Welfare : Jurnal Pengabdian Masyarakat
Volume 3, Issue 3, 2025
e-ISSN : 2986-5824
https://jurnalfebi.iainkediri.ac.id/index.php/Welfare

Pengenalan dan Pencegahan Ransomware dalam Dunia Penerbangan: Penguatan Literasi Siber bagi Siswa SMK Dirgantara Putra Bangsa

Faiz Albanna[1], Faiz Albanna[2], Gallis Nawang Ginusti[3], Irfan Abdulhafizh Karnaen[4], Yunus Purnama[5], Irwina Meilani[6], Adipura Danang Maulana[7], Andi Syaputra[8]
Sekolah Tinggi Teknologi Kedirgantaraan Yogyakarta
faiz@sttkd.ac.id[1], ristiani@sttkd.ac.id[2]

Article Info

Volume 3 Issue 3
September 2025

DOI :
10.30762/welfare.v3i3.2637

Article History
Submission: 19-08-2025
Revised: 21-08-2025
Accepted: 22-08-2025
Published: 25-09-2025

Keywords:
Aviation industry, Cybersecurity, Ransomware, Service learning.

Kata Kunci:
Industri penerbangan, Keamanan siber, *Ransomware*, *Service learning.*

Abstract

The increasing integration of digital technology in the aviation industry highlights the need to improve cybersecurity literacy, particularly concerning ransomware threats. This community service program aimed to enhance students' understanding of ransomware threats and prevention strategies at SMK Dirgantara Putra Bangsa. The program involved collaborative efforts of lecturers and vocational students from STTKD through four stages: planning, preparation, implementation, and evaluation. An interactive seminar method was applied with support from professional speakers from Rumahweb. Evaluation was conducted using digital-based pre-test and post-test questionnaires. Results showed a significant increase in average scores from 15.29 to 21.38, with a strong positive correlation (r = 0.731) and high statistical significance (p = 0.000). The activity was documented and published on YouTube and Harian Jogja to extend its impact. This initiative demonstrates the effectiveness of collaboration between vocational education and industry in raising cybersecurity awareness among young learners through experiential learning.

Abstrak

Meningkatnya integrasi digital di industri penerbangan mendorong perlunya peningkatan literasi keamanan siber, khususnya terkait ransomware. Kegiatan pengabdian ini bertujuan meningkatkan pemahaman siswa SMK Dirgantara Putra Bangsa mengenai ancaman dan pencegahan *ransomware*. Kegiatan dirancang dengan pendekatan *service learning,* melibatkan dosen dan taruna STTKD dalam empat tahap: perencanaan, persiapan, pelaksanaan, dan evaluasi. Metode seminar interaktif digunakan dengan dukungan narasumber profesional dari Rumahweb. Evaluasi dilakukan melalui kuesioner pre-test dan post-test berbasis digital. Hasil menunjukkan peningkatan rata-rata nilai dari 15,29 menjadi 21,38, dengan korelasi positif (r = 0,731) dan signifikansi tinggi (p = 0,000). Dokumentasi kegiatan dipublikasikan melalui YouTube dan Harian Jogja untuk memperluas dampak. Program ini membuktikan efektivitas kolaborasi antara pendidikan vokasi dan dunia industri dalam meningkatkan kesadaran keamanan siber generasi muda melalui pembelajaran berbasis pengalaman.

1. PENDAHULUAN

Sampah merupakan

Peningkatan konektivitas dan digitalisasi dalam berbagai sektor kehidupan telah mendorong transformasi yang signifikan, namun di sisi lain juga memperluas peluang bagi pelaku kejahatan siber untuk meluncurkan serangan berskala besar. Salah satu bentuk serangan yang paling merugikan dan terus berkembang adalah *ransomware*, yaitu jenis perangkat lunak berbahaya (*malware*) yang mengenkripsi data korban dan meminta tebusan (*ransom*) agar data tersebut dapat dipulihkan. Serangan ini menargetkan data penting milik individu maupun organisasi dengan cara mengenkripsi *file* dan menuntut tebusan untuk mengembalikannya (Kapoor *et al.*, 2022). Meskipun teknologi keamanan terus berkembang, lemahnya kesadaran dan kesiapsiagaan pengguna serta kerentanan sistem informasi, terutama pada skala kecil dan

Korespondensi:
Aziza Anggi Maiyanti
azizaanggimaiyanti@iainkediri.ac.id

menengah, memungkinkan serangan ini melampaui lapisan keamanan dasar dan menyebabkan gangguan signifikan terhadap operasional bisnis (Kara, 2024; Kapoor *et al*., 2022).

Fenomena *ransomware* bukanlah hal baru, namun serangannya mengalami peningkatan yang signifikan dalam beberapa tahun terakhir. Peristiwa besar seperti serangan *WannaCry* dan *Petya* pada tahun 2017 menjadi bukti nyata bahwa dampak *ransomware* tidak dapat dianggap remeh. Dalam waktu singkat, ribuan mesin di lebih dari 150 negara terdampak, menyebabkan kerugian finansial yang besar bagi berbagai sektor, termasuk kesehatan, pendidikan, serta minyak dan gas (Gudimetla, 2022; Mansfield-Devine, 2017). Di masa pandemi Covid-19, kerentanan ini semakin meningkat karena pergeseran sistem kerja ke arah daring atau kerja jarak jauh yang melemahkan pengawasan keamanan siber. Kampanye *phishing*, yaitu upaya penipuan daring dengan menyamar sebagai pihak tepercaya untuk mencuri informasi sensitif, bertema pandemi menjadi sarana yang efektif bagi penyerang untuk mengeksploitasi informasi sensitif pengguna (Saleous, Ismail, Aldaajeh, & Madathil, 2022).

Kondisi serupa juga terjadi di Indonesia. Berdasarkan penelitian Parulian *et al*. (2021), tercatat lebih dari 741 juta ancaman siber terjadi antara Januari hingga Juli 2021, dengan jenis serangan seperti *Denial of Service* (*DoS*), *phishing*, dan pencurian data pribadi. Dalam konteks transportasi udara, ancaman ini semakin relevan mengingat banyaknya sistem yang terintegrasi dengan teknologi informasi, seperti sistem reservasi tiket, data penumpang, dan sistem komunikasi pesawat (Lutfah, 2022). Serangan siber terbaru yang menyerang Pusat Data Nasional (PDN) turut memperkuat urgensi peningkatan kesadaran dan kesiapan siber, meskipun Direktorat Jenderal Perhubungan Udara memastikan tidak ada gangguan terhadap layanan navigasi penerbangan (Antara, 2024).

Sebagai respons terhadap meningkatnya ancaman tersebut, Direktorat Jenderal Perhubungan Udara melalui kerja sama dengan Badan Siber dan Sandi Negara (BSSN) telah membentuk Tim Tanggap Insiden Siber Sektor Transportasi Udara atau *Indonesia Aviation Sector Computer Security Incident Response Team* (*IAS-CSIRT*) serta menyelenggarakan forum seperti *Cyber Security in Aviation* sebagai upaya penguatan sistem keamanan siber nasional di sektor penerbangan (Humas DJPUb, 2022; Humas DJPUc, 2022). Namun demikian, mitigasi risiko siber juga memerlukan keterlibatan aktif dari lembaga pendidikan yang menghasilkan sumber daya manusia di bidang penerbangan.

Sekolah Menengah Kejuruan (SMK) Dirgantara Putra Bangsa, yang berlokasi di Sleman, Yogyakarta, merupakan salah satu institusi pendidikan yang mempersiapkan lulusan sebagai tenaga kerja tingkat menengah di sektor transportasi udara dan pariwisata, khususnya dalam bidang staf maskapai dan pramugari/pramugara (SMKS Dirgantara Putra Bangsa, 2024). Para siswa dibekali dengan kompetensi melalui pembelajaran kelas dan praktik kerja lapangan (*on the job training*/*OJT*) di berbagai bandar udara dan maskapai mitra. Namun, berdasarkan pengamatan, pembekalan yang diberikan sebelum praktik kerja masih terbatas pada aspek pelayanan penumpang, bagasi, kargo, dan bea cukai, tanpa mencakup aspek penting terkait keamanan siber, khususnya mengenai ancaman *ransomware* di sektor penerbangan (Ristiani *et al*., 2024).

Kerentanan terhadap serangan siber, seperti yang terjadi pada sistem reservasi dan teknologi informasi di bandar udara, menunjukkan perlunya pengetahuan dasar mengenai keamanan siber bagi para calon tenaga kerja di bidang penerbangan (Humas DJPUa, 2018). Oleh karena itu, kegiatan pengabdian kepada masyarakat ini bertujuan untuk memberikan pembekalan mengenai pengenalan dan pencegahan *ransomware* di bidang transportasi udara kepada siswa dan siswi SMK Dirgantara Putra Bangsa.

Melalui penguatan kapasitas siswa dalam mengenali dan mencegah serangan *ransomware*, kegiatan ini menawarkan solusi strategis dalam mendukung ketahanan siber nasional, khususnya di bidang penerbangan. Kajian teoritis menunjukkan bahwa pemberdayaan sumber daya manusia melalui edukasi keamanan siber dapat menjadi langkah awal yang efektif dalam pencegahan kejahatan siber berbasis sosial dan teknologi (Saleous *et al*., 2022). Dengan adanya kegiatan ini, diharapkan lulusan SMK Dirgantara Putra Bangsa tidak hanya kompeten secara teknis dalam pelayanan penerbangan, tetapi juga memiliki kesadaran terhadap ancaman siber yang relevan dengan lingkungan kerja mereka di masa depan.

2. METODE

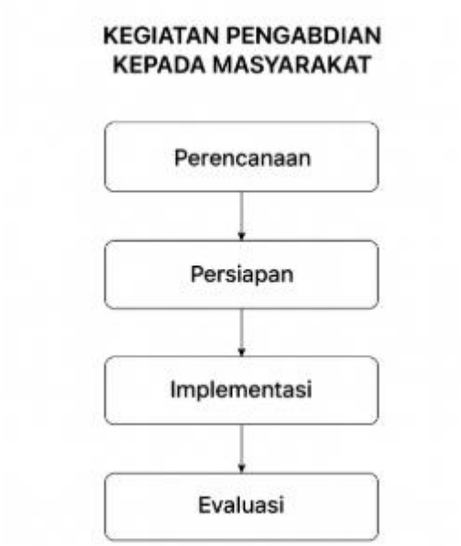
Metode Kegiatan pengabdian kepada masyarakat ini merupakan bagian dari implementasi program kolaborasi pendidikan vokasi antara dosen dan taruna Sekolah Tinggi Teknologi Kedirgantaraan (STTKD), yang dirancang dengan pendekatan *service learning*. Kegiatan ini menyasar siswa kelas X SMK Dirgantara Putra Bangsa, Sleman, Yogyakarta, dan dilaksanakan secara luring pada 12 Maret 2025 dengan melibatkan 24 peserta. Metode utama yang digunakan

adalah ceramah interaktif yang dipadukan dengan diskusi dan evaluasi menggunakan instrumen digital (*Google Form*). Seluruh kegiatan dilaksanakan melalui empat tahap, yaitu: perencanaan, persiapan, implementasi, dan evaluasi.

Pada tahap perencanaan, tim dosen melakukan koordinasi langsung dengan pihak sekolah untuk menjadwalkan kegiatan, menentukan lokasi, serta menyepakati topik pengabdian yang relevan, yaitu keamanan siber dengan fokus pada isu *ransomware* di sektor transportasi udara. Materi disiapkan oleh tim dosen dengan melibatkan narasumber profesional dari luar institusi. Tahap persiapan mencakup penyusunan surat tugas dan izin kegiatan, pengembangan instrumen evaluasi berupa *pre-test* dan *post-test*, perencanaan logistik, dokumentasi, serta strategi peningkatan partisipasi melalui *doorprize*. Selain itu, dilakukan pembagian peran antara dosen dan taruna, termasuk penyiapan luaran seperti artikel ilmiah, *press release*, dokumentasi *video*, dan hak cipta materi visual.

Pelaksanaan kegiatan dimulai dengan pengisian kuesioner *pre-test* oleh peserta untuk mengukur pengetahuan awal. Materi kemudian disampaikan oleh narasumber dalam format interaktif yang mendorong partisipasi aktif melalui tanya jawab. Taruna berperan mendukung aspek teknis, distribusi materi, dan pengelolaan acara. Tahap evaluasi mencakup pengisian *post-test* untuk menilai peningkatan pemahaman, serta refleksi terbuka untuk mengumpulkan umpan balik peserta. Hasil evaluasi dianalisis secara deskriptif kuantitatif melalui perbandingan skor rata-rata *pre-test* dan *post-test*, dengan indikator keberhasilan meliputi peningkatan skor dan keterlibatan aktif selama kegiatan.

Seluruh rangkaian pengabdian mencerminkan kolaborasi lintas peran antara delapan dosen dari berbagai program studi, empat taruna, pihak sekolah, dan narasumber eksternal. Pembagian tugas yang terstruktur tidak hanya mendukung efektivitas kegiatan, tetapi juga memberikan pengalaman pembelajaran nyata bagi taruna dalam konteks profesional. Dengan pendekatan *service learning*, kegiatan ini diharapkan dapat meningkatkan kesadaran dan literasi keamanan siber di kalangan pelajar yang kelak akan memasuki sektor transportasi udara.



Gambar 1. Proses pengabdian

3. HASIL DAN PEMBAHASAN

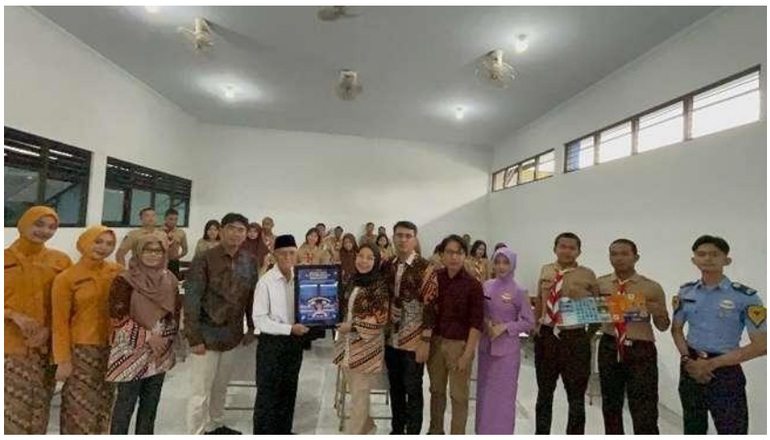
Kegiatan pengabdian kepada masyarakat ini merupakan bagian dari implementasi Tri Dharma Perguruan Tinggi dalam bentuk penyuluhan literasi digital kepada siswa tingkat menengah. Kegiatan ini mengambil tema keamanan siber, khususnya mengenai *ransomware*, yaitu jenis *malware* yang dapat mengenkripsi data korban dan meminta tebusan untuk mengembalikannya. Narasumber utama pada kegiatan ini adalah Bapak Yeni Setiawan, seorang praktisi di bidang *web development* dan *marketing support* dari perusahaan Rumahweb. Dengan latar belakang sebagai salah satu perusahaan *hosting* terbesar di Indonesia yang berbasis di Yogyakarta, Rumahweb memiliki pengalaman luas dalam menghadapi berbagai bentuk ancaman siber, termasuk *ransomware*. Kehadiran narasumber dari kalangan profesional ini memberikan nilai tambah berupa transfer pengetahuan praktis yang kontekstual dan aplikatif bagi para peserta.

Kegiatan ini diikuti oleh siswa kelas X SMK Dirgantara Putra Bangsa dan disampaikan dengan pendekatan komunikatif. Materi yang disampaikan mencakup pengertian *ransomware*, studi kasus serangan *ransomware* di Indonesia dari tahun 2017 hingga 2024, cara kerja *malware* ini dalam menyerang sistem komputer, langkah-langkah yang harus dilakukan saat terkena

serangan, serta tindakan preventif untuk menghindari kerugian akibat *ransomware*. Siswa diberikan contoh-contoh nyata dan situasi aplikatif, sehingga mereka dapat memahami konsep teknis dalam konteks kehidupan sehari-hari, misalnya pentingnya tidak sembarangan mengunduh *file* atau mengklik tautan mencurigakan. Langkah preventif lainnya yaitu menyimpan cadangan data di tempat terpisah seperti perangkat eksternal secara berkala, selalu menggunakan perangkat dan apilkasi versi terbaru yang dilengkapi sistem keamanan, serta menggunakan aintivirus yang andal.

Salah satu poin penting yang disampaikan narasumber adalah pentingnya respons cepat ketika mencurigai adanya infeksi. Jika ditemukan aktivitas tidak biasa pada perangkat, pengguna disarankan untuk segera memutus koneksi *internet* guna mencegah penyebaran *ransomware* ke sistem atau jaringan lain. Tindakan ini juga harus diikuti dengan mematikan atau mencabut perangkat penyimpanan eksternal, seperti *hard drive*, untuk melindungi data cadangan dari enkripsi oleh *ransomware*. Langkah-langkah sederhana namun krusial ini menjadi bagian penting dalam upaya tanggap darurat dan merupakan bentuk perlindungan awal sebelum penanganan teknis lanjutan dilakukan.

Sesi tanya jawab yang interaktif membantu peserta untuk mengaitkan materi dengan pengalaman pribadi mereka dalam penggunaan perangkat digital. Dokumentasi kegiatan pengabdian dapat dilihat pada Gambar 1.



Gambar 2. Dokumentasi kegiatan pengabdian

Untuk mengetahui efektivitas penyampaian materi, dilakukan *pre-test* dan *post-test* kepada 24 siswa peserta kegiatan. Hasil dari analisis statistik deskriptif menunjukkan bahwa rata-rata nilai *pre-test* sebesar 15,29 meningkat menjadi 21,38 pada *post-test*. Nilai standar deviasi untuk *pre-test* adalah 7,387 dan meningkat menjadi 8,510 pada *post-test*, sedangkan nilai *Standard Error Mean* masing-masing sebesar 1,508 dan 1,737. Rangkuman hasil statistik deskriptif tersebut dapat dilihat pada Tabel 1 berikut.

Tabel 1. Output SPSS Rata-Rata Hasil *Pre-Test* dan *Post-Test*

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	PRE	15.29	24	7.387	1.508
	POST	21.38	24	8.510	1.737

Hipotesis yang diuji adalah sebagai berikut: H_0 menyatakan tidak terdapat perbedaan signifikan antara nilai *pre-test* dan *post-test*, sedangkan H_a menyatakan terdapat perbedaan signifikan antara kedua nilai tersebut. Uji korelasi antara nilai *pre-test* dan *post-test* menghasilkan koefisien sebesar 0,731 dengan nilai signifikansi sebesar 0,000, yang menunjukkan adanya hubungan positif yang kuat antara hasil *pre* dan *post*, sebagaimana disajikan dalam Tabel 2.

Tabel 2. *Output* SPSS Korelasi *Pre-Test* dan *Post-Test*

		N	Correlation	Sig.
Pair 1	PRE & POST	24	.731	.000

Selanjutnya, uji *Paired Sample Test* menunjukkan nilai signifikansi (*Sig. 2-tailed*) sebesar 0,000, yang lebih kecil dari tingkat signifikansi 0,05. Dengan demikian, H_0 ditolak dan H_a diterima, yang berarti terdapat perbedaan signifikan antara nilai *pre-test* dan *post-test*. Rata-rata selisih nilai sebesar -6,083 dengan interval kepercayaan 95% antara -8,583 hingga -3,584 menunjukkan peningkatan pemahaman yang signifikan setelah pelatihan. Detail hasil uji hipotesis disajikan pada Tabel 3.

Tabel 3. *Output* SPSS Hasil Uji Hipotesis

		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference				
					Lower	Upper			
Pair 1	PRE - POST	-6.083	5.919	1.208	-8.583	-3.584	-5.035	23	.000

Selain peningkatan pengetahuan siswa, kegiatan ini menghasilkan luaran berupa dokumentasi video yang dipublikasikan di kanal YouTube STTKD (https://www.youtube.com/watch?v=gEIEyXtQfo4) dan mendapat perhatian media massa melalui publikasi di Harian Jogja pada tanggal 17 April 2025 (https://m.harianjogja.com/pendidikan/read/2025/04/17/642/1210549/sttkd-gelar-materi-kenali-dan-lindungi-diri-dari-ransomware). Publikasi ini memperkuat posisi STTKD sebagai institusi pendidikan tinggi yang aktif dalam kegiatan literasi digital, sekaligus menjangkau masyarakat luas dalam membangun kesadaran akan pentingnya keamanan data dan perlindungan terhadap serangan siber.

Kegiatan ini tidak hanya berdampak pada peningkatan pengetahuan teknis peserta, tetapi juga berkontribusi dalam membentuk kesadaran kritis siswa mengenai pentingnya menjaga keamanan data pribadi dalam kehidupan digital yang semakin kompleks. Literasi digital ini sangat penting terutama di era transformasi digital, di mana pelajar merupakan pengguna aktif perangkat teknologi dan internet. Selain itu, kegiatan ini juga memperkenalkan STTKD sebagai institusi yang peduli terhadap isu-isu digital yang relevan dengan kebutuhan masa kini. Kegiatan ditutup dengan sesi pengenalan kampus oleh Unit Penerimaan Taruna Baru (PTB), yang disampaikan secara edukatif dan informatif sebagai bagian dari strategi promosi institusi berbasis edukasi.

Secara keseluruhan, kegiatan pengabdian ini dapat dikategorikan berhasil karena memenuhi indikator keberhasilan dari segi peningkatan pengetahuan peserta, partisipasi aktif siswa, keterlibatan narasumber profesional, serta dokumentasi dan publikasi luaran. Keberhasilan ini menunjukkan bahwa kolaborasi antara akademisi, praktisi, dan institusi pendidikan menengah dapat menciptakan sinergi positif dalam peningkatan literasi digital generasi muda yang lebih cakap dan siap menghadapi tantangan dunia siber.

Kegiatan pengabdian ini sejalan dengan prinsip *Experiential Learning Theory* oleh Kolb (1984), yang menekankan pembelajaran melalui pengalaman langsung dan refleksi. Pendekatan seminar interaktif, diskusi, serta studi kasus nyata memungkinkan siswa mengaitkan teori dengan praktik nyata, meningkatkan pemahaman dan penerapan konsep keamanan siber secara efektif.

Selain itu, keterlibatan lintas sektor antara akademisi, praktisi, dan institusi pendidikan menengah dapat dianalisis melalui kerangka kerja *Community of Practice* (Wenger, 1998), yang menjelaskan bagaimana interaksi sosial dalam komunitas profesional mempercepat transfer pengetahuan dan pembelajaran sosial. Ini sejalan dengan penelitian Gregson (2020) yang menegaskan peran aktif praktisi dalam memperkuat relevansi dan daya serap materi pembelajaran vokasi.

Peningkatan kesadaran kritis siswa terhadap keamanan data pribadi juga dapat dikaitkan dengan konsep *Digital Literacy* Eshet-Alkalai (2004), yang mengintegrasikan kemampuan teknis dan etis dalam menggunakan teknologi secara bertanggung jawab. Kegiatan ini berhasil menggabungkan aspek tersebut sehingga siswa tidak hanya mengerti teknis, tetapi juga memahami pentingnya keamanan data dan perilaku digital yang aman.

4. KESIMPULAN

Kegiatan pengabdian ini berhasil meningkatkan kapasitas siswa SMK Dirgantara Putra Bangsa dalam mengenali dan mencegah serangan *ransomware*, khususnya dalam konteks industri penerbangan. Melalui pendekatan seminar interaktif yang dikombinasikan dengan diskusi dan evaluasi berbasis digital, peserta menunjukkan peningkatan pengetahuan yang signifikan setelah mengikuti kegiatan. Pelibatan narasumber profesional serta dukungan teknis dari taruna memberikan nilai tambah pada proses pembelajaran. Selain peningkatan skor hasil *post-test*, siswa juga menunjukkan partisipasi aktif dan antusiasme tinggi selama sesi berlangsung. Materi yang disampaikan secara kontekstual dan aplikatif membantu siswa memahami ancaman keamanan digital dalam kehidupan sehari-hari maupun lingkungan kerja masa depan. Dokumentasi dan publikasi kegiatan melalui media massa dan *platform* digital turut memperluas dampak pengabdian ini ke masyarakat luas. Secara keseluruhan, kegiatan ini memberikan kontribusi nyata dalam membentuk generasi muda yang lebih sadar, waspada, dan siap menghadapi tantangan keamanan siber di era transformasi digital.

5. UCAPAN TERIMA KASIH

Penghargaan diberikan kepada Pusat Penelitian dan Pengabdian kepada Masyarakat serta Program Studi Manajemen Transportasi Udara Sekolah Tinggi Teknologi Kedirgantaraan (STTKD) Yogyakarta yang telah mendanai kegiatan pengabdian ini. Terima kasih kepada SMK Dirgantara Putra Bangsa yang telah menjadi mitra pengabdian pengabdian.

DAFTAR PUSTAKA

Antara. (2024, July 10). *Layanan penerbangan tak terganggu serangan siber di PDN*. https://www.medcom.id/ekonomi/bisnis/zNAQmRnN-layanan-penerbangan-tak-terganggu-serangan-siber-di-pdn

Eshet-Alkalai, Y. (2004). Digital literacy: A conceptual framework for survival skills in the digital era. *Journal of Educational Multimedia and Hypermedia*, *13*(1), 93-106. https://www.learntechlib.org/p/4793

Gregson, M. (2020). In Practice: The Importance of Practitioner Research in Vocational Education. *Education Sciences*, *10*(3), 79. https://doi.org/10.3390/educsci10030079

Gudimetla, S. R. (2022). Ransomware prevention and mitigation strategies. *Journal of Innovative Technologies, 5*(1), 1–19. https://acadexpinnara.com/index.php/JIT/article/view/39

Humas DJPUa. (2018, May 16). *Dirjen PHB Udara - Tangkal cyber attack di penerbangan dengan aviation cyber security*. https://hubud.kemenhub.go.id/hubud/website/berita/3623

Humas DJPUb. (2022, July 10). *Antisipasi insiden siber di sektor penerbangan Ditjen Hubud launching Indonesia Aviation Sector Computer Security Incident Response Team (IAS-CSIRT)*. https://hubud.kemenhub.go.id/hubud/website/berita/4479

Humas DJPUc. (2022, July 10). *Kemenhub perkuat keamanan siber penerbangan melalui Cyber Security in Aviation Conference*. https://hubud.kemenhub.go.id/hubud/website/berita/4480

Kara, P. (2024, July 12). *The growing menace of ransomware*. https://www.cybersecurityintelligence.com/blog/the-growing-menace-of-ransomware-7775.html

Kapoor, A., Gupta, A., Gupta, R., Tanwar, S., Sharma, G., & Davidson, I. E. (2022). Ransomware detection, avoidance, and mitigation scheme: A review and future directions. *Sustainability, 14*(8), 1–24. https://doi.org/10.3390/su14010008

Kolb, D. A. (2014). *Experiential learning: Experience as the source of learning and development* (2nd ed.). New Jersey: Pearson Education.

Lutfhah, D. (2022). Potensi ancaman serangan siber pada sistem penerbangan Indonesia. *Hukum Pidana dan Pembangunan Hukum, 5*(1), 54–62. https://doi.org/10.25105/hpph.v5i1.16247

Mansfield-Devine, S. (2017). Ransomware: The most popular form of attack. *Computer Fraud & Security, 2017*(10), 15–20. https://doi.org/10.1016/S1361-3723(17)30092-1

Parulian, S., Pratiwi, D. A., & Yustina, M. C. (2021). Ancaman dan solusi serangan siber di Indonesia. *Telecommunications, Networks, Electronics, and Computer Technologies, 1*(2), 85–92. https://doi.org/10.17509/telnect.v1i2.40866

Ristiani, D., Dyahjatmayanti, G. N., Ginusti, F., Albanna, F., Martanti, I. F. R., Dewantari, A., & Awan. (2024). Pembekalan praktik kerja lapangan melalui pelatihan penanganan penumpang, bagasi, kargo, dan bea cukai untuk siswa dan siswi SMK Penerbangan Sriwijaya. *Jurnal Pengabdian Mandiri, 3*(1), 13–22. https://mail.bajangjournal.com/index.php/JPM/article/view/7281

Saleous, H., Ismail, M., Aldaajeh, S., & Madathil, N. (2022). COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities. *Digital Communications and Networks, 9*(1), 1–17. https://doi.org/10.1016/j.dcan.2022.06.005

SMKS Dirgantara Putra Bangsa. (2024, July 12). *Profil SMKS Dirgantara Putra Bangsa*. https://dirgantara.sch.id/profile-sekolah

Wenger, E. (1998). *Communities of practice: learning, meaning, and identity*. Cambridge: Cambridge University Press.

Zunaidi, A., Maghfiroh, FL. (2025), *Kewirausahaan dan Manajemen Bisnis UMKM Teori, Praktik, dan Strategi Menuju UMKM Berkelanjutan.* Indramayu: Penerbit Adab.

Zunaidi, A. (2024). *Metodologi Pengabdian Kepada Masyarakat Pendekatan Praktis untuk Memberdayakan Komunitas*. Yayasan Putra Adi Dharma.