

## SOSIALISASI PENGENALAN RANSOMWARE SEBAGAI PENINGKATAN KEAMANAN DATA SISWA DI SMK PANTI KARYA

Ade Napila<sup>1</sup>, Andrian Hidayat<sup>2</sup>

<sup>1,2</sup> Fakultas Ilmu Komputer, Universitas Pamulang, Jl. Surya Kencana No.1, Pamulang Bar., Kec. Pamulang, Kota Tangerang Selatan, Banten, Indonesia, 15417  
e-mail: <sup>1</sup> dosen02667@unpam.ac.id

### Abstract

*In the digital era, data security is a major concern, especially in the education sector which stores sensitive information about students and institutions. One of the biggest threats to data security is ransomware attacks, a type of malware that encrypts the victim's data and demands a ransom payment for recovery. These attacks have become a serious threat to schools and educational institutions due to weak security systems and lack of user awareness of cyber threats. This service aims to introduce the concept of ransomware, analyze its impact on student data security, and identify effective steps to prevent such attacks in educational environments. The socialization methods used include literature studies, analysis of ransomware attack cases on educational institutions, and prevention strategies that can be implemented by schools and educators. The results of the study show that ransomware can cause data loss, operational disruption, and significant financial losses for educational institutions. Therefore, increasing awareness and education about cybersecurity is a very important step. In addition, implementing preventive measures such as regular data backups, using up-to-date security software, and training educators and students on good digital security practices can help reduce the risk of ransomware attacks. With this service, it is hoped that SMK Panti Karya will be more prepared in facing ransomware threats and be able to implement better security strategies to protect student data.*

*Keywords: Ransomware, Internet, Cyber Attack, SMK Panti Karya. Data Security.*

### Abstrak

Dalam era digital, keamanan data menjadi perhatian utama, terutama di sektor pendidikan yang menyimpan informasi sensitif mengenai siswa dan institusi. Salah satu ancaman terbesar terhadap keamanan data adalah serangan *ransomware*, yaitu jenis *malware* yang mengenkripsi data korban dan menuntut pembayaran tebusan untuk pemulihan. Serangan ini telah menjadi ancaman serius bagi sekolah dan institusi pendidikan karena lemahnya sistem keamanan serta kurangnya kesadaran pengguna terhadap ancaman siber. Pengabdian ini bertujuan untuk memperkenalkan konsep *ransomware*, menganalisis dampaknya terhadap keamanan data siswa, serta mengidentifikasi langkah-langkah efektif untuk mencegah serangan tersebut di lingkungan pendidikan. Metode sosialisasi yang digunakan meliputi studi literatur, analisis kasus serangan ransomware pada institusi pendidikan, serta strategi pencegahan yang dapat diterapkan oleh pihak sekolah dan tenaga pendidik. Hasil penelitian menunjukkan bahwa *ransomware* dapat menyebabkan kehilangan data, gangguan operasional, serta kerugian finansial yang signifikan bagi institusi pendidikan. Oleh karena itu, peningkatan kesadaran dan edukasi mengenai keamanan siber menjadi langkah yang sangat penting. Selain itu, implementasi langkah-langkah pencegahan seperti backup data secara berkala, penggunaan perangkat lunak keamanan yang mutakhir, serta pelatihan kepada tenaga pendidik dan siswa mengenai praktik keamanan digital yang baik dapat membantu mengurangi risiko serangan ransomware. Dengan adanya pengabdian ini, diharapkan SMK Panti Karya lebih siap dalam menghadapi ancaman ransomware serta mampu menerapkan strategi keamanan yang lebih baik untuk melindungi data siswa.

Kata kunci : *Ransomware*, Internet, Serangan Siber, SMK Panti Karya. Keamanan Data.

## 1. PENDAHULUAN

Dalam era digital yang semakin berkembang, data menjadi aset yang sangat berharga, terutama dalam lingkungan pendidikan. Sekolah dan institusi pendidikan menyimpan berbagai data penting seperti data pribadi siswa, catatan akademik, serta informasi administratif lainnya. Namun, dengan meningkatnya ketergantungan pada teknologi digital, ancaman keamanan siber juga semakin meningkat, salah satunya adalah serangan *ransomware*. (Whitman & Mattord., 2021).

*Ransomware* merupakan jenis *malware* yang mengenkripsi data korban dan menuntut pembayaran tebusan agar data dapat dipulihkan. Menurut Stallings & Brown (2018) dalam bukunya yang berjudul *Computer Security: Principles and Practice*, *ransomware* adalah salah satu bentuk serangan siber yang paling berkembang pesat dalam beberapa tahun terakhir, dengan teknik yang semakin canggih untuk mengeksploitasi kelemahan sistem. Serangan ini sering menargetkan institusi yang memiliki sistem keamanan lemah, termasuk sekolah. Kurangnya kesadaran dan pemahaman tentang *ransomware* di kalangan tenaga pendidik dan siswa dapat meningkatkan risiko serangan ini.

Menurut laporan dari Symantec (2020), sektor pendidikan menjadi salah satu target utama serangan *ransomware*, mengingat banyaknya data sensitif yang tersimpan dalam sistem sekolah dan kurangnya anggaran untuk keamanan siber. Hal ini diperkuat oleh pendapat Whitman & Mattord (2021) yang menyatakan bahwa keamanan informasi di institusi pendidikan sering kali diabaikan dibandingkan dengan sektor bisnis, sehingga meningkatkan kerentanannya terhadap serangan siber. Oleh karena itu, penting untuk meningkatkan pemahaman mengenai *ransomware* agar dapat mencegah potensi ancaman terhadap keamanan data siswa. Serangan *ransomware* pada institusi pendidikan tidak hanya menyebabkan kehilangan data tetapi juga dapat mengganggu proses belajar mengajar. Menurut Verizon (2021) dalam laporan tahunan *Data Breach Investigations Report*, lebih dari 30% serangan siber yang terjadi di sektor pendidikan melibatkan *ransomware*, yang berdampak pada kelangsungan operasional institusi tersebut. Hal ini menunjukkan bahwa perlindungan terhadap serangan siber harus menjadi prioritas utama bagi sekolah dan universitas.

Selain itu, serangan *ransomware* sering kali menargetkan institusi dengan sistem keamanan yang lemah dan sumber daya yang terbatas dalam menangani ancaman siber. Menurut laporan dari Kaspersky (2022), kurangnya kesadaran dan pelatihan mengenai keamanan siber di kalangan staf dan siswa menjadi faktor utama yang meningkatkan risiko serangan. Oleh karena itu, penting bagi sekolah untuk tidak hanya meningkatkan infrastruktur keamanan tetapi juga memberikan edukasi yang memadai kepada seluruh pemangku kepentingan. Upaya pencegahan *ransomware* tidak hanya melibatkan peningkatan teknologi keamanan, tetapi juga edukasi kepada seluruh pemangku kepentingan di institusi pendidikan. Schneier (2019) menyebutkan bahwa kesadaran pengguna merupakan lapisan pertahanan utama dalam keamanan siber. Oleh karena itu, kegiatan pengabdian masyarakat ini bertujuan untuk mengenalkan konsep *ransomware* serta langkah-langkah pencegahan yang dapat diterapkan guna meningkatkan keamanan data siswa.

SMK Panti Karya merupakan salah satu instansi pendidikan islam terpadu yang murid-muridnya adalah remaja yang pasti mengenal internet. Sejauh ini belum pernah diadakan sosialisasi terkait *Ransomware* yang pada dasarnya berperan sebagai ilmu edukasi agar murid-murid mengenal konsep serta cara pencegahan *Ransomware* di SMK Panti Karya.

Dengan demikian, di dalam kegiatan Pengabdian Kepada Masyarakat ini, kami akan melakukan sosialisasi terkait pengenalan, konsep dan bimbingan kepada murid-murid SMK Panti Karya agar menjadi sebuah pembelajaran terkait *Ransomware* untuk menghindari infeksi dan eksploitasi *Ransomware* yang bertebaran di internet.

## 2. METODE

Metode kegiatan Pengabdian Kepada Masyarakat ini berupa sosialisasi terkait *Ransomware* secara efektif di lingkungan SMK Panti Karya sebagai bekal ilmu tambahan bagi para siswa baik saat masih berada di lingkungan sekolah maupun jika telah kembali ke masyarakat atau keluarga masing-masing. Materi yang disampaikan berupa pengenalan apa itu *Ransomware*, cara kerja dan perkembangannya saat ini, pencegahan infeksi *Ransomware*, serta contoh dan dampaknya di zaman modern seperti saat ini. Setelah kegiatan penyampaian materi selesai, adapun kegiatan yang

dilakukan selanjutnya yaitu dilanjutkan dengan sesi tanya jawab. Berikut adalah tahapan – tahapan yang dilakukan atau dilaksanakan pada saat pelaksanaan Pengabdian Kepada Masyarakat di SMK Panti Karya:

a. Tahap Persiapan

Tahap persiapan kegiatan Pengabdian Kepada Masyarakat yang dilakukan pada kegiatan ini diantaranya meliputi:

1) Kunjungan Awal

Pada tahap pertama ini dilakukan kunjungan ke lokasi SMK Panti Karya yang berlokasi di jalan Kamboja Desa Rawa Kalong RT. 02/06 Kecamatan Gunung Sindur Kabupaten Bogor Provinsi Jawa Barat. Kunjungan ini dilakukan untuk bertukar informasi antara Kepala Yayasan SMK Panti Karya dengan pelaku kegiatan Pengabdian Kepada Masyarakat untuk menentukan hal-hal yang berkaitan dengan kegiatan Pengabdian Kepada Masyarakat yang akan dilakukan seperti tempat kegiatan, waktu kegiatan, jumlah peserta, serta sarana dan prasarana yang dibutuhkan.

2) Menentukan Tempat Kegiatan

Langkah selanjutnya adalah menentukan tempat yang akan diadakannya kegiatan Pengabdian Kepada Masyarakat tersebut. Lalu diputuskan tempat yang digunakan untuk menyampaikan materi penyuluhan atau sosialisasi Langkah selanjutnya adalah menentukan tempat yang akan diadakannya kegiatan Pengabdian Kepada Masyarakat tersebut. Tempat yang digunakan adalah untuk menyampaikan materi penyuluhan atau sosialisasi mengenai *Ransomware* di SMK Panti Karya.

3) Menentukan Waktu Kegiatan dan Penyusunan Materi

Langkah berikutnya adalah menentukan waktu pelaksanaan kegiatan Pengabdian Kepada Masyarakat, dimana untuk waktunya dilakukan selama 4 jam dalam 1x pertemuan yang meliputi penyusunan materi yang berkaitan dengan sosialisasi terkait *Ransomware*.

b. Tahap Penyuluhan

Pada saat pelaksanaan kegiatan Pengabdian Kepada Masyarakat tersebut digunakan beberapa metode penyuluhan diantaranya sebagai berikut:

1) Metode Sosialisasi

Metode sosialisasi dipilih untuk memberikan penjelasan tentang sosialisasi terkait *Ransomware*, meliputi pengertian, perkembangan, serta contoh dan dampaknya di zaman modern ini.

2) Metode Simulasi

Metode simulasi ini diberikan kepada para peserta sosialisasi dengan memberikan contoh umum tentang studi kasus sosialisasi terkait *Ransomware*.

3) Metode Tanya Jawab

Metode tanya jawab sangat penting bagi para peserta sosialisasi. Metode ini memungkinkan para peserta dalam hal ini para murid-murid dan dewan guru dalam menggali pengetahuan sebanyak-banyaknya tentang sosialisasi terkait *Ransomware*.

### 3. HASIL DAN PEMBAHASAN

Hasil dari kegiatan pengabdian kepada masyarakat ini adalah berupa pengetahuan yang diperoleh para peserta kegiatan dalam hal ini para murid-murid SMK Panti Karya mengenai *Ransomware*, yang bisa menjadi tambahan pengetahuan sehingga para santri bisa memiliki sifat berhati-hati dan bertindak preventif terhadap data-data pribadi dan data-data di lingkungan sekolah agar tidak terinfeksi *Ransomware* dan dimanfaatkan oleh orang-orang yang tidak bertanggung jawab. Juga bagi para murid-murid bisa mensosialisasikan hasil ilmu yang didapat kepada masyarakat baik di lingkungan sekolah maupun lingkungan rumah. Berikut foto sosialisasi



dari kegiatan ini dapat dilihat pada gambar 1.

Gambar 1. Sosilasi Kegiatan Pkm

Pembahasan ruang lingkup pada kegiatan pengabdian kepada masyarakat kali ini mencakup pemahaman mengenai *Ransomware*. Peserta cukup antusias atas materi yang dipaparkan oleh tim pengabdian dari Universitas Pamulang mengenai contoh studi kasus, contoh infeksi file *Ransomware* karena isu teknologi begitu pesat saat ini perkembangannya serta sesuai dengan kebutuhan pengetahuan. Adapun materi yang dipaparkan oleh dosen Fakultas Ilmu Komputer Universitas Pamulang diantaranya, mengenai pentingnya data

pribadi, ancaman-ancaman di internet, contoh studi kasus *Ransomware* dan cara pencegahannya, yang dibawakan oleh Ade Napila S.Kom., M.Kom. serta Andrian Hidayat, S.Kom., M.Kom. Untuk kegiatan pembahasan materi diatas dirangkum dalam table kegiatan dibawah ini.

WAKTU	KEGIATAN	PIC
09:00-09:05	Pembukaan	Andrian Hidayat, M. Kom
09:10-09:15	Sambutan Panitia	Andrian Hidayat, M. Kom
09:15-09:25	Sambutan Pihak Pondok Pesantren Nafidatunnajah	Ust. Anwar
09:25-09:50	Materi	Ade Napila, M.Kom
09:50-10:00	Tanya Jawab	Dosen & Peserta
10:00-10:05	Tanda tangan IA	Suhardi, S.Ag. dan Andrian Hidayat, M. Kom
10:10-10:20	Penutup dan Doa	Ust. Anwar

Tabel.I Susunan Acara

#### 4. KESIMPULAN

Kesimpulan dari hasil kegiatan pengabdian kepada masyarakat ini, dapat disimpulkan beberapa hal sesuai tujuan dari PKM di SMK Panti Karya diharapkan dengan semakin pesatnya perkembangan teknologi dan informasi, para peserta memiliki kemampuan lebih yang dibutuhkan yang menunjang dan sesuai dengan perkembangan zaman mengenai Tindakan preventif dalam menjaga data-data pribadi dan

data-data sekolah (umum) di tengah pesatnya teknologi dan informasi.

Adapun beberapa saran yang dapat disampaikan untuk pengembangan dari kegiatan pengabdian kepada masyarakat ini antara lain:

1. Kegiatan pengabdian kepada masyarakat ini bisa dijadikan acuan untuk mensosialisasikan Tindakan preventif di instansi lainnya.

2. Kegiatan pengabdian kepada masyarakat ini berfokus simulasi dan tata cara Tindakan preventif dalam menjaga data pribadi, dan bisa dikembangkan dengan menambahkan materi lainnya seperti keamanan computer dalam bersocial masyarakat, keamanan internet dan lainnya.

#### DAFTAR PUSTAKA

- [1] Kaspersky. (2022). Ransomware and Cyber Threats in Education. Kaspersky Lab.
- [2] Brynjolfsson, A. M. (2020). *The Second Machine Age*.
- [3] National Institute of Standards and Technology (NIST). (2020). Framework for Improving Critical Infrastructure Cybersecurity. U.S. Department of Commerce.
- [4] Schneier, B. (2019). *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World*. W.W. Norton & Company.
- [5] Stallings, W., & Brown, L. (2018). *Computer Security: Principles and Practice*. Pearson Education.
- [6] Symantec. (2020). Internet Security Threat Report. Symantec Corporation.
- [7] Verizon. (2021). Data Breach Investigations Report. Verizon Enterprise.
- [7] Whitman, M. E., & Mattord, H. J. (2021). *Principles of Information Security*. Cengage Learning.