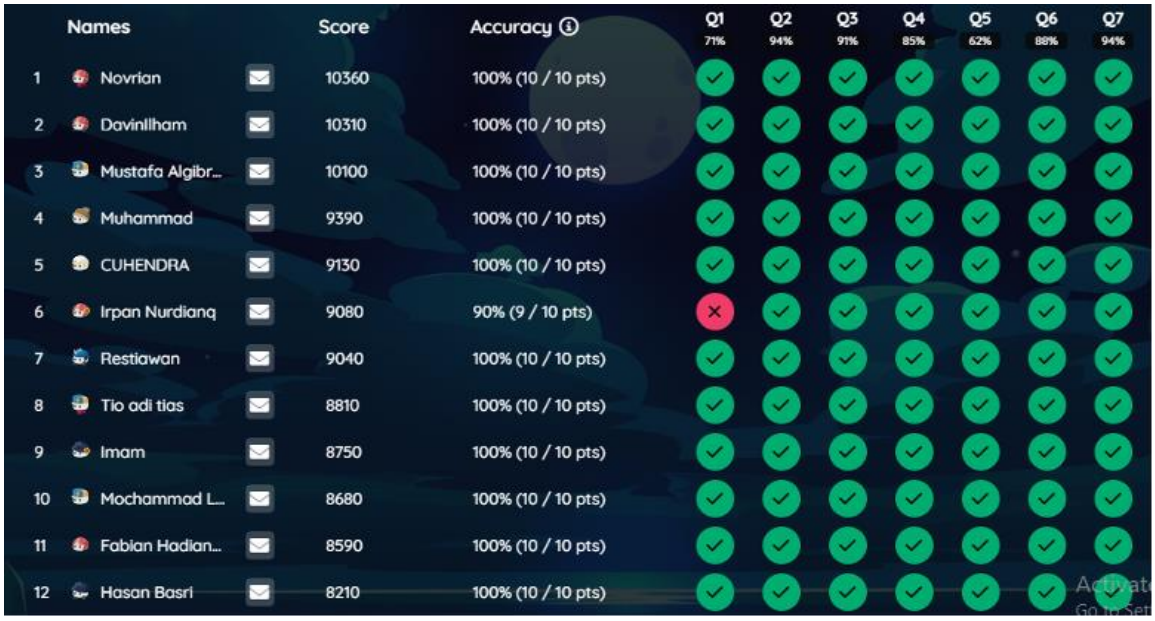
Gambar 3. Para peserta webinar di layar kedua

Penelitian ini melakukan analisis data dengan membandingkan pengetahuan peserta webinar melalui hasil pre-test dan post-test untuk mengukur peningkatan pemahaman mahasiswa setelah mengikuti webinar. Hasil pre-test dapat dilihat pada Gambar 4 dan post-test di Gambar 5.



	Names	Score	Accuracy	Q1 46%	Q2 54%	Q3 62%	Q4 62%	Q5 38%	Q6 62%	Q7 54%
1	Irpan Nurdiana	9340	100% (10 / 10 pts)	✓	✓	✓	✓	✓	✓	✓
2	Novrian	9170	100% (10 / 10 pts)	✓	✓	✓	✓	✓	✓	✓
3	Mustafa Algibr...	8260	100% (10 / 10 pts)	✓	✓	✓	✓	✓	✓	✓
4	Muhammad	8190	90% (9 / 10 pts)	✗	✓	✓	✓	✓	✓	✓
5	Im	7980	90% (9 / 10 pts)	✓	✓	✓	✓	✗	✓	✓
6	Restiawan	7820	90% (9 / 10 pts)	✓	✓	✓	✓	✗	✓	✓
7	Davinllham	7030	80% (8 / 10 pts)	✗	✗	✓	✓	✓	✓	✓
8	Surgino Irfandi	5650	70% (7 / 10 pts)	✓	✓	✓	✓	!	✓	✗
9	Mey mey	710	10% (1 / 10 pts)	!	✗	!	!	✗	!	!
10	Naradina	0	0% (0 / 10 pts)	!	!	!	!	!	!	!
11	Noven	0	0% (0 / 10 pts)	!	!	!	!	!	!	!
12	Edi Priono	0	0% (0 / 10 pts)	✗	!	!	!	!	!	!

Gambar 4. Hasil pre-test webinar



	Names	Score	Accuracy	Q1 71%	Q2 94%	Q3 91%	Q4 85%	Q5 62%	Q6 88%	Q7 94%
1	Novrian	10360	100% (10 / 10 pts)	✓	✓	✓	✓	✓	✓	✓
2	Davinllham	10310	100% (10 / 10 pts)	✓	✓	✓	✓	✓	✓	✓
3	Mustafa Algibr...	10100	100% (10 / 10 pts)	✓	✓	✓	✓	✓	✓	✓
4	Muhammad	9390	100% (10 / 10 pts)	✓	✓	✓	✓	✓	✓	✓
5	CUHENDRA	9130	100% (10 / 10 pts)	✓	✓	✓	✓	✓	✓	✓
6	Irpan Nurdianq	9080	90% (9 / 10 pts)	✗	✓	✓	✓	✓	✓	✓
7	Restiawan	9040	100% (10 / 10 pts)	✓	✓	✓	✓	✓	✓	✓
8	Tio adi tias	8810	100% (10 / 10 pts)	✓	✓	✓	✓	✓	✓	✓
9	Imam	8750	100% (10 / 10 pts)	✓	✓	✓	✓	✓	✓	✓
10	Mochammad L...	8680	100% (10 / 10 pts)	✓	✓	✓	✓	✓	✓	✓
11	Fabian Hadian...	8590	100% (10 / 10 pts)	✓	✓	✓	✓	✓	✓	✓
12	Hasan Basri	8210	100% (10 / 10 pts)	✓	✓	✓	✓	✓	✓	✓

Gambar 5. Hasil post-test webinar

Hasil analisis data pre-test dan post-test menunjukkan adanya peningkatan pemahaman peserta setelah mengikuti kegiatan webinar. Berdasarkan analisis deskriptif, rata-rata nilai pre-test sebesar 52,5 meningkat menjadi 85,3 pada post-test, dengan selisih peningkatan sebesar 32,8 poin. Hal ini menunjukkan bahwa kegiatan edukasi yang diberikan mampu meningkatkan pengetahuan mahasiswa mengenai keamanan siber. Selain itu, berdasarkan perhitungan N-Gain diperoleh nilai sebesar 0,69 yang termasuk dalam kategori sedang (mendekati tinggi). Hasil ini menunjukkan bahwa kegiatan webinar memiliki tingkat efektivitas yang baik dalam meningkatkan pemahaman mahasiswa. Hampir seluruh peserta mengalami peningkatan nilai, kecuali satu peserta yang telah memperoleh nilai maksimal sejak pre-test.

Analisis lebih lanjut menunjukkan adanya peningkatan jumlah peserta yang mencapai nilai sempurna dari 3 orang pada pre-test menjadi 11 orang pada post-test. Tidak ditemukan adanya penurunan nilai pada peserta, yang menunjukkan bahwa kegiatan webinar mampu mengakomodasi berbagai tingkat kemampuan awal peserta secara merata. Sebagian besar peserta yang awalnya

memiliki nilai rendah pada pre-test mengalami peningkatan yang cukup signifikan pada post-test. Hal ini menunjukkan bahwa materi yang disampaikan dalam webinar dapat diterima dan dipahami dengan baik oleh mahasiswa. Namun, terdapat satu peserta yang tidak mengalami peningkatan nilai, yang kemungkinan disebabkan oleh faktor eksternal seperti kurangnya partisipasi atau kendala teknis selama kegiatan berlangsung. Hal ini menjadi bahan evaluasi untuk pelaksanaan kegiatan serupa di masa mendatang.

Temuan ini sejalan dengan penelitian sebelumnya yang menyatakan bahwa peningkatan cybersecurity awareness melalui pendekatan edukatif merupakan salah satu faktor penting dalam memperkuat keamanan sistem informasi(Chandarman and Niekerk, 2017). Selain itu, efektivitas metode pembelajaran berbasis edukasi dalam meningkatkan pemahaman konsep juga didukung oleh penelitian (Arbanas and Hrustek, 2019) yang menekankan pentingnya strategi pembelajaran dalam keamanan sistem informasi. Dengan demikian, hasil kegiatan ini memperkuat bahwa pendekatan edukatif seperti webinar dapat menjadi solusi efektif dalam meningkatkan literasi keamanan siber, khususnya dalam menghadapi ancaman ransomware.

Secara keseluruhan, hasil kegiatan pengabdian ini menunjukkan bahwa webinar series merupakan metode edukasi yang efektif dalam meningkatkan literasi keamanan siber mahasiswa, khususnya terkait ancaman ransomware pada Pusat Data Nasional. Oleh karena itu, kegiatan serupa dapat terus dikembangkan sebagai upaya peningkatan kesadaran dan pengetahuan keamanan siber di kalangan mahasiswa maupun masyarakat umum.

KESIMPULAN

Kegiatan pengabdian ini menunjukkan bahwa pendekatan edukatif berbasis webinar series efektif dalam meningkatkan pengetahuan mahasiswa mengenai isu keamanan siber, khususnya dalam menghadapi ancaman ransomware. Berdasarkan hasil analisis pre-test dan post-test, terdapat peningkatan rata-rata nilai sebesar 32,8 poin, yang mencerminkan efektivitas metode pembelajaran yang digunakan. Sebanyak 34 dari 50 peserta mengalami peningkatan nilai, dengan 11 peserta mencapai nilai sempurna pada post-test, yang menunjukkan pemahaman yang baik terhadap materi yang diberikan. Dengan demikian, webinar series dapat menjadi salah satu alternatif metode edukasi yang efektif dalam meningkatkan literasi keamanan siber di kalangan mahasiswa.

Sebagai rekomendasi, kegiatan serupa dapat dikembangkan dengan cakupan peserta yang lebih luas, tidak hanya terbatas pada mahasiswa tetapi juga masyarakat umum. Selain itu, diperlukan pengembangan materi yang lebih interaktif dan berkelanjutan, seperti pelatihan praktik langsung atau simulasi serangan siber, untuk meningkatkan pemahaman secara lebih mendalam. Penelitian atau kegiatan selanjutnya juga disarankan untuk mengeksplorasi metode edukasi lain serta mengukur dampak jangka panjang dari peningkatan literasi keamanan siber terhadap perilaku pengguna dalam menghadapi ancaman digital.

DAFTAR PUSTAKA

Alraizza, A. and Algarni, A. (2023) ‘Ransomware Detection Using Machine Learning: A Survey’, *Big Data and Cognitive Computing*, 7(3). Available at: https://doi.org/10.3390/bdcc7030143.

Ansori, A. (2024) ‘Mitigation of Malware Ransomware Virus’, *MATICS: Jurnal Ilmu Komputer dan Teknologi Informasi (Journal of Computer Science and Information Technology)*, 16(2), pp. 76–83. Available at: https://doi.org/10.18860/mat.v16i2.28794.

Arbanas, K. and Hrustek, N.Ž. (2019) ‘Key success factors of information systems security’, *Journal*

of Information and Organizational Sciences, 43(2), pp. 131–144. Available at: https://doi.org/10.31341/jios.43.2.1.

Caroscio, E. *et al.* (2022) 'Analyzing the Ransomware Attack on D.C. Metropolitan Police Department by Babuk', *SysCon 2022 - 16th Annual IEEE International Systems Conference, Proceedings* [Preprint]. Available at: https://doi.org/10.1109/SysCon53536.2022.9773935.

Chandarman, R. and Niekerk, B. Van (2017) 'Students ' Cybersecurity Awareness at a Private Tertiary Educational', *The African Journal of Information and Communication (AJIC)*, (20), pp. 133–155.

Fikri Irfan Adristi and Erika Ramadhani (2024) 'Analisis Dampak Kebocoran Data Pusat Data Nasional Sementara 2 (PDNS 2) Surabaya: Pendekatan Matriks Budaya Keamanan Siber dan Dimensi Budaya Nasional Hofstede', *Selekta Manajemen: Jurnal Mahasiswa Bisnis & Manajemen*, 02(06), pp. 196–212. Available at: https://journal.uii.ac.id/selma/index.

Kementerian Komunikasi dan Informatika (2024) *Antisipasi Perang Digital, Wamenkominfo Paparkan Urgensi Pembentukan Angkatan Siber.*

Kumar, J. (2023) 'Enhancing Public Awareness and Education of Ransomware Attacks', *Authorea Preprints*, 12. Available at: https://www.authorea.com/doi/full/10.36227/techrxiv.24634806.v1?commit=1390bbb35ca8e4214049cff3bb29bc241c2f155e.

Moallem, A. (2019) 'Cyber Security Awareness Among College Students', *Advances in Intelligent Systems and Computing*, 782, pp. 79–87. Available at: https://doi.org/10.1007/978-3-319-94782-2_8.

Sahatatua, R., Gusmaria, Y., Astawa, I. K., Suherman, A. M., Setiady, T., & Tinambunan, W.D. (2024) 'Cyber law analysis of E-KTP data leakage: A case approach of 102 million KTP data allegedly leaked from the Ministry of Social Affairs to a hacker forum', *Journal of Multidisciplinary Academic and Practice Studies*, 2(3), pp. 261–265. Available at: https://doi.org/10.35912/JOMAPS.V2I3.2219.

Von Solms, R. and Van Niekerk, J. (2013) 'From information security to cyber security', *Computers and Security*, 38, pp. 97–102. Available at: https://doi.org/10.1016/j.cose.2013.04.004.