e-ISSN : 2964 - 4533
p-ISSN : 2985-914X

PEMANAS: Jurnal Pengabdian Masyarakat Nasional
Vol. 3, No. 2 November 2023, Hal 122 - 130

MENINGKATKAN KESADARAN CYBER SECURITY DI SEKTOR PERBANKAN

Rahmat Rian Hidayat[1], Arbi Abdul Kahfi[2], Agus Sulomo[3], Naima Amaliah[4]

[1]Program Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana Jakarta, [2]Program Studi Pendidikan Administrasi Perkantoran, Fakultas Ekonomi dan Bisnis, Universitas Negeri Yogyakarta
*e-mail: rahmat.rian@mercubuana.ac.id [1], arbiabdulkahfi@uny.ac.id[2], agus_sulomo@yahoo.com [3], naimaamaliah94@gmail.com[4]

ABSTRACT

As information becomes increasingly important in companies, information threats and vulnerabilities also increase, as evidenced by the emergence of certain hacks/information leaks that impact organizations. Information security awareness is important to any organization's efforts to safeguard information. All organizational efforts to safeguard information may become ineffective due to such risks. Therefore, awareness is the starting point for all personnel in a company to pursue or understand knowledge about cyber security. With security awareness, an employee can focus his or her attention on one or more potential problems or dangers. So, to create awareness among the public or bank employees, one way is to deliver material, through Community Service events with the theme of cyber security. This activity was carried out online using zoom media which was attended by 524 participants and consisted of several lecturers as resource persons who used educational and evaluation methods in delivering the material. Based on the activities that have been carried out and the evaluation results during this community service activity, we can conclude that the community service program has been able to provide benefits for participants in this training, especially in building awareness of information security in the banking environment. Participants were able to understand well based on the evaluation results which showed that 93% of participants were able to answer questions with scores that passed the standard

Keywords: *Awareness, Cyber, Digital, Information,*

ABSTRAK

Seiring dengan semakin pentingnya informasi dalam perusahaan, ancaman dan kerentanan informasi juga meningkat, terbukti dengan munculnya peretasan/kebocoran informasi tertentu yang berdampak pada organisasi. Kesadaran keamanan informasi merupakan kontribusi penting bagi upaya organisasi mana pun untuk menjaga informasi.Seluruh upaya organisasi untuk menjaga informasi mungkin menjadi tidak efektif akibat risiko tersebut. Oleh karena itu, kesadaran menjadi titik awal bagi seluruh personel di suatu perusahaan untuk menekuni atau memahami pengetahuan mengenai cyber security. Dengan kesadaran keamanan, seorang karyawan dapat memusatkan perhatiannya pada satu atau lebih potensi masalah atau bahaya. Sehingga, untuk menciptakan kesadaran di kalangan Masyarakat atau pun karyawan bank salah satu cara yang dilakukan yaitu pemberian materi, melalui acara Pengabdian Masyarakat yang bertemakan cyber security. Kegiatan ini dilakukan secara online menggunakan media zoom yang diikuti oleh 524 peserta serta terdiri dari beberapa dosen sebagai narasumber yang menggunakan metode edukasi dan evaluasi dalam penyampaian materi. Berdasarkan kegiatan yang telah dilaksanakan dan hasil evaluasi selama kegiatan pengabdian masyarakat ini, dapat kami simpulkan bahwa program pengabdian masyarakat telah mampu memberikan manfaat bagi peserta pelatihan ini, terutama dalam membangun kesadaran dalam keamanan informasi di lingkungan bank. Peserta dapat memahami dengan baik berdasarkan hasil evaluasi yang menunjukkan 93% peserta mampu menjawab soal dengan hasil skor melewati standar.

Kata Kunci: *Cyber, Digital, Informasi, Kesadaran*

e-ISSN : 2964 - 4533
p-ISSN : 2985-914X

PEMANAS: Jurnal Pengabdian Masyarakat Nasional
Vol. 3, No. 2 November 2023, Hal 122 - 130

1. PENDAHULUAN

Dunia siber dalam lingkup skala global telah berhasil menyatukan antar negara, perusahaan, dan individu. Pentingnya waktu dan tempat dalam aspek komunikasi telah memudar seiring berjalannya waktu. Meskipun masyarakat informasi digital telah meningkatkan kesejahteraannya secara signifikan, hal ini juga membawa bahaya dari berbagai ancaman dunia siber. Sasaran penyerangan dapat diakses dengan murah dari mana saja di dunia, dan server perintah yang melaksanakan operasi dapat berlokasi di negara mana pun, sehingga menyembunyikan pelaku sebenarnya (Lehto, 2015).

Salah satu contoh serangan cyber yang terjadi di Indonesia adalah serangan ransomware yang menyebabkan layanan perbankan PT Bank Syariah Indonesia Tbk (BSI) lumpuh serta kebocoran data nasabah. Sekelompok peretas yang mengidentifikasikan dirinya dengan nama Lock Bit mengklaim telah berhasil mencuri sebesar 1,5 terabyte (TB) data nasabah dari sistem BSI. Selain data nasabah, dokumen lain yang diklaim telah dicuri meliputi dokumen finansial, dokumen legal, perjanjian kerahasiaan, password akses internal serta layanan perusahaan. Adapun, data nasabah yang diduga bocor terdiri dari nama, nomor HP, alamat, nomor rekening, saldo rekening rata-rata, riwayat transaksi, pekerjaan, dan tanggal pembukaan rekening.

Karena pentingnya cyber security dalam lingkungan digital saat ini khususnya dunia perbankan, hal ini menjadi topik yang hangat dibicarakan. Beberapa peneliti telah menggunakan algoritma pembelajaran mesin yang kuat. Hal ini telah didemonstrasikan dalam sistem deteksi intrusi berdasarkan fitur Decision Tree-Recursive Feature Elimination (DT-RFE) dari pembelajaran ansambel (Jia et al., 2018). Pada awalnya, disediakan DT-RFE untuk memilih karakteristik dan mengurangi ukuran fitur. Menghapus data asing dan tidak terhubung dari database untuk meningkatkan kualitas sumber daya dan menghemat waktu proses. Fang et al (2019) mengintegrasikan teknik DT dan RFE dalam pembelajarannya untuk membangun pembelajaran ansambel susun. Mereka mempresentasikan pendekatan deteksi DoS berdasarkan pembelajaran mesin. Teknik yang diusulkan didasarkan pada tanda tangan yang berasal dari pola lalu lintas internet. Eksperimen ini memanfaatkan kumpulan data terbaru.

Strategi *cyber security*, perilaku manusia, dan teknologi berfungsi untuk mengamankan aset digital. Seperti terlihat pada Gambar 1, risiko *cyber security* di sektor jasa keuangan menawarkan tantangan. Penjahat dunia maya menggandakan kekuatan alat penyerang sekaligus memangkas biaya chip, sebanding dengan prediksi hukum Moore yang memperkirakan jumlah komponen pada chip silikon akan berlipat ganda setiap dua tahun (Maglaras et al., 2018). Kelompok kriminal yang terlibat dalam operasi gelap melakukan serangan siber yang dapat menimbulkan Denial of Service (DoS), mencuri data atau rahasia negara akibat pembobolan data, meminta pembayaran melalui ransomware, dan lain sebagainya.

Sebelum memulai serangan, penyerang memperoleh kendali atas sejumlah besar komputer. Ini adalah sistem yang rentan. Penyerang menggunakan file berbahaya atau pendekatan peretasan lainnya untuk mengeksploitasi kelemahan sistem guna mendapatkan kendali atas mesin (Behal & Kumar, 2017). Struktur serangan DDoS dan tujuan pelakunya selalu berubah. Penjahat masih dihukum karena operasi DDoS berbasis botnet yang menyebabkan kerugian miliaran dolar pada target mereka (Bawany et al., 2017).

Kesadaran keamanan informasi merupakan kontribusi penting bagi upaya organisasi mana pun untuk menjaga informasi. Namun, dimensi ini sering kali kurang dihargai. Seluruh upaya organisasi untuk menjaga informasi mungkin menjadi tidak efektif akibat risiko tersebut. Oleh karena itu, kesadaran menjadi titik awal bagi seluruh personel di suatu perusahaan untuk menekuni atau memahami pengetahuan mengenai keamanan informasi teknis (Imam Suhartadi, 2021). Dengan kesadaran keamanan, seorang karyawan dapat memusatkan perhatiannya pada satu atau lebih potensi masalah atau bahaya. Sehingga, untuk menciptakan kesadaran di kalangan Masyarakat atau pun

e-ISSN : 2964 - 4533
p-ISSN : 2985-914X
PEMANAS: Jurnal Pengabdian Masyarakat Nasional
Vol. 3, No. 2 November 2023, Hal 122 - 130

karyawan bank salah satu cara yang dilakukan yaitu pemberian materi, melalui acara Pengabdian Masyarakat yang bertemakan *cyber security*.

Gambar 1. Masalah *cyber security* dalam layanan perbankan

2. METODE

Pengabdian kepada masyarakat adalah usaha untuk menyebarluaskan ilmu pengetahuan, teknologi, dan seni kepada masyarakat. Kegiatan tersebut harus mampu memberikan suatu nilai tambah bagi masyarakat, baik dalam kegiatan ekonomi, kebijakan, dan perubahan perilaku (sosial). Kegiatan ini terdiri dari beberapa dosen sebagai narasumber dan sesuai dengan judul yang diajukan pada proposal maka saya menyampaikan presentasi tentang Cyber Security Awareness di Amar Bank berdasarkan ISO 27001:2013.

Berdasarkan hasil identifikasi masalah yang dilakukan di lapangan, maka metode pendekatan yang dilakukan adalah:

a. Metode Edukasi bertujuan untuk memberikan pemahaman bahwa permasalahan yang dihadapi dan penyampaian solusi serta target capaian.
b. Metode Evaluasi program dengan tujuan untuk mengetahui tingkat pemahaman materi yang telah disampaikan.

3. HASIL DAN PEMBAHASAN

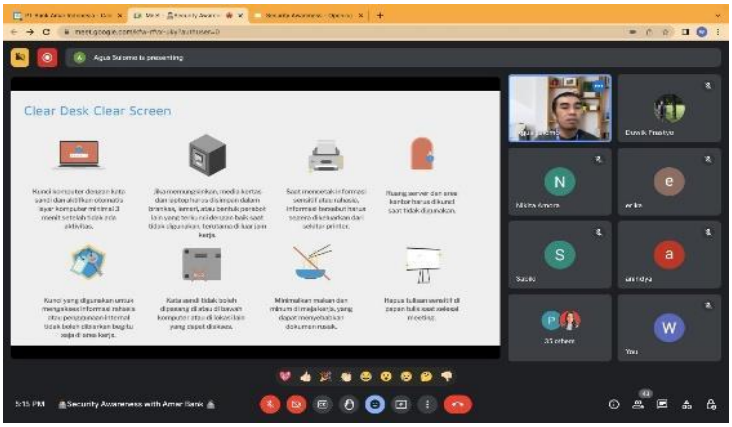
Tingkat kesadaran dan pemahaman karyawan cyber security perlu terus ditingkatkan dan dijaga karena dunia digital termasuk salah satu aspek lingkungan yang mengalami perkembangan sangat cepat. Berdasarkan hal tersebut, maka diperlukannya pelatihan untuk meningkatkan pemahaman dan pengetahuan karyawan terhadap cyber security. Total peserta yang mengikuti pelatihan ini adalah 524 orang.

Metode edukasi dan pelatihan dilakukan dengan mempresentasikan materi secara online dengan menggunakan aplikasi zoom. Berikut ini adalah salah satu dari slide dari profil pembicara pada saat presentasi materi (gambar 2 dan 3)

e-ISSN : 2964 - 4533
p-ISSN : 2985-914X

PEMANAS: Jurnal Pengabdian Masyarakat Nasional
Vol. 3, No. 2 November 2023, Hal 122 - 130

Gambar 2. Pelaksanaan Penyampaian Pemateri



Gambar 3. Pelaksanaan Penyampaian Pemateri

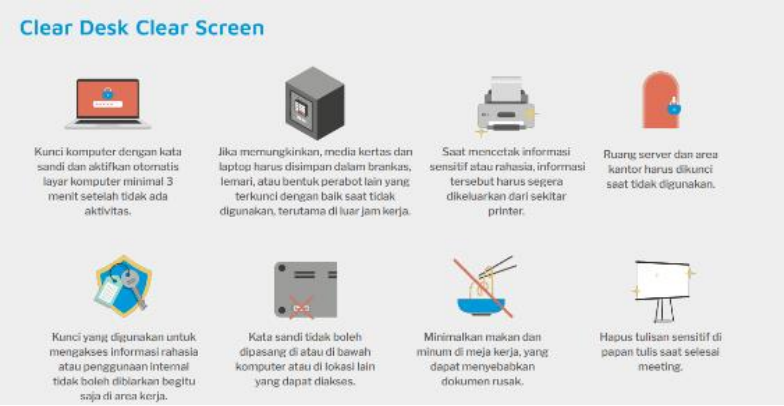
Materi pelatihan dimulai dengan pemaparan akan pentingnya kesadaran akan keamanan digital (gambar 4)

Gambar 4. Pentingnya Security Awareness

Setelah peserta memahami pentingnya keamanan dalam lingkup informasi, materi dilanjutkan dengan ini mengajarkan tiga cara yang perlu dilakukan untuk memastikan keamanan data bisa dijaga dengan lebih baik. Cara yang pertama adalah dengan Clean Desk Clear Screen (gambar 5)

e-ISSN : 2964 - 4533
p-ISSN : 2985-914X

PEMANAS: Jurnal Pengabdian Masyarakat Nasional
Vol. 3, No. 2 November 2023, Hal 122 - 130



Gambar 5. *Clear Desk Clear Screen*

Cara kedua menggunakan mobile device security (gambar 6) karena saat ini penggunaan handphone sudah sama seperti komputer atau laptop sehingga, keamanan digital pada handphone perlu dilakukan

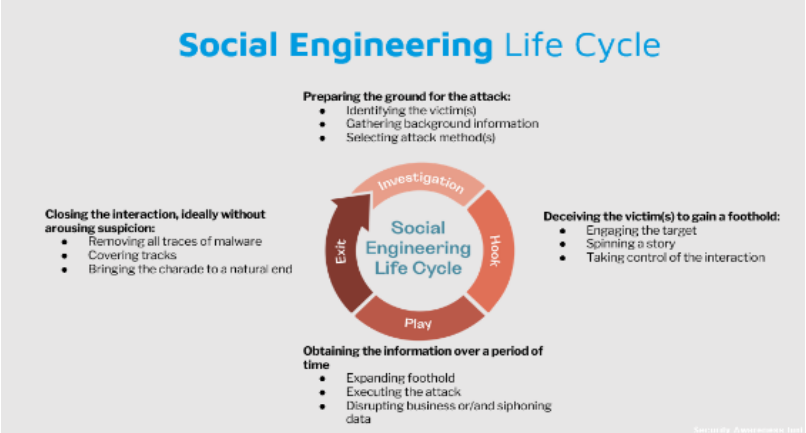
Gambar 6. *Mobile Device Security*

Cara ketiga melalui pendekatan secara fisik (gambar 7). Tidak hanya informasi dalam bentuk digital, banyak informasi penting berbentuk fisik. Konsep physical security mengedepankan ketelitian dan kehati-hatian dari pengguna.

Gambar 7. Physical Security

e-ISSN : 2964 - 4533
p-ISSN : 2985-914X
PEMANAS: Jurnal Pengabdian Masyarakat Nasional
Vol. 3, No. 2 November 2023, Hal 122 - 130

Selain memberikan cara untuk meningkatkan keamanan informasi, pelatihan ini juga memberikan materi pembelajaran yang terkait dengan jenis penyerangan yang umum dilakukan oleh orang yang tidak bertanggung jawab yang pertama yaitu social engineering. Ini adalah kegiatan untuk mendapatkan informasi rahasia/penting dengan cara menipu pemilik informasi tersebut. Proses social engineering terlihat pada gambar 8



Gambar 8. *Social Engineering Life Cycle*

Cara kedua yang dilakukan adalah phising. Ini merupakan tindakan yang dilakukan dengan modus mengambil identitas korban dengan menyamar sebagai institusi/perusahaan yang sah untuk memikat korban memberikan informasi sensitif. Serangan ini sering kali terjadi melalui email. Tahapan phising bisa dilihat pada gambar 9

Gambar 9. Serangan *Phishing*

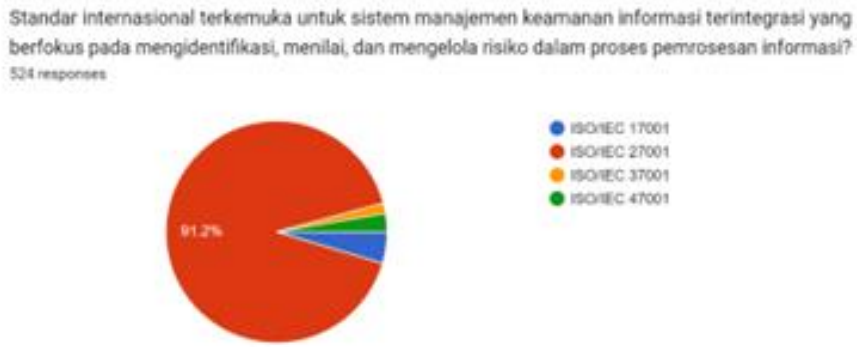
Penyampaian Undang-Undang yang berkaitan dengan perlindungan data pribadi juga disampaikan pada materi ini (gambar 10).

e-ISSN : 2964 - 4533
p-ISSN : 2985-914X

PEMANAS: Jurnal Pengabdian Masyarakat Nasional
Vol. 3, No. 2 November 2023, Hal 122 - 130

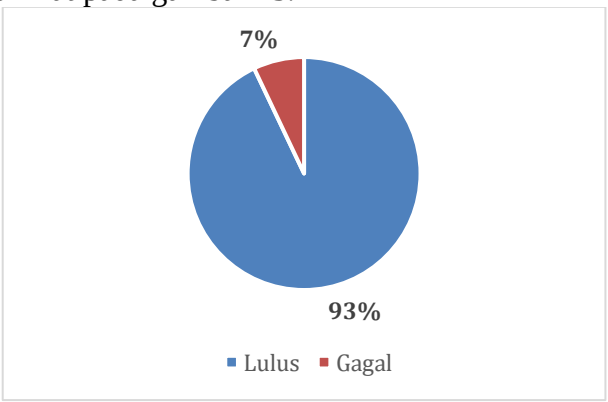
Gambar 10. Ketentuan UU Perlindungan Data Pribadi

Metode evaluasi menjadi metode yang terakhir dilakukan untuk mengetahui tingkat tercapainya tujuan dari pengabdian Masyarakat ini. Untuk memperoleh hasil tersebut, kuis terkait dengan materi cyber security awareness dilakukan melalui media gform dengan contoh salah satu pertanyaan dan hasil jawaban peserta dapat dilihat pada gambar 11 berikut ini



Gambar 11. Hasil Evaluasi Peserta

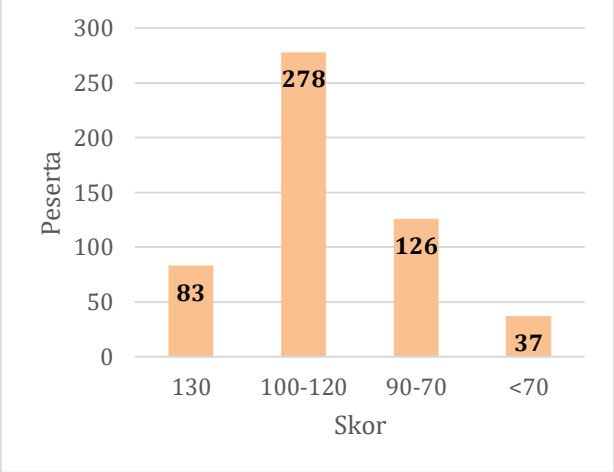
Begitu juga dengan hasil keseluruhan peserta pada gambar 12 dengan nilai maksimal yang bisa diperoleh peserta adalah 130 dengan batas standar kelulusan adalah 70. Hasil ini menunjukkan bahwa kurang dari 10% peserta yang masih kurang memahami cyber security karena memperoleh skor dibawah batas standar. Namun, lebih dari 90% peserta sudah mengetahui dan memahami pentingnya cyber security khususnya pada dunia perbankan karena memperoleh nilai lebih dari batas kelayakan. Rincian nilai peserta bisa dilihat pada gambar 13.



Gambar 12. Hasil Evaluasi Peserta

e-ISSN : 2964 - 4533
p-ISSN : 2985-914X

PEMANAS: Jurnal Pengabdian Masyarakat Nasional
Vol. 3, No. 2 November 2023, Hal 122 - 130



Gambar 13. Rincian Skor Peserta

4. KESIMPULAN

Berdasarkan kegiatan yang telah dilaksanakan dan hasil evaluasi selama kegiatan pengabdian masyarakat ini, dapat kami simpulkan bahwa program pengabdian masyarakat telah mampu memberikan manfaat bagi peserta pelatihan ini, terutama dalam membangun kesadaran dalam keamanan informasi di lingkungan bank, karyawan atau staf, Peserta dapat menyimak dengan baik dengan hasil evaluasi yang menunjukkan 93% peserta mampu menjawab soal dengan hasil skor melewati standar. Jadi pengabdian masyarakat ini dengan Judul Meningkatkan kesadaran cyber security di sektor perbankan digital dapat dinyatakan "BERHASIL"

Hasil pengabdian masyarakat ini diharapkan dapat berguna karyawan bank digital tersebut dan kegiatan pengabdian serupa dengan fokus yang berbeda di kemudian hari. Masih terdapat beberapa batasan atau kekurangan yang ada pada pengabdian Masyarakat ini, seperti isi dari pada kuesioner dalam beberapa pertanyaan yang mungkin kedepannya dapat ditingkatkan dan dikembangkan agar mendapatkan hasil yang memuaskan lagi. Kegiatan ini perlu dilakukan secara berkala.

5. UCAPAN TERIMAKASIH

Kami menyampaikan rasa terima kasih kami yang sebesar-besarnya kepada Bank Digital (Amar Bank) atas partisipasinya dalam acara pengabdian masyarakat ini. Kami juga berterima kasih kepada semua pihak yang terlibat karena telah memberikan dukungan mereka untuk memastikan kegiatan ini berjalan dengan baik.

REFERENSI

Bawany, N. Z., Shamsi, J. A., & Salah, K. (2017). DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions. *Arabian Journal for Science and Engineering*, *42*(2), 425–441. https://doi.org/10.1007/s13369-017-2414-5

Behal, S., & Kumar, K. (2017). Detection of DDoS attacks and flash events using information theory metrics–An empirical investigation. *Computer Communications*, *103*, 18–28. https://doi.org/https://doi.org/10.1016/j.comcom.2017.02.003

Fang, X., Xu, M., Xu, S., & Zhao, P. (2019). A deep learning framework for predicting cyber attacks rates. *EURASIP Journal on Information Security*, *2019*(1), 5. https://doi.org/10.1186/s13635-019-0090-6

Imam Suhartadi. (2021). *Webinar Cybersecurity Ignite 2021 Menambah Wawasan Keamanan Siber*. https://investor.id/it-and-telecommunication/267079/webinar-cybersecurity-ignite-2021-menambah-wawasan-keamanan-siber

e-ISSN : 2964 - 4533
p-ISSN : 2985-914X
PEMANAS: Jurnal Pengabdian Masyarakat Nasional
Vol. 3, No. 2 November 2023, Hal 122 - 130
Jia, Y., Qi, Y., Shang, H., Jiang, R., & Li, A. (2018). A Practical Approach to Constructing a Knowledge Graph for Cybersecurity. *Engineering*, *4*(1), 53–60. https://doi.org/https://doi.org/10.1016/j.eng.2018.01.004

Lehto, M. (2015). Cyber security competencies - Cyber security education and research in finnish universities. *European Conference on Information Warfare and Security, ECCWS*, *2015-Janua*(December), 179–188.

Maglaras, L. A., Kim, K.-H., Janicke, H., Ferrag, M. A., Rallis, S., Fragkou, P., Maglaras, A., & Cruz, T. J. (2018). Cyber security of critical infrastructures. *ICT Express*, *4*(1), 42–45. https://doi.org/https://doi.org/10.1016/j.icte.2018.02.001