AMMA : Jurnal Pengabdian Masyarakat
Volume 1, No.12 Januari (2023)
ISSN 2828-6634 (media online)
Hal 1594-1601

Pengenalan *Cyber Security* Sebagai Fundamental Keamanan Data Pada Era Digital

Yuda Samudra[1*], Amin Hidayat[2], Meidy Fajar Wahyu[3]

[1,2,3]Fakultas Ilmu Komputer, Teknik Informatika, Universitas Pamulang, Tangerang Selatan, Indonesia
[1*]dosen02623@unpam.ac.id , [2]dosen02615@unpam.ac.id , [3]dosen02614@unpam.ac.id

Abstrak - 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. 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. Melindungi aset digital merupakan perhatian yang penting bagi perusahaan, karena serangan siber memengaruhi kinerja bisnis dan reputasi. Banyak metode dan teknik yang dapat dilakukan untuk menunjang proses pengarahan kepada para peserta didik dalam memanfaatkan peluang besar dengan adanya dampak dari pekembangan teknologi internet. Salah satu pengenalan *Cyber Security* dan bagaimana cara mengamankan data pribadi pada perangkat gadget yang saat ini para siswa-siswi sudah pandai dalam menggunakan perangkat tersebut, namun tetapi masih minimnya pengetahuan tentang keamanan data. Dengan pengenalan *cyber security* sebagai fundamental keamanan data pada era digital, diharapkan siswa-siswi memiliki kesadaran tentang pentingnya data pribadi agar tidak terjadi penyalahgunaan data oleh orang yanag tidak bertanggung jawab sehingga merugikan berbagai pihak yang datanya disalahgunakan. Maka, Kegiatan Pengabdian Kepada Masyarakat ini bertujuan untuk memberikan pengarahan kepada siswa dan siswi dengan melakukan penyuluhan tatap muka dengan para siswa-siswi untuk memperkenalkan tentang pentingnya keamana data pada era digital dan dukungan pemahaman tentang *cyber security* serta *cyber crime* yang terjadi pada era saat ini. Dalam kegiatan ini berupa materi pelatihan dan praktek pada saat pelatihan berlangsung. Materi pelatihan berisi dasar tentang pengenalan dampak postif terhadap kemajuan teknologi internet, bagiamana penerapan keamanan data, serta implementasi penggunaan e-commerce yang aman untuk pengamanan data pribadi. Pada persiapan pelatihan, Tim pengabdian melakukan uji coba penerapan keamanan data dalam penggunaan e-commerce sebagai bahan yang kemudian akan dibahas pada saat pelaksanaan pelatihan. Pelatihan diberikan dalam bentuk ceramah yang dilanjutkan dengan tanya jawab. Mulai dari pengenalan dampak postif terhadap kemajuan teknologi internet, kemudian akan diajarkan bagaimana cara menerapakan keamanan data pada produk digitalsaat bertransaksi online, sehingga cara mengamankan data tersebut diketahui oleh banyak orang, selanjutnya perserta didik juga akan dibekali praktek cara penggunaan system keamanan pada gadget serta memahami bagaimana alur transaksi yang aman pada website, e-commerce maupun game. Pelatihan dilaksanakan pada ruang Lab komputer Madrasah Aliyah Negeri 1 Kota Tangerang Selatan, sehingga para peserta didik dapat langsung ikut mempraktekan apa yang sedang dipelajari dalam pelatihan ini.

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

Abstract *- Cyber crime is a relatively new crime, which is carried out by people who are experts or who have expertise in the field of computers and information technology. When viewed from the perspective of crime, crime through cyberspace (internet) can have an impact inside and outside the virtual world. The limited space and time in carrying out activities using the internet as a medium makes it difficult for an activity in cyberspace to be detected conventionally. In the case of cyber threats, based on data analysis of the ID-SIRTII (Indonesian Security Incident Response Team On Internet Infrastructure) traffic monitoring system, it was noted that the incidence of cyber attacks in Indonesia has reached one million incidents and will increase every day due to system and application weaknesses that do not exist. is known. Protecting digital assets is an important concern, as cyber attacks affect a company's performance and reputation. Many methods and techniques can be used to support the process of directing students to take advantage of great opportunities with the impact of the development of internet technology. One of the introductions to Cyber Security and how to enter personal data on gadget devices that currently students are good at using these devices, but still lacks knowledge about data security. With the introduction of cyber security as fundamental data security in the digital era, it is hoped that students will have an awareness of the importance of personal data so that data does not occur by irresponsible people so as to harm various parties whose data is misused. So, this Community Service Activity aims to provide direction to students by conducting face-to-face counseling with students to introduce the importance of data security in the digital era and support understanding of cyber security and cyber crimes that occur in the*

current era. This activity is in the form of training materials and practices during the training. The material contains a basic introduction to the impact of training on the advancement of internet technology, how to implement data security, and the application of safe e-commerce usage for personal data security. In preparation for the training, the service team tested the application of data in the use of e-commerce as material which was then discussed during the training. The training was given in the form of a lecture followed by a question and answer session. Starting from the introduction of the impact of post-advancement internet technology, then they will be taught how to apply security data to digital products when transacting online, so that the way the data is known by many people, then students will also be provided with practices on how to use security systems on gadgets and understand how to flow. secure transactions on websites, e-commerce and games. The training was held in the Computer Lab of Madrasah Aliyah Negeri 1, South Tangerang City, so that students could immediately practice what they were learning in this training.

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

1. PENDAHULUAN

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 penyimpan 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 terjangkit program jahat jenis *ransomware* bernama *WannaCry*. *Malware* bermodus menyandera data dan meminta tebusan uang itu telah mengunci sistem dan data pasien di RS Dharmais 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 disandera 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 *web site* 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 menunjukan 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)

Contoh lain adalah pada perkembangan aplikasi web menjadi tantangan tersendiri bagi para pengembangan aplikasi web dalam mengembangkan aspek keamanan. Aplikasi web merupakan platform aplikasi yang cukup rentan terhadap serangan dari peretas. *SQL Injection*, *Phising*, dan *Cross-Site Scripting (XSS)* merupakan beberapa jenis serangan yang dapat menyerang aplikasi berbasis web. Dalam meningkatkan sistem keamanan dari sebuah aplikasi berbasis web maka perlu dilakukan sebuah tahapan pengujian keamanan dari aplikasi berbasis web tersebut. Pengujian keamanan dilakukan dengan melakukan uji teknin-teknik serangan yang mungkin terhadap aplikasi target. Terdapat banyak sumber daya yang ditawarkan untuk melakukan pengujian aplikasi berbasis web. Namun, penggunaan sumber daya tersebut masih yang bersifat manual dan belum terintegrasi (Yudha & Panji, 2018).

Dalam sistem hukum pidana Indonesia, kejahatan siber termasuk ke dalam kategori tindak pidana khusus meskipun dengan unsur yang utamanya dapat dipadankan dengan beberapa pasal-pasal di dalam KUHP tetapi dilakukan dengan cara-cara yang baru *(new design).* Saat ini, Indonesia telah memiliki Undang-Undang No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik yang disahkan pada bulan Maret tahun 2008 dan telah dirubah dengan Undang-Undang No. 19 Tahun 2016 yang disahkan dan diundangkan pada tanggal 25 November 2016, terdapat bentuk-bentuk pengaturan hukum pidana yang baru yang menambah aturan hukum pidana baik secara materiil maupun secara formiil, yang secara asasnya dapat dipakai berdasarkan ketentuan yang terdapat dalam Pasal 103 KUHP dan Pasal 284 ayat (2) KUHAP (Ersya, 2017).

Teknologi yang semakin berkembang saat ini yang seiring dengan kebutuhan manusia akan tekhnologi tersebut mengakibatkan berbagai inovasi dan penemuan baru yang juga semakin berkembang. Hal ini dapat dilihat dari banyaknya penemuan-penemuan berbasis teknologi (*gadget*) seperti *smartphone*, *laptop*, televisi, *air conditioner*, *personal computer (PC)*, gelombang radio, dsb. Namun dibalik semakin maju dan berkembangnya teknologi ini, teknologi tidak hanya memberikan dampak positif bagi masyarakat melainkan juga dampak negatif yang tidak luput dari pemanfaatan teknologi itu sendiri. Salah satu bentuk nyata dari dampak negatif teknologi itu sendiri adalah *Cybercrime. Cybercrime* atau dalam bahasa Indonesia disebut dengan kejahatan dunia maya adalah pelanggaran yang hanya dapat dilakukan menggunakan komputer, jaringan komputer atau bentuk lain dari teknologi komunikasi informasi (McGuire, Mike, & Samantha Dowling, 2013).

Keamanan *cyber* pada hakikatnya merupakan isu dalam studi keamanan yang terbilang masih sangat baru. Isu ini muncul ketika semua aspek kehidupan politik, militer, ekonomi, sosial dan budaya terhubung ke dunia maya. Ancaman cyber yang berpotensi sebagai ancaman adalah *cyber terrorism*, *cyber crime* dan *cyber war*. Asia Tenggara sebagai salah satu kawasan penting di dunia dengan tingkat pertumbuhan ekonomi yang cukup tinggi tidak terlepas dari ancaman tersebut. Penelitian ini bertujuanuntuk membahas strategi seperti apakah yang paling tepat dalam menjaga keamanan *cyber* di kawasan Asia Tenggara (Ramadhan, 2019).

Melindungi aset digital merupakan perhatian yang penting bagi perusahaan, karena serangan siber memengaruhi kinerja bisnis dan reputasi sebuah perusahaan. Tiga konsep dasar keamanan yang penting untuk informasi di internet adalah kerahasiaan (*confidentiality*), integritas (*integrity*),

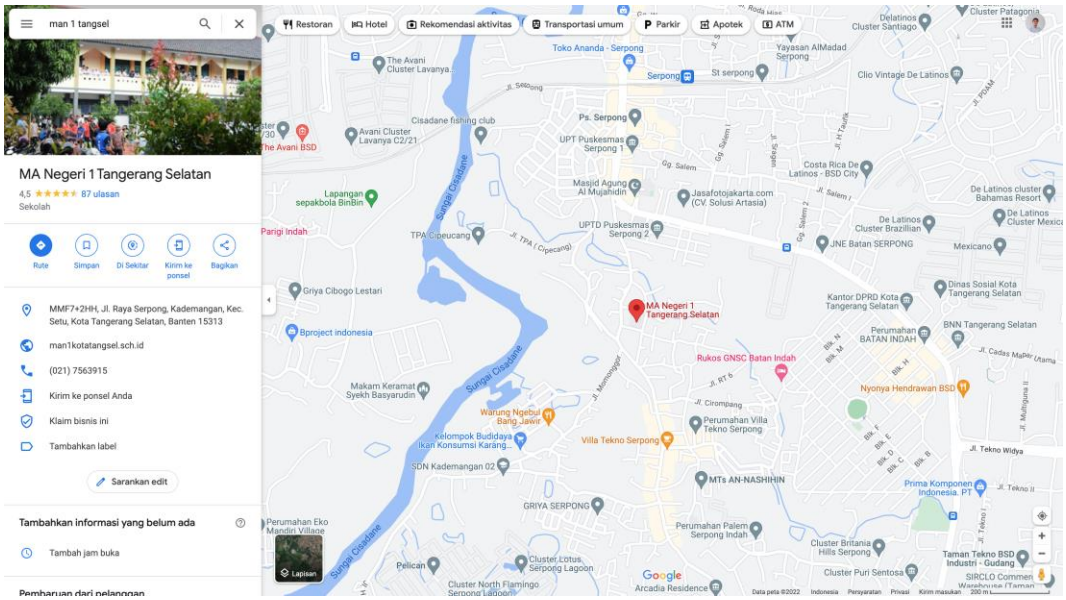
AMMA : Jurnal Pengabdian Masyarakat
Volume 1, No.12 Januari (2023)
ISSN 2828-6634 (media online)
Hal 1594-1601

dan ketersediaan (*availability*). Konsep yang berkaitan dengan orang-orang yang menggunakan informasi itu adalah *authentication*, *authorization*, dan *nonrepudiation.* Keamanan informasi menjadi suatu hal yang mahal pada saat ini, sehingga *ethical hacking* diperlukan untuk menjamin sebuah sistem informasi perusahaan tersebut cukup handal. Dengan begitu dapat menjaga reputasi perusahaan tersebuat di mata pelangannya (Kelrey & Muzaki, 2019).

Hacking secara empiris berpengaruh terhadap *cyber security compliance* di sektor keuangan, *phising* secara empiris berpengaruh terhadap *cyber security compliance* di sektor keuangan, dan *malware* secara empiris berpengaruh terhadap *cyber security compliance* di sektor keuangan (Kwarto & Angsito, 2018).

2. METODE PELAKSANAAN

Metode dalam kegiatan "Pengenalan *Cyber Security* Sebagai Fundamental Keamanan Data Pada Era Digital" 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 pelaksaanan PKM dilapangan dengan langkah-langkah sebagai berikut:

1. Koordinasi dengan pihak Madrasah Aliyah Negeri 1 Tangerang Selatan.
2. Persiapan Penyeluhan dan Pelatihan.

AMMA : Jurnal Pengabdian Masyarakat
Volume 1, No.12 Januari (2023)
ISSN 2828-6634 (media online)
Hal 1594-1601

3. Penyuluhan Materi *Cyber Security*
4. Pelatihan *Cyber Security* Dengan *Biometrics Access*
5. Diskusi dan Sesi Tanya Jawab
6. 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	Dimas Wahyu Hidayat
2	09:10 – 09:30	Sambutan - Kepala Sekolah - Ketua PKM	 - Drs.. H. Ridwan Fahmi Lubis - Yuda Samudra, M.Kom.
3	09:30 – 10:30	Pemaparan Materi dan Praktik - *Cyber Security* - Standar Keamanan - Keamanan Data Pribadi - *Biometrics Access*	 - Amin Hidayat, M.Kom. - Meidy Fajar Wahyu, S.T., M.Kom.
4	10:30 – 11:00	Tanya Jawab	Dimas Wahyu Hidayat
5	11:00 – 11:15	Penyerahan Cindramata	Yuda Samudra, M.Kom.
6	11:15 – 11:30	Penutup	Dimas Wahyu Hidayat
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.*

AMMA : Jurnal Pengabdian Masyarakat
Volume 1, No.12 Januari (2023)
ISSN 2828-6634 (media online)
Hal 1594-1601

Gambar 3.1 Persiapan Penyampaian Materi

Persiapan penyampaian dilakukan oleh tim pengabdi 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 Yuda Samudra, S.Kom., M.Kom., Amin Hidayat, S.Kom., M.Kom. dan Meidy Fajar Wahyu, S.T., M.Kom. dalam bidang *Cyber Security* serta penerapan pada era digital saat ini

Gambar 3.3 Peserta PKM

AMMA : Jurnal Pengabdian Masyarakat
Volume 1, No.12 Januari (2023)
ISSN 2828-6634 (media online)
Hal 1594-1601

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

1. *Layer 1 : Data Defense*
   Data dapat dilindungi melalui penggunaan Daftar kontrol akses (ACLs) pada file dan folder, enkripsi dan strategi backup and restore yang efektif.

2. *Layer 2 : Application Defense*
   Lapisan keamanan aplikasi mengontrol akses ke informasi sensitif. Ini termasuk server web, *e- commerce*, layanan internet dan suara. Aplikasi dapat dilindungi melalui penggunaan otentikasi, otorisasi dan kebijakan *password*.
3. *Layer 3 : Host Defence*
   Host merupakan komputer yang menjalankan aplikasi klien dan server.
4. *Layer 4 : Network Defense*
   Segmen jaringan terdiri dari dua atau lebih perangkat yang berkomunikasi satu sama lain pada bagian jaringan fisik atau logis yang sama. Jika segmennya logis, mereka disebut sebagai virtual local area networks (VLAN).
5. *Layer 5 : Perimeter Defense*
   Jaringan ditambahkan antara jaringan yang dilindungi dan jaringan eksternal untuk memberikan lapisan keamanan tambahan.
6. *Layer 6 : Physical Defense*
   Akses fisik ke komputer akan memberi pencuri data kesempatan untuk menonaktifkan kata sandi.
7. *Layer 7 : Policies, Procedures, dan Awareness*
   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 "Pengenalan *Cyber Security* Sebagai Fundamental Keamanan Data Pada Era Digital". 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.

Ersya, M. P. (2017). Permasalahan Hukum dalam Menanggulangi Cyber Crime di Indonesia. *Journal of Moral and Civic Education*, *1*(1), 50-62.

Kelrey, A. R., & Muzaki, A. (2019). Pengaruh Ethical Hacking Bagi Keamanan Data Perusahaan. *Cyber Security dan Forensik Digital*, *2*(2), 77-81.

Kwarto, F., & Angsito, M. (2018). Pengaruh Cyber Crime Terhadap Cyber Security Compliance Di Sektor Keuangan. *Jurnal Akuntansi Bisnis*, *11*(2).

McGuire, Mike, and Samantha Dowling, (2013) Cyber crime: A review of the evidence Chapter 4: Improving the cyber crime evidence base

Novianto, F. (2020). EVALUATION OF E-GOVERNMENT INFORMATION SECURITY USING THE DEFENSE IN DEPTH MODEL. *Cyber Security dan Forensik Digital*, *3*(1), 14-19.

Ramadhan, I. (2019). Strategi Keamanan Cyber Security di Kawasan Asia Tenggara. *Jurnal Asia Pacific Studies*, *3*(2), 181-192.

Sama, H., Licen, L., Saragi, J. S. D., Erline, M., Kelvin, K., Hartanto, Y., ... & Devalia, M. (2021). Studi Komparasi Framework NIST dan ISO 27001 sebagai Standar Audit dengan Metode Deskriptif Studi Pustaka. *Rabit: Jurnal Teknologi Dan Sistem Informasi Univrab*, *6*(2), 116-121.

Yudha, F., & Panji, A. M. (2018). Perancangan aplikasi pengujian celah keamanan pada aplikasi berbasis web. *Cyber Security Dan Forensik Digital*, *1*(1), 1-6.