Puan Journal Indonesia
Edisi Juli 2024
Vol. 6 No. 1
Published by Asosiasi Idebahasa Kepri

PELATIHAN PENGGUNAAN KEAMANAN SIBER SISTEM INFORMASI PERUSAHAAN DAN KOMUNIKASI INTERNAL

Training on the Use of Cybersecurity of Corporate Information Systems and Internal Communications

Anintyo Herdadi
Universitas Media Nusantara Citra, Jakarta, Indonesia
e-mail: anintyo.herdadi@mncu.ac.id

Ilmi Sila Ayu
Universitas Media Nusantara Citra, Jakarta, Indonesia
e-mail: ilmisilaayu@gmail.com

Abstract

Data security and information systems in a company are very important because they transport a company's data progress. Currently, there are many crimes in the field of technology, so a security system is needed so that data cannot be accessed and stolen by unauthorized people. The aim of this research is to provide outreach in training on the use of cyber security in a company. The right way to use to build security information in a company includes: 1. Making a study of policies regarding various information systems. Using an encryption system in data transfer 3. Choosing safe software for the organization 4. Increasing the security of passwords used .5 Implementing an Information Security Management System. Carrying out this service can help employees and company management of PT Unisystem Utama in maintaining data security from people who do not have the right to use data owned by the company.

Keywords-- *Data Security, encryption, Company*

1. PENDAHULUAN

Serangan di ruang siber (*cyberspace*) sendiri merupakan konsekuensi logis dari berkembangnya era teknologi informasi. Identifikasi bentuk serangan siber dapat terlihat pada hal-hal seperti kriminalitas siber, botnets, serangan terhadap institusi finansial-keuangan, penyebaran *Multi Purpose Malcode*, aktivitas siber yang disponsori oleh negara, dan aktivitas *hacking*. Berbagai bentuk tren ini menggunakan instrumen *cyberspace* sebagai saluran utama dalam melaksanakan tindakannya. Keamanan Siber sesuai dengan definisinya, *cyber security* adalah aktifitas pencegahan dan pengamanan terhadap sumber daya telematika agar tidak terjadinya kriminalitas di dunia *cyber* (*Cyber Crime*). *Cyber security* juga dapat diartikan upaya untuk menahan dari penyerangan-penyerangan di dunia *cyber*. Berikut adalah elemen-elemen pokok dari *cyber security* yaitu; *security policy document, information infrastructure, perimeter defense, network monitoring system, system information and event management, network security assessment, human resource* dan *security awareness*. Dalam sistem informasi dikenal istilah "*Hardening*" yaitu sebuah cara untuk memperkuat keamanan infrastruktur sistem

informasi seperti komputer maupun hal lainnya. Keamanan yang diperkuat biasanya pada sisi jaringan, sistem komputer, penutupan *port* yang rentan akan serangan, maupun dari segi *firewall* nya. Dilihat dari sisi sumber daya manusia, praktisi *cyber security* dapat dikelompokkan menjadi 3 kelompok besar yaitu analis keamanan, spesialis forensik, *hacker* (peretas) [1].

Dalam beberapa dekade terakhir ini, perkembangan teknologi informasi dan komunikasi secara positif telah berkontribusi terhadap perkembangan ekonomi global dan berdampak pada produktivitas, persaingan, dan keterlibatan warga negara yang lebih tinggi. Akan tetapi, karena pihak pemerintah, pengusaha, dan masyarakat kini jauh lebih terkoneksi di dunia maya, beberapa tantangan terkait ancaman dunia maya membutuhkan lebih banyak perhatian untuk mengembangkan keamanan dunia maya (*cyber security*) yang lebih kuat. Menurut ISO (*International Organization for Standardization*), ISO/IEC 27032 mengutip dari sejumlah sumber, *cyber security* atau *cyberspace security* adalah preservasi dari kerahasiaan, integritas, dan ketersediaan informasi di *cyberspace*. Adapun *cyberspace* merujuk pada lingkungan yang kompleks dan merupakan hasil dari interaksi antara orang, peranti lunak, dan layanan-layanan internet melalui penggunaan aneka perangkat teknologi dan berbagai koneksi jaringan dan lingkungan yang tidak memiliki wujud [2].

Keamanan siber merupakan sebuah rangkaian aktivitas yang diarahkan untuk melindungi dari ancaman, gangguan, serangan jaringan komputer (perangkat keras dan perangkat lunak), terkait informasi di dalamnya, dan elemen-elemen ruang siber lainnya. Keamanan siber dapat digunakan sebagai sarana melindungi terhadap pengawasan yang tidak diinginkan, seperti kegiatan intelijen. Dengan demikian, keamanan siber adalah semua mekanisme perlindungan yang digunakan untuk meminimalisir gangguan pada ketersediaan (*availability*), integritas (*integrity*), dan kerahasiaan (*confidentiality*) dari sebuah informasi. Kerahasiaan data merujuk pada akses yang disetujui terhadap sebuah data, yang berarti hanya pihak yang memiliki akses saja yang dapat membukanya. Usaha untuk mendapatkan akses dengan cara mencuri informasi diartikan sebagai tindakan membahayakan kerahasiaan data. Selanjutnya, dalam upaya perlindungan terhadap data pribadi Menurut *Privacy International* dalam Azmi (2020) dikenal istilah perlindungan data (*data protection*). Definisi perlindungan data adalah sebuah aturan hukum yang bertujuan untuk memberikan perlindungan terhadap data pribadi yang dimiliki oleh seseorang. Bagi masyarakat modern, melindungi data dari penyalahgunaan adalah sangat penting. Itu sebabnya diperlukan hukum perlindungan data yang mengatur perusahaan dan pemerintah karena dua entitas ini memiliki peran yang signifikan untuk mencegah adanya penyelewengan oleh oknum yang tidak bisa dipertanggung jawabkan tindakannya [3].

Segala usaha dan upaya buat tingkatkan yang dilakukan dalam menjaga keamanan siber yakni diperingkatkan dalam *Global Cybersecurity Index* (GCI) oleh *International Telecommunication Union* (ITU) terhadap 193 negara anggotanya. Berdasarkan pengkajian nilai oleh GCI pada tahun 2017, Indonesia terletak pada barisan negara-negara di Asia-Pasific dikira belum mempunyai pertahanan dan juga tanggung jawab besar pada saat memerangi kejahatan siber. Penilaian yang dilakukan oleh GCI terhadap keamanan siber didasarkan atas 5 pilar yaitu status hukum, pengukuran didasari oleh adanya institusi legal dan kerangka keamanan siber. Kedua adalah teknisi, didasari oleh sumber institusi teknis serta pelaksanaan teknologi. Selanjutnya adalah koordinasi, didapat bersumber pada pengkoordinasian antara pembentuk prosedur yang berlaku dan perkembangan strategi keamanan siber. Kemudian kapasitas, pengukuran bersumber pada riset

serta pengembangan, pembelajaran, serta program pelatihan, pihak profesional dan aparatur yang telah bersertifikat. Pilar terakhir adalah kerjasama, berdasarkan adanya kemitraan, timbulnya kerangka kolaborasi serta pembagian jaringan informasi [4].

Menurut Penelitian [5] Studi kasus terkait ancaman dan solusi dalam lingkungan digital memberikan wawasan praktis tentang serangan yang pernah terjadi dan tindakan yang diambil untuk mengatasi mereka. Dalam penelitian ini, analisis terhadap berbagai studi kasus serangan *cyber* dapat memberikan pemahaman mendalam tentang taktik dan strategi yang berhasil dalam melawan serangan *cyber*. Dari sini, dapat ditemukan solusi efektif untuk meningkatkan keamanan *cyber* secara keseluruhan, termasuk upaya identifikasi ancaman yang lebih baik, peningkatan kesadaran pengguna tentang kebijakan keamanan, dan pengembangan sistem deteksi dini yang kuat.

Dalam organisasi sebuah lembaga, seringkali dijumpai pegawai atau bawahan kurang bergairah dan bersemangat dalam bekerja karena informasi mengenai pekerjaan kurang dapat dipahami, perintah-perintah yang terlalu banyak, kurang perhatian, dan penghargaan dari atasan dan ditunjang oleh adanya kecenderungan bawahan merasa segan pada atasan, takut dan khawatir pada atasan, sehingga mereka menyembunyikan perasaan pikiran padahal hal itu justru tidak efektif dan efisien. Hal ini tentu sangat berpengaruh terhadap kemajuan organisasinya, khususnya berpengaruh terhadap pencapaian efektifitas kerja [6]. Organisasi pada saat ini umumnya dituntut untuk lebih proaktif dalam menghadapi perubahan sesuai perkembangan zaman, sifat proaktif ini dapat dilakukan oleh organisasi dengan baik jika para pegawainya yang menentukan maju mundurnya suatu organisasi dapat bekerja seoptimal mungkin dalam bidang pekerjaannya masing-masing [7].

2. METODE

Untuk mencapai tujuan yang telah ditetapkan, maka kegiatan pengabdian kepada masyarakat ini dilakukan dengan menggunakan dua metode sebagai berikut.

1. Ceramah
   Metode ini dilakukan dengan menyampaikan teori tentang Keamanan Siber dan Komunikasi Internal dengan menghadirkan nara sumber memahami tentang bagaimana cara Keamanan siber dan komunikasi internal yang mudah. Materi yang disampaikan adalah langkah-langkah pembuatan Keamanan siber dan komunikasi internal yang mudah yang dapat dimanfaatkan oleh Perusahaan untuk menjaga keamanan data dan cara berkomunikasi secara internal. Teori ini dimaksudkan agar nantinya lebih memudahkan para pengguna dalam menjaga keamanan data.
2. Praktek
   Metode ini dilakukan dengan memberikan kesempatan Karyawan untuk langsung mempraktekan cara penggunaaan Siber dan praktek komunikasi internal. Pemateri langsung mempraktekkan teori yang telah diberikan oleh narasumber. Narasumber langsung membimbing dalam melakukan praktek.
3. Diskusi
   Metode ini dilakukan dengan memberikan kesempatan kepada peserta unutk bertanya atau berbagi penalaman tentang pemasalahan atau kesulitan yang ditemui saat menggunakan. Metode diskusi ini bertujuan agar para pemakai lebih aktif dalam dalam menyampaikan permasalahan-

permasalahan dan nantinya juga dapat pemakai agar dapat memberikan informasi yang efektif dan efisein kepada karyawan

Kegiatan pengabdian ini dilaksanakan pada PT Unisystem Utama pada Karyawan dan Manajemen Perusahaan dengan Tema Sosialisasi: Keamanan Siber Sistem Informasi Perusahaan dan komunikasi internal perusahaan. Pengabdian ini diikuti oleh banyak karyawan pada PT tersebut. Pengabdian ini berjalan dengan lancar dan terlihat antusiasme karyawan dalam mengikuti kegiatan tersebut. Kegiatan pengabdian masyarakat berupa pelatihan yang dapat memberikan manfaat dengan menerapkan beberapa metode pelaksanaan kegiatan. Penjelasan penggunaan metode dapat dilihat pada tabel berikut.

Tabel 1. Metode Pelaksanaan

Permasalahan	**Solusi**	**Metode**
Pemahaman dibidang Keamanan Siber	Memberikan pembinaan memanfaatkan siber secara jelas serta proses pengerjaannya	Pelatihan dan diskusi
Pelatihan dalam menjaga keamanan system Informasi perusahaan	Memberikan pembinaan Pemanfaatan aplikasi siber dalam menjaga keamanan data	Pelatihan dan diskusi
Cara Pengemabangan komunikasi internal pada Perusahaan	Mengembangkan program komunikasi internal yang efektif untuk meningkatkan kesadaran karyawan mengenai pentingnya keamanan data dan praktik terbaik dalam menjaga kerahasiaan data.	Pelatihan dan diskusi
Penggunaan Komunikasi yang efektif mengenai kebijakan keamanan data perusahaan	Komunikasi yang efektif mengenai kebijakan keamanan data perusahaan dan prosedur yang harus diikuti oleh seluruh karyawan.	Pelatihan dan diskusi

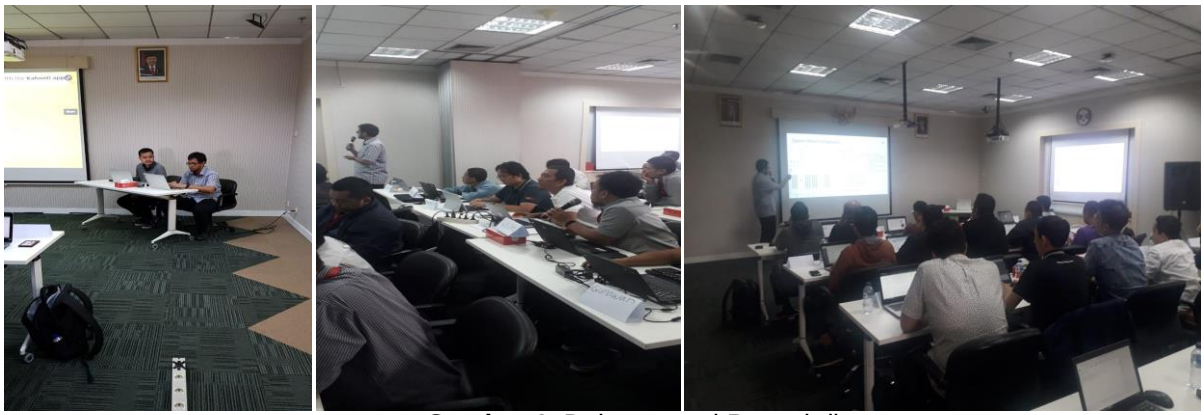
3. HASIL DAN PEMBAHASAN

Berdasarkan hasil yang diperoleh dalam kegiatan pelaksanaan pengabdian yang dilakukan pada PT Unisystem Utama dapat diperoleh:

1. Peserta pengabdian sangat antusias mendengarkan pembicara dalam menjelaskan pengabdian ini diharapkan para peserta bisa memahami, menerapkan keamanan data agara terhindar dari kejahatan dari orang orang yang tidak berhak untuk mengakses data serta Mengembangkan program komunikasi internal yang efektif untuk meningkatkan kesadaran karyawan mengenai pentingnya keamanan data dan praktik terbaik dalam menjaga kerahasiaan data.
2. Dalam pelaksaan kegiatan begitu baik respon dan tanggap karyawan dalam kegiatan pengabdian masyarakat ini sehingga bisa diterapkan dalam perusahaan tersebut.
3. Dalam kegiatan pengabdian tersebut tim pengabdian mempraktekkan cara serta langkah langkah dalam menggunakan system keamanan data yang digunakan dalam system pengabdian tersebut.
4. Dalam pengabdian tersebut begitu baik respon dan rasa ingin tau anggota pengabdian sehingga anggota pengabdian meminta agar pengabdian berikutnya bisa dilaksanakan pada PT tersebut.

Dalam kegiatan pengabdian masyarakat ini ada bebarapa pembahasan yang dilakukan Awal pertemuan terlebih dahulu kita memberikan materi atau penjelasan tentang aplikasi Keamanan Data system Informasi dengan tujuan agar para karyawan lebih memahami tentang aplikasi Keamanan Data system Informasi sehingga nanti saat dilakukan praktek tidak terjadi kendala atau masalah. Materi ini bertujuan untuk memantapkan pengetahuan Keamanan Data system Informasi tentang aplikasi ini dan nantinya akan memudahkan karyawan untuk menjalankan aplikasi dalam menjaga keamanan data perusahaan. Pelatihan ini dilaksanakan dengan 1 orang Dosen yang memiliki kompetensi dibidang komputer. Materi yang diberikan disampaikan dengan Viewer, dengan panduan modul (modul internet dan modul power point) untuk mempermudah menangkap materi yang disampaikan instruktur.

Teknik pelaksanaan kegiatan pengabdian ini dilaksanakan oleh 3 instruktur, 1 orang menjelaskan materi dengan menyorotkan melalui Viewer, sedang 2 instruktur yang lain melakukan pendampingan langsung dan selanjutnya instruktur bergantian menyampaikan materi kepada peserta. Materi yang disampaikan kepada peserta atau karyawan yaitu melalui Power Point setelah itu dilanjutkan dengan praktek cara penggunaan aplikasi keamanan siber yang bertujuan untuk menguji serta menjaga data dari orang-orang yang tidak berhak. Praktek ini agar karyawan lebih paham dalam penggunaan sehingga tidak terjadi kesalahan saat menggunakan aplikasi tersebut dalam menjaga keamanan data. Peserta sangat antusias dalam menerima serta mempraktekkan sesuai arahan dari narasumber. Karyawan disini juga aktif bertanya jika mengalami kesulitan saat menjalankan aplikasi. Peserta juga aktif bertanya tentang aplikasi ini.



Gambar 1. Dokumentasi Pengabdian

4. KESIMPULAN

Setelah pengabdian kepada masyarakat selesai dilaksanakan maka dapat diambil kesimpulan diantaranya:

1. Pengabdian ini memberikan pengetahun cara pengamanan Data system informasi secara efektif dan efesien serta Mengembangkan program komunikasi internal yang efektif untuk meningkatkan kesadaran karyawan mengenai pentingnya keamanan data dan praktik terbaik dalam menjaga kerahasiaan data.
2. Pengabdian ini mampu meningkatkan pemahaman dan kemampuan dalam penggunakan siber keamaan dalam menjaga data dari tindakan kejahatan dan mengembangkan program komunikasi internal yang efektif.

5. SARAN

Berdasarkan hasil dari kegiatan yang telah dilakukan maka dapat dirumuskan beberapa saran sebagai berikut:

1. Perusahaan mampu menggunakan sarana Siber kemanan system informasi untuk menjaga data dan Mengembangkan program komunikasi internal.
2. Perlu dilakukan kegiatan pelatihan yang intensif dan berkesinambungan dalam membina penggunaan siber keamanan system Informasi.

UCAPAN TERIMA KASIH

Terima kasih kami ucapkan kepada perusahan yang sudah memberikan waktu dan kesempatan dalam kegiatan pengabdian ini, terima kasih juga tim pengabdian ucapkan kepada pihak kampus yaitu Universitas Media Nusantara Citra Jakarta yang sudah memfasilitasi pengabdian ini berjalan lancar dan tak lupa Tim pengabdian ucapkan kepada pengelola jurnal yang sudah mempublish jurnal ini sesuai dengan waktu yang sudah ditetapkan.

DAFTAR PUSTAKA

[1] C. 'Rahmawati, "Tantangan Dan Ancaman Keamanan Siber Indonesia Di Era Revolusi Industri 4.0," *Semin. Nas. Sains Teknol. dan Inov. Indones. (SENASTINDO AUU)*, vol. 1, no. 1, pp. 299–306, 2019.

[2] E. Budi, D. Wira, and A. Infantono, "Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0," *Pros. Semin. Nas. Sains Teknol. dan Inov. Indones.*, vol. 3, no. November, pp. 223–234, 2021, doi: 10.54706/senastindo.v3.2021.141.

[3] M. P. Aji, "Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]," *J. Polit. Din. Masal. Polit. Dalam Negeri dan Hub. Int.*, vol. 13, no. 2, pp. 222–238, 2023, doi: 10.22212/jp.v13i2.3299.

[4] F. Indah and A. Q. Sidabutar, "Peran Cyber Security Terhadap Keamanan Data Penduduk Negara Indonesia (Studi Kasus: Hacker Bjorka)," *J. Bid. Penelit. Inform.*, vol. 1, no. 1, p. 2, 2022, [Online]. Available: https://ejournal.kreatifcemerlang.id/index.php/jbpi/article/view/78%0Ahttps://ejournal.kreatifcemerlang.id/index.php/jbpi/article/download/78/8

[5] E. Soesanto, A. Romadhon, B. Dwi Mardika, and M. Fahmi Setiawan, "Analisis dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital Untuk Mengamankan Objek Vital dan File," *SAMMAJIVA J. Penelit. Bisnisdan Manaj.*, vol. 1, no. 2, p. 186, 2023.

[6] A. K. Wicaksono and Y. Soesatyo, "Hubungan Komunikasi Internal Organisasi Dengan Keefektifan Kerja Guru Dan Karyawan Di Sekolah Menengah Kejuruan Negeri (Smkn) 2 Trenggalek," *Abi Krisma Wicaksono Prodi*, no. X, 2015, [Online]. Available: https://core.ac.uk/download/pdf/230758536.pdf

[7] M. E. 2013 Ningrum, "Peranan Komunikasi Internal Di Lingkungan Kerja," *Indept*, vol. 3, no. 1, pp. 25–30, 2013.