Dharma Nusantara:
Jurnal Ilmiah Pemberdayaan dan Pengabdian kepada Masyarakat
E-ISSN: E-ISSN: 2986-2914
Email: jurnal@stiki.ac.id

Pelatihan Keamanan Jaringan dan Antisipasi Kejahatan Siber bagi Siswa SMK N 1 Padang Cermin, Lampung

Donaya Pasha[1], Masnia Rahayu[2], Heni Sulistiani[3*], Alvi Suhartanto[4], Muhammad Hamdan Sobirin[5], Zahra Kharisma Sangha[6], Fahreza Aditya Aryatama[7]

[1,2,4,5,6,7]Universitas Teknokrat Indonesia, Fakultas Teknik dan Ilmu Komputer, Teknologi Informasi, Jl. ZA. Pagar Alam No.9-11 Labuhan Ratu Bandar Lampung, Indonesia
[3]Universitas Teknokrat Indonesia, Fakultas Teknik dan Ilmu Komputer, Sistem Informasi Akuntansi, Jl. ZA. Pagar Alam No.9-11 Labuhan Ratu Bandar Lampung, Indonesia

Email Korespondensi:
henisulistiani@teknokrat.ac.id

Abstrak

Kegiatan Pengabdian Kepada Masyarakat (PKM) ini bertujuan untuk memberikan pengenalan dan pelatihan keamanan jaringan dan antisipasi kejahatan siber kepada siswa SMKN 1 Padang Cermin jurusan Teknik Komputer dan Jaringan (TKJ). Ketrampilan menggunakan teknologi merupakan salah satu luaran wajib bagi siswa SMK, untuk dapat menguasai teknologi dalam mengantisipasi keamanan jaringan dan kejahatan siber tidak cukup hanya di dapat dari pelajaran di dalam kelas, oleh karena itu perlu diberikan kegiatan penunjang lain seperti pelatihan untuk menambah pengetahuan dan pengalaman siswa dalam pengenalan keamanan jaringan dan kejahatan siber. Kegiatan PKM ini memberikan pelatihan secara tatap muka kepada siswa jurusan teknik komputer dan jaringan. Berdasarkan hasil kuisioner yang diberikan kepada siswa dan hasil kerja siswa dapat disimpulkan bahwa pelatihan dapat meningkatan kemampuan siswa, hal tersebut terlihat dari hasil kuisioner tentang pemahaman siswa terkait keamanan jaringan dan antisipasi kejahatan siber.
Kata Kunci: Cybersecurity; Jaringan; Keamanan; Kejahatan; Siber

1. Pendahuluan

Di era digital saat ini, internet telah menjadi bagian tak terpisahkan dari kehidupan manusia. Kehadiran internet membuka berbagai peluang dan kemudahan dalam berbagai aspek kehidupan, termasuk dalam dunia pendidikan. Akses informasi yang mudah, komunikasi yang lancar, dan berbagai platform edukasi online menjadi beberapa contoh manfaat internet bagi masyarakat.

Dalam beberapa dekade terakhir, kemajuan dalam teknologi informasi dan komunikasi telah berkontribusi secara positif pada pertumbuhan ekonomi dunia sambil meningkatkan produktivitas, persaingan, dan keterlibatan masyarakat. Akan tetapi, karena pemerintah, pengusaha, dan masyarakat semakin terhubung di dunia maya, ada beberapa tantangan yang terkait dengan ancaman dunia maya yang memerlukan pengembangan keamanan dunia maya yang lebih kuat (Budi, Wira, & Infantono, 2021). Menurut ISO (*International Organization for Standardization*), ISO/IEC 27032 menyatakan bahwa keamanan *cyberspace* atau *cyberspace* adalah menjaga kerahasiaan, integritas, dan ketersediaan informasi di dunia maya (Cakrawala, 2021). *Cyberspace* adalah lingkungan yang kompleks di mana orang, peranti lunak, dan layanan layanan internet berinteraksi melalui berbagai perangkat teknologi, berbagai koneksi jaringan, dan lingkungan yang tidak wujud.

Keamanan siber adalah praktik yang melindungi komputer, server, perangkat seluler, sistem elektronik, jaringan, dan data dari serangan jahat . Dalam era teknologi saat ini, keamanan siber telah menjadi masalah yang semakin penting. Ancaman terhadap objek penting dan keamanan file terus meningkat. Serangan malware, peretasan, dan serangan jaringan yang kompleks adalah beberapa contoh kegagalan keamanan sistem digital yang dieksploitasi oleh penjahat siber yang semakin mahir dan mahir. Selain itu, dengan semakin banyaknya informasi yang dikirim dan disimpan secara elektronik, masalah keamanan file menjadi semakin sulit (Soesanto, Romadhon, Mardika, & Setiawan, 2023). Ancaman terhadap objek penting dan keamanan file terus meningkat. Serangan malware, peretasan, dan serangan jaringan yang kompleks adalah beberapa contoh kegagalan keamanan sistem digital yang dieksploitasi oleh penjahat cyber yang semakin mahir dan mahir. Selain itu, dengan semakin banyaknya informasi yang dikirim dan disimpan secara elektronik, masalah keamanan file menjadi semakin sulit (Rosy, 2020).

Peningkatan jumlah dan kompleksitas serangan siber yang mengancam sistem komputer dan data di seluruh dunia dalam beberapa tahun terakhir. Serangan seperti pencurian data, serangan malware, peretasan, dan serangan DDoS telah menyebabkan kerugian finansial, kerusakan reputasi, dan gangguan pada operasi bisnis (Susanto, Antira, Kevin, Stanzah, & Majid, 2023). Komponen keamanan siber untuk memandu kebijakan keamanan informasi dalam sebuah organisasi yaitu *confidentiality* (kerahasiaan), *integrity* (integritas), dan *availability* (ketersediaan) (Sandrawati, 2022). Ancaman ini semakin marak terjadi di Indonesia, termasuk di kalangan pelajar. Hal ini dapat dilihat dari data Badan Siber dan Sandi Negara (BSSN) yang menunjukkan bahwa jumlah kasus kejahatan siber di Indonesia mengalami peningkatan yang signifikan dalam beberapa tahun terakhir. Pada tahun 2023, BSSN mencatat terdapat 403.990.813 anomali dengan jenis trafik anomali tertinggi yaitu *Generic Trojan RAT* yang mengindikasikan adanya aktivitas *backdoor communication* menuju domain *malicious* yang terindikasi sebagai *command and control server* milik *threat actor*. Terdapat 4.001.905 aktivitas *Advanced Persistent Threat* (APT) dan 1.011.209 aktivitas *ransomware* (BSSN, 2023).

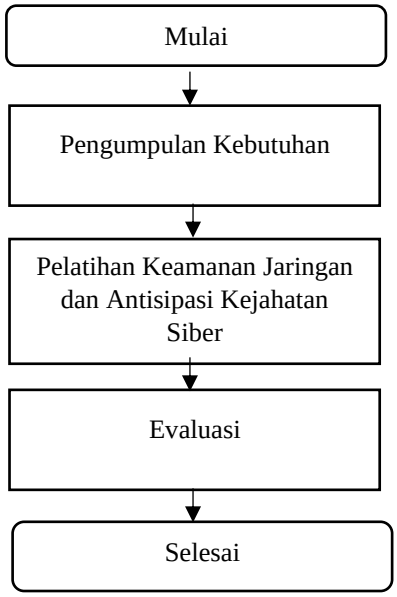
Siswa sekolah merupakan salah satu kelompok yang paling rentan terhadap ancaman keamanan jaringan dan kejahatan siber. Hal ini dikarenakan mereka masih dalam usia yang mudah terpengaruh dan belum memiliki pemahaman yang mendalam tentang keamanan siber. Beberapa faktor yang menyebabkan hal tersebut terjadi, antara lain:

a. Kurangnya pengetahuan dan pemahaman tentang keamanan siber
   Siswa masih dalam usia yang mudah terpengaruh dan belum memiliki pemahaman yang mendalam tentang keamanan siber. Hal ini membuat mereka mudah terjebak dalam modus penipuan *online* atau menjadi korban peretasan.
b. Keingintahuan yang tinggi
   Siswa memiliki rasa ingin tahu yang tinggi dan senang mencoba hal-hal baru. Hal ini dapat membuat mereka membuka situs web berbahaya atau mengunduh file yang terkontaminasi *malware* tanpa sepengetahuan orang tua atau guru.
c. Penggunaan internet yang tidak terkontrol
   Banyak siswa yang memiliki akses internet tanpa pengawasan orang tua atau guru. Hal ini membuat mereka mudah terpapar konten berbahaya atau menjadi korban *cyberbullying*.

Keadaan ini diperparah dengan minimnya edukasi dan pelatihan tentang keamanan siber di sekolah-sekolah. Hal ini menyebabkan banyak siswa yang tidak mengetahui bagaimana cara melindungi diri dari ancaman siber. Mengingat tingginya risiko keamanan siber bagi siswa, perlu dilakukan upaya untuk meningkatkan kesadaran dan pengetahuan mereka tentang keamanan jaringan dan antisipasi kejahatan siber. SMK N 1 Padang Cermin, seperti banyak sekolah lainnya di Indonesia, belum memiliki program edukasi dan pelatihan tentang keamanan siber secara menyeluruh. Hal ini dikarenakan keterbatasan sumber daya dan tenaga pengajar yang kompeten di bidang keamanan siber. Kondisi ini dikhawatirkan dapat berakibat fatal bagi siswa, seperti kehilangan data pribadi, menjadi korban penipuan online, bahkan menjadi pelaku kejahatan siber. Oleh karena itu, perlu dilakukan upaya untuk meningkatkan kesadaran dan pengetahuan siswa tentang keamanan jaringan dan antisipasi kejahatan siber di SMK N 1 Padang Cermin.

2. Metode

Kegiatan pengabdian yang dilakukan oleh tim menggunakan metode pelatihan seacra tatap muka di SMK N 1 Padang Cermin. Kegiatan pengabdian ini merupakan salah satu bentuk implementasi kerjasama antara Fakultas Teknik dan Ilmu Komputer dengan SMK N 1 Padang Cermin, serta pelaksanaan kegiatan Hima *Goes to School*. Peserta yang terlibat dalam kegiatan ini yaitu Siswa/I SMK kelas XIII pada jurusan Teknik Komputer dan Jaringan (TKJ). Tahapan yang dilakukan sebelum dan setelah kegiatan pelatihan dapat dilihat pada Gambar 1.



Gambar 1. Tahapan Kegiatan Pengabdian

Berdasarkan Gambar 1, dapat diuraikan secara rinci tentang tahapan kegiatan pengabdian sebagai berikut:

1. Pengumpulan Kebutuhan
   Pada tahap ini sebelumnya dilakukan komunikasi dengan pihak sekolah SMK N 1 Padang Cermin tekait dengan kegiatan apa yang dibutuhkan, setelah itu pihak pemateri menyiapkan materi terkait dengan kegiatan yang nantinya akan diberikan. Data yang dikumpulkan pada tahap ini di analisis dan diskusikan dengan tim Pengabdian Kepada Masyarakat Universitas Teknokrat Indonesia yang selanjutnya mempersiapkan bahan dan koordinasi waktu untuk memberikan kegiatan sesuai dengan yang diminta oleh pihak Sekolah
2. Pelatihan
   Peserta kegiatan ini diikuti oleh siswa/i SMK N 1 Padang Cermin. Kegiatan ini juga melibatkan mahasiswa dari Program Studi Teknologi Informasi, Universitas Teknokrat Indonesia untuk membatu tim Dosen dalam proses pendampingan pada saat pelatihan. Sistematika pelatihan yaitu memberikan pengetahuan dasar tentang keamanan jaringan, konsep dasar kejahatan siber kemudian dilanjutkan praktik untuk antisipasi kejahatan siber.
3. Evaluasi
   Tahap evaluasi dilakukan untuk mengukur kesuksesan kegiatan pelatihan Keamanan Jaringan dan Antisipasi Kejahatan Siber di SMK N 1 Padang Cermin. Evaluasi dilakukan dengan cara memberikan kuisioner, tujuan dari langkah ini yaitu untuk mengetahui peningkatan pengetahuan siswa terkait pelatihan yang telah diberikan.

3. Hasil dan Pembahasan

Pelatihan keamanan jaringan dan antisipasi kejahatan siber bagi siswa SMK N 1 Padang Cermin merupakan kegiatan yang penting untuk meningkatkan kesadaran siswa tentang keamanan online dan membekali mereka

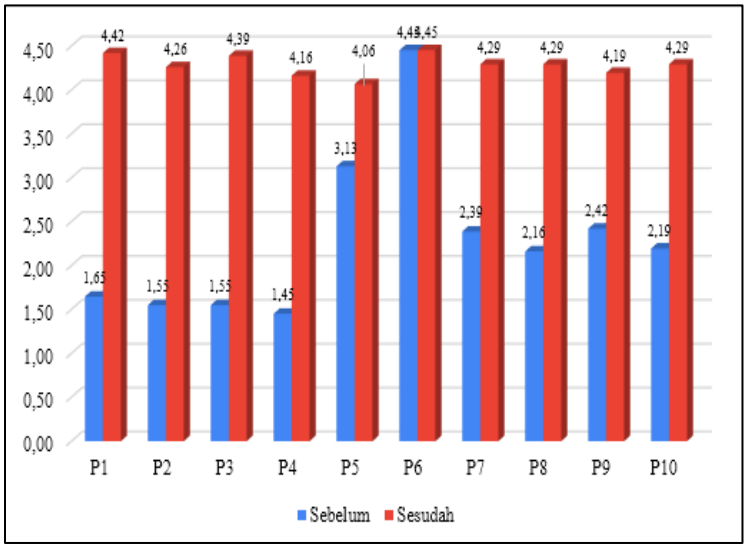
dengan pengetahuan dan keterampilan untuk melindungi diri dari ancaman siber. Kegiatan ini diharapkan dapat membantu siswa untuk menggunakan internet dengan aman dan bertanggung jawab. Tujuan dari adanya kegiatan pelatihan ini antara lain:

a) Meningkatkan kesadaran siswa tentang keamanan jaringan dan antisipasi kejahatan siber.
b) Memberikan pengetahuan dan keterampilan kepada siswa untuk melindungi diri dari ancaman siber.
c) Mendorong siswa untuk menggunakan internet dengan aman dan bertanggung jawab.

Kegiatan pelatihan ini dilakukan di SMK N 1 Padang Cermin pada Tanggal 5 Februari 2024. Berikut ini adalah dokumentasi kegiatan seperti pada Gambar 2.

Gambar 2. Dokumentasi kegiatan pelatihan

Setelah dilakukan pelatihan, selanjutnya dilakukan kegiatan evaluasi yang bertujuan untuk mengetahui hasil dari kegiatan tersebut. Evaluasi dilakukan dengan cara memberikan kuisioner terkait dengan pengetahuan tentang pengenalan dan praktik keamanan jaringan dan antisipasi kejahatan siber. Dengan adanya pelatihan yang diberikan oleh tim pengabdian dapat meningkatkan pengetahuan dan kemampuan siswa dalam keamanan jaringan dan mengetahui tentang bagaimana cara mengantisipasi kejahatan siber. Dari setiap indikator pernyataan kuesioner yang dibagikan sebelum dan sesudah pelatihan, terdapat peningkatan dari rata-rata tiap indikator. Hasil peningkatan tersebut dapat dilihat pada Gambar 3.



Gambar 3. Grafik peningkatan tiap indikator pertanyaan

Rata-rata penilaian tiap indikator dari pelatihan keamanan jaringan dan antisipasi kejahatan siber mengalami peningkatan dari rata-rata 2,29 meningkat menjadi 4,96. Peningkatan nilai rata-rata sebelum dan sesudah dilaksanakan pelatihan sebesar 1,99.

4. Kesimpulan

Berdasarkan hasil pembahasan terkait dengan pelatihan keamanan jaringan dan antisipasi kejahatan siber diperoleh hasil bahwa rata-rata penilaian tiap indikator dari pelatihan terdapat peningkatan dari rata-rata 2,29 meningkat menjadi 4,96. Peningkatan nilai rata-rata sebelum dan sesudah dilaksanakan pelatihan sebesar 1,99 (Gambar 3), hal tersebut dikarenakan pelatihan yang diberikan kepada siswa oleh tim dosen Universitas Teknokrat Indonesia bersifat umpan balik, artinya jika siswa mengalami kendala terkait teknis dan kurangnya pemahaman materi terkait dengan pelatihan yang diberikan, siswa mendapat tutorial secara langsung bagaimana langkah dalam menyelesaikan suatu permasalahan.

5. Referensi

BSSN. (2023). *Lanskap Keamanan Siber Indonesia Tahun 2023.* Jakarta: BSSN.

Budi, E., Wira, D., & Infantono, A. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. *Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia*, 223-234.

Cakrawala. (2021, Mei 25). *Apa Itu Cyber Security? Mengapa Cyber Security Kini Makin Penting?* Retrieved from infokomputer: https://infokomputer.grid.id/read/122710604/apa-itu-cyber-security-mengapa-cyber-security-kini-makin-penting?page=all

Rosy, A. F. (2020). Kerjasama internasional Indonesia: memperkuat keamanan nasional di bidang keamanan siber. *Journal of Government Science (GovSci) : Jurnal Ilmu Pemerintahan*, 118-129.

Sandrawati, N. A. (2022). Antisipasi Cybercrime dan Kesenjangan Digital dalam Penerapan TIK di KPU. *Electoral Governance Jurnal Tata Kelola Pemilu Indonesia*, 232-257.

Soesanto, E., Romadhon, A., Mardika, B. D., & Setiawan, M. F. (2023). Analisis dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital Untuk Mengamankan Objek Vital dan File. *SAMMAJIVA : Jurnal Penelitian Bisnis dan Manajemen*, 172-191.

Susanto, E., Antira, L., Kevin, K., Stanzah, E., & Majid, A. A. (2023). ManajemenKeamanan Cyber di Era Digital. *Jurnal Bisnis dan Kewirausahaan (Journal of Business and Entrepreneurship)*, 23-33.