APPA : Jurnal Pengabdian kepada Masyarakat
Volume 2, No. 6 April 2025
ISSN 3025-0889 (media online)
Hal 707-711

MENGHADAPI ANCAMAN SIBER DENGAN TINDAKAN PROAKTIF DEMI KEAMANAN TEKNOLOGI YANG BERKELANJUTAN

Adrian Dwi Ramadhani[1*], Aditia Warman[2], Aldi Al Kahfi[3], Edgar Dani Yudistira[4], Gilang Perdana[5], Maria Inasensia Mesak[6], Matius Enrico Melsasail[7], Muhammad Zidan Nursalim[8], Muhammad Ilyas Iztiharudin Sudrajat[9]

[1-9]Fakultas Ilmu Komputer, Teknik Informatika, Universitas Pamulang, Jl. Raya Puspiptek No. 46, Kel. Buaran, Kec. Serpong, Kota Tangerang Selatan. Banten 15310, Indonesia
Email: [1*]adrianramadhani387@gmail.com, [2]adtwarman17@gmail.com, [3]aldialkahfi21@gmail.com, [4]edgardani030712@gmail.com, [5]perdanagilang673@gmail.com, [6]MariaMesak14@gmail.com, [7]danzidan100@gmail.com, [8]muhamadilyas2911@gmail.com
(* : coressponding author)

Abstrak− Di era digital, ancaman siber terus berkembang seiring pesatnya adopsi teknologi (Smith et al., 2021; Wibisono, 2020). Artikel ini membahas pentingnya tindakan proaktif dalam menghadapi ancaman siber untuk memastikan keamanan teknologi yang berkelanjutan. Dengan meningkatnya risiko seperti peretasan data, malware, dan phishing (Johnson, 2020; Setiawan & Putri, 2019), langkah-langkah preventif seperti edukasi keamanan, penerapan teknologi keamanan, dan kesadaran pengguna menjadi kunci utama. Tindakan proaktif ini tidak hanya melindungi individu tetapi juga mendukung keberlanjutan teknologi yang aman dan efisien (Clark et al., 2019).

Kata Kunci: Keamanan Siber, Tindakan Proaktif, Teknologi Berkelanjutan, Edukasi Digital, Ancaman Dunia Maya

Abstract− *In the digital era, cyber threats continue to evolve as technology adoption accelerates (Smith et al., 2021; Wibisono, 2020). This article discusses the importance of proactive measures in addressing cyber threats to ensure sustainable technology security. With increasing risks such as data breaches, malware, and phishing (Johnson, 2020; Setiawan & Putri, 2019), preventive steps such as security education, implementation of security technology, and user awareness are key. These proactive measures not only protect individuals but also support the sustainability of safe and efficient technology (Clark et al., 2019).*

Keywords: *Cybersecurity, Proactive Measures, Sustainable Technology, Digital Education, Cyber Threats*

1. PENDAHULUAN

Di era digital, transformasi teknologi memberikan manfaat besar bagi berbagai aspek kehidupan manusia. Internet, perangkat pintar, dan sistem berbasis teknologi telah merevolusi cara individu dan institusi berinteraksi, berkomunikasi, dan bertransaksi (Klein, 2018; Rahman et al., 2021). Penggunaan teknologi yang masif ini tidak hanya mempercepat berbagai proses, tetapi juga membuka peluang baru di sektor ekonomi, pendidikan, dan pemerintahan. Namun, perkembangan pesat ini disertai dengan tantangan besar berupa ancaman siber.

Ancaman siber, seperti peretasan data, malware, ransomware, dan phishing, terus berkembang dengan kompleksitas yang meningkat. Phishing, sebagai contoh, telah menjadi metode serangan yang sering memanfaatkan kelengahan pengguna dalam mengenali tautan atau email palsu (Miller & Rose, 2022; Arifin & Sari, 2020). Sementara itu, ransomware yang mengenkripsi data korban dan menuntut pembayaran tebusan menjadi semakin merajalela, bahkan menargetkan institusi besar seperti rumah sakit dan lembaga pemerintah (Smith et al., 2021; Wibisono, 2020). Tidak hanya itu, eksploitasi sistem digital dan serangan Distributed Denial of Service (DDoS) juga sering kali mengakibatkan gangguan signifikan pada infrastruktur kritis.

Selain ancaman teknis, kurangnya literasi digital di berbagai lapisan masyarakat menjadi salah satu faktor utama yang memperburuk dampak serangan siber. Banyak pengguna yang belum memahami pentingnya langkah-langkah preventif seperti penggunaan kata sandi yang kuat, autentikasi dua faktor (2FA), serta pembaruan perangkat lunak secara berkala (Johnson, 2020; Setiawan & Putri, 2019). Oleh karena itu, tindakan proaktif yang melibatkan peningkatan literasi digital dan penerapan teknologi keamanan menjadi sangat penting.

APPA : Jurnal Pengabdian kepada Masyarakat
Volume 2, No. 6 April 2025
ISSN 3025-0889 (media online)
Hal 707-711

Tindakan proaktif tidak hanya terbatas pada aspek teknis tetapi juga mencakup pendekatan edukasi dan kolaborasi antar pemangku kepentingan. Teknologi berbasis kecerdasan buatan (AI) dan analisis big data kini semakin diandalkan untuk mendeteksi pola-pola anomali yang dapat mengindikasikan potensi serangan siber (Clark et al., 2019). Hal ini menunjukkan bahwa upaya kolektif diperlukan untuk menciptakan ekosistem digital yang aman dan berkelanjutan.

Keamanan siber yang kuat memberikan manfaat tidak hanya untuk perlindungan individu tetapi juga mendukung keberlanjutan berbagai sektor. Dalam sektor pendidikan, misalnya, penerapan keamanan yang baik melindungi data sensitif siswa dan institusi. Di sektor ekonomi, keamanan digital meningkatkan kepercayaan konsumen dalam melakukan transaksi online. Di pemerintahan, sistem yang aman mendukung stabilitas layanan publik dan melindungi informasi sensitif.

Dengan demikian, pentingnya tindakan proaktif dalam menghadapi ancaman siber tidak dapat diabaikan. Upaya yang terkoordinasi antara individu, institusi, perusahaan, dan pemerintah menjadi kunci untuk mengurangi risiko dan memastikan keberlanjutan teknologi dalam mendukung aktivitas kehidupan modern.

2. METODE PELAKSANAAN

2.1 Persiapan

Tahap persiapan dimulai dengan identifikasi tingkat pemahaman peserta terhadap isu-isu keamanan siber yang berkembang di dunia digital saat ini. Proses ini diawali dengan observasi awal mengenai kesadaran peserta terhadap keamanan siber. Observasi dilakukan melalui wawancara, diskusi kelompok, atau kuisioner untuk mengukur sejauh mana peserta memahami ancaman digital serta praktik keamanan yang sudah mereka terapkan dalam kehidupan sehari-hari.

Setelah mendapatkan gambaran awal, survei yang lebih mendalam dilakukan untuk menggali pengetahuan peserta mengenai berbagai ancaman digital, seperti phishing, malware, ransomware, dan kebocoran data. Survei ini bertujuan untuk mengetahui jenis ancaman yang paling sering dihadapi peserta dan dampaknya terhadap data pribadi maupun organisasi. Hasil survei ini menjadi dasar dalam merancang materi edukasi yang lebih spesifik dan relevan sesuai kebutuhan peserta.

Materi edukasi mencakup pengenalan mendalam tentang berbagai ancaman siber, di antaranya phishing yang bertujuan memanipulasi individu agar mengungkapkan informasi pribadi, malware yang merupakan perangkat lunak berbahaya yang dapat merusak sistem, ransomware yang mengunci akses data dan meminta tebusan, serta kebocoran data yang menyebabkan informasi pribadi jatuh ke pihak yang tidak bertanggung jawab. Selain mengenalkan jenis-jenis ancaman, materi ini juga mencakup langkah-langkah pencegahan proaktif, seperti penggunaan kata sandi yang kuat dan unik, penerapan autentikasi dua faktor (2FA) untuk menambah lapisan keamanan, serta perlindungan perangkat melalui antivirus dan firewall.

Dengan pendekatan ini, peserta diharapkan lebih siap memahami dan menghadapi berbagai ancaman siber yang mungkin ditemui di dunia maya serta mampu menerapkan praktik keamanan digital yang efektif dalam kehidupan sehari-hari.

2.2 Pelaksanaan

Kegiatan pengabdian masyarakat dilaksanakan dengan tahapan yang terstruktur, mencakup survei, pelatihan, dan evaluasi. Tahap awal berupa penyebaran survei kepada siswa SMK An Nurmaniyah untuk mengidentifikasi pemahaman awal mereka terkait ancaman siber dan praktik keamanan digital. Survei ini bertujuan untuk mengetahui sejauh mana pengetahuan siswa terhadap ancaman seperti phishing, malware, dan serangan siber lainnya.

Selanjutnya, dilakukan pelatihan menggunakan metode interaktif seperti simulasi penggunaan VirusTotal. VirusTotal adalah alat untuk menganalisis file dan URL guna mendeteksi ancaman keamanan. Simulasi ini membantu siswa memahami cara memanfaatkan teknologi untuk melindungi data pribadi mereka. Sesi pelatihan juga mencakup diskusi kelompok tentang studi kasus serangan siber, memberikan kesempatan kepada siswa untuk mengenali dan merancang solusi atas ancaman yang mungkin mereka hadapi di dunia maya.

APPA : Jurnal Pengabdian kepada Masyarakat
Volume 2, No. 6 April 2025
ISSN 3025-0889 (media online)
Hal 707-711

3. ANALISA DAN PEMBAHASAN

3.1 Meningkatkan Kesadaran Mengenai Pencegahan Ancaman Siber

Gambar 1. Pemaparan Materi Pencegahan Ancaman Siber

Peningkatan kesadaran tentang pentingnya menjaga keamanan data pribadi menjadi fokus utama dalam pemaparan ini. Materi disampaikan kepada siswa-siswi TKJ An Nurmaniyah dengan tujuan memberikan pemahaman mengenai berbagai ancaman siber, seperti peretasan, pencurian data, dan phishing. Dalam sesi ini, siswa diberikan pengetahuan terkait risiko yang mungkin dihadapi serta langkah-langkah pencegahan yang dapat dilakukan, seperti membuat kata sandi yang kuat, menghindari tautan atau lampiran yang mencurigakan, dan menggunakan perangkat lunak keamanan. Dengan pemahaman yang baik, siswa diharapkan dapat membangun kebiasaan digital yang aman serta mampu melindungi data pribadi mereka dari berbagai ancaman siber. Kegiatan ini tidak hanya bertujuan untuk meningkatkan kesadaran, tetapi juga membentuk perilaku proaktif dalam menjaga keamanan di dunia digital.

3.2 Pemaparan Masalah dan Studi Kasus

Gambar 2. Pemaparan Studi Kasus

Penggunaan Wi-Fi publik menjadi salah satu topik penting dalam pemaparan kepada siswa-siswi TKJ An Nurmaniyah. Meskipun mudah diakses dan gratis, Wi-Fi publik sering kali menyimpan risiko keamanan yang serius. Salah satu ancaman yang paling umum adalah serangan man-in-the-middle, di mana peretas dapat mencuri data sensitif yang dikirim melalui jaringan

APPA : Jurnal Pengabdian kepada Masyarakat
Volume 2, No. 6 April 2025
ISSN 3025-0889 (media online)
Hal 707-711

tersebut. Risiko lainnya meliputi penyebaran malware melalui koneksi yang tidak aman, pengintaian aktivitas online oleh pihak yang tidak bertanggung jawab, serta keberadaan jaringan Wi-Fi palsu yang sengaja dibuat untuk mengecoh pengguna.

Sebagai studi kasus, siswa diperkenalkan pada insiden pencurian data yang kerap terjadi di lokasi seperti kafe atau bandara. Dalam situasi ini, peretas memanfaatkan kerentanan jaringan Wi-Fi untuk mencuri informasi penting, seperti kredensial login, data kartu kredit, dan informasi sensitif lainnya. Untuk mencegah risiko tersebut, siswa diberikan solusi praktis, seperti menghindari akses ke situs web yang memerlukan login atau data penting, serta menonaktifkan pengaturan koneksi otomatis ke Wi-Fi publik. Dengan memahami risiko dan langkah pencegahan ini, siswa diharapkan dapat lebih bijak dalam menggunakan jaringan publik dan mampu melindungi data pribadi mereka dari ancaman siber.

3.3 Pelatihan Penggunaan Virustotal

Gambar 3. Pemaparan Penggunaan Virustotal

Dalam pelatihan ini, siswa dan siswi dilatih untuk mengunggah file atau memasukkan URL yang ingin diperiksa. Mereka diajarkan cara membaca hasil analisis dari berbagai mesin antivirus, sehingga dapat membedakan antara ancaman nyata dan false positive.

Selama pelatihan, siswa dan siswi juga diberikan panduan tentang pentingnya memeriksa file atau tautan yang diterima dari sumber yang tidak dikenal. Dengan pelatihan ini, mereka diharapkan dapat memahami langkah-langkah yang diperlukan untuk melindungi diri dari ancaman siber. Selain itu, pelatihan ini bertujuan untuk meningkatkan kesadaran akan pentingnya mengecek keamanan file dan URL sebelum membukanya. Siswa dan siswi yang telah mengikuti pelatihan diharapkan dapat lebih waspada dan mampu mengidentifikasi potensi ancaman sejak dini.

3.4 Sesi Evaluasi

Gambar 4. Evaluasi dan Foto Bersama Siswa

APPA : Jurnal Pengabdian kepada Masyarakat
Volume 2, No. 6 April 2025
ISSN 3025-0889 (media online)
Hal 707-711

Sesi evaluasi dilakukan untuk mengukur efektivitas kegiatan edukasi dan pelatihan yang telah dilaksanakan. Evaluasi ini dilakukan dengan memberikan kuisioner kepada peserta untuk mengetahui sejauh mana pemahaman mereka meningkat setelah mengikuti sesi edukasi dan pelatihan. Kuisioner mencakup pertanyaan tentang konsep ancaman siber, seperti phishing, malware, ransomware, serta langkah-langkah pencegahan yang telah diperkenalkan, seperti penggunaan kata sandi yang kuat, autentikasi dua faktor (2FA), dan perlindungan perangkat menggunakan antivirus.

Hasil evaluasi menunjukkan bahwa sebagian besar peserta mengalami peningkatan pemahaman yang signifikan, terutama dalam mengenali ancaman siber

4. KESIMPULAN

Kegiatan edukasi dan pelatihan mengenai keamanan siber kepada siswa-siswi TKJ An Nurmaniyah telah memberikan dampak positif dalam meningkatkan kesadaran mereka terhadap ancaman siber dan langkah-langkah pencegahan. Dengan pendekatan diskusi, pemaparan masalah, pelatihan interaktif, dan evaluasi, peserta menunjukkan peningkatan pemahaman yang signifikan, terutama dalam mengenali ancaman seperti phishing, malware, ransomware, dan kebocoran data. Selain itu, mereka juga mulai memahami pentingnya menerapkan langkah-langkah keamanan, seperti penggunaan kata sandi yang kuat, autentikasi dua faktor, dan perlindungan perangkat dengan antivirus.

REFERENCES

Smith, J., Johnson, T., & White, L. (2021). Emerging cybersecurity threats in a digital era. *Journal of Cyber Security Research, 15*(4), 120-135.

Wibisono, H. (2020). Sosialisasi digital security dalam meningkatkan edukasi bermedia digital. *Journal of Cyber Security*, 3(2), 45-48.

Setiawan, H., & Putri, A. (2019). Strategi pencegahan ancaman siber melalui edukasi masyarakat. *Jurnal Teknologi Informasi dan Komputer*, 10(1), 25-30.

Clark, R. M., & Thomas, K. (2019). *Proactive measures for sustainable cybersecurity*. New York: Springer Publishing.

Klein, B. (2018). *Digital innovation and its implications for cybersecurity*. London: Routledge.

Rahman, A., Suryani, T., & Putra, D. F. (2021). Pemahaman literasi digital masyarakat Indonesia dalam menghadapi ancaman siber. *Jurnal Komunikasi dan Teknologi Informasi*, 8(3), 78-89.

Miller, R., & Rose, A. (2022). Phishing and its impact on modern internet users. *Cyber Threat Analysis, 6*(1), 102-115.

Arifin, T., & Sari, M. (2020). Meningkatkan literasi keamanan siber melalui pendidikan teknologi. *Jurnal Ilmu Komputer Indonesia*, 12(2), 54-62.

Johnson, K. (2020). Emerging proactive cybersecurity technologies. *International Journal of Cyber Studies*, 9(3), 245-268.

Schneider, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world*. W.W. Norton & Company.