p-ISSN: 2502-101X
e-ISSN: 2598-2400
Volume 10 Nomor 1 Tahun 2025

IMPLEMENTASI HUMAN FIREWALL UNTUK MENCEGAH ANCAMAN SOCIAL ENGINEERING DALAM MEWUJUDKAN KEAMANAN SIBER

Firman Faidin[1)], H.A. Danang Rimbawa[2)], J.W. Saputro[3)].

[1),2),3)] Program Studi Rekayasa Pertahanan siber, Fakultas Sains dan Teknologi Pertahanan, Universitas Pertahanan, Bogor, Indonesia
*e-mail: firman.faidin@tp.idu.ac.id

(*Received* 22 Oktober 2024, *Accepted* 17 Januari 2025)

Abstract

The rapid development of information and communication technology has provided many conveniences in various aspects of life. However, on the other hand, this also brings increasing cyber security threats, one of which is the threat of social engineering. Therefore, this research aims to analyze the implementation of a human firewall to prevent social engineering threats in realizing cyber security. The research method used is a qualitative research method with in-depth interviews with several key informants including cyber security managers, employees involved in training programs, and cyber security experts in PT. Mekar Armada Jaya Magelang. From the results of the research that has been carried out, it can be concluded that the implementation of a human firewall is effective in preventing social engineering threats and improving cyber security. The integration of enabling technology with human training strengthens the company's defenses, while clear security policies and top management support help overcome the challenges of participation and organizational culture change. However, challenges such as low employee participation and resistance to cultural change remain. For greater success, the training approach should be relevant to the employee's role, use technology to increase engagement, and involve employees in the development of training materials. The success and failure case studies found show that this strategy can be adapted and improved continuously.

Keywords: human firewall, cyber security, social engineering

Abstrak

Perkembangan teknologi informasi dan komunikasi yang begitu cepat dan telah memberikan banyak kemudahan dalam berbagai aspek kehidupan. Namun, di sisi lain, hal ini juga membawa ancaman keamanan siber yang semakin meningkat, salah satunya adalah ancaman social engineering. Oleh karena itu, penelitian ini bertujuan untuk menganalisis implementasi human firewall untuk mencegah ancaman social engineering dalam mewujudkan keamanan siber. Metode penelitian yang digunakan adalah metode penelitian kualitatif dengan wawancara mendalam kepada beberapa key informan diantaranya manajer keamanan siber, karyawan yang terlibat dalam program pelatihan, dan pakar keamanan siber di PT. Mekar Armada Jaya Magelang. Dari hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa implementasi human firewall efektif dalam mencegah ancaman social engineering dan meningkatkan keamanan siber. Integrasi teknologi yang memungkinkan dengan pelatihan manusia memperkuat pertahanan perusahaan, sementara kebijakan keamanan yang jelas dan dukungan manajemen puncak membantu mengatasi tantangan partisipasi dan perubahan budaya organisasi. Namun, tantangan seperti rendahnya partisipasi karyawan dan resistensi terhadap perubahan budaya tetap ada. Agar lebih berhasil, pendekatan pelatihan harus relevan dengan peran karyawan, menggunakan teknologi untuk meningkatkan keterlibatan, dan melibatkan karyawan dalam pengembangan materi pelatihan. Studi kasus keberhasilan dan kegagalan yang ditemukan menunjukkan bahwa strategi ini dapat diadaptasi dan ditingkatkan secara terus menerus.

Kata Kunci: *firewall manusia, keamanan siber, rekayasa sosial*

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang sangat cepat dan telah memberikan banyak kemudahan dalam berbagai aspek kehidupan (Hidayah, 2020). Rekayasa sosial adalah teknik manipulasi psikologis yang digunakan oleh penyerang untuk mengelabui

individu agar memberikan informasi rahasia atau melakukan tindakan tertentu yang dapat membahayakan keamanan sistem. (Wojcicki, 2019). Metode ini mengandalkan manipulasi emosi dan keyakinan manusia, bukan hanya serangan teknis yang mengeksploitasi kerentanan perangkat keras atau perangkat lunak. Penyerang rekayasa sosial sering kali berpura-pura menjadi entitas tepercaya seperti teman, kolega, atau institusi resmi, dan mereka menggunakan berbagai taktik seperti phishing, pretexting, baiting, dan tailgating (Alharthi & Regan, 2020). Phishing melibatkan pengiriman email atau pesan palsu yang tampaknya berasal dari sumber yang sah untuk mengelabui korban agar mengungkapkan kredensial login atau informasi pribadi lainnya. Pretexting membuat skenario palsu untuk mendapatkan akses ke informasi penting dengan berpura-pura menjadi seseorang yang memiliki otoritas. Baiting menggunakan umpan, seperti perangkat penyimpanan yang terinfeksi malware, untuk memikat korban.

Namun di sisi lain, hal ini juga membawa ancaman keamanan siber yang semakin meningkat. Keamanan siber yang juga dikenal sebagai keamanan informasi adalah praktik dan upaya yang dilakukan untuk melindungi sistem, perangkat, jaringan, dan data dari ancaman digital (Taib et al., 2019). Di era digital yang semakin terhubung ini, keamanan siber menjadi sangat penting untuk memastikan kerahasiaan, integritas, dan ketersediaan informasi serta sistem yang mengelolanya. Pentingnya keamanan siber tidak dapat diabaikan mengingat setiap kelompok atau individu semakin bergantung pada teknologi informasi dan komunikasi dalam menjalankan aktivitas sehari-hari (Dianta & Zusrony, 2019). Pelanggaran keamanan siber dapat menyebabkan konsekuensi yang signifikan seperti kebocoran data dan kerugian finansial hingga hilangnya kepercayaan dari pelanggan atau mitra bisnis.

Berbagai ancaman dapat mengancam keamanan siber, termasuk malware, yaitu perangkat lunak berbahaya seperti virus, worm, trojan, dan ransomware) dan serangan siber, yaitu upaya terkoordinasi untuk menembus sistem dan jaringan (Arfan Dwi Madya dkk, 2023). Salah satu ancaman keamanan siber yang semakin meningkat adalah rekayasa sosial. Rekayasa sosial mengacu pada taktik rekayasa sosial yang digunakan untuk mengelabui individu agar memberikan informasi rahasia atau melakukan tindakan yang menguntungkan penyerang. Rekayasa sosial mengeksploitasi kelemahan manusia seperti rasa ingin tahu, kepercayaan, atau ketakutan, untuk mendapatkan informasi atau akses tidak sah ke sistem atau jaringan.

Salah satu contoh serangan rekayasa sosial yang terkenal adalah insiden Target pada tahun 2013 (Witjaksono & Kriswibowo, 2023). Penyerang berhasil mengakses sistem pembayaran Target dengan mengeksploitasi kerentanan pada vendor pihak ketiga yang memiliki akses ke jaringan Target. Mereka menggunakan teknik phishing untuk mencuri kredensial login dari karyawan vendor dan kemudian menembus sistem target, yang mengakibatkan kebocoran data kartu kredit lebih dari 40 juta pelanggan. Insiden ini menunjukkan betapa seriusnya dampak serangan rekayasa sosial terhadap keamanan dan reputasi sebuah organisasi besar.

Studi kasus Vitadiar (2021) serangan rekayasa sosial yang signifikan menyoroti kerentanan yang ada pada sistem keamanan yang tidak memadai. Pada tahun 2016, sebuah perusahaan teknologi besar menjadi korban serangan phishing yang melibatkan email yang terlihat resmi yang meminta karyawan untuk mengklik tautan dan memasukkan kredensial login mereka. Hasilnya, penyerang berhasil mengakses sistem internal perusahaan dan mencuri data sensitif. Contoh lainnya adalah serangan pretexting yang menimpa sebuah perusahaan jasa keuangan pada tahun 2019, di mana penyerang menyamar sebagai penyedia layanan TI dan berhasil mengelabui karyawan untuk menginstal perangkat lunak berbahaya, yang kemudian memberikan akses penuh ke sistem perusahaan. (Ballqish, Amelia, 2023).

Ancaman rekayasa sosial menunjukkan bahwa kelemahan utama dalam sistem keamanan siber sering kali berasal dari faktor manusia. Bahkan teknologi keamanan yang

canggih sekalipun tidak akan efektif jika pengguna akhir tidak menyadari atau kurang terlatih dalam menghadapi ancaman-ancaman ini (Anthony, 2019). Oleh karena itu, konsep human firewall menjadi sangat penting dalam strategi keamanan siber. Firewall manusia mengacu pada serangkaian tindakan yang melibatkan pelatihan dan mendidik pengguna untuk meningkatkan kesadaran dan kemampuan mereka dalam mengenali dan mencegah serangan rekayasa sosial (Salama & Al-Turjman, 2023). Ini bukan hanya tentang teknologi, tetapi juga tentang menciptakan budaya keamanan di dalam organisasi. Menerapkan firewall manusia membutuhkan pendekatan yang komprehensif dan berkelanjutan. Program pelatihan harus dirancang untuk memberikan karyawan pengetahuan dan keterampilan yang diperlukan untuk mengidentifikasi dan menanggapi ancaman rekayasa sosial. Ini termasuk memahami berbagai teknik yang digunakan oleh penyerang, cara mengidentifikasi email phishing, dan tindakan apa yang harus dilakukan jika Anda mencurigai adanya upaya penipuan.

Keberhasilan penerapan firewall manusia juga tergantung pada dukungan dari manajemen puncak dan kebijakan perusahaan yang mendukung. Kebijakan keamanan yang jelas dan prosedur yang terdefinisi dengan baik akan memastikan bahwa semua anggota organisasi memahami peran mereka dalam menjaga keamanan siber. Prosedur respon yang cepat terhadap insiden keamanan juga penting untuk meminimalisir dampak yang ditimbulkan jika terjadi pelanggaran. Teknologi pendukung juga berperan penting dalam memperkuat firewall manusia. Alat-alat seperti sistem deteksi dan pencegahan intrusi, perangkat lunak anti-phishing, dan solusi manajemen identitas dapat membantu mengidentifikasi dan mencegah upaya rekayasa sosial. Namun, teknologi ini harus diintegrasikan dengan pelatihan manusia untuk mencapai hasil yang optimal. Pengguna perlu memahami cara menggunakan alat-alat ini dengan benar dan mengapa langkah-langkah keamanan tertentu perlu diikuti.

Beberapa penelitian seperti yang dilakukan oleh (Jensen et al., 2020) telah berhasil mengimplementasikan firewall manusia dengan hasil yang signifikan. Sebagai contoh, sebuah perusahaan multinasional berhasil mengurangi insiden phishing hingga 70% setelah menerapkan program pelatihan yang komprehensif dan berkelanjutan. Program ini mencakup pelatihan online, lokakarya, dan simulasi serangan phishing. Selain itu, perusahaan ini juga menerapkan kebijakan keamanan yang ketat dan menggunakan perangkat teknologi untuk mendeteksi dan mencegah serangan. Studi kasus ini menunjukkan bahwa dengan pendekatan yang tepat, firewall manusia dapat menjadi komponen yang efektif dalam strategi keamanan siber.

Namun, menerapkan firewall manusia juga memiliki tantangan dan keterbatasan. Tidak semua karyawan memiliki tingkat pemahaman atau minat yang sama terhadap pelatihan keamanan. Oleh karena itu, program pelatihan harus dirancang untuk menarik minat dan relevan dengan pekerjaan mereka sehari-hari. Selain itu, mengubah budaya organisasi membutuhkan waktu dan komitmen yang berkelanjutan dari semua tingkat manajemen. Untuk mengatasi tantangan-tantangan ini, perusahaan dapat mengadopsi pendekatan yang adaptif dan fleksibel, yang memungkinkan program pelatihan disesuaikan dengan kebutuhan spesifik karyawan dan organisasi (Bossomaier et al., 2019).

Pentingnya firewall manusia dalam mencegah ancaman rekayasa sosial tidak dapat diabaikan. Meskipun teknologi terus berkembang, faktor manusia tetap menjadi elemen kunci dalam menjaga keamanan siber. Dengan menggabungkan pelatihan, kebijakan yang tepat, dan teknologi yang mendukung, organisasi dapat menciptakan lingkungan yang lebih aman dan tahan terhadap serangan siber (Astakhova, 2020). Firewall manusia bukan hanya tentang melindungi data dan sistem, tetapi juga tentang membangun budaya keamanan yang kuat di seluruh organisasi.

Dari latar belakang yang telah disebutkan di atas, penelitian ini dilakukan untuk menganalisis implementasi human firewall untuk mencegah ancaman social engineering

dalam mewujudkan keamanan siber. Penelitian ini diharapkan dapat memberikan kontribusi yang signifikan terhadap literatur keamanan siber dan memberikan panduan praktis bagi organisasi dalam mengimplementasikan human firewall untuk meningkatkan keamanan siber mereka.

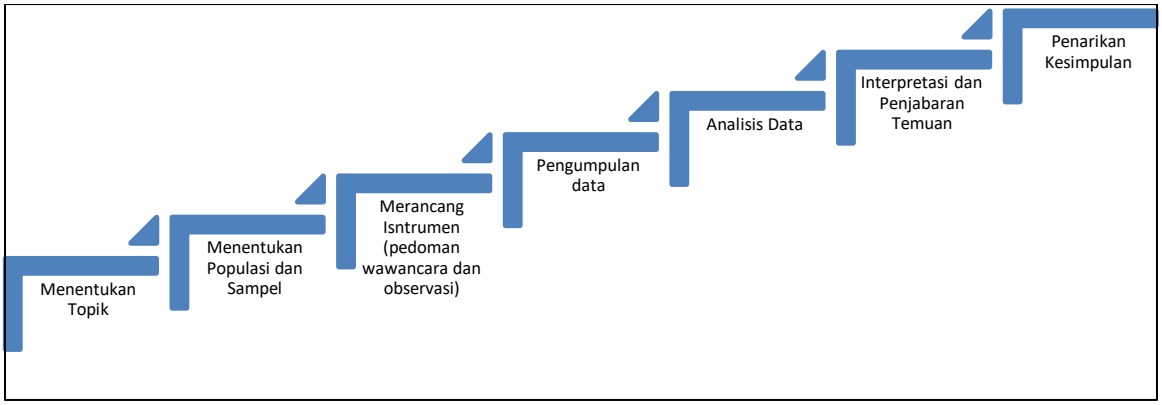
METODE

Penelitian ini menggunakan metode penelitian kualitatif untuk menganalisis Implementasi Human Firewall untuk Mencegah Ancaman Social Engineering dalam Mewujudkan Keamanan Siber. Pendekatan kualitatif dipilih karena memberikan pemahaman yang mendalam tentang pengalaman, persepsi, dan praktik yang terlibat dalam penerapan human firewall di berbagai organisasi. Menurut Best dan Kahn (Sandelowski, 1994). Istilah penelitian deskriptif sering digunakan untuk menggambarkan tiga jenis investigasi yang berbeda. Penelitian deskriptif adalah metode penelitian yang berusaha menggambarkan dan menginterpretasikan objek sesuai dengan keadaan yang sebenarnya (Morrow, 2001). Menurut Gay (Rowan & Wulff, 2007), metode Deskriptif adalah metode penelitian yang melibatkan pengumpulan data untuk menguji hipotesis atau menjawab pertanyaan mengenai kebenaran status subjek penelitian. Penelitian deskriptif menentukan dan melaporkan apa adanya.

Dalam sebuah penelitian, populasi dapat diartikan sebagai sasaran penelitian, responden, atau partisipan yang membantu peneliti dengan memberikan informasi yang berkaitan dengan topik penelitian. Menurut (Sudiyono, 2011) Populasi adalah generalisasi geografis yang meliputi: obyek/subyek yang mempunyai kualitas dan karakteristik tertentu yang ditetapkan oleh peneliti mengenai pembelajaran, dan kemudian ditarik kesimpulannya. Populasi adalah subjek penelitian (Arikunto, 2009). Penelitian ini menggunakan pendekatan wawancara dengan sasaran penelitian adalah beberapa informan kunci yaitu manajer keamanan siber, karyawan yang terlibat dalam program pelatihan, dan pakar keamanan siber di PT. Wawancara ini bertujuan untuk mengumpulkan perspektif tentang efektivitas pelatihan, tantangan yang dihadapi, dan strategi yang digunakan untuk meningkatkan kesadaran dan keterampilan karyawan dalam mengenali dan mencegah ancaman rekayasa sosial.

Data dalam penelitian ini merupakan data primer dimana peneliti mengumpulkannya langsung dari sumber pertama dan lokasi objek penelitian yang diterapkan. Data dalam penelitian ini diperoleh dari hasil wawancara langsung dengan pihak-pihak terkait. Dengan menggunakan daftar pertanyaan atau pertanyaan tertulis (kuesioner) dan melalui observasi atau pengamatan langsung di wilayah penelitian.

Peneliti mengumpulkan informasi/data dari responden manajer keamanan siber, karyawan yang terlibat dalam program pelatihan, dan pakar keamanan siber di PT. Mekar Armada Jaya Magelang. Dalam penelitian ini, dilakukan wawancara mendalam yang bertujuan untuk mengidentifikasi emosi, perasaan, dan pendapat partisipan mengenai subjek penelitian tertentu. Dalam penelitian ini, wawancara dilakukan secara tatap muka. Pertanyaan yang digunakan telah direncanakan dengan baik dan disusun secara hati-hati untuk menghasilkan jenis data yang dibutuhkan peneliti untuk menjawab pertanyaan penelitian. Skema tahapan penelitian dapat dilihat pada Gambar 1.



Gambar 1. Skema Tahapan Penelitian Skema Tahapan Penelitian

HASIL DAN PEMBAHASAN

Hasil

Dari hasil wawancara yang dilakukan, ditemukan beberapa temuan penting. Program pelatihan human firewall di PT. Mekar Armada Jaya dirancang secara komprehensif dan berkelanjutan. Karyawan dari berbagai departemen diwajibkan untuk mengikuti pelatihan dasar tentang keamanan siber, yang mencakup pengenalan teknik rekayasa sosial seperti phishing, pretexting, dan baiting.

"Kami menggunakan pendekatan berbasis kasus nyata untuk membuat materi pelatihan menjadi lebih relevan dan menarik," ujar seorang instruktur pelatihan. Modul pelatihan juga mencakup langkah-langkah praktis yang harus diambil jika karyawan mencurigai adanya upaya penipuan.

Namun, implementasi human firewall PT. Mekar Armada Jaya Magelang bukan tanpa tantangan. Salah satu masalah utama yang dihadapi adalah rendahnya tingkat partisipasi dan ketertarikan karyawan terhadap program pelatihan. "Beberapa karyawan merasa bahwa pelatihan ini tidak relevan dengan tugas mereka sehari-hari atau menganggapnya sebagai beban tambahan," kata manajer SDM. Untuk mengatasi masalah ini, perusahaan mulai mengintegrasikan materi keamanan siber ke dalam pelatihan reguler dan mempersonalisasi modul pelatihan agar lebih relevan dengan peran spesifik karyawan. Selain itu, mengubah budaya organisasi juga merupakan tantangan besar. "Membangun kesadaran keamanan siber bukanlah tugas yang mudah, terutama dalam organisasi yang besar dan beragam seperti kami," tambah manajer keamanan siber. Dukungan dari manajemen puncak sangat penting dalam mendorong perubahan budaya ini. Di PT. Mekar Armada Jaya Magelang, manajemen puncak menunjukkan komitmen mereka dengan terlibat langsung dalam sesi pelatihan dan mengkomunikasikan pentingnya keamanan siber di setiap kesempatan.

Untuk menjaga agar pengetahuan tetap segar, perusahaan mengadakan sesi pelatihan lanjutan setiap enam bulan sekali. Selain itu, simulasi serangan phishing dilakukan secara berkala untuk menguji kesiapan dan respon karyawan. "Simulasi ini sangat efektif untuk mengidentifikasi kelemahan dan memberikan pelajaran langsung kepada karyawan," jelas sang instruktur. Karyawan yang berhasil mengenali serangan diberi penghargaan, sementara mereka yang gagal mendapatkan sesi pembelajaran tambahan.

Untuk mengatasi tantangan ini, mereka mengadopsi pendekatan pelatihan yang lebih adaptif dan interaktif. "Kami menggunakan teknologi seperti e-learning dan gamifikasi untuk membuat pelatihan menjadi lebih menarik dan dapat diakses oleh semua karyawan," ujar seorang pengembang program pelatihan. Dengan modul yang dapat diakses kapan saja dan di mana saja, karyawan memiliki fleksibilitas yang lebih tinggi dalam mengikuti pelatihan. Perusahaan juga melibatkan karyawan dalam proses pengembangan materi pelatihan. "Dengan

melibatkan karyawan, mereka merasa lebih terlibat dan memiliki tanggung jawab yang lebih besar terhadap keamanan siber," jelas instruktur pelatihan. Karyawan diundang untuk berbagi pengalaman dan memberikan masukan tentang konten pelatihan, yang kemudian digunakan untuk meningkatkan program.

Perusahaan menggunakan berbagai perangkat teknologi seperti sistem deteksi dan pencegahan intrusi (IDS/IPS), perangkat lunak anti-phishing, dan solusi manajemen identitas untuk memperkuat pertahanan mereka. "Teknologi ini membantu kami mengidentifikasi dan mencegah upaya rekayasa sosial sejak dini," jelas seorang pakar keamanan siber di perusahaan tersebut. Namun, teknologi ini tidak akan efektif tanpa dukungan pengguna yang terlatih. Oleh karena itu, pelatihan juga mencakup cara menggunakan alat ini dengan benar. "Karyawan harus memahami bagaimana cara menggunakan teknologi ini dan mengapa langkah-langkah tertentu perlu diikuti," tambahnya. Sebagai contoh, karyawan dilatih untuk melaporkan email phishing yang terdeteksi oleh perangkat lunak anti-phishing, serta mengikuti prosedur keamanan yang telah ditetapkan ketika menggunakan sistem manajemen identitas.

Pembahasan

Salah satu temuan utama dari penelitian ini adalah bahwa penerapan *firewall* manusia telah terbukti efektif dalam meningkatkan kesadaran dan kemampuan karyawan untuk mengenali dan mencegah ancaman rekayasa sosial. Para informan kunci termasuk manajer keamanan siber dan karyawan yang terlibat dalam program pelatihan, melaporkan bahwa pelatihan yang komprehensif dan berkelanjutan memainkan peran penting dalam membangun pertahanan manusia yang kuat. Pelatihan ini mencakup modul-modul tentang pengenalan teknik-teknik rekayasa sosial, cara mengidentifikasi email phishing, dan langkah-langkah yang harus diambil ketika menghadapi upaya penipuan. Beberapa organisasi yang diamati telah berhasil mengurangi insiden phishing hingga 70% setelah menerapkan program pelatihan *firewall* manusia. Simulasi serangan rutin juga membantu karyawan untuk tetap waspada dan meningkatkan kemampuan mereka dalam menghadapi ancaman nyata. Program pelatihan berbasis kasus yang interaktif dan nyata membuat karyawan lebih mudah memahami dan mengingat langkah-langkah keamanan yang harus mereka lakukan.

Meskipun efektivitas *firewall* manusia sudah jelas, penelitian ini juga mengidentifikasi beberapa tantangan yang dihadapi dalam implementasinya. Salah satu tantangan utama adalah rendahnya tingkat partisipasi dan minat karyawan terhadap program pelatihan keamanan siber. Beberapa karyawan merasa bahwa pelatihan ini tidak relevan dengan pekerjaan mereka sehari-hari, atau mereka merasa terlalu sibuk untuk mengikuti pelatihan intensif. Hal ini menunjukkan bahwa pendekatan yang lebih personal dan relevan mungkin diperlukan untuk meningkatkan partisipasi. Selain itu, mengubah budaya organisasi juga merupakan tantangan besar. Mengubah pola pikir karyawan dari yang hanya mengandalkan teknologi untuk keamanan, menjadi lebih proaktif dalam menjaga keamanan siber melalui perilaku mereka sehari-hari, membutuhkan waktu dan komitmen yang berkelanjutan. Dukungan dari manajemen puncak sangat penting untuk mendorong perubahan budaya ini. Beberapa organisasi melaporkan bahwa manajemen yang kurang terlibat atau tidak memberikan dukungan penuh menjadi kendala dalam menerapkan program *human firewall*.

Penelitian ini menemukan beberapa strategi yang efektif untuk mengatasi tantangan-tantangan tersebut dan memperkuat penerapan *human firewall*. Pendekatan pelatihan yang adaptif dan disesuaikan dengan kebutuhan spesifik karyawan terbukti lebih berhasil dalam meningkatkan partisipasi dan efektivitas. Program pelatihan yang menggunakan studi kasus yang relevan dengan pekerjaan sehari-hari karyawan, serta memanfaatkan teknologi seperti e-learning dan gamifikasi, dapat membuat pelatihan menjadi lebih menarik dan mudah diakses (Diogenes & Ozkaya, 2019; Gulyas & Kiss, 2022). Selanjutnya, melibatkan karyawan dalam proses pelatihan melalui pendekatan interaktif dan kolaboratif juga dapat memberikan hasil

yang positif. Simulasi serangan, diskusi kelompok, dan latihan praktis membantu karyawan untuk lebih memahami dan mengingat langkah-langkah keamanan yang harus mereka ambil. Beberapa organisasi bahkan melibatkan karyawan dalam pengembangan materi pelatihan, sehingga mereka merasa lebih terlibat dan memiliki tanggung jawab yang lebih besar terhadap keamanan siber. Kebijakan keamanan yang mendukung dan prosedur yang jelas sangat penting untuk memastikan bahwa semua anggota organisasi memahami peran mereka dalam menjaga keamanan siber. Kebijakan yang mengatur penggunaan email, manajemen kata sandi, dan respons terhadap insiden keamanan harus disosialisasikan dengan baik kepada semua karyawan. Prosedur yang jelas dan mudah diikuti akan membantu karyawan mengambil tindakan yang tepat saat menghadapi ancaman.

Integrasi Teknologi dan Pelatihan

Integrasi antara teknologi pendukung dan pelatihan manusia juga ditemukan sebagai faktor penting dalam memperkuat *firewall* manusia. Alat-alat seperti sistem deteksi dan pencegahan intrusi, perangkat lunak anti-phishing, dan solusi manajemen identitas dapat membantu mengidentifikasi dan mencegah upaya rekayasa sosial. Namun, teknologi ini harus diintegrasikan dengan pelatihan yang memadai bagi pengguna untuk memanfaatkan alat ini secara efektif. Organisasi yang berhasil menerapkan *firewall* manusia umumnya menggunakan kombinasi pelatihan dan teknologi untuk menciptakan lapisan pertahanan yang lebih kuat. Sebagai contoh, penggunaan simulasi serangan phishing yang didukung oleh perangkat lunak anti-phishing dapat memberikan pengalaman langsung kepada karyawan tentang cara mengidentifikasi dan menanggapi serangan tersebut. Selain itu, penggunaan alat manajemen identitas yang memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses sistem, dapat mengurangi risiko akses yang tidak sah karena rekayasa sosial.

KESIMPULAN

Dari hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa implementasi human firewall di PT. Mekar Armada Jaya Magelang efektif dalam mencegah ancaman rekayasa sosial dan meningkatkan keamanan siber. Integrasi teknologi yang memungkinkan dengan pelatihan manusia memperkuat pertahanan perusahaan, sementara kebijakan keamanan yang jelas dan dukungan manajemen puncak membantu mengatasi tantangan partisipasi dan perubahan budaya organisasi. Namun, tantangan seperti rendahnya partisipasi karyawan dan resistensi terhadap perubahan budaya tetap ada. Agar lebih berhasil, pendekatan pelatihan harus relevan dengan peran karyawan, menggunakan teknologi untuk meningkatkan keterlibatan, dan melibatkan karyawan dalam pengembangan materi pelatihan. Studi kasus keberhasilan dan kegagalan yang ditemukan menunjukkan bahwa strategi ini dapat diadaptasi dan ditingkatkan secara terus menerus..

DAFTAR PUSTAKA

Alharthi, D. N., & Regan, A. C. (2020). Social engineering defense mechanisms: A taxonomy and a survey of employees' awareness level. Intelligent Computing: Proceedings of the 2020 …. https://doi.org/10.1007/978-3-030-52249-0_35

Anthony, B. (2019). Social Engineering: The Human Element of Cybersecurity. search.proquest.com. https://search.proquest.com/openview/de962d722378732c5e7e2cb9049cf9a1/1?pq-origsite=gscholar&cbl=18750&diss=y

Arfan Dwi Madya, Bagas Djoko Haryanto, & Devi Putri Ningsih. (2023). Keefektifan Metode Proteksi Data dalam Mengatasi Ancaman Cybersecurity. Indonesian Journal of

Education And Computer Science, 1(3), 127–135. https://doi.org/10.60076/indotech.v1i3.236

Arikunto, S. (2009). Dasar-Dasar Evaluasi Pendidikan. PT. Bumi Aksara.

Astakhova, L. V. (2020). A corporate employee is a subject of corporate information security management. Scientific and Technical Information Processing. https://doi.org/10.3103/S0147688220020069

Ballqish, Amelia, A. (2023). Perlindungan Hukum Terhadap Nasabah Bank Syariah Indonesia Dari Serangan Cybercrime. Journal of Engineering Research, 84. https://repository.uinjkt.ac.id/dspace/handle/123456789/74011%0Ahttps://repository.uinjkt.ac.id/dspace/bitstream/123456789/74011/1/BALLQISH AMELIA ASSIFFA - FSH.pdf

Bossomaier, T., D'Alessandro, S., & Bradbury, R. (2019). Human dimensions of cybersecurity. books.google.com. https://books.google.com/books?hl=en&lr=&id=8lW9DwAAQBAJ&oi=fnd&pg=PP1&dq=human+firewall++social+engineering+cyber+security&ots=itEV7TWhSy&sig=KKJXA2EMedJsGadgu9cl2t_Zjgg

Dianta, I. A., & Zusrony, E. (2019). Analisis Pengaruh Sistem Keamanan Informasi Perbankan Pada Nasabah Pengguna Internet Banking. INTENSIF: Jurnal Ilmiah Penelitian Dan Penerapan Teknologi Sistem Informasi, 3(1), 1. https://doi.org/10.29407/intensif.v3i1.12125

Diogenes, Y., & Ozkaya, E. (2019). Cybersecurity–Attack and Defense Strategies: Counter modern threats and employ state-of-the-art tools and techniques to protect your organization against …. books.google.com. https://books.google.com/books?hl=en&lr=&id=E7zHDwAAQBAJ&oi=fnd&pg=PP1&dq=human+firewall++social+engineering+cyber+security&ots=tmpeGymugS&sig=H7Cc1b_owUECL_LHw9nxsCJLhTU

Gulyas, O., & Kiss, G. (2022). Cybersecurity threats in the banking sector. … on Control, Decision and Information …. https://ieeexplore.ieee.org/abstract/document/9804140/

Hidayah, I. R. (2020). Representasi Social Engineering Dalam Tindak Kejahatan Dunia Maya (Analisis Semiotika Pada Film Firewall). Tibanndaru : Jurnal Ilmu Perpustakaan Dan Informasi, 4(1), 30. https://doi.org/10.30742/tb.v4i1.905

Jensen, M. L., Wright, R., Durcikova, A., & ... (2020). Building the Human Firewall: Combating Phishing through Collective Action of Individuals Using Leaderboards. Available at SSRN …. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3622322

Morrow, V. (2001). Using qualitative methods to elicit young people's perspectives on their environments: some ideas for community health initiatives. Health Education Research. https://academic.oup.com/her/article-abstract/16/3/255/703087

Rowan, N., & Wulff, D. (2007). Using qualitative methods to inform scale development. Qualitative Report. https://eric.ed.gov/?id=EJ800203

Salama, R., & Al-Turjman, F. (2023). Cyber-Security Countermeasures and Vulnerabilities to Prevent Social-Engineering Attacks. Artificial Intelligence of Health-Enabled …. https://doi.org/10.1201/9781003322887-7

Sandelowski, M. (1994). Focus on qualitative methods. The use of quotes in qualitative research. Research in Nursing &health. https://doi.org/10.1002/nur.4770170611

Sudiyono, A. (2011). Pengantar Evaluasi Pendidikan. Rajawali Pers.

Taib, R., Yu, K., Berkovsky, S., Wiggins, M., & ... (2019). Social engineering and organizational dependencies in phishing attacks. … on Human-Computer …. https://doi.org/10.1007/978-3-030-29381-9_35

Vitadiar, T. Z., Permadi, G. S., Putra, R. A. Y., & Putri, U. S. (2021). Etika &Hukum Cyber. eprints.unhasy.ac.id. https://eprints.unhasy.ac.id/230/

Witjaksono, D. K., & Kriswibowo, A. (2023). Fondasi Kemananan Siber Untuk Layanan Pemerintah. Al-Ijtima`i: International Journal of Government and Social Science, 9(1), 21–38. https://doi.org/10.22373/jai.v9i1.2057

Wojcicki, N. M. (2019). Phishing Attacks: Preying on Human Psychology to Beat the System and Developing Cybersecurity Protections to Reduce the Risks. World Libraries. http://worldlibraries.dom.edu/index.php/worldlib/article/view/579