Peningkatan Kesadaran Keamanan Siber melalui Bimbingan Teknis bagi CSIRT dan Tim TIK pada OPD dan BUMD Kabupaten Madiun

Andria*

[1]Sistem Informasi/Teknik
Universitas PGRI Madiun
[1*]andria@unipma.ac.id

***Abstrak*— Meningkatnya ketergantungan terhadap teknologi digital di sektor pemerintahan menghadirkan tantangan baru dalam menjaga keamanan informasi. Ancaman siber yang terus berkembang menuntut aparatur pemerintah untuk memiliki kesadaran dan pemahaman yang memadai terkait keamanan siber. Kegiatan pengabdian kepada masyarakat ini bertujuan untuk meningkatkan kesadaran keamanan siber (*cyber security awareness*) melalui bimbingan teknis yang ditujukan kepada anggota CSIRT dan Tim TIK pada OPD dan BUMD di Kabupaten Madiun. Metode pelaksanaan mencakup penyampaian materi interaktif, studi kasus insiden nyata, diskusi, serta simulasi penanganan insiden siber. Hasil kegiatan menunjukkan peningkatan partisipasi aktif dan pemahaman peserta terhadap konsep dasar keamanan siber, struktur organisasi CSIRT, serta langkah-langkah mitigasi ancaman digital. Testimoni peserta juga mengindikasikan pentingnya pelatihan lanjutan serta kebutuhan pembentukan sistem keamanan informasi internal yang lebih terstruktur. Kegiatan ini diharapkan menjadi langkah awal dalam membangun budaya keamanan siber yang berkelanjutan di lingkungan pemerintah daerah.**
Kata kunci— keamanan siber, CSIRT, OPD, BUMD, kesadaran siber, pengabdian masyarakat

***Abstract*— The growing reliance on digital technology within the government sector presents new challenges in securing information. The ever-evolving cyber threats demand that government personnel possess adequate awareness and understanding of cybersecurity. This community service activity aimed to enhance cybersecurity awareness through technical training provided to members of the CSIRT and IT teams from local government agencies (OPD) and regional-owned enterprises (BUMD) in Madiun Regency. The implementation methods included interactive material delivery, real incident case studies, discussions, and cyber threat simulation exercises. The results of the activity indicated increased active participation and improved understanding among participants regarding fundamental cybersecurity concepts, CSIRT organizational structure, and digital threat mitigation strategies. Participant testimonials also highlighted the importance of continued training and the need to establish more structured internal information security systems. This initiative is expected to serve as an initial step toward building a sustainable cybersecurity culture within local government institutions.**
Keywords— cybersecurity, CSIRT, government agencies, local enterprises, cyber awareness, community service.

I. Pendahuluan

Perkembangan teknologi digital di sektor pemerintahan memberikan dampak signifikan terhadap peningkatan efisiensi pelayanan publik dan manajemen informasi. Namun, di sisi lain, transformasi ini juga memunculkan tantangan baru, khususnya dalam hal keamanan informasi. Ketergantungan yang tinggi terhadap sistem digital membuat instansi pemerintahan rentan terhadap berbagai bentuk serangan siber seperti malware, phishing, dan ransomware [1].

Serangan siber terhadap institusi pemerintahan menunjukkan tren peningkatan setiap tahun. Laporan tahunan dari Badan Siber dan Sandi Negara (BSSN) mencatat bahwa pada tahun 2023 terjadi ribuan insiden siber yang sebagian besar menargetkan sektor pemerintahan [2]. Hal ini menunjukkan adanya celah dalam sistem pengamanan maupun pada sisi sumber daya manusianya.

Salah satu strategi yang diadopsi pemerintah adalah pembentukan *Computer Security Incident Response Team (CSIRT)* di berbagai instansi, termasuk di tingkat pemerintah daerah. CSIRT bertugas untuk merespons, menangani, dan menganalisis insiden siber secara sistematis [3]. Namun, pembentukan tim saja tidak cukup. Kapasitas dan kesadaran anggota CSIRT dan tim Teknologi Informasi dan Komunikasi (TIK) juga perlu ditingkatkan secara berkelanjutan.

Penelitian terdahulu menunjukkan bahwa pelatihan keamanan informasi berbasis pendekatan sistematis seperti model *ADDIE* mampu meningkatkan kesadaran dan keterampilan pegawai dalam menjaga keamanan data [4]. Selain itu, program

pelatihan yang disertai simulasi dan studi kasus nyata terbukti efektif dalam meningkatkan pemahaman tentang risiko-risiko siber [5].

Kesadaran keamanan informasi merupakan salah satu faktor kunci dalam membangun budaya keamanan siber yang berkelanjutan. Tanpa pemahaman yang memadai, pegawai berpotensi menjadi titik lemah dalam sistem pertahanan siber organisasi [6].

Penelitian adalah suatu usaha sistematis untuk menyelidiki masalah tertentu dengan tujuan mencari jawaban secara ilmiah. Ini melibatkan proses pengumpulan, pengolahan, analisis, dan penarikan kesimpulan dari data untuk memahami fenomena atau masalah yang diteliti [7].

Berdasarkan permasalahan tersebut, kegiatan ini dirancang dalam bentuk Bimbingan Teknis (BIMTEK) sebagai bagian dari program pengabdian kepada masyarakat. Kegiatan ini ditujukan kepada anggota CSIRT dan Tim TIK dari Organisasi Perangkat Daerah (OPD) dan Badan Usaha Milik Daerah (BUMD) di Kabupaten Madiun, dengan tujuan untuk:

- Meningkatkan kesadaran dan pemahaman dasar terkait keamanan siber;
- Memberikan pelatihan dasar tentang penanganan insiden dan praktik aman penggunaan teknologi;
- Mendukung terbentuknya budaya keamanan siber yang kolaboratif dan berkelanjutan di lingkungan pemerintah daerah.

Pelatihan keamanan siber yang terstruktur tidak sekadar menyampaikan informasi, namun juga membentuk sikap dan keterampilan kognitif yang berdampak pada perilaku, meskipun banyak kampanye gagal mengubah perilaku pengguna sasaran [8].

Pengembangan budaya keamanan siber melalui pelatihan dan kebijakan organisasi terbukti memainkan peran penting dalam keberlanjutan kesadaran keamanan di berbagai sektor [9].

Studi empiris menunjukkan bahwa metode pelatihan berbasis simulasi interaktif secara signifikan meningkatkan kesadaran pegawai sektor publik dan swasta [10].

Pelatihan publik untuk menghadapi kejahatan siber dengan pendekatan kasus nyata telah terbukti efektif dalam meningkatkan pengetahuan dan kesiapsiagaan masyarakat [11].

Tinjauan terhadap program pelatihan keamanan siber menegaskan pentingnya pendekatan yang komprehensif—menggabungkan teori, praktik, dan evaluasi berkelanjutan—untuk menghasilkan perubahan perilaku yang nyata [12].

II. Metodologi Penelitian

Penelitian ini dilaksanakan dalam bentuk kegiatan pengabdian kepada masyarakat yang difokuskan pada peningkatan kesadaran keamanan siber melalui Bimbingan Teknis (BIMTEK) kepada anggota CSIRT dan Tim TIK dari Organisasi Perangkat Daerah (OPD) dan Badan Usaha Milik Daerah (BUMD) di Kabupaten Madiun.

2.1 Jenis Penelitian

Jenis penelitian yang digunakan adalah penelitian terapan berbasis pengabdian kepada masyarakat, dengan pendekatan kualitatif deskriptif. Penelitian ini difokuskan untuk menggambarkan proses dan dampak pelaksanaan bimbingan teknis keamanan siber melalui observasi langsung, dokumentasi kegiatan, serta testimoni dari peserta. Pendekatan ini digunakan untuk memahami tingkat partisipasi, respon peserta, serta dinamika yang muncul selama pelatihan berlangsung.

2.2 Subjek dan Lokasi Kegiatan

Subjek kegiatan adalah anggota CSIRT dan Tim TIK dari OPD dan BUMD di lingkungan Pemerintah Kabupaten Madiun. Kegiatan ini dilaksanakan secara luring.

2.3 Tahapan Pelaksanaan

Kegiatan dilakukan melalui beberapa tahap sebagai berikut:

1. Persiapan
    - Penyusunan modul dan materi pelatihan yang mencakup konsep dasar keamanan siber, ancaman umum, peran CSIRT, serta teknik mitigasi insiden.

- Koordinasi dengan Diskominfo Kabupaten Madiun sebagai mitra utama.

2. Pelaksanaan Bimbingan Teknis

Kegiatan BIMTEK dilaksanakan selama 1 hari dengan rincian sebagai berikut:

- Pengenalan keamanan siber, jenis ancaman digital, peran dan struktur CSIRT, kebijakan perlindungan data, serta simulasi sederhana serangan siber (contoh kasus phishing dan ransomware).
- Praktik manajemen insiden, diskusi kelompok antar peserta, dan penyusunan draft prosedur respon insiden sederhana.

3. Evaluasi dan Dokumentasi

- Observasi selama pelatihan untuk menilai partisipasi dan interaksi peserta.
- Pengumpulan testimoni dari peserta terkait kebermanfaatan kegiatan.
- Dokumentasi berupa foto, video, dan hasil kerja kelompok sebagai lampiran kegiatan.

2.4 Teknik Pengumpulan Data

- Observasi langsung: Merekam dinamika pembelajaran dan keterlibatan peserta dalam diskusi dan simulasi.
- Wawancara singkat dan testimoni: Menggali persepsi dan evaluasi peserta terhadap kegiatan.
- Dokumentasi visual dan tertulis: Digunakan untuk laporan kegiatan dan bukti proses pengabdian.

2.5 Teknik Analisis Data

Data kualitatif dianalisis secara naratif untuk menangkap pengalaman, tanggapan, serta usulan dari peserta mengenai pelatihan dan penguatan peran CSIRT di lingkungan kerja pemerintah daerah.

III. Hasil dan Pembahasan

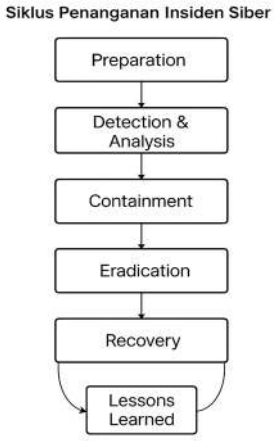
Kegiatan Bimbingan Teknis (BIMTEK) *Cyber Security Awareness* bagi anggota CSIRT dan Tim TIK dari OPD dan BUMD Kabupaten Madiun menghasilkan sejumlah temuan yang signifikan dalam konteks peningkatan kesadaran keamanan siber. Hasil ini disajikan berdasarkan data observasi, partisipasi peserta, serta testimoni yang diperoleh selama dan setelah kegiatan.

A. Partisipasi dan Aktivitas Peserta

Kegiatan ini di ikuti oleh 50 peserta yang terdiri dari anggota CSIRT dan Tim TIK dari berbagai OPD dan BUMD di Kabupaten Madiun. Berdasarkan observasi lapangan, para peserta menunjukkan partisipasi aktif dalam sesi diskusi dan simulasi.

Materi yang bersifat praktikal seperti identifikasi kebocoran akun, dan manajemen akun seperti pengelolaan kata sandi mendapatkan respons positif dan menarik perhatian peserta.

Untuk memudahkan pemahaman peserta terhadap alur penanganan insiden siber, disampaikan pula model siklus penanganan insiden yang meliputi: *Preparation, Detection, Containment, Eradication, Recovery*, dan *Lessons Learned* sebagaimana ditunjukkan pada Gambar 3. Model ini menjadi referensi utama dalam simulasi yang dilakukan peserta selama kegiatan berlangsung.



Gambar 1. Model Siklus Penanganan Insiden Siber

Model pada Gambar 3 menggambarkan siklus penanganan insiden siber yang digunakan dalam BIMTEK sebagai kerangka berpikir peserta. Model ini diadaptasi dari praktik umum dalam struktur kerja CSIRT dan terdiri dari enam tahapan utama:

1. Preparation (Persiapan)

   Tahap awal yang mencakup penyusunan kebijakan, pembentukan tim tanggap insiden, peningkatan

kesadaran pengguna, serta penyediaan sumber daya yang dibutuhkan.

2. Detection & Analysis (Deteksi dan Analisis)
   Proses identifikasi kejadian yang mencurigakan, pengumpulan bukti digital, serta analisis pola serangan untuk menentukan jenis dan dampaknya.
3. Containment (Pengendalian)
   Langkah-langkah sementara untuk membatasi penyebaran insiden, mencegah kerusakan lebih lanjut, dan menjaga integritas sistem.
4. Eradication (Pemusnahan)
   Upaya menghapus komponen berbahaya dari sistem (misalnya malware), serta menutup celah keamanan yang dimanfaatkan oleh pelaku.
5. Recovery (Pemulihan)
   Pemulihan sistem ke kondisi normal dengan memastikan semua layanan berjalan kembali secara aman dan stabil.
6. Lessons Learned (Evaluasi dan Pembelajaran)
   Evaluasi terhadap seluruh proses insiden untuk dokumentasi, peningkatan kebijakan, dan pencegahan kejadian serupa di masa depan. Hasil evaluasi ini menjadi input untuk tahap *Preparation* berikutnya, membentuk siklus berkelanjutan.

Model ini dipilih karena sederhana dan aplikatif, serta mampu menjembatani pemahaman peserta mengenai alur penanganan insiden siber secara sistematis.

B. Testimoni dan Evaluasi Kualitatif

Dari total 50 peserta yang mengikuti kegiatan BIMTEK, sebanyak 88% peserta (44 orang) menyatakan bahwa kegiatan ini sangat bermanfaat dalam meningkatkan pemahaman mereka mengenai konsep dasar keamanan siber dan peran strategis CSIRT di lingkungan instansi masing-masing. Pendekatan berbasis studi kasus nyata dan metode interaktif dianggap sangat efektif dalam menyampaikan materi.

Sekitar 82% peserta (41 orang) menilai bahwa simulasi serangan siber seperti phishing dan ransomware memberikan pengalaman praktis yang memperkuat kesadaran mereka terhadap celah-celah keamanan digital yang sering kali diabaikan dalam operasional sehari-hari.

Salah satu peserta menyampaikan:

"Simulasi yang diberikan membuat saya menyadari betapa rentannya sistem kami terhadap serangan siber sederhana. Pelatihan ini membuka perspektif baru."

Sementara itu, 76% peserta (38 orang) menyampaikan harapan agar pelatihan ini dapat dilanjutkan secara berkala, serta ditingkatkan ke level teknis lanjutan. Beberapa dari mereka juga menyarankan materi tambahan seperti penggunaan alat analisis log, forensic tools berbasis open-source, dan latihan penanganan insiden berbasis skenario aktual.

C. Analisis dan Implikasi

Kegiatan ini menunjukkan bahwa peningkatan kesadaran keamanan siber tidak hanya bergantung pada pemberian materi, tetapi juga pada metode penyampaian yang mendorong partisipasi aktif. Penggunaan simulasi nyata, studi kasus, dan diskusi lintas OPD/BUMD terbukti mampu memfasilitasi kolaborasi dalam memahami peran strategis CSIRT serta membentuk pola pikir responsif terhadap ancaman digital.

Berdasarkan hasil evaluasi yang dilakukan, terdapat peningkatan sebesar 32% dalam tingkat kesadaran keamanan siber peserta, dari rata-rata 58% sebelum BIMTEK menjadi 90% setelah BIMTEK. Ini menunjukkan bahwa pendekatan pelatihan berbasis interaktif dan kontekstual mampu memberikan dampak signifikan terhadap pemahaman peserta.

Temuan ini sejalan dengan penelitian terdahulu yang menyatakan bahwa pelatihan dengan metode simulasi dan studi kasus dapat meningkatkan efektivitas transfer pengetahuan dalam isu keamanan informasi [4].

Kegiatan ini juga membuka peluang lanjutan seperti:

- Pengembangan SOP respons insiden yang seragam antar instansi,

- Pembentukan forum komunikasi CSIRT lintas OPD/BUMD,
- Penyelenggaraan pelatihan bersertifikasi pada level intermediate dan advanced.

Kegiatan ini menunjukkan bahwa peningkatan kesadaran keamanan siber tidak hanya bergantung pada pemberian materi, tetapi juga metode penyampaian yang mendorong partisipasi aktif. Penggunaan simulasi nyata serta diskusi kelompok antar-instansi dapat memfasilitasi kolaborasi lintas OPD/BUMD dalam pembentukan dan penguatan CSIRT daerah.

D. Dokumentasi

Berikut dokumentasi kegiatan Bimbingan Teknis (BIMTEK) *Cyber Security Awareness* bagi anggota CSIRT dan Tim TIK dari OPD dan BUMD Kabupaten Madiun, penyampaian materi difokuskan pada aspek dasar mengenai keamanan siber, termasuk pengenalan jenis-jenis ancaman digital, kebijakan perlindungan data, dan peran strategis CSIRT dalam menanggulangi insiden siber.

Gambar 2. Pemaparan Materi

Pada sesi pemaparan materi, narasumber tidak hanya menyampaikan konsep-konsep dasar terkait keamanan siber, namun juga menyertakan pemaparan studi kasus nyata yang pernah terjadi di lingkungan pemerintahan, baik di tingkat daerah maupun nasional. Studi kasus yang diangkat meliputi insiden kebocoran data, serangan ransomware, serta kegagalan sistem akibat kelalaian dalam pengelolaan akses dan autentikasi. Pemaparan ini bertujuan untuk memberikan konteks faktual kepada peserta mengenai urgensi penerapan kebijakan keamanan informasi di instansi masing-masing.

Setelah penyampaian materi utama, kegiatan dilanjutkan dengan sesi interaktif yang melibatkan diskusi dua arah antara narasumber dan peserta. Dalam sesi ini, peserta diberi kesempatan untuk mengajukan pertanyaan, menyampaikan pandangan, serta berdiskusi mengenai permasalahan keamanan siber yang mereka hadapi di lingkungan kerja sehari-hari. Interaksi ini memperkuat pemahaman peserta karena materi disesuaikan dengan konteks nyata yang mereka alami.

Sebagai bagian dari evaluasi pemahaman awal, peserta juga diajak untuk mengikuti kuis singkat yang berisi pertanyaan seputar topik yang telah dipaparkan. Kuis dilakukan secara digital dengan sistem real-time untuk menciptakan suasana belajar yang dinamis dan kompetitif. Hasilnya menunjukkan bahwa peserta secara umum mampu menangkap inti materi dengan baik.

Gambar 3. Sesi Interaktif

Selama seluruh rangkaian sesi, peserta tampak sangat antusias dan aktif. Hal ini tercermin dari banyaknya pertanyaan yang diajukan, tingginya partisipasi dalam diskusi, serta keterlibatan dalam kuis dan studi kasus. Antusiasme ini menjadi indikator bahwa pendekatan pembelajaran yang diterapkan

berhasil membangkitkan minat dan meningkatkan kesadaran peserta terhadap pentingnya keamanan siber dalam mendukung layanan publik yang andal dan terpercaya

Kegiatan ditutup dengan sesi foto bersama sebagai bentuk dokumentasi dan penegas kebersamaan seluruh peserta dan narasumber dalam mendukung peningkatan kesadaran keamanan siber di lingkungan pemerintah daerah.

Gambar 4. Dokumentasi Kegiatan Foto Bersama

IV. Kesimpulan

Kegiatan Bimbingan Teknis Cyber Security Awareness bagi anggota CSIRT dan Tim TIK dari OPD dan BUMD di Kabupaten Madiun telah menunjukkan hasil yang positif dan signifikan. Observasi dan testimoni menunjukkan adanya peningkatan pemahaman peserta mengenai konsep dasar keamanan siber, identifikasi ancaman, dan manajemen insiden. Selain itu, kegiatan ini juga membangun kesadaran baru dalam membentuk sistem keamanan informasi internal yang lebih baik di masing-masing instansi.

Metode pelatihan yang berbasis pada simulasi dan studi kasus terbukti efektif untuk mendorong partisipasi aktif dan kolaborasi antar peserta. Kegiatan ini tidak hanya berhasil mencapai tujuannya dalam meningkatkan kesadaran keamanan siber, tetapi juga membuka peluang tindak lanjut berupa pengembangan prosedur operasional standar (SOP), penguatan struktur CSIRT daerah, dan pelatihan lanjutan berbasis sertifikasi.

Dengan demikian, kegiatan ini dapat dianggap sebagai langkah awal yang strategis dalam membangun budaya keamanan siber yang berkelanjutan di lingkungan pemerintahan daerah. Hasil kuis menunjukkan adanya peningkatan kesadaran keamanan siber sebesar 32%, dari rata-rata 58% sebelum BIMTEK menjadi 90% setelah BIMTEK. Hal ini mengindikasikan bahwa pendekatan pelatihan berbasis kasus nyata dan interaktif berhasil meningkatkan pemahaman peserta secara signifikan.

Pada akhir kegiatan, peserta menyampaikan antusiasme dan komitmen untuk mengimplementasikan materi pelatihan di lingkungan kerja masing-masing. Dokumentasi kegiatan ini menjadi landasan untuk evaluasi program serta pengembangan pelatihan lanjutan di masa depan.

Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada Dinas Komunikasi dan Informatika Kabupaten Madiun atas dukungan dan kerjasama yang telah diberikan dalam pelaksanaan kegiatan ini. Ucapan terima kasih juga disampaikan kepada seluruh peserta dari OPD dan BUMD yang telah aktif berpartisipasi selama kegiatan berlangsung. Kegiatan ini tidak akan berhasil tanpa kontribusi dan semangat kolaboratif dari semua pihak yang terlibat.

Referensi

[1] A. Yulianto, “Cybersecurity Policy and Its Implementation in Indonesia,” *Law Research Review Quarterly*, vol. 7, no. 1, pp. 69–82, 2021.

[2] Badan Siber dan Sandi Negara, “Lanskap Keamanan Siber Indonesia Tahun 2023,” 2024.

[3] BSSN, *Panduan Pembentukan CSIRT Sektor Pemerintahan Daerah*, Jakarta: BSSN, 2022.

[4] K. F. Ma’ruf dan M. M. Rochman, “Guidelines for Developing Information Security Training and Awareness Programs in Government Agency: The Perspective of ADDIE Instructional Design Models,” *PEOPLE: Int. J. Soc. Sci.*, vol. 5, no. 2, pp. 863–877, 2019.

[5] S. P. Saragih, I. Svinarky, “Pelatihan Cyber Security Awareness Kepada Masyarakat Menghadapi Perkembangan Kejahatan Siber,” *PUAN INDONESIA*, vol. 6, no. 2, pp. 565–572, 2023.

[6] E.Wanda, M. Hijriatin, “Cybersecurity Awareness in HR: Protecting Employee Data in the Digital Era,” *International Journal of Engineering, Science and Information Technology*, vol. 1, no. 4, pp. 20–28, 2021

[7] S. Nugroho, *Metodologi Penelitian Ilmiah*, Yogyakarta: Deepublish, 2020.
[8] G. Bada, A. M. Sasse, dan J. R. C. Nurse, *"Cyber Security Awareness Campaigns: Why do they fail to change behaviour?"*, 2019.
[9] B. Uchendu, J. R. C. Nurse, G. Bada, dan S. Furnell, *"Developing a cyber security culture: Current practices and future needs"*, 2021.
[10] M. Neri, dkk., *"Enhancing employees information security awareness in private and public sector organisations"*, *Computers & Security*, 2022
[11] S. P. Saragih, I. Svinarky, *"Pelatihan Cyber Security Awareness Kepada Masyarakat Menghadapi Perkembangan Kejahatan Siber"*, *PUAN INDONESIA*, vol. 6, no. 2, 2023
[12] *Security Awareness Training for the Workforce: Moving Beyond*, *PMC*, 2021.