ANALISIS TINGKAT KESADARAN KEAMANAN SIBER PENGGUNA TERHADAP ANCAMAN SCIAL ENGINEERING

Nurul Fauzia[1], Nur Annisa Afriliyani Anwar[2], Farhan Fachruddin[3], Rakhmadi Rahman[4]
nrlfauziah2211@gmail.com[1], nuranisaanwar18@gmail.com[2],
farhanfarhanfachruddin@gmail.com[3], rakhmadi.rahman@ith.ac.id[4]
Institusi Teknologi Bacharuddin Jusuf Habibie

ABSTRAK

Perkembangan teknologi informasi yang pesat menyebabkan meningkatnya ancaman keamanan siber, salah satunya adalah serangan social engineering. Serangan ini memanfaatkan manipulasi psikologis pengguna untuk memperoleh informasi sensitif, sehingga faktor manusia menjadi titik lemah utama dalam sistem keamanan siber. Penelitian ini bertujuan untuk menganalisis tingkat kesadaran keamanan siber pengguna terhadap ancaman social engineering berdasarkan dimensi pengetahuan, sikap, dan perilaku. Metode penelitian yang digunakan adalah pendekatan kualitatif deskriptif melalui studi literatur dengan menganalisis lima jurnal ilmiah yang relevan. Hasil penelitian menunjukkan bahwa tingkat kesadaran keamanan siber pengguna berada pada kategori sedang. Pengguna umumnya memiliki pengetahuan dasar mengenai social engineering, namun penerapan perilaku keamanan yang konsisten masih rendah. Hal ini menunjukkan adanya kesenjangan antara pengetahuan dan perilaku pengguna dalam menghadapi ancaman social engineering. Oleh karena itu, diperlukan upaya peningkatan kesadaran keamanan siber melalui edukasi dan pelatihan yang berkelanjutan guna mengurangi risiko serangan social engineering.
Kata Kunci: Keamanan Siber, Social Engineering, Kesadaran Pengguna, Keamanan Informasi.

ABSTRACT

The rapid development of information technology has led to an increase in cybersecurity threats, particularly social engineering attacks. These attacks exploit human psychological vulnerabilities to obtain sensitive information, making the human factor the weakest link in cybersecurity systems. This study aims to analyze the level of users' cybersecurity awareness toward social engineering threats based on the dimensions of knowledge, attitude, and behavior. The research employs a qualitative descriptive approach through a literature review by analyzing five relevant academic journals. The results indicate that users' cybersecurity awareness is generally at a moderate level. Although users possess basic knowledge of social engineering, consistent implementation of secure behavior remains limited. This finding highlights a gap between users' knowledge and their actual behavior in responding to social engineering threats. Therefore, continuous cybersecurity education and training are essential to improve user awareness and reduce the risk of social engineering attacks.
Keywords: *Cybersecurity, Social Engineering, User Awareness, Information Security.*

PENDAHULUAN

Perkembangan teknologi informasi yang pesat membawa dampak signifikan terhadap peningkatan ancaman keamanan siber. Salah satu ancaman yang paling sering terjadi adalah social engineering, yaitu teknik serangan yang memanfaatkan manipulasi psikologis manusia untuk memperoleh informasi sensitif atau akses ke sistem. Berbeda dengan serangan teknis, social engineering lebih menargetkan kelemahan faktor manusia, sehingga sering kali berhasil meskipun sistem keamanan teknologi telah diterapkan. Rendahnya tingkat kesadaran keamanan siber pengguna menjadi salah satu penyebab utama keberhasilan serangan social engineering. Banyak pengguna masih kurang memahami bentuk-bentuk serangan seperti phishing, smishing, dan vishing, serta belum menerapkan perilaku aman dalam aktivitas digital sehari-hari. Kondisi ini menunjukkan

bahwa keamanan siber tidak hanya bergantung pada teknologi, tetapi juga pada tingkat pengetahuan, sikap, dan perilaku pengguna. Oleh karena itu, diperlukan analisis terhadap tingkat kesadaran keamanan siber pengguna dalam menghadapi ancaman social engineering. Penelitian ini bertujuan untuk mengkaji tingkat kesadaran tersebut berdasarkan dimensi pengetahuan, sikap, dan perilaku, sehingga dapat menjadi dasar dalam merancang strategi edukasi keamanan siber yang lebih efektif.

Tinjauan Pustaka

A. Keamanan Siber

Keamanan siber merupakan upaya untuk melindungi sistem informasi, jaringan, dan data dari berbagai ancaman digital yang dapat mengganggu kerahasiaan, integritas, dan ketersediaan informasi. Keamanan yang efektif tidak hanya bergantung pada teknologi, tetapi juga pada kesadaran dan perilaku pengguna sebagai bagian dari sistem.

B. Social Engineering

Social engineering adalah metode serangan yang memanfaatkan manipulasi psikologis untuk menipu pengguna agar memberikan informasi sensitif atau melakukan tindakan tertentu. Bentuk serangan social engineering yang umum meliputi phishing, smishing, dan vishing. Serangan ini sulit dideteksi karena menyerupai interaksi normal dan memanfaatkan tingkat kepercayaan pengguna.

C. Model Knowledge–Attitude–Behaviour (KAB)

Model Knowledge–Attitude–Behaviour (KAB) digunakan untuk mengukur tingkat kesadaran pengguna terhadap keamanan siber. Model ini menilai kesadaran melalui tiga aspek utama, yaitu pengetahuan pengguna tentang keamanan, sikap pengguna terhadap risiko keamanan, dan perilaku aktual pengguna dalam menerapkan praktik keamanan siber.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode studi literatur. Data penelitian diperoleh dari lima jurnal ilmiah yang membahas kesadaran keamanan siber, social engineering, dan perilaku pengguna. Jurnal-jurnal tersebut dianalisis untuk mengidentifikasi tingkat kesadaran pengguna berdasarkan model Knowledge–Attitude–Behaviour (KAB). Tahapan penelitian meliputi pengumpulan literatur yang relevan, pengelompokan data berdasarkan dimensi pengetahuan, sikap, dan perilaku, serta analisis deskriptif untuk menarik kesimpulan mengenai tingkat kesadaran keamanan siber pengguna terhadap ancaman social engineering.

HASIL DAN PEMBAHASAN

Hasil analisis menunjukkan bahwa secara umum tingkat kesadaran keamanan siber pengguna berada pada kategori sedang. Dari aspek pengetahuan, sebagian besar pengguna telah mengenal istilah social engineering dan bentuk serangannya, namun pemahaman mendalam mengenai mekanisme dan ciri-ciri serangan masih terbatas. Hal ini menyebabkan pengguna sulit membedakan antara komunikasi asli dan komunikasi palsu. Dari aspek sikap, pengguna cenderung menyadari pentingnya keamanan siber, tetapi sering kali menganggap risiko serangan sebagai hal yang jarang terjadi. Sikap kurang waspada ini meningkatkan peluang keberhasilan serangan social engineering, terutama ketika serangan dikemas dalam bentuk yang meyakinkan. Pada aspek perilaku, hasil penelitian menunjukkan bahwa masih banyak pengguna yang belum konsisten menerapkan praktik keamanan, seperti memverifikasi sumber informasi, menjaga kerahasiaan data pribadi, dan menghindari tautan mencurigakan. Temuan ini menunjukkan adanya kesenjangan antara pengetahuan dan perilaku, sehingga edukasi keamanan siber

perlu difokuskan tidak hanya pada peningkatan pengetahuan, tetapi juga pada perubahan perilaku pengguna.

KESIMPULAN

Berdasarkan hasil penelitian, dapat disimpulkan bahwa tingkat kesadaran keamanan siber pengguna terhadap ancaman social engineering masih belum optimal. Meskipun pengguna memiliki pengetahuan dan sikap yang cukup baik, penerapan perilaku aman dalam aktivitas digital masih perlu ditingkatkan. Faktor manusia tetap menjadi titik lemah utama dalam sistem keamanan siber.

Saran

Diperlukan upaya berkelanjutan untuk meningkatkan kesadaran keamanan siber pengguna melalui program edukasi, pelatihan, dan simulasi serangan social engineering. Selain itu, penelitian selanjutnya dapat mengembangkan metode pengukuran kesadaran pengguna secara kuantitatif atau mengimplementasikan sistem edukasi interaktif untuk meningkatkan perubahan perilaku pengguna.

DAFTAR PUSTAKA

Allen, M. (2007). Social engineering: A means to violate a computer system. SANS Institute.

Andress, A. (2007). Surviving security: How to integrate people, process, and technology. Taylor & Francis.

Gartner. (2005). Management update: How business can defend against social engineering attacks. Gartner Research.

Hoare, C. A. R. (1978). Communicating Sequential Processes. Communications of the ACM, 21(8), 666–677.

Rafizan, O. (2011). Analisis penyerangan social engineering. Jurnal Keamanan Informasi, 115–126.

Rahmawati, R., & Putra, D. A. (2021). Measurement of information security awareness level: A case study of mobile banking app users to prevent social engineering. Syntax Idea, 3(8), 1681–1694.