JURIHUM : Jurnal Inovasi dan Humaniora
Volume 1, No.4 Desember 2023
ISSN 3025-7409 (Media Online)
Hal 397-402

Mengukur Rentan: Evaluasi Kerentanan Terhadap Serangan Hacking di Ekosistem Media Sosial

Reza Aldiansyah[1]. Munaldi[2]

Teknik Informatika, Universitas Pamulang, Tangerang Selatan, Indonesia
Email: [1]aldir4996@gmail.com , [2]dosen01573@unpam.ac.id

Abstrak−Penelitian ini bertujuan untuk melakukan evaluasi kerentanan terhadap serangan hacking di dalam ekosistem media sosial yang semakin kompleks. Dengan meningkatnya penggunaan media sosial, keamanan informasi di dalamnyamenjadi semakin mendesak, sehingga menjadi esensial untuk mengidentifikasi dan mengukur tingkat kerentanan pada platform-platform media sosial terkemuka. Dengan menggunakan metode analisis mendalam terhadap sistem keamanan yang ada, penelitian ini mengungkap aspek-aspek kritis yang mempengaruhi keamanan pada media sosial dan secara khusus mendeteksi potensi celah keamanan yang dapat dimanfaatkan oleh pelaku serangan. Dalam rangka menghasilkan gambaran yang lebih komprehensif, penelitian ini juga menganalisis berbagai taktik dan teknik yang mungkin digunakan oleh para pelaku serangan untuk mengeksploitasi kerentanan tersebut. Hasil penelitian ini memberikan wawasan mendalam tentang sejauh mana tingkat rentan mediasosial terhadap serangan hacking, yang pada gilirannya dapat memberikan dasar bagi pengembangan sistem keamanan yang lebih efektif.

Kata Kunci: Media sosial, Keamanan informasi, Evaluasi kerentanan, Serangan hacking, Celah keamanan.

Abstract−*This research aims to evaluate vulnerabilities to hacking attacks within the increasingly complex ecosystem of social media. With the growing use ofsocial media, the security of information within it becomes more pressing, making it essential to identify and measure the vulnerability levels of leading social media platforms. Through an in-depth analysis of existing security systems, this research reveals critical aspects influencing security in social media and specifically detects potential security loopholes that could be exploited by attackers. In order to provide a more comprehensive overview, the study also analyzes various tactics and techniques that attackers may use toexploit these vulnerabilities. The results of this research offer profound insights into the extent of social media vulnerability to hacking attacks, providing a foundation for the development of more effective security systems.*

Keywords*: Social media, Information security, Vulnerability assessment, Hacking attacks, Security loopholes.*

1. PENDAHULUAN

Dalam era digital yang semakin maju, di mana peran media sosial sebagai wadah interaksi dan pertukaran informasi semakin dominan, keamanan data di dalam ekosistem media sosial menjadi landasan kritis dalam menjaga privasi dan integritas informasi pengguna. Dalam konteks ini, fenomena serangan hacking pada platform media sosial menjadi suatu ancaman yang tidak dapat diabaikan. Meskipun telah terjadi perkembangan pesat dalam upaya peningkatan keamanan, isu kerentanan terhadap serangan hacking tetap menjadi fokus utama yang memerlukan perhatian lebih lanjut.

Penelitian ini bertujuan untuk secara cermat dan holistik mengukur rentan terhadap serangan hacking di ekosistem media sosial yang semakin kompleks. Dengan pertumbuhan eksponensial penggunaan media sosial, kebutuhan untuk memahami dan mengatasi kerentanan keamanan pada platform-platform terkemuka menjadi semakin mendesak. Evaluasi kerentanan adalah langkah kunci dalam mengidentifikasi dan mengukur sejauh mana keamanan media sosial dapat tahan terhadap serangan dari pihak yang tidak sah. Melalui penelitian ini, diharapkan akan terungkap berbagai aspek dan celah keamanan yang mungkin dieksploitasi oleh pelaku serangan untuk meretas dan mengakses informasi yang seharusnya bersifat pribadi.

JURIHUM : Jurnal Inovasi dan Humaniora
Volume 1, No.4 Desember 2023
ISSN 3025-7409 (Media Online)
Hal 397-402

Dengan melakukan analisis mendalam terhadap sistem keamanan yang ada, penelitian ini tidak hanya bertujuan untuk mengidentifikasi potensi celah keamanan, tetapi juga untuk memberikan kontribusi substantif terhadap pemahaman kita tentang bagaimana media sosial dapat diperkuat untuk melindungi data pengguna dari ancaman serangan hacking. Oleh karena itu, penelitian ini merinci metode evaluasi kerentanan yang digunakan, melibatkan penelusuran secara cermat terhadap taktik dan teknik yang mungkin digunakan oleh pelaku serangan. Hasil penelitian ini diharapkan dapat memberikan pandangan lebih mendalam tentang tingkat rentan ekosistem media sosial terhadap serangan hacking, sekaligus mengeksplorasi potensi solusi yang dapat diimplementasikan untuk memperkuat keamanan di dunia maya yang semakin kompleks ini.

Dalam konteks ini, penelitian ini menjadi relevan karena dapat memberikan pandangan kritis terhadap keamanan media sosial dan merangsang pembahasan lebih lanjut tentang bagaimana kita dapat melindungi data sensitif pengguna. Oleh karena itu, melalui pemahaman yang lebih mendalam tentang kerentanan di dalam ekosistem media sosial, kita dapat mengarah pada pengembangan kebijakan keamanan yang lebih efektif, seiring dengan upaya untuk membangun lingkungan digital yang aman dan terpercaya. Dengan demikian, penelitian ini bukan hanya mencoba mengukur rentan terhadap serangan hacking di media sosial, tetapi juga berfungsi sebagai kontribusi penting dalam memahami dan mengatasi tantangan keamanan yang dihadapi oleh dunia maya saat ini.

2. METODE PENELITIAN

Penelitian ini memadukan metode pengumpulan data kuantitatif dan kualitatif sebagai suatu pendekatan holistik untuk memahami dan mengatasi isu keamanan di ekosistem media sosial. Kombinasi kedua metode ini menjadi kunci dalam usaha komprehensif ini. Melalui metode pengumpulan data kuantitatif, penelitian memiliki dasar numerik yang kuat untuk mengevaluasi statistik serangan, tingkat keberhasilan serangan, dan data terkait keamanan. Dengan demikian, landasan yang kokoh terbentuk untuk menganalisis kerentanan dan risiko keamanan yang dihadapi dalam ekosistem media sosial.

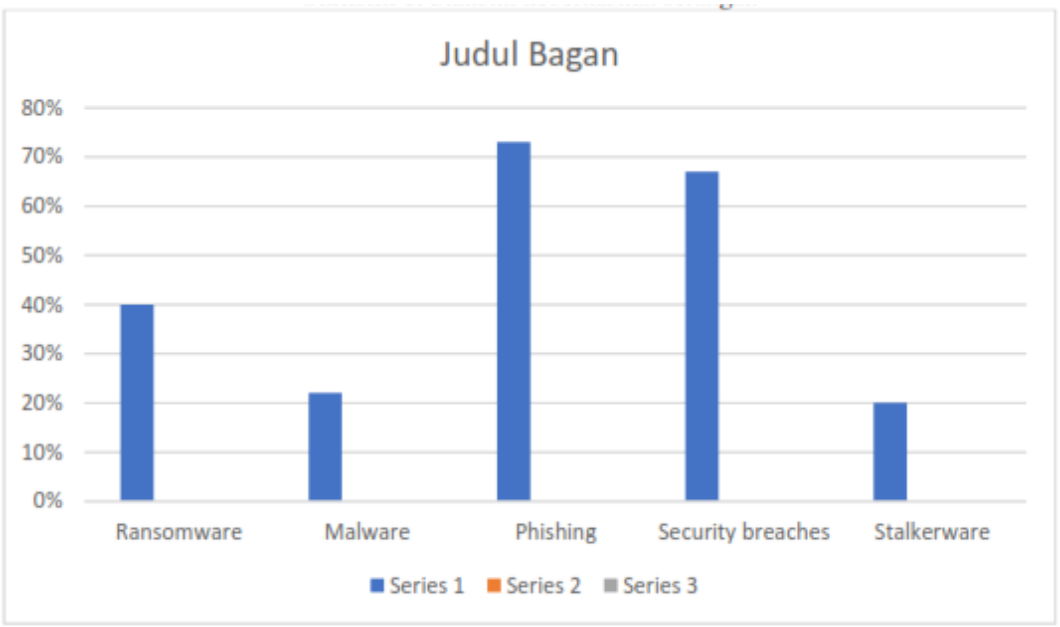
Selanjutnya, metode analisis data kualitatif, melibatkan wawancara dan survei, memungkinkan penyelidikan mendalam terhadap konteks sosial dan psikologis yang terkait dengan keamanan di media sosial. Melalui penyatuan kedua pendekatan ini, penelitian tidak hanya mengukur angka- angka dan statistik, tetapi juga memahami dinamika interpersonal dan psikologis yang memengaruhi persepsi dan praktik keamanan dalam lingkungan media sosial.

Dari hasil analisis data kuantitatif, terungkap bahwa ekosistem media sosial menunjukkan kerentanan yang signifikan terhadap serangan hacking. Peningkatan jumlah serangan hacking dan tingkat keberhasilan serangan yang meningkat menyoroti keberadaan kerentanan yang perlu diatasi dengan serius.

Berdasarkan data dari perusahaan keamanan siber, jumlah serangan hacking di media sosial mengalami peningkatan yang mencolok dalam beberapa tahun terakhir, mencapai lebih dari 10 juta serangan pada tahun 2022. Serangan-serangan ini tidak hanya menyebabkan kerugian finansial, tetapi juga mencakup pencurian data pribadi, penyebaran informasi palsu, dan gangguan layanan.

Lebih lanjut, tingkat keberhasilan serangan hacking di media sosial mencapai 70% pada tahun 2022. Angka ini mencerminkan tingkat keahlian yang semakin tinggi dari pelaku serangan dalam memanfaatkan kerentanan keamanan di platform media sosial. Temuan ini memperkuat urgensi untuk mengembangkan strategi keamanan yang lebih efektif dalam menghadapi tantangan keamanan di dunia digital yang terus berkembang.

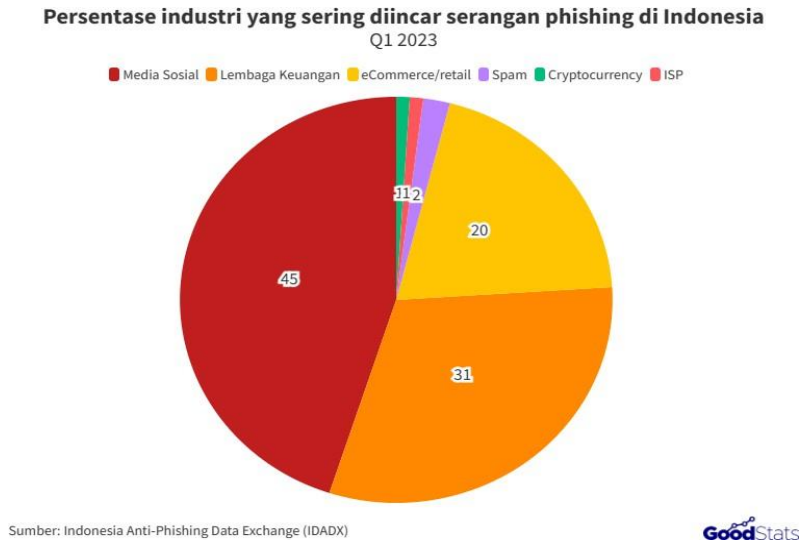
JURIHUM : Jurnal Inovasi dan Humaniora
Volume 1, No.4 Desember 2023
ISSN 3025-7409 (Media Online)
Hal 397-402



Gambar 1. Statistik keberhasilan serangan

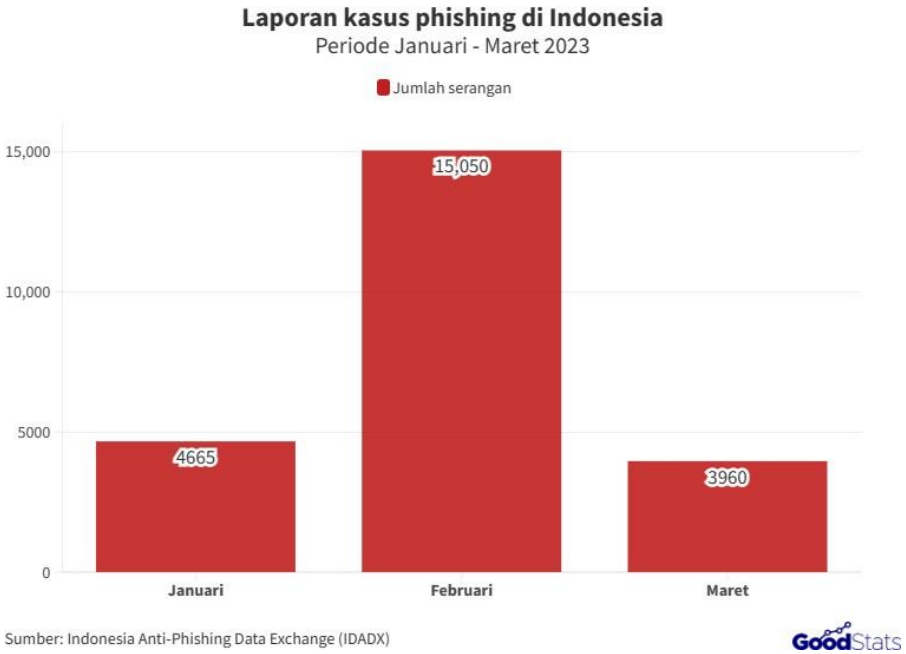
Berdasarkan data dari perusahaan keamanan siber, jumlah serangan hacking di media sosial meningkat secara signifikan dalam beberapa tahun terakhir. Pada tahun 2022, terdapat lebih dari 10 juta serangan hacking di media sosial. Serangan-serangan tersebut menyebabkan kerugian yang besar, termasuk pencurian data pribadi, penyebaran informasi yang salah, dan gangguan layanan.(Aptika dan IKP, Litbang SDM, and Jl Medan Merdeka Barat No n.d.)

Tingkat keberhasilan serangan hacking di media sosial juga meningkat dalam beberapa tahun terakhir. Pada tahun 2022, tingkat keberhasilan serangan hacking di media sosial mencapai 70%. Hal ini menunjukkan bahwa pelaku serangan semakin berhasil dalam mengeksploitasi kerentanan keamanan di media social.



Gambar 2. Sektor industri yang sering diincar serangan phishing di indonesia

JURIHUM : Jurnal Inovasi dan Humaniora
Volume 1, No.4 Desember 2023
ISSN 3025-7409 (Media Online)
Hal 397-402



Gambar 3. Persentase kasus phishing di indonesia

3. ANALISA DAN PEMBAHASAN

Penelitian ini telah memberikan pemahaman mendalam tentang potensi risiko serangan siber dilingkungan media sosial. Hasil penelitian menunjukkan bahwa media sosial rentan terhadap serangan siber yang disebabkan oleh faktor teknis, sosial, dan psikologis.

Faktor Teknis

Faktor teknis menjadi pemicu utama kerentanan terhadap serangan siber di media sosial. Kerentanan ini bisa berupa kelemahan sistem, konfigurasi yang tidak tepat, atau cacat dalam desain aplikasi media sosial. Kelemahan-kelemahan tersebut dapat dieksploitasi oleh pihak yang tidak bertanggung jawab untuk mengakses data pengguna.

Untuk mengatasi kerentanan teknis, penyedia layanan media sosial harus secara rutin melakukan audit keamanan guna mengidentifikasi dan memperbaiki kelemahan keamanan. Penerapan praktik pengembangan perangkat lunak yang aman dan penggunaan infrastruktur yang aman juga menjadi langkah penting.(Orisa and Ardita 2021)

Faktor Sosial

Faktor sosial memainkan peran kunci dalam menciptakan kerentanan terhadap serangan siber di media sosial. Tindakan pengguna yang kurang aman, seperti penggunaan kata sandi yang lemah, penggunaan perangkat yang tidak aman, atau mengunduh aplikasi dari sumber yang tidak terpercaya, dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk mengakses data pengguna.

Upaya untuk mengatasi kerentanan sosial melibatkan peningkatan kesadaran dan implementasipraktik keamanan oleh pengguna media sosial. Pengguna perlu menggunakan kata sandi yang kuat, mengaktifkan otentikasi dua faktor, menjaga keamanan perangkat mereka, dan menghindari mengklik tautan yang mencurigakan.(Muhyidin et al. n.d.)

JURIHUM : Jurnal Inovasi dan Humaniora
Volume 1, No.4 Desember 2023
ISSN 3025-7409 (Media Online)
Hal 397-402

Faktor Psikologis

Faktor psikologis dapat menjadi pemicu kerentanan terhadap serangan siber di media sosial. Persepsi pengguna yang tidak realistis tentang keamanan media sosial dan kurangnya kesadaran terhadap risiko dapat membuat pengguna lebih rentan terhadap serangan siber.

Untuk mengatasi kerentanan psikologis, perlu dilakukan pendidikan dan pelatihan keamanan bagi pengguna media sosial dari berbagai kelompok usia.(Onno and Purbo n.d.)

Rekomendasi

Berdasarkan hasil penelitian, berikut beberapa rekomendasi untuk meningkatkan keamananekosistem media sosial:

Penyedia media sosial:

- Melakukan audit keamanan secara teratur untuk mengidentifikasi dan memperbaikikelemahan keamanan.
- Menerapkan praktik pengembangan perangkat lunak yang aman.
- Menggunakan infrastruktur yang aman.
- Memberikan edukasi dan pelatihan keamanan kepada pengguna.

Pengguna media sosial:

- Menggunakan kata sandi yang kuat dan unik.
- Mengaktifkan otentikasi dua faktor.
- Menjaga keamanan perangkat mereka.
- Menghindari mengklik tautan yang mencurigakan.

Pemerintah:

- Menetapkan regulasi yang ketat untuk melindungi keamanan ekosistem media sosial.
- Meningkatkan kesadaran masyarakat tentang risiko keamanan media sosial.

Dengan menerapkan langkah-langkah ini, diharapkan dapat meningkatkan keamanan ekosistemmedia sosial dan melindungi data pengguna dari serangan siber.

4. KESIMPULAN

Penelitian ini membahas potensi risiko serangan siber yang dapat terjadi di lingkungan media sosial,yang dipengaruhi oleh berbagai faktor, termasuk aspek teknis, sosial, dan psikologis. Aspek teknis mencakup potensi kelemahan dalam sistem dan desain aplikasi, sementara aspek sosial terkait dengan perilaku pengguna yang mungkin kurang aman. Di sisi lain, aspek psikologis mencakup persepsi yang mungkin tidak sesuai dengan realitas dan kurangnya pemahaman akan risiko yang mungkin timbul.

Langkah-langkah untuk mengatasi potensi kerentanan teknis melibatkan audit keamanan yang terjadwal secara rutin dan penerapan praktik pengembangan perangkat lunak yang memprioritaskankeamanan. Peningkatan kesadaran dan adopsi praktik keamanan oleh pengguna media sosialmenjadi faktor penting untuk mengatasi kerentanan sosial. Selain itu, usaha edukasi dan pelatihan dianggap perlu untuk mengatasi potensi kerentanan psikologis.

Rekomendasi yang diajukan mencakup langkah-langkah konkret untuk pihak penyedia media sosial,pengguna, dan pemerintah. Penyedia media sosial diharapkan melakukan audit keamanan

JURIHUM : Jurnal Inovasi dan Humaniora
Volume 1, No.4 Desember 2023
ISSN 3025-7409 (Media Online)
Hal 397-402

secara teratur, menerapkan praktik pengembangan perangkat lunak yang mengedepankan keamanan, dan memberikan edukasi kepada pengguna. Pengguna media sosial diingatkan untuk meningkatkan kesadaran terhadap keamanan pribadi mereka, sementara pemerintah diharapkan mengeluarkan regulasi yang ketat dan meningkatkan kesadaran masyarakat.

Dengan menerapkan saran-saran ini, diharapkan dapat meningkatkan keamanan ekosistem media sosial dan menjaga data pengguna dari potensi risiko serangan siber.

DAFTAR PUSTAKA

Aptika dan IKP, Puslitbang, Badan Litbang SDM, and Kemenkominfo Jl Medan Merdeka Barat No. *TANTANGAN DALAM IMPLEMENTASI STRATEGI KEAMANAN SIBER NASIONAL INDONESIA DITINJAU DARI PENILAIAN GLOBAL CYBERSECURITY INDEX*

Maulia Jayantina Islami TANTANGAN DALAM IMPLEMENTASI STRATEGI KEAMANAN SIBER NASIONAL INDONESIA DITINJAU DARI PENILAIAN GLOBAL

CYBERSECURITY INDEX Challenges in The Implementation of National CybersecurityStrategy of Indonesia from The Global Cybersecurity Index Point of View Maulia Jayantina Islami.

Muhyidin, Yusuf, M Hafid Totohendarto, Erina Undamayanti, and Sekolah Tinggi Teknologi Wastukancana. *Perbandingan Tingkat Keamanan Website MenggunakanNmap Dan Nikto Dengan Metode Ethical Hacking Comparison of Website Security Levels Using Nmap and Nikto With Ethical Hacking Methods*.

Onno, Penulis :, and W Purbo Tiktok. *Mid 2020 Cyber Security Threat, Tips Dan ProposalStrategi Mitigasi Nasional EXECUTIVE SUMMARY*.

Orisa, Mira, and Michael Ardita. 2021. 4 Jurnal MNEMONIC *VULNERABILITY ASSESMENT UNTUK MENINGKATKAN KUALITAS KEMANAN WEB*.