AbdiMU
Jurnal AbdiMU : Pengabdian Kepada Masyarakat
Volume 5 No. 1 | Mei 2025 : 37-41
DOI: 10.32627
https://jurnal.masoemuniversity.ac.id/index.php/abdimu/index
e-ISSN: 2797-3468

Sosialisasi Keamanan Data dan Informasi Era Digital di MA Cimalaka Kabupaten Sumedang

Ridwan Zulkifli
Informatika, Universitas Ma`soem, Indonesia
ridwan.zulkifli12@gmail.com

Received : Feb' 2024 Revised : Mar' 2025 Accepted : May' 2025 Published : May' 2025

ABSTRACT
The digital era has brought fundamental changes in the management, storage, and transmission of data and information across various sectors, including government, industry, education, and daily life. The rapid development of information technology, such as cloud computing, the Internet of Things (IoT), and big data has enhanced efficiency and ease in data processing. However, on the other hand, this progress also opens gaps to various security threats that are becoming increasingly complex and sophisticated. Cyber attacks such as hacking, data theft, DDoS (Distributed Denial of Service) attacks, phishing, malware, and ransomware have become a serious challenge in maintaining the confidentiality, integrity, and availability of data and information. This research aims to provide comprehensive knowledge about various aspects of data and information security in the digital era, including protection techniques used to secure data from both internal and external threats. This activity uses the Participatory Action Research (PAR) method, which was conducted in MA Cimalaka, Sumedang Regency. The results indicate that participants have understood the importance of data security in facing various challenges in the digital era.

***Keywords** : Access; Data; Information; Risk; Security.*

ABSTRAK
Era digital telah membawa perubahan mendasar dalam pengelolaan, penyimpanan, dan transmisi data dan informasi di berbagai sektor, termasuk pemerintahan, industri, pendidikan, dan kehidupan sehari-hari. Perkembangan teknologi informasi yang pesat, seperti komputasi awan, *Internet of Things* (IoT), dan big data telah meningkatkan efisiensi dan kemudahan dalam pengolahan data. Namun, di sisi lain, kemajuan ini juga membuka celah terhadap berbagai ancaman keamanan yang semakin kompleks dan canggih. Serangan siber seperti peretasan (*hacking*), pencurian data, serangan DDoS (*Distributed Denial of Service*), *phishing, malware*, dan *ransomware* menjadi tantangan serius dalam menjaga kerahasiaan, integritas, dan ketersediaan data dan informasi. Penelitian ini bertujuan untuk memberikan pengetahuan secara komprehensif tentang berbagai aspek keamanan data dan informasi di era digital, termasuk teknik perlindungan yang digunakan untuk mengamankan data dari ancaman internal maupun eksternal. Kegiatan ini menggunakan metode *Participatory Action Research* (PAR), yang dilaksanakan di MA Cimalaka Kabupaten Sumedang. Hasil kegiatan menunjukkan bahwa peserta telah memahami pentingnya keamanan data dalam menghadapi berbagai tantangan di era digital.

Kata Kunci : Akses; Data; Informasi; Kemanan; Risiko.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi (TIK) yang pesat telah membawa perubahan mendasar dalam berbagai aspek kehidupan manusia. Era

digital ditandai dengan masifnya penggunaan teknologi dalam pengelolaan, penyimpanan, dan transmisi data, baik di sektor publik maupun swasta. Dalam konteks bisnis, data telah menjadi aset strategis yang bernilai tinggi. Perusahaan dalam hal ini MA Cimalaka yang memiliki data-data yang berkaitan dengan data guru, siswa, nilai dan data-data penting lainnya yang digunakan untuk kepentingan perusahaan atau organisai, pengambilan keputusan, hingga personalisasi layanan bagi masyarakat. Namun, di balik berbagai manfaat yang ditawarkan oleh era digital, muncul tantangan besar terkait keamanan data dan informasi.

Ancaman siber semakin meningkat, baik dalam hal jumlah, kompleksitas, maupun dampaknya. Serangan siber seperti peretasan (*hacking*), pencurian data (*data breach*), serangan *ransomware, malware, phishing*, dan *Distributed Denial of Service* (DDoS) telah menjadi permasalahan serius bagi organisasi dan individu. Serangan tersebut dapat menyebabkan kerugian finansial yang besar, kerusakan reputasi, gangguan operasional, hingga pelanggaran hukum terkait privasi dan perlindungan data. Selain ancaman eksternal dari peretas dan kelompok kriminal siber, ancaman internal (*insider threat*) juga menjadi tantangan yang signifikan. Kelalaian karyawan, penggunaan perangkat pribadi (BYOD) yang tidak terkontrol, serta penyalahgunaan hak akses oleh pihak internal dapat membuka celah bagi pelanggaran keamanan data. Fenomena ini semakin diperburuk dengan meningkatnya penggunaan jaringan nirkabel publik yang rentan terhadap penyadapan (*eavesdropping)* dan serangan *man-in-the-middle* (MITM).

Seiring dengan meningkatnya ancaman siber, upaya untuk memperkuat keamanan data dan informasi menjadi kebutuhan mendesak. Peran pengguna juga menjadi faktor krusial dalam menjaga keamanan data dan informasi. Rendahnya kesadaran pengguna terhadap risiko keamanan, seperti penggunaan kata sandi yang lemah, mengunduh file dari sumber yang tidak tepercaya, atau tertipu oleh email phishing, menjadi celah yang sering dimanfaatkan oleh peretas. Oleh karena itu, pendidikan dan pelatihan kesadaran keamanan siber (*cybersecurity awareness training*) perlu ditingkatkan untuk membangun budaya keamanan di tingkat individu dan organisasi.

Penelitian ini bertujuan untuk memberikan alih pengetahuan tentang pentingnya data dan keamanan data, memberikan alih pengetahuan tentang langkah-langkah pencegahan serangan yang ditimbulkan oleh internal, memberikan edukasi terhadap siswa/siswa MA cimalaka agar bijak menggunakan media sosial dan data pribadi. Dengan memahami tantangan dan solusi yang ada, diharapkan penelitian ini dapat memberikan kontribusi dalam memberikan kesadaran sejak dini terhadap siswa/siswi untuk lebih bijak menggunakan media sosial dan data pribadi serta memberikan alih pengetahuan terdapat guru dan tenaga pendidik untuk memberikan pengetahuan dan langkah-langkah pencegahan serangan baik dari internal atau external. Selain itu, dapat menjadi acuan awal bagi organisasi dan individu dalam merancang strategi perlindungan data yang efektif, guna meningkatkan kepercayaan dan kelancaran operasional di era digital.

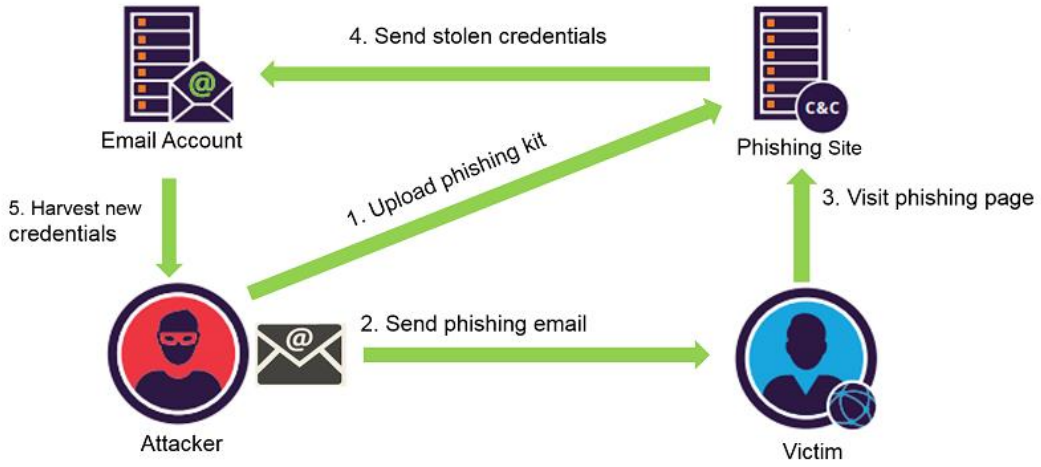
METODE

Kegiatan ini menggunakan metode *Participatory Action Research* (PAR) yang diselenggarakan di MA Cimalaka Kabupaten Sumedang pada tanggal 22 Juli 2024. Kegiatan ini menggunakan metode presentasi yang memiliki pendekatan efektif dalam penyelenggaraan seminar karena memungkinkan narasumber untuk menyampaikan materi secara terstruktur dan sistematis kepada peserta. Dalam konteks seminar "Keamanan Data dan Informasi Era Digital," metode presentasi dapat diimplementasikan dengan memperhatikan beberapa aspek utama, yaitu persiapan materi, pengaturan teknis, pelaksanaan presentasi, interaksi dengan peserta.

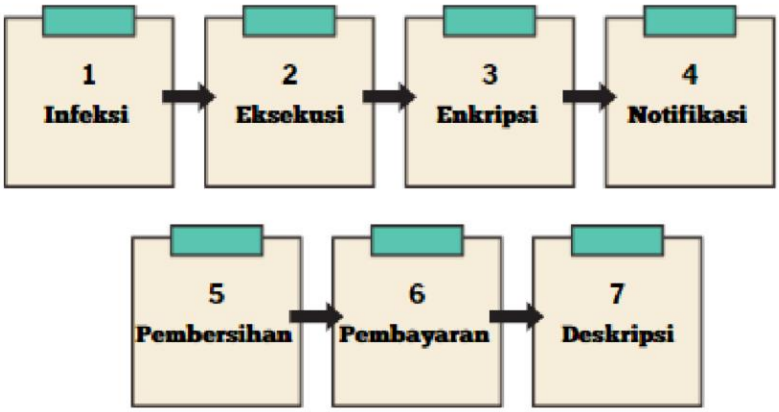
HASIL DAN PEMBAHASAN

Setelah pelaksanaan seminar "Keamanan Data dan Informasi Era Digital," beberapa hasil signifikan berhasil dicapai, baik dari segi pemahaman peserta, partisipasi aktif, maupun umpan balik yang diperoleh. Hasil ini mencerminkan efektivitas metode yang diterapkan dalam meningkatkan kesadaran dan pengetahuan peserta terkait isu keamanan data.

Alhamdulillah, 85% peserta menyatakan bahwa mereka mendapatkan wawasan baru tentang teknik pengamanan data dan strategi menghadapi ancaman siber. Tingkat partisipasi aktif selama sesi diskusi dan tanya jawab mencapai 78% dari total peserta. Sebanyak 92% peserta menyatakan bahwa sesi diskusi panel sangat bermanfaat dalam memperkaya pemahaman, 93% peserta merasa bahwa materi seminar sangat relevan dengan kehidupan keseharian dan lingkungan kerja, 88% peserta menilai bahwa narasumber mampu menyampaikan materi dengan jelas dan sistematis, dan 90% peserta menyatakan bahwa penyampaian materi melalui kombinasi presentasi dan diskusi panel sangat efektif dalam meningkatkan pemahaman. Kesimpulannya sebanyak 95% peserta menyatakan bahwa mereka puas dengan keseluruhan pelaksanaan seminar. Berikut adalah skema serangan phising.



Gambar 1. Skema Serangan Phising



Gambar 2. Skema Serangan Ransome

Gambar 3. Penyampaian Materi

PENUTUP

Selama pelaksanaan seminar, peserta telah mendapatkan pemahaman yang lebih mendalam tentang pentingnya keamanan data dalam menghadapi berbagai tantangan di era digital. Materi yang disampaikan mencakup konsep dasar keamanan data, jenis ancaman siber, teknik perlindungan data, serta peran regulasi dan teknologi dalam memperkuat sistem keamanan. Partisipasi aktif dari peserta dalam sesi diskusi dan tanya jawab mencerminkan antusiasme yang tinggi dan ketertarikan peserta terhadap topik ini. penyampaian materi telah berjalan efektif.

DAFTAR PUSTAKA

[1] Sarno, R,. & Iffano, I, Sistem Manajemen Keamanan Informasi, Surabaya: Itspress, 2009.

[2] Syafrizal, M, in *ISO 17799 : Standar Sistem Manajemen Keamanan Informasi*,

Yogyakarta, Seminar Nasional Teknologi, 2007.
[3] Tim Direktorat Keamanan Informasi, Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik, Jakarta: Kominfo, 2011.
[4] Hidayat, M. N, "Kajian Tata Kelola Keamanan Informasi Berdasarkan Information Security Management System (ISMS) ISO 27001:2005 untuk Outsourcing Teknologi Informasi Pada PT. Kereta Api Indonesia (Persero)," Program Studi Magister Teknologi Informasi Fasilkom UI, Jakarta, 2011.
[5] Mufadhol, "Kerahasiaan Dan Keutuhan Keamanan Data Dalam Menjaga Integritas Dan Keberadaan Informasi Data," *Jurnal Transformatika,* vol. VI, no. 2, p. 80, 2009.
[6] Whitman, M.E., & Mattord, H.J, Management of Information Security, Third Edition, Boston: Course Technology, 2010.
[7] ISACA, in *Certified Information Security Manager : Review Manual 200*, USA, ISACA, 2011,
[8] Justanieah, M, Information Security Management System an ISO 27001 Introduction, Jeddah: ISACA, 2009.
[9] BSI Group, "Transition Guide - Moving from ISO/IEC 27001:2005 to ISO/IEC 27001:2013," BSI Group, United Kingdom, 2014.