APPA : Jurnal Pengabdian kepada Masyarakat
Volume 2, No. 03, Tahun 2024
ISSN 3025-0889 (media online)
Hal 347-350

Cybersecurity : Jenis Serangan Dan Bagaimana Peretas Melakukannya Serta Langkah Pengamanannya

Firdha Rofika[1], Sabita Adelia[2], Adi Saputra[3], Angga Fahreza[4], Krisna Nur Aedi Aripin[5], Dafa Rizqi Setiawan[6], Fadzle Izza Rizwaan[7], Muhammad Rafli Alwaan[8], Muhammad Rizky Ramadhan[9], Raden Muhammad Vito Nugroho[10], Dede Handayani[11*]

[1-11]Jurusan Teknik Informatika, Universitas Pamulang, Jl. Raya Puspitek No. 46 buaran, Serpong, Kota Tangerang Selatan, Provinsi Banten, Indonesia, 15310.
Email: [1]brylianafz@gmail.com, [2]sabitaaw@gmail.com, [3]acpeymilan02@gmail.com, [4]anggafahreza45@gmail.com, [5]krisnanuraa@gmail.com, [6]dafarizqis07@gmail.com, [7]fadzleizzarizwaan@gmail.com, [8]muhammadraflialwaan@gmail.com, [9]rizkyrama7383@gmail.com, [10]ramving26@gmail.com, [11*]dosen02411@unpam.ac.id
(* : coressponding author)

Abstrak - Pengabdian kepada masyarakat adalah cara bagi akademisi untuk memberikan dampak positif pada lingkungan sekitarnya. Inisiatif ini dilaksanakan di SMK Fadilah dengan fokus pada tema "Keamanan Siber: Jenis Serangan, Cara Operasi Peretas, dan Langkah Pengamanan." Tujuan utamanya adalah untuk meningkatkan kesadaran dan pemahaman siswa tentang ancaman siber yang semakin kompleks, seperti serangan *phishing*, *malware*, dan *brute force*. Peserta juga mendapatkan wawasan tentang teknik peretasan yang umum digunakan untuk membobol sistem serta mempelajari strategi perlindungan, termasuk penggunaan kata sandi yang kuat, pembaruan perangkat lunak secara rutin, dan penerapan *firewall*. Program ini menggunakan metode ceramah interaktif, simulasi. Hasil kegiatan ini menunjukkan peningkatan pemahaman siswa terhadap konsep keamanan siber dan langkah pencegahan yang dapat diterapkan dalam kehidupan sehari-hari. Melalui inisiatif ini, diharapkan siswa SMK Fadilah lebih siap menghadapi tantangan keamanan digital di era modern.

Kata Kunci : Layanan Masyarakat, Keamanan Siber, Kesadaran Keamanan Digital

Abstract *- Community service is a way for academics to make a positive impact on their surroundings. This particular initiative took place at SMK Fadilah, focusing on "Cybersecurity: Types of Attacks, How Hackers Operate, and Security Measures." The primary objective was to enhance students' awareness and understanding of increasingly complex cyber threats, such as phishing, malware, and brute force attacks. Participants also gained insights into common hacking techniques used to breach systems and learned about protective strategies, including the use of strong passwords, regular software updates, and firewall implementation. The program employed interactive lectures, simulations as teaching methods. The outcome of this activity demonstrated an improvement in students' comprehension of cybersecurity concepts and preventive measures applicable to daily life. Through this initiative, SMK Fadilah students are expected to be better prepared to face digital security challenges in the modern era..*

Keywords : *Community Service, Cyber Security, Digital Security Awareness*

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang pesat telah membawa dampak signifikan dalam berbagai aspek kehidupan. Namun, di balik manfaat yang ditawarkan, ancaman terhadap keamanan siber (*cybersecurity*) juga semakin meningkat. Serangan siber seperti *phishing*, *malware*, hingga *brute force attacks* kini menjadi tantangan besar bagi individu maupun organisasi. Ancaman ini tidak hanya merugikan secara materi, tetapi juga mengancam privasi dan data pribadi pengguna.[1]

APPA : Jurnal Pengabdian kepada Masyarakat
Volume 2, No. 03, Tahun 2024
ISSN 3025-0889 (media online)
Hal 347-350

Gambar 1. Ketua PKM

Bagi siswa SMK, khususnya di bidang teknologi informasi, pemahaman tentang keamanan siber sangatlah penting. Sebagai generasi muda yang tumbuh di era digital, mereka perlu memiliki kemampuan untuk mengenali ancaman siber dan memahami langkah-langkah pencegahan yang tepat. Hal ini bertujuan untuk melindungi diri sendiri, institusi, maupun masyarakat di lingkungan mereka dari risiko keamanan siber.[2]

Kegiatan pengabdian kepada masyarakat ini dirancang untuk meningkatkan kesadaran siswa SMK Fadilah mengenai ancaman keamanan siber dan memberikan pemahaman mendalam tentang jenis-jenis serangan yang umum terjadi, bagaimana peretas melakukannya, serta langkah-langkah pengamanan yang dapat diterapkan. Melalui kegiatan ini, diharapkan siswa tidak hanya mampu mengenali risiko, tetapi juga memiliki keterampilan dasar dalam melindungi data dan sistem yang mereka gunakan.[3]

Metode yang digunakan meliputi ceramah interaktif, simulasi serangan siber untuk memberikan pengalaman belajar yang lebih mendalam. Dengan demikian, siswa diharapkan tidak hanya mendapatkan teori, tetapi juga keterampilan praktis yang dapat diterapkan dalam kehidupan sehari-hari. Inisiatif ini merupakan bagian dari upaya mendukung penguatan literasi digital dan keamanan siber di kalangan siswa SMK sebagai bekal menghadapi tantangan di era digital.[4]

2. METODE

Kegiatan Pengabdian kepada Masyarakat ini menggunakan pendekatan seminar yang langsung melibatkan seluruh siswa di SMK Fadilah. Tujuan dari seminar ini adalah untuk meningkatkan kesadaran dan pemahaman siswa mengenai keamanan siber, dengan fokus pada dampak positif dan negatifnya dalam konteks keselamatan digital. Sebagai bagian dari program ini, diadakan sesi tanya jawab untuk memberikan kesempatan kepada siswa untuk mengajukan pertanyaan dan memperdalam pemahaman mereka terhadap materi yang disampaikan.

Tahap awal dari program ini mencakup serangkaian perencanaan yang meliputi:

1. Melakukan survei lokasi dan koordinasi dengan bagian Humas SMK Fadilah yang beralamat di Jl. Pendidikan, Parigi, Kec. Pd. Aren, Kota Tangerang Selatan, Banten 15227.
2. Menyiapkan materi edukasi dan alat bantu praktis untuk pelaksanaan seminar.
3. Mendiskusikan topik-topik terkait keamanan siber untuk mengukur pemahaman dasar siswa.
4. Memberikan penjelasan tambahan kepada siswa yang belum sepenuhnya memahami materi hingga mereka dapat memahaminya dengan baik.
5. Memberikan soal untuk memastikan siswa menyerap materi dengan baik, dengan jawaban yang benar mendapatkan hadiah berupa Sticker dan Bingkisan sebagai bentuk apresiasi.

APPA : Jurnal Pengabdian kepada Masyarakat
Volume 2, No. 03, Tahun 2024
ISSN 3025-0889 (media online)
Hal 347-350

6. Menyusun laporan akhir setelah kegiatan selesai.
7. Mempublikasikan laporan akhir untuk disebarkan kepada pembaca yang lebih luas.

Target audiens dari kegiatan ini adalah siswa kelas 10 dan kelas 11 SMK Fadilah. Seminar ini dilaksanakan di ruang kelas dengan pemimpin dan pembicara program yang merupakan mahasiswa dari Program Studi Teknik Informatika Universitas Pamulang.

Kegiatan Pengabdian kepada Masyarakat ini dilaksanakan pada tanggal 13 November 2024, bertempat di SMK Fadilah, Jl. Pendidikan, Parigi, Kec. Pd. Aren, Kota Tangerang Selatan, Banten 15227

3. HASIL DAN PEMBAHASAN

3.1 Kegiatan Pemaparan Materi

Gambar 2. Narasumber menjelaskan Materi

Pada kegiatan PKM (Pengabdian Kepada Masyarakat) ini kelompok kami menjelaskan tentang *Cyber Security* : Jenis Serangan dan Bagaiman Peretas Melakukannya serta Langkah Pengamanannya kepada para siswa/siswi SMK Fadilah di Tangerang Selatan, kegiatan ini dilakukan dengan memaparkan Materi tentang Pengenalan dasar-dasar *Cyber Security*, Ancaman *Cyber Security*, Masa Depan *Cyber Security* dan Praktik Demontrasi Serangan.

Cyber merupakan istilah yang merujuk pada segala sesuatu yang terkait dengan dunia digital dan security merupakan kondisi atau tindakan yang diambil untuk melindungi dari ancaman bahaya atau kerugian.

Jenis-jenis ancaman *Cyber Security* yaitu *Malware*, *Phising*, *DDoS*, *MitM*, *SQL Injection* dan *XSS*. Contoh dan cara menghadapi ancaman ***Phishing*** yaitu ***Phishing*** adalah serangan siber di mana penyerang menyamar sebagai entitas tepercaya untuk mencuri informasi sensitif, seperti kata sandi, nomor kartu kredit, atau data pribadi, melalui email, pesan teks, atau situs web palsu. Biasanya, korban diarahkan untuk mengklik tautan atau mengunduh file berbahaya yang terlihat sah. Untuk menghadapinya, pengguna harus berhati-hati terhadap pesan mencurigakan, memverifikasi keaslian pengirim, menghindari mengklik tautan atau lampiran dari sumber yang tidak dikenal, serta mengaktifkan filter anti-phishing pada email. Edukasi dan kewaspadaan menjadi kunci utama untuk mencegah jatuh dalam perangkap phishing.

Contoh yang lain ancaman ***Malware*** ancaman ini meliputi virus, worm, trojan, *ransomware*, dan *spyware*. *Malware* sering disebarkan melalui lampiran email, unduhan dari situs tidak tepercaya, atau tautan mencurigakan. Untuk menghadapinya, pastikan perangkat lunak antivirus selalu aktif dan diperbarui, gunakan firewall untuk membatasi akses tidak sah, unduh perangkat lunak hanya dari sumber resmi, dan hindari mengklik tautan atau file dari pengirim yang mencurigakan. Selain itu, lakukan pemindaian rutin pada sistem untuk mendeteksi dan menghapus malware yang mungkin telah menyusup.

APPA : Jurnal Pengabdian kepada Masyarakat
Volume 2, No. 03, Tahun 2024
ISSN 3025-0889 (media online)
Hal 347-350

Kebutuhan *Cyber Security* pada Kebutuhan di Dunia Profesional, menurut Permintaan (*Demand*) terhadap keamanan siber (*cyber security*) di pemerintahan dan perusahaan diperkirakan akan terus meningkat pada tahun 2024. Beberapa faktor yang berkontribusi terhadap peningkatan permintaan ini termasuk meningkatnya ancaman siber yang lebih kompleks dan canggih, terutama dengan munculnya teknologi baru seperti kecerdasan buatan generatif. Banyak organisasi menyadari pentingnya memiliki langkah-langkah keamanan yang kuat untuk melindungi data dan infrastruktur mereka dari serangan yang dapat menyebabkan kerugian besar.

Tantangan yang dihadapi termasuk kekurangan tenaga ahli keamanan siber, di mana banyak organisasi melaporkan kesulitan dalam menarik dan mempertahankan profesional yang berkualitas. Selain itu, ketidaksetaraan dalam kesiapan keamanan siber antara organisasi besar dan kecil menjadi perhatian utama, dengan banyak usaha kecil masih kurang dilindungi. Dengan demikian, baik pemerintah maupun perusahaan diharapkan akan meningkatkan investasi mereka dalam solusi keamanan siber dan pelatihan untuk mengatasi tantangan ini.

4. KESIMPULAN

Kegiatan pengabdian kepada masyarakat yang dilakukan di SMK Fadilah dengan tema "*Cybersecurity*: Jenis Serangan, Cara Operasi Peretas, dan Langkah Pengamanan" berhasil meningkatkan pemahaman siswa tentang ancaman keamanan digital dan strategi pencegahannya. Melalui metode ceramah interaktif dan simulasi, siswa mendapatkan wawasan mendalam tentang berbagai jenis serangan siber, seperti *phishing*, *malware*, dan *brute force*, serta cara peretas melakukan serangan tersebut.

Selain itu, para peserta juga mempelajari langkah-langkah pencegahan, seperti pentingnya penggunaan kata sandi yang kuat, pembaruan perangkat lunak secara berkala, dan implementasi *firewall*. Berdasarkan hasil evaluasi, terdapat peningkatan signifikan dalam pemahaman siswa terhadap konsep-konsep keamanan siber, yang ditunjukkan melalui hasil *post-test* yang lebih baik dibandingkan *pre-test*.

Kegiatan ini juga menunjukkan bahwa pendekatan pembelajaran berbasis pengalaman, seperti simulasi serangan siber, sangat efektif dalam membantu siswa memahami materi secara lebih mendalam. Oleh karena itu, kami merekomendasikan agar kegiatan serupa diadakan secara rutin, baik di SMK Fadilah maupun institusi pendidikan lainnya, untuk mendukung literasi digital dan kesiapan generasi muda dalam menghadapi tantangan keamanan di era digital.

Dengan meningkatnya kesadaran dan pemahaman siswa tentang keamanan siber, diharapkan mereka mampu melindungi data pribadi serta sistem yang digunakan dari ancaman siber, sehingga menjadi individu yang lebih siap dalam menghadapi era digital yang semakin kompleks.

DAFTAR PUSTAKA

Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley*.
Gordon, L., & Loeb, M. (2002). *The Economics of Information Security. Journal of Computer Security, 11(4), 561-590.*
Adianto, T., Ali, Y., & Saptono, E. (2020). Penilaian Risiko Serangan Siber Sistem Manajemen Keamanan Informasi PT. UAV. Manajemen Pertahanan, 6(1), 52-72.
Magrisa, D. (2020). Kerjasama Badan Siber dan Sandi Negara (BSSN) Indonesia dengan Department of Foreign Affairs and Trade (DFAT) Australia dalam Pengembangan Keamanan Siber.
BSSN. (2019). Indonesia *Cyber Security Monitoring Repor*t 2019. Jakarta: Pusat Operasi Keamanan Siber Nasional Badan Siber dan Sandi Negara.
Alizah, M. D. (2020). Sentimen Analisis Terkait Lockdown pada Sosial Media Twitter. Jurnal Teknologi Informasi dan Ilmu Komputer, 7(2), 103-114.