Jurnal Informatika Universitas Pamulang **ISSN: 2541-1004**
Penerbit: Fakultas Ilmu Komputer Universitas Pamulang **e-ISSN: 2622-4615**
Vol. 8, No. 4, Desember 2023 (642-648) **https://doi.org/10.32493/informatika.v8i4.35931**

Analisa Penyerangan untuk Cyber Security Social Engineering

Afrizal Zein[1*]
[1]Information Sistem, Universitas Pamulang, Indonesia
e-mail:[1]dosen01495@unpam.ac.id
*Corresponding author

Submitted Date: November 25th, 2023 Reviewed Date: December 4th, 2023
Revised Date: December 20th, 2023 Accepted Date: December 30th, 2023

Abstract

In the increasingly advanced digital era, threats to cyber security are increasing. One frequently used attack technique is social engineering, which involves psychological and social manipulation of individuals to gain confidential information or access to computer sistems. To counter this threat, there needs to be an effective solution. This study presents a critical analysis of such measures and tools to better address these issues. To combat cybersecurity social engineering, organisations have policies in place. These policies are implemented through a sistematic approach to ensure the protection of sensitive information. After conducting a comprehensive evaluation of recent research studies on the subject, our examination revealed the need to offer. To ensure an understanding of social engineering risks and the optimal methods to deal with them, employee training is essential. To prevent falling victim to harmful schemes, it is important to take protective measures. These measures can include introducing awareness programmes, educating non-technical personnel, implementing new security networks, using specialised software, and enforcing security protocols. The issue of social engineering is a major threat that cannot be ignored. It is important to take this issue seriously and implement measures that can protect individuals and organisations.

Keywords: Social Engineering Threats, Security Policies, Social Engineering Solutions.

Abstrak

Dalam era digital yang semakin maju, ancaman pada keamanan *cyber* semakin meningkat. Salah satu teknik serangan yang sering digunakan adalah *social engineering*, yang melibatkan manipulasi psikologis dan sosial terhadap individu untuk mendapatkan informasi rahasia atau akses ke sistem komputer. Untuk mengatasi ancaman ini, perlu ada solusi yang efektif. Studi ini menyajikan analisis kritis terhadap langkah-langkah dan alat-alat tersebut untuk mengatasi masalah-masalah ini dengan lebih baik. Untuk memerangi rekayasa sosial keamanan siber, organisasi mempunyai kebijakan yang sudah ada. Kebijakan-kebijakan ini diterapkan melalui pendekatan sistematis untuk memastikan perlindungan informasi sensitif. Setelah melakukan evaluasi komprehensif terhadap studi penelitian terbaru mengenai subjek ini, pemeriksaan kami mengungkapkan perlunya menawarkan. Untuk menjamin pemahaman tentang risiko rekayasa sosial dan metode optimal untuk menanganinya, pelatihan karyawan sangatlah penting. Untuk mencegah agar tidak menjadi korban skema yang merugikan, penting untuk mengambil tindakan perlindungan. Langkah-langkah ini dapat berupa memperkenalkan program kesadaran, mendidik personel non-teknis, menerapkan jaringan keamanan baru, menggunakan perangkat lunak khusus, dan menegakkan protokol keamanan. Isu rekayasa sosial merupakan ancaman besar yang tidak bisa diabaikan. Penting untuk menanggapi masalah ini dengan serius dan menerapkan langkah-langkah yang dapat melindungi individu dan organisasi.

Kata Kunci: Ancaman Rekayasa Sosial, Kebijakan Keamanan, Solusi Rekayasa Sosial.

1. Pendahuluan

Ancaman siber semakin kompleks, dan salah satu metode serangan yang paling menonjol adalah *social Engineering*(Razzaq et al., 2022). Pendahuluan ini membahas urgensi dan perluasan isu *social engineering* dalam lingkup keamanan siber dan mengenalkan solusi untuk menghadapinya. *Social engineering* adalah teknik

ISSN: 2541-1004
e-ISSN: 2622-4615
https://doi.org/10.32493/informatika.v8i4.35931

serangan yang mengandalkan manipulasi psikologis dan persuasi untuk memanipulasi individu atau entitas kepercayaan agar mengungkapkan informasi sensitif, seperti kata sandi, data pribadi, atau akses ke sistem. Taktik seperti *phising, pretexting*, dan insinyur sosial lainnya digunakan secara luas untuk meretas jaringan, mencuri data, atau menyebabkan kerugian serius. Ancaman *social engineering* telah berkembang menjadi serangan yang semakin canggih dan ditargetkan.

Serangan *social engineering* dapat menyebabkan kerugian finansial yang besar, hilangnya data penting, dan merusak reputasi individu, perusahaan, atau entitas. Dalam beberapa kasus, serangan tersebut dapat mengancam keberlanjutan operasional organisasi atau merusak kepercayaan publik(Slamet, 2022).

Dengan perubahan tren kerja yang semakin mengarah pada fleksibilitas dan akses jarak jauh ke sistem dan data, peluang bagi penyerang *social engineering* untuk mengeksploitasi kerentanan dalam sistem dan perilaku individu semakin besar. Keadaan ini menimbulkan kebutuhan mendesak untuk memahami dan menghadapi ancaman ini. Banyak individu, baik dalam konteks pribadi maupun bisnis, mungkin tidak cukup sadar akan bahaya *social engineering* dan bagaimana cara mengidentifikasi serta melindungi diri dari serangan ini. Edukasi dan pemahaman yang lebih baik sangat diperlukan.

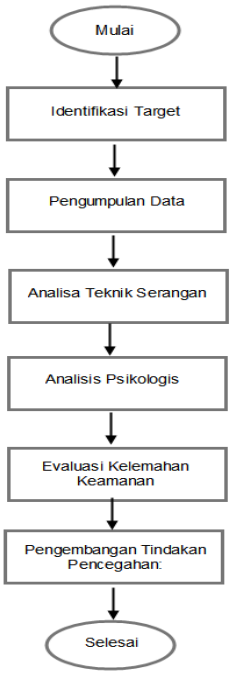
Definisi serangan yang direkayasa secara sosial seperti yang dinyatakan oleh adalah "eksploitasi psikologis yang digunakan penipu untuk memanipulasi kelemahan manusia dengan terampil dan melakukan serangan emosional terhadap orang yang tidak bersalah. " Rekayasa sosial melampaui kerentanan teknis dari pengguna sistem(Tyas Darmaningrat et al., 2022). Ini adalah tindakan penipuan di mana pengguna yang menjadi korban dimanipulasi untuk mengungkapkan informasi rekayasa sosial termasuk *phishing* informasi rahasia dan serangan yang ditargetkan berdasarkan informasi yang diperoleh. Serangan siber yang direkayasa secara sosial seperti itu termasuk gangguan atau infeksi sistem informasi yang kompleks, transfer dana yang tidak sah, dan pencurian kredensial.

Hasil analisis kami mengungkapkan kesenjangan mendasar dalam keamanan saat ini pendekatan kesadaran keamanan saat ini. Kami menyediakan peta jalan yang menunjukkan cara mengatasi kesenjangan ini di masa depan. Peta jalan kami merupakan visi instrumental untuk mengurangi ancaman sosial dengan menangani semua aspek psikologis yang relevan dalam pertahanannya(Magister, Diajukan, Rahmadani, & Sekar Putri, 2022).

Tujuan penelitian dari Analisis Penyerangan untuk *Cyber Security Social Engineering* adalah menganalisis dan mengidentifikasi berbagai taktik yang digunakan dalam serangan *social engineering* dan Memahami bagaimana penyerang memanipulasi psikologi individu untuk mendapatkan akses atau informasi sensitif(Kaur & Ramkumar, 2022).

2. Metode Penelitian

Metodologi yang digunakan dalam penelitian ini adalah analisis kualitatif. Tinjauan literatur yang sistematis dilakukan dalam penelitian ini untuk menilai langkah-langkah industri saat ini, kebijakan, dan alat untuk mengatasi ancaman rekayasa sosial(Wibowo & Fatimah, 2017).



Gambar 1. *FlowChart* Proses Perancangan Penelitian.

a. Mulai

Langkah awal dalam penelitian adalah memulai proses analisis penyerangan *social engineering.*

b. Identifikasi Target.

Tentukan target penelitian, apakah itu individu, perusahaan, atau kelompok tertentu yang menjadi sasaran penyerangan.

c. Pengumpulan Data

Kumpulkan informasi terkait serangan, termasuk modus operandi, teknik *social engineering* yang digunakan, dan sumber daya yang dimanfaatkan oleh penyerang.

d. Analisis Teknik Serangan

Identifikasi dan analisis teknik-teknik yang digunakan dalam penyerangan *social engineering*, seperti rekayasa sosial*, phishing, pretexting*, dll.

e. Analisis Psikologis

Pahami faktor psikologis yang dimanfaatkan oleh penyerang, seperti kepercayaan, ketidaktahuan, atau keinginan untuk membantu.

f. Evaluasi Kelemahan Keamanan

Tinjau sistem keamanan yang ada dan identifikasi kelemahan atau celah yang dapat dimanfaatkan oleh penyerangan *social engineering*.

g. Pengembangan Tindakan Pencegahan

Berdasarkan temuan analisis, kembangkan strategi dan tindakan pencegahan untuk meningkatkan keamanan dan mengurangi risiko serangan.

h. Selesai

Selesaikan penelitian dan pastikan bahwa langkah-langkah pencegahan telah diimplementasikan.

Analisis ini akan memeriksa lebih lanjut hasil yang dicapai oleh organisasi setelah mengadopsi berbagai upaya tersebut. Studi ini menggunakan berbagai strategi pencarian literatur dan basis data, serta kriteria untuk menentukan inklusi dan eksklusi literatur. Strategi pencarian yang digunakan didasarkan pada langkah-langkah, kebijakan, dan alat yang direkomendasikan untuk mengatasi ancaman rekayasa sosial. Studi ini menggunakan berbagai *database* untuk menemukan literatur yang mengidentifikasi atau menyajikan langkah-langkah, kebijakan, dan alat yang diadopsi oleh industri untuk mengatasi ancaman rekayasa sosial(Dwi Madya, Djoko Haryanto, Ningsih, & Sinlae, 2023). Basis data yang digunakan adalah Embase, EBSCO, Google Scholar, dan IEEE Xplore. Strategi pencarian menggunakan pola kata kunci untuk mencari literatur yang relevan. Kata kunci yang Kata kunci yang digunakan adalah 'rekayasa sosial', 'ancaman siber', 'ancaman rekayasa sosial', 'tindakan rekayasa sosial', 'kebijakan rekayasa sosial', 'alat rekayasa sosial', 'solusi rekayasa rekayasa sosial', 'aplikasi rekayasa sosial', 'perangkat lunak untuk ancaman rekayasa sosial', dan 'alat dan perangkat lunak untuk ancaman rekayasa sosial'. Literatur atau artikel dengan satu atau beberapa kemunculan satu atau beberapa kata kunci dipertimbangkan untuk kriteria kelayakan. Sebanyak 2.973 karya yang relevan muncul terhadap kata kunci yang digunakan. literatur yang relevan muncul terhadap kata kunci yang digunakan. Untuk memisahkan dan menyaring studi, kriteria kelayakan literatur diimplementasikan untuk menentukan apakah sebuah buku akan disertakan atau tidak disertakan dalam penelitian ini.

Alat yang paling kuat yang digunakan penyerang dalam serangan yang direkayasa secara sosial adalah akses ke pengetahuan yang berkaitan dengan sebuah organisasi dan juga para penggunanya (Anggraeni Vigim, Sofia, Nelly Nur Apandi, & Purnomo, 2021). Karena rekayasa sosial peretas sering menggunakan manipulasi, pelanggaran sistem suatu organisasi dapat dikendalikan dengan alat pencegahan seperti *firewall*, alat keamanan jaringan, dan alat penanganan respons insidental. Alat untuk melawan serangan yang direkayasa secara sosial dikembangkan oleh organisasi berdasarkan implementasi agregat yang tersedia yang tersedia pada saat itu.

Karena serangan yang direkayasa secara sosial telah menjadi perdagangan yang menguntungkan, organisasi membutuhkan kontemporer untuk mengidentifikasi kerentanan mereka. Menerapkan konfigurasi *proxy* otomatis seperti *firewall* kontrol grup, membantu dalam membatasi aktivitas jaringan yang berbahaya di sisi pengguna akhir(Putu, Pratama, Eka, & Arista, 2019). Proxy secara eksplisit memaksa setiap komunikasi jaringan keluar dari suatu organisasi menjadi disisir melalui *proxy* penyaringan konten. Menerapkan konfigurasi *proxy* otomatis juga membantu mengontrol akses pengguna ke Internet melalui browser web dan menyediakan data jaringan yang lebih aman perdagangan manusia. Memaksa lalu lintas data yang sah untuk dialihkan melalui server *proxy* dan menerapkan Penyaringan jalan keluar dapat mencegah *malware* mempengaruhi sistem informasi organisasi.

Selain itu, mengingat fakta bahwa domain spam tidak berbasis reputasi, domain spam yang baru lahir yang baru lahir di alam dapat menimbulkan masalah. IP di bawah spam yang baru lahir seperti itu digunakan untuk meluncurkan serangan dalam beberapa menit setelah mendaftarkan teknologi yang ada, yang tidak selalu cukup untuk mengatasi masalah ini. Namun, (Anggraini & Sutabri, 2024) yang ditingkatkan terhadap inspeksi *host* yang baru lahir yang baru lahir akan memberikan lapisan perlindungan tambahan bagi perusahaan. Penyaringan kontemporer ini adalah efektif dalam

mengidentifikasi spam, ancaman tingkat lanjut, *phishing*, dan serangan rekayasa sosial.

Selain itu, penggunaan filter ini yang dikombinasikan dengan pencarian domain *real-time* yang cepat menggunakan data besar teknik korelasi akan mengatasi masalah domain berbahaya yang baru lahir.

Keandalan alat pendeteksi *malware* bergantung pada kode. Untuk perlindungan tambahan yang ditingkatkan, biometrik digunakan untuk mengatasi masalah positif palsu dalam sistem verifikasi identitas(Hadiprakoso et al., 2021).

Dengan alat biometrik terkini seperti pengenalan wajah, tanda tangan suara, dan sidik jari, peluang akses ilegal diminimalkan. Alat biometrik juga sangat terkait dengan karyawan dan identitas pribadi mereka. Ciri-ciri biometrik tidak dapat dengan mudah diduplikasi atau dibagikan, yang membuatnya lebih tahan dan lebih unggul untuk pencegahan terhadap serangan yang direkayasa secara sosial daripada metode tradisional kata sandi saja. Pengenalan biometrik membutuhkan pengguna pada saat otentikasi, yang mencegah pengguna menyangkal klaim palsu dan memeriksa serangan pada tingkat pengguna untuk mencegah serangan sekunder sekunder dan serangan tersier. Selain itu, alat biometrik menangkal metode penyimpanan fisik seperti otentikasi, yang tidak didasarkan pada identitas yang dirasakan karyawan. Sebaliknya, ini membedakan pengguna yang sah berdasarkan ciri-ciri unik dari sifat biologis mereka.

Organisasi juga dapat mengadopsi sistem inferensi *neuro fuzzy* menggunakan jaringan syaraf, untuk perlindungan yang lebih baik terhadap rekayasa sosial. Menggabungkan sistem inferensi fuzzy, menggunakan model buatan digunakan untuk kemampuan belajar mandiri. Logika dapat dirancang untuk membuat *phishing* yang dapat memprediksi sendiri pendekatan deteksi dan menggunakannya untuk daftar hitam URL, untuk memastikan peretas tidak dapat menggeneralisasikannya. Daftar hitam situs dapat mencegah serangan terhadap kelemahan manusia.

Beberapa perusahaan memilih untuk menggunakan intelijen berbasis lokasi untuk verifikasi yang lebih baik dari lokasi yang tepat orang yang berwenang bertransaksi dengan sistem informasi organisasi. Informasi ini biasanya dikumpulkan melalui perangkat karyawan dan interaksi dapat diverifikasi di seluruh saluran. Perusahaan semakin meningkatkan keamanan mereka melalui Pertanyaan Keamanan Dinamis, di mana perusahaan mengharuskan karyawan untuk menyimpan satu langkah proses otentikasi pada catatan pribadi, untuk memprediksi peretasan yang direkayasa secara sosial(Surya Mahendra Muhammad Wali Harry Idwan & Eka Yuliastuti Dimas Sasongko Gede Arna Jude Saskara Alfina, 2022).

3. Hasil dan Pembahasan

Hasil Analisis Penyerangan *Cyber Security* :

Serangan yang dianalisis adalah serangan *social engineering* dengan fokus pada rekayasa sosial dan teknik *phishing*.

Sasaran serangan terutama adalah karyawan perusahaan ABC, dengan penyerang berupaya mendapatkan akses ke data sensitif dan informasi kredensial. Penyerang menggunakan informasi publik dari media sosial dan situs web perusahaan untuk membuat skenario rekayasa sosial yang meyakinkan. Mereka menciptakan situasi darurat atau kebutuhan mendesak untuk mengecoh karyawan.

Serangan *phishing* dilakukan melalui *email* palsu yang menyamar sebagai komunikasi internal perusahaan. Tautan atau lampiran berbahaya digunakan untuk mencuri informasi *login* atau menginstal *malware*. menggunakan alat dan teknik yang melibatkan penyamaran identitas dan penyusupan digital. Jejak digital menunjukkan bahwa serangan ini berasal dari server yang disamarkan dan sulit untuk dilacak. Penyerang diduga merupakan kelompok atau individu yang memiliki pengetahuan teknis yang cukup dan akses ke sumber daya yang memadai. Motivasi mereka kemungkinan besar terkait dengan pencurian data untuk keuntungan finansial.

Kelemahan dalam kesadaran keamanan karyawan, kurangnya pelatihan keamanan siber, dan kebijakan keamanan yang lemah adalah faktor utama yang memfasilitasi serangan ini.

Tidak ada bukti korelasi langsung dengan serangan keamanan siber sebelumnya. Namun, serangan ini memiliki beberapa kesamaan dengan tren serangan *social engineering* yang terjadi secara global.

Peningkatan kesadaran keamanan karyawan melalui pelatihan dan pendidikan. Penguatan kebijakan keamanan perusahaan, termasuk verifikasi identitas yang ketat. Implementasi sistem deteksi *phishing* yang canggih dan pemantauan jejak digital secara *real-time*. Pembaruan keamanan perangkat lunak dan sistem operasi secara teratur.

Pengenalan sistem keamanan yang lebih canggih, termasuk sistem deteksi ancaman dan keamanan yang dapat beradaptasi.

3.1 *Phishing* Sosial

Phishing sosial menggunakan teknik yang melibatkan akun media sosial karyawan di platform seperti seperti Facebook dan Twitter. Tujuan dari serangan tersebut adalah untuk mendapatkan akses ke jaringan organisasi organisasi melalui akun pribadi jejaring sosial. Serangan biasanya dirancang dalam bentuk posting dan tautan yang mengarahkan pengguna ke situs web berbahaya. Pencerminan halaman media sosial yang digunakan oleh karyawan yang tidak menaruh curiga adalah titik akses lain yang semakin sering digunakan oleh para insinyur sosial menggunakan. Aplikasi palsu, dan tautan yang diposting oleh penyerang untuk menarik perhatian karyawan menjadi tantangan tersendiri bagi keamanan organisasi terhadap serangan yang direkayasa secara sosial.

3.2 Serangan *Spear Phishing*

Spear-phishing merupakan tahap awal dalam serangan *Advanced Persistent Threat (APT*), yang dilakukan untuk menciptakan titik masuk ke dalam sebuah sistem informasi. Jenis serangan ini menargetkan target tertentu kelompok staf tertentu dalam suatu organisasi. *Spear phishing* dirancang dengan menyisir profil sosial, situs web, dan blog karyawan. Beberapa serangan *phishing* bahkan mungkin mengandung *malware* seperti Trojan, yang diarahkan untuk tujuan utama memata-matai industri. Salah satu tujuan utama dari *spearphishing* adalah melakukan penipuan keuangan.

3.3 Pencurian Merek

Peretas mengotomatiskan eksploitasi seperti pencurian merek untuk memikat staf. Dalam pencurian merek, karyawan ditipu percaya bahwa mereka berinteraksi dengan layanan atau situs web yang sah. Ini bersifat sosial serangan yang direkayasa secara sosial ini menggunakan metode *typosquatting* (pembajakan URL) atau mendaftarkan domain mereka nama domain mereka dengan sedikit kesalahan pengejaan. Domain-domain tersebut diubah secara tipografi untuk mengelabui pengguna yang tidak memperhatikan *header email*. *Typosquatting* menyebabkan pelanggaran merek dagang dan hilangnya kepercayaan pada organisasi asli.

3.4 Penipuan E-mail

Di antara semua teknik serangan yang direkayasa secara sosial, penipuan email adalah yang paling bergantung pada faktor manusia untuk berhasil. Perekayasa sosial menggunakan teknik ini untuk meningkatkan kepanikan di antara karyawan. Contohnya termasuk 'Panggilan Pengacara', 'surat tawaran pekerjaan' atau pemberitahuan dari IRS (Internal Revenue Services)(Henderson et al., 2023). Organisasi dapat terkena serangan seperti itu, di mana email tersebut dirancang agar terlihat seperti berasal dari tingkat manajemen internal yang lebih tinggi. *Spoofing* ini Tren ini menunjukkan bahwa serangan yang direkayasa secara sosial beradaptasi dan menyesuaikan diri dengan organisasi upaya organisasi dalam menetapkan tindakan pencegahan.

Namun, literatur telah dengan jelas menunjukkan yang terpenting dari keempat masalah ini, dan akar penyebab potensial untuk mereka, adalah kurangnya pengguna, administrasi, dan rekayasa sosial organisasi kesadaran. Dengan demikian, fokus utama dari penelitian saya adalah dalam konteks spesifik kesadaran rekayasa sosial dalam domain keamanan siber. Lebih khusus lagi, keadaan saat ini penelitian di bidang ini menunjukkan bahwa kesadaran rekayasa sosial dan efektif untuk mengatasi ancaman rekayasa sosial sangat kurang.

Penelitian yang ditinjau menunjukkan beberapa keterbatasan yang mungkin dihadapi organisasi saat menerapkan penanggulangan, kebijakan, dan alat untuk mencegah serangan rekayasa sosial. Pertama, keterbatasan dalam mengimplementasikan langkah-langkah pencegahan muncul dari kemampuan, keahlian, pendidikan, dan pendidikan, dan ciri-ciri kepribadian personel. Perbedaan di antara staf dapat menyebabkan tantangan besar dalam proses implementasi tindakan pencegahan. Selain itu, perbedaan dalam pelatihan pelatihan dan tingkat kesadaran di antara karyawan juga membatasi tingkat keberhasilan penanggulangan ini . Teknik peretas untuk mendapatkan informasi spesifik organisasi terus berkembang. Menyimpan data sensitif tergantung pada kemampuan manajemen untuk membujuk dan meyakinkan karyawan untuk mengubah perilaku mereka dalam mengekspos informasi rahasia rahasia yang dapat digunakan oleh peretas.

Analisis implementasi kebijakan mengungkapkan bahwa kesalahan manusia dalam mengikuti kebijakan merupakan tantangan yang dihadapi organisasi saat menangani tindakan

pencegahan terhadap serangan serangan yang direkayasa. Literatur juga menunjukkan bahwa kurangnya pernyataan kebijakan yang jelas menghambat kemampuan karyawan untuk memahami peran mereka dalam proses pencegahan. Selain itu, pencegahan proaktif melalui pengawasan memakan waktu dan mahal bagi bisnis karena mengganggu operasi sehari-hari. Terakhir, keterbatasan dalam proses kebijakan keamanan implementasi kebijakan keamanan untuk mengendalikan rekayasa sosial muncul dari hambatan kurangnya kejelasan kebijakan, dan fakta bahwa ada alat yang terbatas untuk melawan serangan semacam itu.

Analisis kami terhadap alat pencegahan yang digunakan oleh organisasi modern terhadap serangan rekayasa sosial mengidentifikasi keterbatasan yang berasal dari ancaman baru yang direkayasa setiap hari. Alat-alat seperti *malware* dan *firewall* juga perlu diperbarui secara teratur untuk memastikan perlindungan tepat waktu perusahaan. Selain itu, alat seperti biometrik menawarkan tantangan seperti rentan terhadap serangan. Alat-alat Kecerdasan Buatan (AI) mahal untuk diimplementasikan dan juga membutuhkan basis pengetahuan yang besar untuk memastikan perlindungan informasi yang menyeluruh. Tingkat profesionalisme, kemam-puan, dan kelengkapan karyawan untuk menggunakan alat tersebut sebagai penanggulangan juga telah disorot dalam literatur sebagai tantangan penting yang yang dihadapi organisasi dalam proses pencegahan.

Di antara tiga parameter tindakan, kebijakan, dan alat untuk melawan serangan yang direkayasa secara sosial serangan yang direkayasa secara sosial, tantangan yang menonjol muncul dari kemampuan karyawan untuk memahami baru yang dapat menjadi sumber kebocoran informasi. Kemampuan karyawan untuk membedakan antara informasi rahasia dan non-rahasia memastikan keamanan organisasi dari rekayasa sosial(Nissim & Wood, 2018). Analisis kritis dari studi yang ditinjau menyoroti bahwa keterbatasan ini dimitigasi dengan meningkatkan kesadaran pengguna akan serangan rekayasa sosial. Peningkatan program kesadaran keamanan informasi tentang perlindungan kata sandi, tidak berbagi informasi terkait pekerjaan di media sosial dan situs web *game* lainnya semuanya dapat dimasukkan untuk meningkatkan meningkatkan kesadaran mereka tentang ancaman yang sebenarnya. Dengan menerapkan program kesadaran ini, organisasi dapat memastikan bahwa karyawan mereka mengetahui semua metode dan teknik rekayasa sosial terbaru teknik terbaru. Kesadaran seperti itu mencegah karyawan menjadi mangsa serangan.

5. Kesimpulan

Analisis penyerangan dalam konteks keamanan siber dengan pendekatan *social engineering* menunjukkan bahwa serangan ini merupakan strategi yang canggih dan kompleks. Beberapa kesimpulan yang dapat ditarik dari analisis ini melibatkan pemahaman tentang cara penyerang memanipulasi faktor sosial untuk mencapai tujuan keamanan siber mereka:
(1) Keterlibatan Faktor Sosial. Penyerangan *social engineering* memanfaatkan aspek-aspek psikologis dan sosial manusia, seperti kepercayaan, ketidaktahuan, dan keinginan untuk membantu. Penyerang mencoba memanipulasi korban agar mengambil tindakan yang merugikan keamanan. (2) Teknik Manipulasi. Analisis menunjukkan adanya berbagai teknik manipulasi, seperti rekayasa sosial, *phishing, pretexting,* dan *baiting*. Penyerang menggunakan metode ini untuk merayu, menipu, atau memancing informasi rahasia dari korban. (3) Peluang Melalui Komunikasi Digital. Serangan ini sering kali dimulai melalui komunikasi digital, seperti email, pesan instan, atau media sosial. Penyerang dapat menyamarkan identitas mereka untuk meningkatkan peluang agar korban terperdaya. (4) Kurangnya Kesadaran Keamanan. Analisis menunjukkan bahwa kurangnya kesadaran keamanan di kalangan pengguna sering kali menjadi celah yang dimanfaatkan oleh penyerang. Pendidikan dan pelatihan keamanan siber bagi pengguna menjadi kunci dalam mencegah serangan ini. (5) Keamanan Organisasi dan Individu. Perusahaan dan individu perlu meningkatkan langkah-langkah keamanan mereka, termasuk penggunaan teknologi keamanan yang canggih, pemantauan aktivitas mencurigakan, dan implementasi kebijakan keamanan yang ketat.
(6) Penyadaran dan Pelatihan. Kesimpulan analisis menekankan pentingnya penyadaran dan pelatihan terkait keamanan siber di semua tingkatan, baik dalam lingkungan bisnis maupun kehidupan sehari-hari. Pengguna yang sadar akan keamanan dapat lebih baik mengidentifikasi potensi serangan.
(7) Kerja sama dan Pertukaran Informasi. Organisasi dan individu perlu bekerja sama dalam pertukaran informasi terkait serangan *social engineering. Sharing best practices*, teknik serangan yang baru muncul, dan indikator serangan dapat memperkuat pertahanan secara kolektif.

Referensi

Anggraeni Vigim, J., Sofia, A., Nelly Nur Apandi, R., & Purnomo, B. (2021). *Identifikasi Risiko Sistem Informasi Teknologi pada Perguruan Tinggi*. *Jurnal Ilmu Manajemen dan Bisnis* (Vol. 12).

Anggraini, D., & Sutabri, T. (2024). IJM: Indonesian Journal of Multidisciplinary Pengembangan Aplikasi Penyaringan Spam e-Mail Menggunakan Teknik Machine Learning dengan Metode Support Vector Machines. *IJM: Indonesian Journal of Multidisciplinary*, *2*. Retrieved from https://journal.csspublishing/index.php/ijm

Dwi Madya, A., Djoko Haryanto, B., Ningsih, D. P., & Sinlae, F. (2023). Keefektifan Metode Proteksi Data dalam Mengatasi Ancaman Cybersecurity. *INDOTECH Indonesian Journal of Education And Computer Science*, *1*(3), 2023.

Hadiprakoso, R. B., Qomariasih, N., Yasa, R. N., Kriptografi, R., Siber, P., Negara, S., & Usa, J. H. (2021). *Identifikasi Malware Androidmenggunakan Pendekatan Analisis Hibrid Dengan Deep Learning*.

Henderson, P., Chugg, B., Anderson, B., Altenburger, K., Turk, A., Guyton, J., … Ho, D. E. (2023). *Integrating Reward Maximization and Population Estimation: Sequential Decision-Making for Internal Revenue Service Audit Selection*. Retrieved from www.aaai.org

Kaur, J., & Ramkumar, K. R. (2022, September 1). The recent trends in cyber security: A review. *Journal of King Saud University - Computer and Information Sciences*. King Saud bin AbdulazizUniversity. https://doi.org/10.1016/j.jksuci.2021.01.018

Magister, P., Diajukan, A., Rahmadani, O., & Sekar Putri, N. (2022). *Analisa Pola-Pola Sosialisasi Pencegahan Modus Social Engineering Oleh Bank Melalui Media Website dan Media Sosial Twitter Tesis S2*.

Nissim, K., & Wood, A. (2018). Is privacy privacy? *Philosophical Transactions of the Royal Society A: Mathematical, Physical and EngineeringSciences*,*376*(2128). https://doi.org/10.1098/rsta.2017.0358

Putu, I., Pratama, A. E., Eka, G., & Arista, Y. (2019). Penerapan Proxy Server Berbasis Clearos 7 Untuk Manajemen Akses Pada Internet. *Jurnal Mantik Penusa*, *3*(1), 66. Retrieved from www.clearos.com

Razzaq, A., Aditya, M., Widya, A., Kuncoro Putri, O., Musthofa, D. L., & Widodo, P. (2022). Serangan Hacking Tools sebagai Ancaman Siber dalam Sistem Pertahanan Negara (Studi Kasus: Predator). *Global Political Studies Journal*,*6*. https://doi.org/10.34010/gpsjournal.v6i1

Slamet. (2022). *Pertahanan Pencegahan Serangan Social Engineering Menggunakan Two Factor Authentication (2fa) Berbasis Sms (Short Message System)*. *Nopember* (Vol. 14).

Surya Mahendra Muhammad Wali Harry Idwan, G., & Eka Yuliastuti Dimas Sasongko Gede Arna Jude Saskara Alfina, G. (2022). *Keamanan Komputer*.

Tyas Darmaningrat, E. W., Noor Ali, A. H., Herdiyanti, A., Subriadi, A. P., Muqtadiroh, F. A., Astuti, H. M., & Susanto, T. D. (2022). Sosialisasi Bahaya dan Upaya Pencegahan Social Engineering untuk Meningkatkan Kesadaran Masyarakat tentang Keamanan Informasi.*Sewagati*,*6*(2). https://doi.org/10.12962/j26139960.v6i2.92

Wibowo, M. H., & Fatimah, N. (2017). *ANCAMAN* Phishing Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime (Vol. 1).