

Pelatihan *Basic Cyber Security* Dan Perlindungan Data Diri Untuk Siswa MAN 1 Kota Tangerang Selatan

Nanang^{1*}, Amin Hidayat², Ade Prima Putra Suhendri³

^{1,2,3}Fakultas Ilmu Komputer, Teknik Informatika, Universitas Pamulang, Tangerang Selatan, Indonesia

^{1*}dosen02599@unpam.ac.id, ²dosen02615@unpam.ac.id, ³dosen02555@unpam.ac.id

Abstrak - *Cybercrime* merupakan kejahatan yang relatif baru yang dilakukan oleh para profesional atau individu yang memiliki keahlian di bidang komputer dan teknologi informasi. Dari sisi dampak kejahatan, kejahatan di dunia maya (Internet) dapat berdampak baik di dalam maupun di luar dunia maya. Ketika aktivitas terjadi melalui media Internet, ruang dan waktu yang tidak terbatas membuat sulit untuk mendeteksi aktivitas di dunia maya dengan menggunakan metode tradisional. Dalam kasus ancaman siber, berdasarkan analisis data sistem pemantauan lalu lintas ID-SIRTII (*Indonesia Security Incident Response Team On Internet Infrastructure*), serangan di dunia maya Indonesia sudah mencapai 1 juta dan ternyata terus meningkat. Kelemahan dalam sistem dan aplikasi menciptakan masalah setiap hari. Melindungi aset digital adalah perhatian utama bagi dunia usaha, karena serangan siber dapat berdampak pada kinerja dan reputasi bisnis. Ada banyak metode dan teknik yang dapat membantu dalam proses membantu siswa memanfaatkan peluang besar yang dihadirkan oleh perkembangan teknologi Internet. Tinjauan mengenai keamanan siber dan perlindungan data pribadi pada gadget menunjukkan bahwa meskipun siswa kini berhasil menggunakan perangkat tersebut, pengetahuan mereka tentang keamanan data masih kurang. Memperkenalkan keamanan siber sebagai dasar keamanan data di era digital penting dilakukan untuk memastikan siswa tidak memiliki akses terhadap data pribadi untuk mencegah penyalahgunaan data oleh oknum yang tidak bertanggung jawab dan menimbulkan kerugian bagi berbagai pihak akibat penyalahgunaan data tentang pentingnya. Oleh karena itu, tujuan dari kegiatan bakti sosial ini adalah untuk memperkenalkan pentingnya keamanan data di era digital dan meningkatkan pemahaman tentang keamanan siber modern dan kejahatan siber melalui konsultasi individu dengan mahasiswa. Kegiatan ini berupa materi pelatihan dan latihan pada saat pelatihan. Materi pelatihan mencakup pengenalan dampak positif kemajuan teknologi Internet, dasar-dasar penerapan keamanan data, dan penggunaan perdagangan elektronik yang aman untuk melindungi informasi pribadi. Untuk persiapan pelatihan, tim pengabdian akan melakukan percobaan penerapan keamanan data dengan menggunakan materi *e-commerce* dan akan membahasnya pada saat pelatihan. Pelatihan akan dilaksanakan dalam bentuk ceramah dan sesi tanya jawab. Dimulai dengan pengenalan dampak positif kemajuan teknologi Internet, Anda akan mempelajari cara menerapkan keamanan data pada produk digital dalam transaksi online, dan banyak orang serta pelajar akan mengetahui cara melindungi data tersebut. Memahami sistem keamanan gadget dan mengamankan alur transaksi di website, *e-commerce*, dan game. Pelatihan dilaksanakan di lab komputer Madrasah Aliya Negeri 1 Selatan Kota Tangerang, sehingga para siswa dapat langsung mempraktekkan apa yang dipelajari selama pelatihan.

Kata Kunci: *Cyber Security, Keamanan Data, Era Digital, Data, Cyber Crime*

Abstract - *Cybercrime* is a relatively new crime committed by professionals or individuals who have expertise in computers and information technology. In terms of the impact of the crime, *cybercrime* (Internet) can have an impact both inside and outside cyberspace. When activities occur through the Internet, unlimited space and time make it difficult to detect cyberspace activities using traditional methods. In the case of cyber threats, based on data analysis of the ID-SIRTII (*Indonesia Security Incident Response Team On Internet Infrastructure*) traffic monitoring system, cyber attacks in Indonesia have reached 1 million and continue to increase. Weaknesses in systems and applications create problems every day. Protecting digital assets is a major concern for the business world, as cyber attacks can impact business performance and reputation. There are many methods and techniques that can help in the process of helping students take advantage of the great opportunities presented by the development of Internet technology. A review of cybersecurity and personal data protection on gadgets shows that although students are now successfully using these devices, their knowledge of data security is still lacking. Introducing cybersecurity as the basis for data security in the digital era is important to ensure that students do not have access to personal data to prevent data misuse by irresponsible individuals and cause losses to various parties due to data misuse about the importance of. Therefore, the purpose of this social service activity is to introduce the importance of data security in the digital era and increase understanding of modern cybersecurity and cybercrime through individual consultations with students. This activity is in the form of training materials and exercises during training. Training materials include an introduction to the positive impacts of advances in Internet technology, the basics of implementing data security, and the use of secure electronic commerce to protect personal information. In preparation for the training, the service team will conduct an experiment on implementing data security using *e-commerce*

materials and will discuss it during the training. The training will be carried out in the form of lectures and question and answer sessions. Starting with an introduction to the positive impacts of advances in Internet technology, you will learn how to apply data security to digital products in online transactions, and many people and students will know how to protect the data. Understanding gadget security systems and securing transaction flows on websites, e-commerce, and games. The training was held in the computer lab of Madrasah Aliya Negeri 1 Selatan Kota Tangerang, so that students could directly practice what they had learned during the training.

Keywords: *Cyber Security, Data Security, Digital Era, Data, Cyber Crime*

1. PENDAHULUAN

Peningkatan mutu pendidikan dapat dicapai melalui beberapa cara, antara lain melalui peningkatan kualifikasi siswa, pelatihan, dan pendidikan atau dengan memberikan kesempatan kepada siswa lewat pelatihan yang terkendali (Muhammad Hasyim, 2014).

Dalam era yang semakin terhubung dan tergantung pada teknologi informasi, keamanan siber menjadi fokus utama dalam menjaga stabilitas dan integritas sistem informasi. Organisasi-organisasi, termasuk instansi pendidikan harus lebih memperhatikan siswa didiknya untuk melekat teknologi dan harus mampu menghadapi ancaman siber yang semakin kompleks. Kualitas Sumber Daya Manusia (SDM) menjadi kunci dalam menyongsong tantangan ini, mengingat bahwa manusia memegang peran sentral dalam keamanan siber. MAN 1 Kota Tangerang Selatan sebagai Institusi pendidikan, diharapkan menyiapkan generasi-generasi handal di bidang komputer dan teknologi informasi. Untuk mengatasi tantangan ini, perlu dilakukan pelatihan *cyber security* dan keamanan data. (Mochammad Machlul Alamin, 2023).

Madrasah berasal dari akar kata dari dasar, yaitu belajar, sedangkan madrasah berarti tempat belajar atau sekolah formal. Madrasah menurut orang awam adalah lembaga pendidikan tingkat dasar dan menengah yang mengajarkan agama Islam saja, perpaduan antara ilmu agama Islam dan ilmu umum, maupun ilmu berbasis ajaran Islam. Pelatihan adalah proses untuk membentuk dan membekali individu dengan meningkatkan pengetahuan, keterampilan, bakat, dan perilaku mereka, menurut (Kasmir, 2016). Manajemen sumber daya manusia adalah modal tanpa bentuk yang diperoleh dari orang-orang yang tidak dapat dikelola oleh bisnis dengan cara yang sama seperti mereka mengelola pekerjaan, produk, dan teknologi. (Snell & Bohlander, 2012).

Tindak pidana siber merupakan tindak pidana yang relatif baru, yang dilakukan oleh orang-orang yang ahli atau yang memiliki keahlian di bidang komputer dan teknologi informasi. Jika dilihat dari segi akibat kejahatan, maka kejahatan melalui dunia maya (internet) dapat berdampak di dalam maupun di luar dunia maya. Tidak terbatasnya ruang dan waktu dalam melakukan aktivitas dengan menggunakan internet sebagai media, menyebabkan sulitnya suatu aktivitas dalam dunia maya dideteksi secara konvensional. Komputer yang dulu sebagai alat pengumpul dan penyimpanan data saat ini dapat digunakan untuk melakukan kejahatan lama (*old fashioned*) dalam kemasan baru. Jika mengikuti kasus-kasus kejahatan komputer dan siber yang terjadi dan jika hal tersebut dikaji dengan menggunakan kriteria peraturan hukum pidana konvensional, maka ternyata bahwa dari segi hukum, kejahatan komputer dan siber bukanlah kejahatan yang sederhana (Ersya, 2017).

Seperti kasus yang terjadi yang menyerang sektor publik di bidang kesehatan, yang sebenarnya tetap bermuara kepada tebusan uang, dua rumah sakit di Jakarta terjebak program jahat jenis *ransomware* bernama *WannaCry*. *Malware* bermodus menyandera data dan meminta tebusan uang itu telah mengunci sistem dan data pasien di RS Dharmas dan RS Harapan Kita. Pembuat *WannaCry* meminta uang Rp 4 juta sebagai tebusan. Hal serupa juga terjadi di Rumah sakit di *Hollywood Presbyterian Medical Center* di Los Angeles, Amerika Serikat (AS). Pihak rumah sakit harus rela merogoh kantongnya untuk mengeluarkan uang hingga 17.000 *dollar* atau sekitar Rp 226 juta demi menebus data yang di sandera penyerang. Menurut administrator rumah sakit Harapan Kita Jakarta untuk bahwa solusi untuk mendapatkan kembali akses yang terputus itu adalah dengan membayar sejumlah uang pada penyerangnya (Kwarto & Angsito, 2018).

Dalam kasus ancaman siber, berdasarkan analisis data sistem monitoring *traffic* ID-SIRTII (Indonesia Security Incident Response Team On Internet Infrastructure) tercatat bahwa insiden serangan di dalam dunia maya di Indonesia mencapai satu juta insiden dan akan cenderung mengalami peningkatan setiap harinya akibat kelemahan sistem dan aplikasi yang tidak diketahui. Dalam hal ini, institusi pemerintah juga tidak luput dari serangan siber di mana dalam kurun waktu 1998 - 2009 sebanyak 2.138 serangan telah dialamatkan terhadap *website* domain milik pemerintah Serangan *Distributed Denial of Service* pada sistem *Domain Name Service* (DNS) CCTLD- ID yaitu domain .id terutama .co.id. Kasus lain juga menyangkut penyebaran *malware* dan *malicious code* yang disisipkan di dalam file dan *website* serta *phising site*, *spionase* industri dan penyanderaan sumber daya informasi kritis, maupun *black campaign* partai politik atau penistaan keyakinan dan penyebaran kabar bohong (*hoax*) untuk tujuan provokasi politis serta rekayasa ekonomi.

Akibat keterbatasan sumber daya dan akses terkait pemeriksaan oleh penegak hukum Indonesia kepada penyelenggara layanan asing di luar negeri, beberapa kasus tersebut belum dapat diatasi walaupun Undang-Undang ITE telah mengaturnya. Sementara dalam konteks global, intensitas serangan siber yang semakin tinggi, bisa dilihat dari serangkaian serangan siber seperti yang dilaporkan dari *The Telegraph* UK, di mana pada bulan Mei 2017 telah terjadi serangan *cyber Wana Crypt0r 2.0* atau yang biasa disebut sebagai virus *WannaCry* menyebar dengan cepat dalam skala masif sepanjang sejarah di tingkat global. Virus tersebut pada awalnya menyebar di Ukraina yang kemudian merembet ke 10 negara lainnya hanya dalam waktu kurang dari dua jam, termasuk Indonesia. Bahkan virus ini kemudian meluas ke 99 negara di dunia. Jika melihat trend global, negara-negara seperti Brazil, Rusia, India, China sudah meningkatkan keamanan *cyber security* mereka. Bahkan perang siber sudah banyak terjadi, sehingga sebagai sebuah negara, termasuk dalam hal ini Indonesia, juga perlu memelihara kedaulatan di ranah siber mengingat bahwa kekerahasiaan, komunikasi antara pejabat publik sekarang pun memasuki dunia digital (Chotimah, 2019).

Berdasarkan laporan dari Badan Siber dan Sandi Negara (BSSN) tercatat bahwa jumlah kasus serangan *cyber* di Indonesia sejak awal tahun 2020 sampai dengan tanggal 12 April 2020 adalah sebanyak 88 juta. Dari angka tersebut, teridentifikasi kasus serangan *trojan activity* sebesar 56%, kasus upaya *information gathering* sebesar 43% dan kasus *web application attack* sebesar 1%. Sedangkan hasil *monitoring* total kasus serangan *cyber* di Indonesia pada akhir tahun 2020 mencapai 495 juta dengan serangan terbanyak berupa *trojan activity* dan pencurian data. Hal tersebut menunjukkan bahwa terjadi peningkatan serangan *cyber* di Indonesia sebesar 205 juta jika dibandingkan dengan jumlah kasus serangan *cyber* pada tahun 2019 yang sebanyak 290 juta kasus (Sama dkk., 2021).

Banyak orang, bisnis, dan bangsa menggunakan Internet secara luas dalam kehidupan sehari-hari mereka untuk menyelesaikan tugas. Namun, dunia maya datang dengan sejumlah risiko yang tidak disadari oleh banyak pengguna internet, terlepas dari kenyataan bahwa ia memberikan banyak peluang dan kemudahan. Penjahat dunia maya dapat menggunakan kecerobohan karyawan sebagai dalih untuk menggunakan internet untuk melakukan tindakan yang membahayakan bisnis atau organisasi tempat mereka bekerja. Untuk memerangi ketidaktahuan tentang pentingnya keamanan dalam aktivitas online, beberapa negara telah membuat dan menerapkan program kesadaran dan pendidikan keamanan siber (Mochammad Machlul Alamin, 2023).

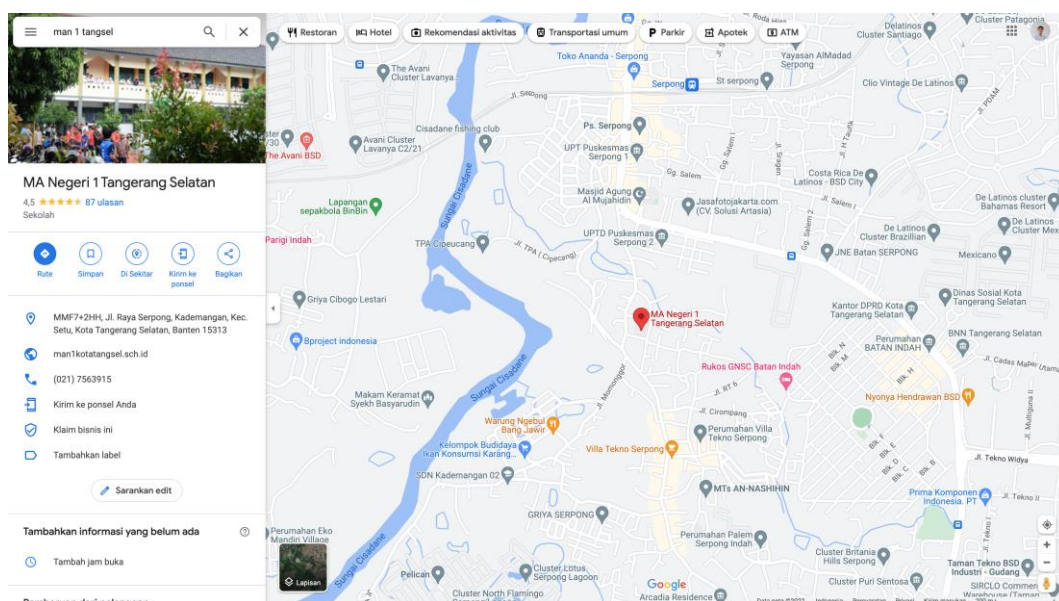
Dalam perkembangannya khususnya pasca amandemen konstitusi Undang-Undang Dasar 1945, hak atas privasi termasuk di dalamnya perlindungan data pribadi diakui sebagai salah satu hak konstitusional warga negara. Hal ini sejalan dengan dimasukkannya bab khusus tentang hak asasi manusia (*bill of rights*) dalam konstitusi, yakni di bab XA Pasal 28A sampai dengan Pasal 28J. Ketentuan mengenai jaminan perlindungan data pribadi dapat ditemukan di dalam Pasal 28G ayat (1), berbunyi Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi (Sentosa Siahaan, 2022).

Tindak pidana siber merupakan tindak pidana yang relatif baru, yang dilakukan oleh orang-orang yang ahli atau yang memiliki keahlian di bidang komputer dan teknologi informasi. Jika dilihat dari segi akibat kejahatan, maka kejahatan melalui dunia maya (internet) dapat berdampak di

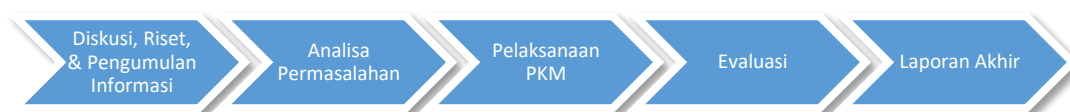
dalam maupun di luar dunia maya. Tidak terbatasnya ruang dan waktu dalam melakukan aktivitas dengan menggunakan internet sebagai media, menyebabkan sulitnya suatu aktivitas dalam dunia maya dideteksi secara konvensional. Komputer yang dulu sebagai alat pengumpul dan penyimpanan data saat ini dapat digunakan untuk melakukan kejahatan lama (old fashioned) dalam kemasan baru. Jika mengikuti kasus-kasus kejahatan komputer dan siber yang terjadi dan jika hal tersebut dikaji dengan menggunakan kriteria peraturan hukum pidana konvensional, maka ternyata bahwa dari segi hukum, kejahatan komputer dan siber bukanlah kejahatan yang sederhana (Ersya, 2017)

2. METODE PELAKSANAAN

Metode dalam kegiatan “Pelatihan *Basic Cyber Security* Dan Perlindungan Data Diri” di Madrasah Aliyah Negeri 1 Kota Tangerang Selatan yang akan dilakukan sebagai bentuk proses pembelajaran, pemahaman dan juga pengetahuan mengenai apa saja hal yang dapat dimanfaatkan dari perkembangan teknologi informasi saat ini adalah dengan penyuluhan dan pelatihan, tahapan pelaksanaan Pengabdian Kepada Masyarakat adalah sebagai berikut :



Gambar 2.1 Lokasi Pelaksanaan PKM



Gambar 2.2 Tahapan Pelaksanaan PKM

Adapun proses pelaksanaan PKM dilapangan dengan langkah-langkah sebagai berikut:

1. Koordinasi dengan pihak Madrasah Aliyah Negeri 1 Tangerang Selatan.
2. Persiapan Penyuluhan dan Pelatihan.
3. Penyuluhan Materi *Cyber Security*
4. Pelatihan *Cyber Security*
5. Perlindungan Data Diri
6. Diskusi dan Sesi Tanya Jawab
7. Kuis

3. HASIL DAN PEMBAHASAN

Target peserta dalam kegiatan ini adalah para siswa dan siswi kelas XII Madrasah Aliyah Negeri 1 Kota Tangerang Selatan dengan total peserta sebanyak 30 orang, yang juga dihadiri oleh Kepala Sekolah, Bagian Kurikulum dan Wali kelas. Kami dengan pihak sekolah sudah berkoordinasi untuk penggunaan ruangan lab komputer dalam penyelenggaraan pelatihan ini agar memudahkan peserta didik dalam mengikuti langkah demi langkah materi praktik yang disampaikan, mengingat kegiatan pelatihan seperti ini dapat memberikan dampak positif terhadap pertumbuhan peserta didik dalam membangun generasi muda yang kreatif, positif dan inovatif.

Tabel 3. 1 Susunan Acara

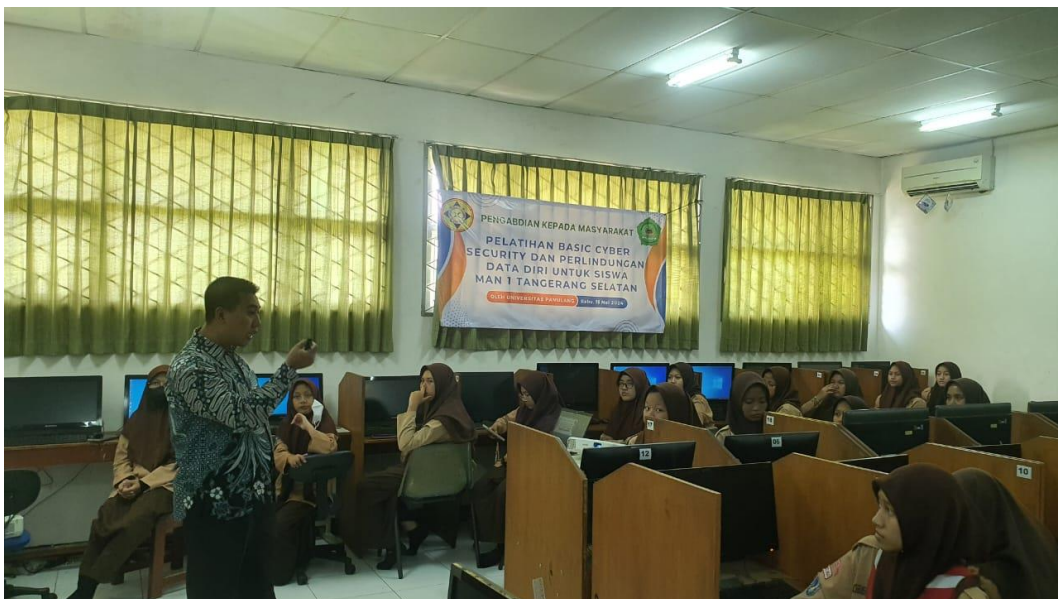
No	Waktu	Kegiatan	Keterangan
1	09:00 – 09:10	Pembukaan	Wahyu Reza Habibi
2	09:10 – 09:30	Sambutan - Kepala Sekolah - Ketua PKM	- H. Ulik Widianoro, M.Pd - Nanang, M.Kom.
3	09:30 – 10:30	Pemaparan Materi dan Praktik - <i>Cyber Security</i> - Standar Keamanan - Perlindungan Data Pribadi - <i>Biometrics Access</i>	- Amin Hidayat, M.Kom. - Ade Prima Putra Suhendri, M.Kom.
4	10:30 – 11:00	Tanya Jawab	Wahyu Reza Habibi
5	11:00 – 11:15	Penyerahan Cindramata	Nanang, M.Kom.
6	11:15 – 11:30	Penutup	Wahyu Reza Habibi
7	11:30 – 12:00	Ramah Tamah	Semua Peserta

Pada praktek *Cyber Security*, peserta didik diberikan pendampingan berupa langkah-langkah sederhana dalam menerapkan teknik *Cyber Security* menggunakan *Standard Biometrics Access* yang diaplikasikan pada media social, *Handphone*, hingga *Laptop/PC*. Sementara pada praktek *e-commerce*, peserta didik diajarkan bagaimana membuat akun pada *marketpace*. Kami para panitia mengarahkan bagaimana cara membuat akun menjadi aman menggunakan standar keamanan *password*, hingga integrasi *Biometrics Access* pada aplikasi yang memerlukan integrasi *Biometrics Access*.



Gambar 3.1 Persiapan Penyampaian Materi

Persiapan penyampaian dilakukan oleh tim pengabdian dengan melakukan *briefing* awal terkait pelaksanaan penyampaian materi, serta pemabgain instruktur dalam penyampaian materi dengan dibantu rekan-rekan mahasiswa yang juga mengikuti kegiatan PKM. Rekan-rekan mahasiswa membantu siswa-siswi untuk penggunaan perangkat PC atau *Laptop* serta *gadget* yang digunakan.



Gambar 3.2 Proses Penyampaian Materi

Proses penyampaian materi dilakukan oleh tim bersama Nanang, S.Kom., M.Kom., Amin Hidayat, S.Kom., M.Kom. dan Ade Prima Putra Suhendri, S.Kom., M.Kom. dalam bidang *Cyber Security* serta penerapan pada era digital saat ini



Gambar 3.3 Peserta PKM

Peserta PKM menyimak pemateri dan adapun pemateri menjelaskan materi tambahan berupa tentang lapisan pertahanan seperti:

1. Kerahasiaan : memastikan bahwa informasi tertentu hanya dapat diakses oleh mereka yang berhak atau memiliki wewenang untuk memperolehnya;
2. Integritas : melindungi akurasi dan kelengkapan informasi melalui sejumlah metodologi pengolahan yang efektif;
3. Ketersediaan : memastikan bahwa informasi terkait dapat diakses oleh mereka yang berwenang sesuai dengan kebutuhan.

Prinsip-prinsip keseluruhan mengatur strategi keamanan dari organisasi manapun.



Gambar 3.4 Foto Bersama

Setelah kegiatan penyampaian materi dan ramah-tamah, peserta PKM melakukan foto Bersama dengan pemateri. Adapun kelengkapan berkas administrasi dilakukan pada sesi ramah tamah dengan pihak sekolah.

4. KESIMPULAN

4.1 Kesimpulan

Terlaksananya kegiatan Pengabdian kepada Masyarakat yang diselenggarakan di Madrasah Aliyah Negeri 1 Kota Tangerang Selatan dengan tema “Pelatihan *Basic Cyber Security* Dan Perlindungan Data Diri”. Dengan ini kami dapat menyimpulkan bahwa :

- Kegiatan PkM ini terlaksana dengan cukup baik, sambutan dari Kepala Sekolah merespon dengan sangat baik terhadap adanya kegiatan ini, serta respon dari peserta didik yang hadir sangat antusias dalam mengikuti seluruh rangkaian kegiatan pelatihan ini.
- Kegiatan PkM kali ini bisa terus berkesinambungan di tahun-tahun selanjutnya. Pasalnya, kegiatan seperti ini dapat memberikan dampak positif terhadap pertumbuhan siswa-siswinya dalam membangun generasi muda yang sadar pada keamanan data, *Cyber Security Awareness*, kreatif, positif dan inovatif.

4.2 Saran

Berdasarkan hasil penyuluhan yang telah dilakukan, diharapkan adanya kegiatan sosialisasi berkelanjutan yang berkaitan dengan ilmu pengetahuan dan teknologi pada tingkat keamanan data yang mendukung dasar-dasar *Cyber Security* sehingga meningkatkan kesadaran akan pentingnya keamanan data pribadi agar tidak disalahgunakan oleh pihak yang tidak bertanggung jawab, juga diharapkan agar kegiatan PKM berikutnya dapat dilakukan dengan tema yang terintegrasi sehingga siswa-siswi memiliki bekal pengetahuan yang mumpuni serta mendapatkan gambaran perkembangan teknologi yang sesuai dengan kebutuhan pasar tenaga kerja professional di bidang *IT Security*.

Demikian saran yang dapat disampaikan, semoga saran tersebut bisa dijadikan sebagai bahan masukan bagi penulis khususnya dan bagi pengguna pada umumnya.

REFERENCES

- Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional*, 10(2), 113-128.
- FaturRohmah, N. (2018). Pelatihan dan Pengembangan Sumber Daya Manusia. *INTIZAM: Jurnal Manajemen Pendidikan Islam*, 3.
- Inda Puspita Sari, A. G. (2021). Pelatihan Penulisan Proposal Kegiatan pada IRMAS di Kecamatan Waras Ilir Kabupaten Musirawas Utara. *Published by LP3MKIL*.
- Kwarto, F., & Angsito, M. (2018). Pengaruh Cyber Crime Terhadap Cyber Security Compliance Di Sektor Keuangan. *Jurnal Akuntansi Bisnis*, 11(2).
- Mochammad Machlul Alamin. (2023). Peningkatan Kualitas SDM Melalui Pelatihan Cyber Security Pada Anggota Polisi Daerah Jawa Timur. *PARTA: Jurnal Pengabdian Kepada Masyarakat*
- Muhammad Hasyim, G. N. (2014). Pelatihan pembuatan proposal kegiatan pada remajadusun ngepuh lor, Desa Banyusidi, Pakis, Magelang, Jawa Tengah. *Jurnal Inovasi dan Kewirausahaan*, 206-210.
- Snell, S., & Bohlander, G. W. (2012). *Managing Human Resources*. Cengage Learning. <https://books.google.co.id/books?id=5WwJAAAAQBAJ>
- Ersya, M. P. (2017). Permasalahan Hukum dalam Menanggulangi Cyber Crime di Indonesia. *Journal of Moral and Civic Education*, 1(1), 50-62.