E-DIMAS: Jurnal Pengabdian kepada Masyarakat, 11(3), 267-273
ISSN 2087-3565 (Print) dan ISSN 2528-5041 (Online)
Available Online at http://journal.upgris.ac.id/index.php/e-dimas

Studi Mengenai Kejahatan dan Keamanan Internet bagi Guru dan Siswa SMK Muhammadiyah Bulakamba

Ginanjar Wiro Sasmito[1], M. Nishom[2], Dega Surono Wibowo[3]
[1,2,3]Program Studi D IV Teknik Informatika Politeknik Harapan Bersama
[1]anjar.dosen@gmail.com

Received: 5 Mei 2019; Revised: 14 Agustus 2020; Accepted: 22 Agustus 2020

Abstract

SMK Muhammadiyah Bulakamba is one of the vocational high schools in Bulakamba, Brebes district. The results of the survey conducted, that almost all teachers, employees, and students (99%) use the internet for learning, social activities, hobbies and other purposes at school and outside school. With maximum internet usage, the potential for internet crime is very high. Internet crime is very important to be known by its users, as well as for teachers, employees, and students of SMK Muhammadiyah Bulakamba. Because the internet crime can cause fatal consequences, such as: data loss, account forgery, data destruction and others. Therefore need a learning for teachers and students of SMK Muhammadiyah Bulakamba regarding internet crime and security. The method implemented is by giving presentations, discussions, training and mentoring. Based on the activities that have been carried out, the results obtained are knowledge, understanding, competence of teachers and students of SMK Muhammadiyah Bulakamba regarding increasing about crime and internet security.

Keywords: *crime; security; internet; SMK Muhammadiyah Bulakamba.*

Abstrak

SMK Muhammadiyah Bulakamba merupakan sekolah menengah kejuruan yang ada di wilayah kecamatan Bulakamba, kabupaten Brebes. Hasil survei yang dilakukan, bahwa hampir semua guru, karyawan, dan siswa (99%) menggunakan internet untuk keperluan pembelajaran, kegiatan sosial, hobi dan lainnya pada saat di dalam maupun di luar sekolah. Dengan penggunaan internet yang maksimal maka potensi terhadap kejahatan internet juga sangat tinggi. Kejahatan internet sangat penting diketahui oleh penggunanya, demikian pula bagi guru, karyawan, dan siswa SMK Muhammadiyah Bulakamba. Ini dikarenakan kejahatan internet dapat menyebabkan akibat yang fatal, seperti: hilangnya data, pemalsuan akun, perusakan data dan lainnya. Oleh karena itu dibutuhkan sebuah pembelajaran bagi guru dan siswa SMK Muhammadiyah Bulakamba mengenai kejahatan dan keamanan internet. Metode yang dilaksanakan yakni dengan memberikan presentasi, diskusi, pelatihan dan pendampingan. Berdasarkan kegiatan yang telah dilaksanakan, maka hasil yang didapatkan adalah pengetahuan, pemahaman, kompetensi guru dan siswa SMK Muhammadiyah Bulakamba mengenai kejahatan dan keamanan internet semakin meningkat.

Kata Kunci: kejahatan; keamanan; internet; SMK Muhammadiyah Bulakamba.

A. PENDAHULUAN

SMK Muhammadiyah Bulakamba merupakan sekolah menengah kejuruan yang ada di wilayah kecamatan Bulakamba, kabupaten Brebes dengan program keahlian yaitu: Teknik Kendaraan Ringan, Teknik Sepeda Motor, Teknik Pengelasan dan Multimedia. SMK Muhammadiyah Bulakamba berdiri di atas lahan ± 8000 m^2, berlokasi di Jl. Raya Bulakamba No. 30 Brebes dengan fasilitas penunjang yang cukup memadai untuk kegiatan belajar mengajar, termasuk fasilitas Teknologi Informasi digunakan dalam membantu pekerjaan mengenai informasi atau yang berhubungan dengan pemrosesan informasi (Kadir, 2005). Pemanfaatan teknologi informasi saat ini bukan merupakan hal yang sulit ditemukan. Oleh karenanya tidak dapat dipungkiri bahwa teknologi informasi telah menjadi kebutuhan dan persyaratan dalam menjalankan bisnis bagi sebuah organisasi (Abdillah, 2011).

Pada tahun 2018 SMK Muhammadiyah Bulakamba memiliki jumlah guru = 70 orang, karyawan = 12 orang dan jumlah siswa = 985 orang. Guru di SMK Muhammadiyah dibagi ke dalam 3 kompetensi yang ada, yakni: Adaptif, Normatif dan Produktif. Guru yang terdapat pada SMK Muhammadiyah Bulakamba secara kompetensi tergolong heterogen sesuai dengan bidang ilmunya, demikian halnya dengan siswa, yakni sesuai dengan program studi masing-masing.

Hasil survei yang dilakukan, bahwa hampir semua guru, karyawan, dan siswa (99%) menggunakan internet untuk keperluan pembelajaran, kegiatan sosial, hobi dan lainnya pada saat di dalam maupun di luar sekolah. Internet merupakan jaringan global yang menghubungkan komputer di dunia walaupun memiliki perbedaan sistem operasi dan mesin (Ahmadi dan Hermawan, 2013) dan komputer dalam jaringan ini menyimpan *file* yang dapat diakses semua jaringan komputer (Strauss, El-Ansary, & Frost, 2003). Dengan penggunaan internet yang maksimal maka potensi terhadap kejahatan internet juga sangat tinggi. Jumlah kejahatan komputer mengalami peningkatan disebabkan karena: aplikasi bisnis, desentralisasi server, transisi dari *single vendor* ke *multi vendor*, meningkatnya kemampuan pemakai, kesulitan penegak hukum mengejar kemajuan dunia TIK, semakin kompleksnya sistem, maka tidak sedikit perusahaan yang menghubungkan sistem informasinya ke jaringan global (Raharjo, 2015).

Keamanan adalah hal yang fundamental dalam dunia teknologi informasi. Di era tersebut pelayanan kepada konsumen merupakan sesuatu yang mutlak untuk bertahan dalam persaingan (Arius, 2006). Kejahatan internet sangat penting diketahui oleh penggunanya, demikian pula bagi guru, karyawan, dan siswa SMK Muhammadiyah Bulakamba. Ini dikarenakan kejahatan internet dapat menyebabkan akibat yang fatal, seperti: hilangnya data, pemalsuan akun, perusakan data dan lainnya. Kejahatan internet merupakan jenis kejahatan yang memanfaatkan sebuah teknologi informasi secara optimal serta memiliki karakteristik yang kuat dengan rekayasa teknologi dengan mengandalkan kredibilitas dan tingginya tingkat keamanan sebuah informasi yang diberikan dan digunakan oleh pengguna internet (Aulia, 2018). Kejahatan internet merupakan segala penggunaan *computer network* yang digunakan untuk tujuan kriminal (Wahid, Abdul dan Labib, 2005).

Kejahatan internet berbanding lurus dengan banyaknya pengguna internet, nilai transaksi bisnis yang meningkat, frekuensi transaksi yang berkembang pesat, bermunculannya aneka ragam komunitas baru, dan sebagainya (William and Sawyer, 2007). Adapun contoh kejahatan internet di antaranya: *phishing*, *spyware*, *malware*, *wiretapping*, *spamming*, *denial of service*, *hacking*, dan *cracking* (Supriyanto, 2005). Bagi sebagian besar guru dan siswa SMK Muhammadiyah Bulakamba, kejahatan internet merupakan hal yang sangat asing, ini dikarenakan keheterogenan bidang ilmu, kompetensi dan pemahaman yang ada.

Di samping itu, setelah memahami mengenai kejahatan yang mengancam di internet, perlu kiranya pengguna internet juga mengetahui strategi pengamanan yang harus dilakukan oleh penggunanya, agar penggunaan internet berjalan aman dan nyaman. Demikian pula bagi guru dan siswa SMK Muhammadiyah Bulakamba, yang beberapa kali akun sosial media guru dan siswanya mengalami peretasan dan disalahgunakan untuk keperluan yang tidak baik, kemudian data yang tersimpan dalam *harddisk* komputer pun beberapa kali mengalami kehilangan/kerusakan, sangat penting untuk mengetahui dan memiliki ketrampilan dalam pengamanan data dan akun yang dimiliki. Masalah keamanan adalah aspek penting dari sebuah sistem, akan tetapi seringkali dihilangkan atau dikurangi apabila mengganggu performasi dari sistem (Patrick W. Dowd, 1998). Adapun jenis-jenis keamanan internet meliputi: keamanan fisik, keamanan jaringan, otorisasi akses, proteksi virus, dan penanganan bencana (Purbo, 2000). Solusi atas permasalahan tersebut adalah dengan memberikan pembelajaran mengenai kejahatan dan keamanan internet.

Kejahatan dan keamanan internet pernah dikaji dan ditulis dalam beberapa artikel ilmiah, di antaranya: Danuri dan Suharnawi menyampaikan bahwa tren teknologi internet dimanfaatkan untuk keperluan sosialisasi dan bisnis baik kalangan pelajar, mahasiswa, karyawan, maupun orang dewasa. Pemanfaatan teknologi ini di samping memberi manfaat, juga berpeluang disalahgunakan untuk melakukan kejahatan, baik dalam bentuk yang biasa atau yang secara spesifik menargetkan suatu infrastruktur sehingga mengakibatkan sesuatu hal yang fatal yang berdampak pada tatanan sosial, ekonomi, bahkan pertahanan negara. Indonesia sendiri dianggap sebagai negara yang sangat berisiko terhadap serangan keamanan teknologi informasi. Oleh karenanya terdapat undang-undang untuk menurunkan risiko tersebut yang telah ditetapkan pemerintah. Dalam pendidikan tinggi juga telah terdapat mata kuliah pendidikan etika bidang teknologi informasi. Diharapkan Indonesia menjadi negara dengan jumlah kejahatan teknologi informasi yang paling sedikit (Danuri & Suharnawi, 2017).

Abidin dalam artikel ilmiahnya bahwa perkembangan internet telah menciptakan dunia baru yang biasa dikenal dengan *cyberspace*. *Cyberspace* menghasilkan beragam bentuk lingkungan yang menciptakan istilah *cybercrime*. *Cybercrime* merupakan bentuk kejahatan yang muncul disebabkan pemanfaatan teknologi internet. *Cybercrime* dianggap sebagai perbuatan menentang hukum yang dilakukan dengan menggunakan jaringan komputer sebagai media, baik untuk mendapatkan keuntungan maupun tidak (Abidin, 2015).

Sari dalam penelitiannya mengenai kejahatan *cyber* menghasilkan bahwa perkembangan teknologi informasi berbasis komputer telah memunculkan kejahatan *cyber* menggunakan data atau informasi ke internet, seperti memalsukan data pada dokumen penting. Terdapat ketentuan hukum yang mengatur mengenai kejahatan teknologi informasi. Dalam pasal-pasal tertentu dijelaskan mengenai kejahatan dengan menggunakan teknologi informasi berbasis internet (Sari, 2018).

Rahmawati dalam penelitiannya juga menyampaikan bahwa kemajuan teknologi informasi menimbulkan ancaman baru di ruang siber yakni kejahatan siber. Kejahatan siber adalah sebuah kejahatan yang muncul karena dampak negatif dari perkembangan internet. Dalam menganalisa dampak kejahatan siber terhadap pertahanan negara, diperlukan identifikasi manajemen risiko yang digunakan untuk mengetahui peluang dan konsekuensi akibat kejahatan siber. (Rahmawati, 2017).

B. PELAKSANAAN DAN METODE

Khalayak Sasaran

Sasaran pemberian pembelajaran mengenai kejahatan dan keamanan internet

adalah 45 orang siswa dan guru SMK Muhammadiyah Bulakamba yang dipandang ada kemauan dan minat untuk belajar, hal ini berdasarkan atas hasil koordinasi dan konsolidasi dengan pihak SMK Muhammadiyah Bulakamba. Dari khalayak sasaran yang strategis tersebut diharapkan berbagai informasi tentang tren perkembangan komputer dan internet, kejahatan internet, dan keamanan internet, dapat diterima dengan baik oleh peserta kegiatan.

Metode Kegiatan

Metode kegiatan yang dilakukan untuk tercapainya tujuan Pengabdian Kepada Masyarakat ini adalah dengan metode presentasi, diskusi, pelatihan dan pendampingan. Presentasi yang dilakukan juga dibarengi dengan demonstrasi beberapa hal yang perlu didemokan seperti tata cara dalam mendapatkan data privasi sampai pada tahap metode pengamanannya. Adapun praktik secara langsung didasari oleh evaluasi awal berupa pemaparan materi yakni presentasi untuk menentukan materi praktikum apa yang akan disampaikan kepada peserta kegiatan.

Kerangka Pemecahan Masalah

Berbagai potensi yang telah dijelaskan akan terealisasi dengan permasalahan sebagai berikut:

1. Bagaimana peserta kegiatan dapat meningkatkan pengetahuan dan kompetensinya di bidang Teknologi Informasi.
2. Memberikan pengetahuan kepada peserta kegiatan mengenai trend perkembangan teknologi informasi, seperti penerapan *Artificial Intelligence* dan *Internet of Thing.*
3. Memberikan pemahaman kepada peserta kegiatan mengenai pentingnya mengamankan data yang bersifat privasi.
4. Memberikan pengetahuan mengenai jenis-jenis kejahatan internet yang mengancam data pribadi yang ada.
5. Memberikan transfer *knowledge* mengenai metode pengamanan data yang tersimpan di internet kepada peserta kegiatan.
6. Memberikan pelatihan, transfer *skill* dan pendampingan mengenai keamanan jaringan: *Firewall*.

Realisasi Pemecahan Masalah

Strategi yang digunakan dalam menyelesaikan masalah yang ada terkait dengan kejahatan dan keamanan internet, setelah dilakukan evaluasi awal serta metode keamanan yang diterapkan, maka akan dilakukan perlakuan berupa presentasi materi, diskusi, pendampingan dan pelatihan sehingga di akhir kegiatan akan diperoleh hasil adanya peningkatan pengetahuan dan ketrampilan peserta kegiatan mengenai kejahatan dan keamanan internet. Adapun materi dan metode yang akan disampaikan tercantum pada Tabel 1.

Tabel 1. Materi Kegiatan dan Metode Pelaksanaan

No	Materi Kegiatan	Metode Pelaksanaan
1	Trend Perkembangan Komputer dan Internet	Presentasi Materi dan Diskusi
2	Ancaman Kejahatan Komputer dan Internet	Presentasi Materi dan Diskusi
3	Keamanan Data Komputer dan Internet	Presentasi Materi dan Diskusi
4	Pengenalan dan Konfigurasi *Firewall*	Praktikum (Pelatihan dan Pendampingan)

C. HASIL DAN PEMBAHASAN

Hasil survei membuktikan bahwa pengetahuan dan pemahaman 90 % guru dan siswa mengenai kejahatan internet yang dapat mengancam data masih sangat minim, terlebih mengenai teknik pengamanan data tersebut. Di samping itu juga beberapa guru dan siswa pernah mengalami kejahatan internet, seperti : akun sosial media yang dapat diakses secara terlarang, hilangnya data yang tersimpan di *harddisk* komputer dan lainnya.

Kegiatan Pengabdian Kepada Masyarakat diselenggarakan pada tanggal 27 s.d 28 Februari 2019 yang dilakukan dengan metode presentasi dan pelatihan/

pendampingan. Presentasi dilakukan untuk menyampaikan informasi umum tentang Trend Perkembangan Komputer dan Internet, Ancaman Kejahatan Komputer dan Internet, Keamanan Data Komputer dan Internet. Sedangkan pelatihan/pendampingan dilakukan untuk materi praktikum *firewall*.

Presentasi

Presentasi yang disampaikan oleh tim pelaksana kegiatan dilaksanakan pada tanggal 27 Februari 2019 di aula SMK Muhammadiyah Bulakamba. Pelaksanaan kegiatan presentasi ini adalah memberikan pengetahuan dan pemahaman kepada guru dan siswa SMK Muhammadiyah Bulakamba mengenai trend teknologi informasi, kejahatan dan keamanan internet . Pada sesi ini peserta diberikan materi mengenai *Trend* Perkembangan Komputer dan Internet, Ancaman Kejahatan Komputer dan Internet, Keamanan Data Komputer dan Internet. Disamping itu peserta juga diberikan privat khusus secara sederhana dalam mengamankan data yang tersimpan di komputer. Adapun privat tersebut diantaranya :

1. *Setting password* BIOS (*Basic Input/Output System*)
2. *Setting Password* di Sistem Operasi Linux dan Windows
3. *Setting Folder Lock* (Untuk memberikan password di folder)
4. *Setting Hide and Show Folder* dan *File*.

Gambar 1. Pelaksanaan Pemaparan Materi dan Diskusi

Pelatihan dan Pendampingan

Kegiatan pelatihan dan pendampingan ini dilakukan pada tanggal 28 Februari 2019 di ruang Laboratorium Komputer 1 dan Laboratorium Komputer 2 SMK Muhammadiyah Bulakamba yang disampaikan langsung oleh mahasiswa. Adapun materi yang disajikan adalah mengenai *Firewall*, dengan rincian sebagai berikut:

1. Pengenalan *Firewall*
2. Cara Kerja *Firewall*
3. Konfigurasi *Firewall*
4. Analisa dan Filter Paket
5. *Bloking* isi dan protokol
6. Autentikasi koneksi dan enkripsi

Dalam sesi ini setiap peserta diwajibkan melakukan uji coba praktikum mengenai *firewall* sesuai dengan rincian materi tersebut. Pada sesi ini peserta diberikan kesempatan untuk diskusi dan konsultasi dengan tim mahasiswa. Selain itu pada sesi ini juga diberikan simulasi mengenai teknik *attack* (menyerang) komputer dengan maksud untuk mencuri data dan teknik atau cara pengamanannya menggunakan *firewall*.

Di samping itu, pada kegiatan ini juga diberikan pelatihan cara mengetahui komputer yang melakukan pencurian data terhadap data privat, yang dengan melakukan pelacakan terhadap IP *Address* komputer yang melakukan penyerangan tersebut menggunakan IP *Scanner*.

Gambar 2. Pelaksanaan Pelatihan dan Pendampingan

Setelah dilakukan studi mengenai kejahatan dan keamanan internet berupa pemaparan materi dan pelatihan, dan berdasarkan hasil penyebaran kuesioner yang dilakukan pasca kegiatan Pengabdian Kepada Masyarakat, maka dapat dihasilkan bahwa

95% guru dan siswa yang merupakan peserta kegiatan ini pengetahuan dan pemahaman mengenai kejahatan dan keamanan internet meningkat, 75% peserta juga telah memiliki ketrampilan mengenai keamanan internet. Kemudian setelah pengetahuan dan pemahamannya meningkat, maka proteksi peserta kegiatan terhadap data privasi dan akun yang terkoneksi di internet akan lebih diproteksi dengan optimal.

D. PENUTUP

Simpulan

Berdasarkan hasil kegiatan pembelajaran mengenai kejahatan dan keamanan internet bagi guru dan siswa SMK Muhammadiyah Bulakamba dapat disimpulkan sebagai berikut:

1. Guru dan Siswa SMK Muhammadiyah Bulakamba telah mendapatkan pengetahuan dan pemahaman mengenai tren perkembangan komputer dan internet
2. Guru dan Siswa SMK Muhammadiyah Bulakamba telah mendapatkan pengetahuan dan pemahaman mengenai ancaman kejahatan internet beserta metode pengamanannya
3. Pemahaman dan kompetensi guru dan siswa mengenai teknik *setting password* pada komputer semakin meningkat
4. Kompetensi guru dan siswa mengenai keamanan komputer menggunakan *firewall* meningkat.

Saran

Saran setelah pelaksanaan kegiatan adalah sebagai berikut:

1. Perlu adanya pelatihan khusus tentang *firewall* agar kompetensi atau *skill* guru dan siswa meningkat
2. Perlu adanya mata pelajaran pada program studi multimedia di SMK Muhammadiyah Bulakamba yang secara khusus membahas mengenai keamanan komputer dan internet
3. Adanya tindak lanjut dari SMK Muhammadiyah Bulakamba untuk memberikan kemudahan dan keleluasaan bagi siswa maupun guru dalam meningkatkan kompetensi mengenai keamanan komputer dan internet pada laboratorium komputer yang terdapat di sekolah.

E. DAFTAR PUSTAKA

Abdillah, J. &. (2011). *Sistem Tata Kelola Teknologi Informasi*. Yogyakarta: Andi.

Abidin, D. Z. (2015). Kejahatan dalam Teknologi Informasi dan Komunikasi. *Jurnal Ilmiah Media Processor*, 10(2), 1–8. Retrieved from http://ejournal.stikom-db.ac.id/index.php/processor/article/view/107/105

Ahmadi dan Hermawan. (2013). *E-Business & E-Commerce*. Yogyakarta: Andi.

Arius, D. (2006). *Computer Security*. Yogyakarta: Andi.

Aulia, T. M. (2018). *Tinjauan Hukum Internasional Atas Perbuatan Hacking dan Cracking Sebagai Bentuk Dari Kejahatan Cybercrime*.

Danuri, M., & Suharnawi. (2017). Trend Cyber Crime Dan Teknologi Informasi Di Indonesia. *Informasi Komputer Akuntansi Dan Manajemen*, 13(2), 55–65.

Kadir, A. dan T. C. (2005). *Pengenalan Teknologi Informasi*. Yogyakarta: Andi.

Patrick W. Dowd, and J. T. M. (1998). Network Security: It's Time To Take It Seriously. *IEEE Computer*, 24–28.

Purbo, O. W. (2000). *Buku pintar Internet: Keamanan Jaringan Internet*. Jakarta: Elex Media Komputindo.

Raharjo, B. (2015). *Keamanan Sistem Berbasis Internet*. Jakarta: PT.INDOCISC.

Rahmawati, I. (2017). the Analysis Ofcyber Crime Threat Risk Management To Increase Cyber Defense. *Jurnal Pertahanan & Bela Negara*, 7(2), 51–66. https://doi.org/10.33172/jpbh.v7i2.193

Sari, N. W. (2018). Kejahatan Cyber dalam Perkembangan Teknologi Informasi Berbasis Komputer. *Jurnal Surya*

Kencana Dua: Dinamika Masalah Hukum dan Keadilan, 5(2), 577–593.

Strauss, J., El-Ansary, A., & Frost, R. (2003). *E-marketing International (3rd Edition)*. New Jersey: Upper Saddle River.

Supriyanto, A. (2005). *Pengantar teknologi Informasi*. Jakarta: Salemba Infotek.

Wahid, Abdul dan Labib, M. (2005). *Kejahatan Mayantara (Cyber Crime)*. Jakarta: PT. Rafika Aditama.

William and Sawyer. (2007). *Using Information Technology*. Yogyakarta: Andi.