Analisis Keamanan Teknologi Dalam Menghadapi Ancaman Phising

Taufiq Fadhly Ramadhan[1], Irfan Ramadhan[2], Aan Ardana Pangestu[3*]

[1] *S1 Teknik Informatika*
Jl. Bhayangkara No 55, Tipes, Kec. Serengan, Kota Surakarta
[1]220103001@mhs.udb.ac.id

[1] *S1 Teknik Informatika*
Jl. Bhayangkara No 55, Tipes, Kec. Serengan, Kota Surakarta
[1]220103019@mhs.udb.ac.id

[1] *S1 Teknik Informatika*
Jl. Bhayangkara No 55, Tipes, Kec. Serengan, Kota Surakarta
[1]220103036@mhs.udb.ac.id

Abstrak— **Phishing telah menjadi tantangan besar dalam keamanan cyber di era digital. Jurnal ini mengulas teknologi keamanan yang digunakan untuk melawan serangan phishing yang semakin kompleks. Penelitian ini mencakup evaluasi tentang filter email dan web, serta penerapan multi-factor authentication (MFA) dan kecerdasan buatan (AI) untuk meningkatkan tingkat keamanan terhadap phishing. Studi ini juga menyoroti tantangan seperti kurangnya kesadaran pengguna dan perlunya pendidikan keamanan siber yang lebih intensif. Dampak regulasi terhadap penanggulangan phishing di Indonesia juga dibahas. Jurnal ini memberikan gambaran menyeluruh tentang teknologi keamanan dan memberikan saran untuk meningkatkan strategi perlindungan cyber dalam menghadapi ancaman phishing yang terus berkembang.**
Kata kunci— Phishing, keamanan cyber, multi-factor authentication, kecerdasan buatan, regulasi.

Abstract— **Phishing has become a significant challenge in cybersecurity in the current digital era. This journal reviews security technologies used to combat increasingly complex phishing attacks. The research includes evaluations of email and web filters, as well as the implementation of multi-factor authentication (MFA) and artificial intelligence (AI) to enhance security against phishing. The study also highlights challenges such as low user awareness and the need for more intensive cybersecurity education. Additionally, the impact of regulations on phishing mitigation in Indonesia is discussed. This journal provides a comprehensive overview of security technologies and offers recommendations to enhance cyber protection strategies against evolving phishing threats.**[1]
Keywords— Phishing, cybersecurity, multi-factor authentication, artificial intelligence, regulation.

I. PENDAHULUAN

Perkembangan teknologi saat ini telah meningkatkan efesiensi waktu dalam bekerja dan memungkinkan berbagai kegiatan dapat dilakukan dengan lebih cepat. Teknoligi ini sangat membantu manusia dalam berbagai hal. Namun, perkembangan yang menimbulkan tantangan baru dengan munculnya berbagai kejahatan berbasis cyber yang berupaya memanfaatkan ketidakmampuan sistem dan kurang sadarnya pengguna sistem informasi.

Phising merupakan suatu bentuk kejahatan cyber yang paling sering ditemukan. Tindakan ini sangat merugikan dalam berbagai hal, sehingga dapat menyebabkan kerugian faninsial jika informasi pribadi yang dapat disalahgunkan. Selain kerugian faninsial phising juga bisa menyebabkan masalah lain seperti kehilangan data pribadi, dan pencenaran nama baik [1].

Mengingat pentingnya kesadaran akan ancaman phising, peneliti akan melakukan analisis terhadap kesadaran masyarakat pengguna internet Indonesia. Penelitian ini akan melihat dan mengukur tingkat kesadaran masyarakat Indonesia terhadap ancaman *phising* yang ada di internet. Dalam penelitian ini akan membahas bagimana kesadaran ancaman *phising* pada pengguna internet di Indonesia, dan apakah ada perbedaan tingkat kesadaran ancaman *phising* dengan info demografis yang berbeda. Selain itu diharapkan menjadi informasi terhadap tingkat kesadaran ancaman *phising* pada masyarakat Indonesia

II. METODOLOGI PENELITIAN

Metode penelitian yang akan digunakan dalam penelitian ini adalah penelitian kualiatif dengan pendekatan studi pustaka. Langkah awal yang melibatkan pemilihan sumber liteatur yang relavan dengan keamanan cyber, infrastruktur TI dan teknologi yang terkait. Jurnal ilmiah, buku referensi, laporan penelitian dan artikel terkini akan menjadi fokus utama untuk mendapatkan wawasan mendalam. Setelah pemilihan sumber, penelitian akan melibatkan riview dan analisis terhadap literatur yang terpilih. Fokus utama analisis adalah pada kerangka kerja keamanan yang umum diterapkan, trend terkini dalam ancaman cyber, serta teknologi dan strategi keamanan yang dapat efektif dalam melindungi infrastruktur TI.[2]

Selanjutnya, temuan literatur akan diklasifikasikan ke dalam kategori utama, seperti aspek teknis, kebijakan keamanan, pelatihan SDM

dan integrasi teknologi keamanan. Tujuannya adalah memberikan pemahaman yang lebih sistematis tentang elemen kunci yang memengaruhi keamanan infrastruktur TI. Pemahaman mendalam tentang area dimana diperlukan penelitian lebih lanjut akan menjadi dasar bagi pengembangan penelitian ini.

Hasil dari studi pustaka ini akan digunakan untuk merangkum temuan liteatur yang mengembangkan kesimpulann tentang komdisi keamanan infrastruktur TI saat ini. Penelitian ini akan Menyusun rekomendasi praktis berdasarkan liteatur yang telah dianalisis dan memberikan penduan bagi organisasi dalam meningkatkan strategi keamanan mereka terhadap ancaman cyber yang terus berkembang. Dengan pendekatan studi pustaka ini, diharapkan penelitian dapat memberikan kontribusi yang berharga terhadap pemahaman dan penanganan efektif terhadap ancaman keamanan cyber dalam konteks infrastruktur TI.[3]

III. HASIL DAN PEMBAHASAN

3.1. Ancaman Cybersecurity

Ancaman cybersecurity merupakan kompleksitas tantangan yang memerlukan pemahaman mendalam untuk melindungi infrastruktur TI dari ancaman yang terus berkembang. Ancaman ini dapat mengintai dari berbagai arah, baik dari luar atau dari dalam organisasi. Untuk memberikan ancaman tersebut ke dalam 3 kategori utama.

3.1.1. Ancaman Fisik

Ancaman fisik mencakup potensi kerusakan atau kehilangan terhadap komponen fisik infrastruktur TI. Ini dapat melibatkan perangkat hardware, perusakan fisik atau sabotase. Ancaman fisik dapat merusak integritas perangkat keras, pusat data atau fasilitas fisik lainnya, dan dampaknya dapat mencakup gangguan operasional, kehilangan data. Upaya pencegahan dan perlindungan terhadap aset fisik, seperti pusat data dan perangkat keras kritis, menjadi esensial untuk mimitigasi risiko fisik.

Ancaman fisik terhadap infrastruktur TImerupakan suatu ancaman yang memerlukan tindakan pencegahan dan perlindungan yang cerman. Potensi kerusakan atau kehilangan terhadap komponen fisik dapat memiliki dampak signifikan terhadap integritas, ketersediaan dan operasional keseluruhan infrastruktur TI. Oleh karena itu, strategi pencegahan dan perlindungan terhadap ancaman fisik menjadi krusial dalam mimitigasi risiko fisik. Dalam pencegahan pencurian hardware dapat menyebabkan kerugian finansial dan kehilangan data penting. Untuk mecegah pencurian, dapat melakukan langkah-langkah berikut:

- Menerapkan sistem keamanan fisik seperti kamera pengawas, kontrol akses dan penjaga keamanan di lokasi pusat atau ruang server
- Melakukan pencatatan inventaris yang akurat dan pemantauan terhadap hardware untuk mendeteksi setiap perubahan.
- Membangun pusat data dengan pertimbangan design tahan bencana untuk melindungi hardware dari gempa, banjir dan kerusakan alam lainnya.
- Mengembangkan prosedur evakuasi dan pemulihan darurat untuk mengatasi ancaman fisik yang dapat menyebabkan kerusakan.
- Memberikan pelatihan kepada karyawan untuk mengenali potensi ancaman dan melaporkannya segera.
- Menerapkan kemanan jaringan untuk mencegah akses yang tidak sah dan melindungi data yang disimpan di hardware.

Ancaman fisik terhadap imfrastruktur TI memerlukan holistik yang mencakup pencegahan, deteksi dan respon cepat. Dengan adanya strategi perlindungan dan tindakan pencegahan yang cermat, organisasi dapat meminimalkan resiko fisik, menjaga integritas hardware dan melinduingi layanan TI yang kritis. Pentingnya untuk terus memperbarui strategi keaman fisik sesuai dengan perkembangan teknologi dan ancaman baru yang muncul.[4]

3.1.2. Ancaman Logikal

Ancaman logikal terhadap infrastruktur TI melibatkan berbagai serangan yang di arahkan kepada aspek digital. Memahami dan menghadapi

ancaman logikal ini memerlukan strategi yang holistik, termasuk deteksi dini, pencegahan dan respons cepat untuk meminimalkan dampak yang mungkin timbul. Malware merupakan jenis istilah umum yang mencakup berbagai jenis software berbahaya, seperti virus, worm, dan trojan. Serangan malware bertujuan untuk menyusup ke dalam sistem komputer dan merusaknya. Virus dapat menempel pada file atau program yang menyebar saat file tersebut di eksekusi. Worm dapat menyebar sendiri melalui jaringan, sedangkan trojan menyamar sebagai program yang berguna untuk mengelabui pengguna dan kemudian mengeksploitasi sistem. Selain merusak sistem, malware juga dapat mencuri data sensitif seperti informasi login.

Sementara itu, *Teknik phising* melibatkan upaya untuk mendapatkan informasi rahasia atau sensitif dengan menyabar sebagai entitas terpecaya. Ini sering dilakukan melalui surel atau situs web palsu yang meniru tampilan situs resmi. Phising dapat mencakup pengiriman surel palsu yang meminta pengguna untuk mengirim informasi data pribadi. Serangan phising juga sangat persuasif, menggunakan manipulasi psikologis untuk membuat pengguna terperangkap dan memberikan informasi sensitif mereka.[5]

Serangan social engineering memanfaatkan manipulasi psikolohis pada manusia untuk mendapatkan informasi rahasia atau akses ke sistem. Penyerang dapat menggunakan berbagai taktik, seperti membangkitkan rasa urgensi atau menciptakan skenario palsu untuk mendapatkan kepercayaan korban. Ini dapat melibatkan panggilan telefon palsu atau interaksi langsung dengan tujuan mengelabui orang untuk memberikan data informasi yang seharus nya tidak diberikan kepada siapapun.

Ransomware adalah jenis malware yang mengenkripsi data pada suatu sistem dan kemudian menuntut pembayaran tebusan agar akses ke data tersebut dikembalikan. Penyerang sering menggunakan enkripsi yang sangat kuat, membuat sulit atau bahkan tidak mungkin untuk memulihkan data tanpa kunci enkripsi yang benar. Umumnya, tebusan diminta kedalam bentuk mata uang kripto untuk mempersulit pelacakan. Ransomware dapat merugikan korban secara finansial dan dapat menyebabkan kerugian data yang signifikan jika tebusan tidak dibayar atau jika data tidak dapat dipulihkan cari cadangan yang memadai.

Untuk melindungi infrastruktur TI dari serangan logikal yang mencakup malware, phising, social engineering dan ransomware, diperlukan strategi pencegahan yang holistik. Ancaman logikal terhadap infrastruktur TI memerlukan pendekatan yang menyeluruh, menggabungkan pencegahan dan respon cepat. Dengan menggunakan kombinasi teknologi keamanan, pelatihan untuk pengguna dan sistem pemantauan yang efektif, organisasi dapat mengurasi risiko dari serangan logikal, melindungi integritas sistem, dan meminimalkan potensi kerugian data. Meningkatkan strategi keamanan sesuai dengan perkembangan teknologi dan taktik serangan cyber yang akan menjadu kunci dalam menjaga keamanan intfrastruktur TI.

3.1.3 Ancaman Operasional

Ancaman operasional merupakan tantangan serius yang timbul dari faktor internal di dalam suatu organisasi, dapat berupa kesalahan manusia, kelalaian atau ketidakpatuhan terhadap prosedur keamanan. Kesalahan manusia seperti konfigurasi sistem yang salah atau penghapusan data tidak sengaja dapat merugikan keberlanjutan operasional. Untuk mengatasi hal ini, pelatihan karyawan secara rutin dan otomatisasi proses dapat menjadi langkah pencegahan yang efektif. Kelalaian yang mencakup kurangnya perhatian dalam tugas, juga dapat memberikan sumber ancaman. Kebijakan keamanan yang jelas dan monitoring aktivitas pengguna membantu mengurangi risiko dari kelalaian ini.

Ancaman juga dapat muncul dari ketidakpatuhan terhadap prosedur keamanan yang telah ditetapkan. Edukasi karyawan tentang pentingnya mematuhi prosedur keamanan. Pengelolaan akses karyawan yang baik, melalui prinsip kepisahan wewenang dan pemantauan akses yang dapat membantu mengurangi risiko.[6]

Pentingnya menerapkan prinsip keamanan pada oprasional juga dapat tidak bisa diabaikan. Analis risiko operasional juga tidak bisa diabaikan. Analisis risiko operasional secara teratur membantu

organisasi mengidentifikasi potensi ancaman dan mengambil tindakan preventif yang sesuai. Perbaikan berkelanjutan berdasarkan temuan dari analisis risiko akan meningkatkan kemampuan organisasi dalam menghadapi ancaman operasional secara efektif. Dengan pendekatan holistik ini, organisasi dapat mengoptimalkan kemanan infrastruktur TI mereka dan melindungi kelangsungan operasional dari potensi risiko internal.[7]

3.2. Hasil Analisis Teknologi keamanan

3.2.1. Menghadapi Ancaman Phising

Dari analisis yang dilakukan, dapat disimpulkan bahwa teknologi keamanan mamainkan peran penting dalam melindungi pengguna dari ancaman phising. Beberapa teknologi utama yang digunakan termasuk filter email, filter web, multi fakctor authentication, serta penggunaan machine learning dan kecerdasan buatan untuk detekti lebih lanjut. Berikut adalah hasil utama dari analisis ini:

- Efektivitas Teknologi Filtering: Teknologi filtering seperti email dan web sangat efektif dalam mengidentifikasi dan mengurangi kemungkinan pengguna terpapar oleh serangan phising. Dengan menggunakan algoritma yang canggih, teknologi ini dapat memblokir atau memperingatkan pengguna terhadap email atau situs web yang mencurigakan.
- Pentingnya Multi-factor Authentication: Implementasi MFA telah terbukti efektif dalam melindungi akun dari akses ilegal yang dapat terjadi akibat dari informasi yang diperoleh melalui phising. Dengan memerlukan lebih dari satu faktor verifikasi, MFA membuat lebih sulit bagi penjahat untuk mengakses akun dengan hanya mencuri kata sandi pengguna.
- Peran Machne dan AI: Pengguna teknologi machine learning dan kecerdasan buatan memungkinkan sistem untuk belajar dari pola perilaku pengguna dan mengidentifikasi pola phising yang baru tidak dikenal denga lebih baik. Hal ini meningkatkan kemampuan sistem untuk menghadapi serangan phising yang semakin kompleks dan berubah-ubah.[8]

3.2.2. Pembahasan Tantangan dalam Keamanan

- Kesesuaian dengan regulasi dan kepatuhan : Organisasi harus dipastikan bahwa implementasi teknologi keamanan mereka mematuhi peraturan perlindungan data yang berlaku di wilayar mereka. Kepatuhan terhadap regulasi seperti GDPR di Uni Eropa atau CCPA di California menjadi penting untuk menghindari potensi sanksi dan menjamin perlindungan data yang adekuat bagi pengguna.
- Pendidikan dan Kesadaran Pengguna: Meskipun teknologi keamanan yang canggih dapat memberikan perlindungan teknis, kesadaran dan pendidikan pengguna tetap menjadi aspek yang penting dalam melawan serangan phising. Pengguna harus dilatih untuk mengenali tanda-tanda phising, seperti email yang meminta informasi sensitif atau tautan yang mencurigakan, serta untuk tidak mengambil tindakan tanpa verifikasi yang tepat.
- Pengembangan Teknik Phising: Penjahat cyber terus mengembangkan teknik phising yang lebih canggih dan menyesuaikan serangan mereka dengan perubahan trend tan teknologi. Hal ini menekankan pentingnya untuk terus memperbarui dan meningkatkan teknologi keamanan untuk mengantisipasi ancaman yang semakin rumit dan serbaguna.[9]

3.3. Pengaruh Kemajuan Teknologi Terhadap Perkembangan Phising

Kemajuan teknologi memberikan dampak yang luar biasa terhadap menjamunya phising sebagai kegiatan kriminal, sehingga menimbulkan banyak akibat:

3.3.1. Peningkatan Keterampilan

Kemajuan teknologi telah memfasilitasi peningkatan kemampuan kriminal di kalangan phiser, yang kini dapat memanfaatkan alat rekayasa canggih untuk membuat konten palsu dan situs web palsu. Perkembangan ini memberikan kesulitan yang cukup besar dalam hal identifikasi.

3.3.2. Social Engirneering yang lebih canggih dengan meningkatnya aksebilitas data pribadi melalui media sosial dan internet, individu dengan niat jahat kini telah memiliki kapasitas untuk terlibat dalam kegiatan yang lebih canggih. Individu memiliki kapasitas untuk menciptakan bentuk komunikasi menarik berdasarkan kepemilikan mereka atas informasi pribadi yang relavan dengan penerima yang dituju.

3.3.3. Kecerdasan Buatan (AI)

Dalam serangan phising yang semakin meluas, dimana AI digunakan untuk mengatur serangan, mengenali target yang potensial, serta menyebarkan pesan pesan yang menarik.

Dampak dari trend ini adalah peningkatan terus-menerus dalam pengembangan sistem deteksi dan perlindungan anti phising, meningkatkan urgensi keamanan cyber, serta kebutuhan untuk meningkatkan pemahaman tentang risiko phising guna menjaga keamanan di ranah digital.

Di Indonesia, undang-undang pidana mengatur pencurian secara menyeluruh dalam Kitab Undang-Undang Hukum Pidana (KHUP). Namun, penyebaran informasi melalui teknik phising dianggap sebagai kejahatan cyber. Pengelompokan ini mencerminkan prinsip hukum lex spesialis drogat lex generalis, yang menyatakan undang-undang khusus memiliki kekuatan hukum yang lebih kuat daripada undang-undang umuum. Ketika topiknya berhubungan dengan ranah yang lebih luas, regulasi beralih dari KHUP ke Undang-Undang Informasi dan Transaksi Elektronik (ITE) nomor 19 tahun 2016.

Analisis Kaspersky Security Network 2021 mengungkapkan bahwa phising memberikan bahwa keamanan cyber yang menonjol pada kuartal keempat tahun 2020, tercatat sebanyak 1,6 juta kasus serangan phising yang terdeteksi. Fenomena ini juga merupakan tantangan serius di seluruh Asia Tenggara, dengan Indonesia menempati posisi teratas dalam frekuensi serangan tersebut.

Peningkatan serangan phising di Indonesia dapat dijelaskan oleh beberapa faktor, antara lain pertumbuhan jumlah pengguna internet yang signifikan, rendahnya kesadaran akan keamanan cyber, serta kerentanan yang ada dalam infrastruktur internet. Selain itu, sebagian besar pengguna internet kurang memahami teknik dan persiapan yang digunakan oleh pelaku phising, yang memperburuk situasi yang sudah ada.

Trend peningkatan upaya untung mengurangi dan memberantas serangan phising juga terlihat di Indonesia. Ada beberapa strategi yang dapat di terapkan untuk mengurangi kejadian serangan phising. Upaya ini mencakup peningkatan pengetahuan dan edukasi tentang keamanan cyber, penerapan teknologu keamanan seperti perlindungan antivirus, keamanan jaringan dan penggunaan sertifikat SSL pada situs web, serta penerapan tindakan hukum yang tegas terhadap pelaku kejahatan cyber yang terlibat serangan phising. Peran aktif dalam lembaga pemerintah dan penegak hukum sangat krusial dalam upaya mitigasi yang efektif terhadap serangan phising di indonesia.[10]

IV. KESIMPULAN

Penelitian ini menunjukan bahwa menggunakan simulasi phising dengan situs web kloning efektif untuk mengukur seberapa sadar dan waspada pengguna terhadap serangan phising. P enelitian ini belum menyentuh beberapa aspek kunci. Salah satunya adalah analisis mendalam mengenai faktor psikologis yang memengaruhi keputusan pengguna untuk memasukkan informasi mereka pada situs kloning. Selain itu, penelitian ini juga belum mengeksplorasi sejauh man tingkat pendidikan sebelumnya tentang keamanan cyber mempengaruhi hasil dari simulasi phising ini. Selain itu, penelitian ini tidak membahas dampak jangka panjang dari pengalaman simulasi phising terhadap perilaku pengguna di masa depan.

Untuk penelitian selanjutnya, disarankan agar dilakukan studi longitudinal yang mengevalusi perubahan perilaku pengguna setelah mereka berpasitipasii dalam simulasi phising. Penelitian juga dapat diperluas umtuk mempertimbangkan analisis terhadap berbagai jenis situs web kloning lainnya, seperti situs perbankan atau e-commerce, untuk mendapatkan pemahaman yang lebih komprehensif tentang kerentanan pengguna. Selain

itu, integrasi pendekatan psikologis yang lebih dalam dan pendidikan keamanan cyber yang lebih intensif dapat memberikan wawasan yang lebih mendalam tentang strategi terbaik umtuk meingkatkan kesadaran dan kewaspadaan pengguna terhadap serangan phising.

UCAPAN TERIMA KASIH

Kami mengucapkan terima kasih kepada semua penulis dan peneliti atas kontribusi berharga dalam jurnal ini tentang keamanan teknnologi dalam menghadapi ancaman phising. Analisis yang disajikan memberikan wawasan yang penting bagi pengembangan strategi perlindungan cyber yang efektif.

REFERENSI

[1] M. Ifan, A. Aziz, and M. R. A. N. B, "Simulasi Dan Upaya Edukasi Keamanan Siber Menggunakan Situs Web Phishing," vol. 1, no. 4, pp. 74–80, 2024.

[2] A. Wibowo *et al.*, "Analisis Keamanan Sistem Operasi dalam Menghadapi Ancaman Phishing dalam Layanan Online Banking," vol. 2, no. 1, doi: 10.38035/jim.v2i1.

[3] N. Vadila and A. R. Pratama, "Analisis Kesadaran Keamanan Terhadap Ancaman Phishing," *Automata*, vol. 2, no. 2, pp. 1–4, 2021.

[4] P. Subarkah and A. N. Ikhsan, "Identifikasi Website Phishing Menggunakan Algoritma Classification And Regression Trees (CART)," *Jurnal Ilmiah Informatika*, vol. 6, no. 2, pp. 127–136, Dec. 2021, doi: 10.35316/jimi.v6i2.1342.

[5] I. Kadek Odie Kharisma Putra, I. Made Adi Darmawan, I. Putu Gede Juliana, K. Kunci, and C. Crime, "TINDAKAN KEJAHATAN PADA DUNIA DIGITAL DALAM BENTUK PHISING CRIMINAL ACTS IN THE DIGITAL WORLD WITH A FORM OF PHISHING," 2022.

[6] A. M. Fikri, B. Pertiwibowo, F. Fachrureza, M. I. Fahri, and R. I. Setyorini, "Edukasi Webinar," *JPPM (Jurnal Pengabdian dan Pemberdayaan Masyarakat)*, vol. 6, no. 1, p. 113, Jun. 2022, doi: 10.30595/jppm.v6i1.7543.

[7] I. Yurita, M. K. Ramadhan, and M. Candra, "Pengaruh Kemajuan Teknologi Terhadap Perkembangan Tindak Pidana Cybercrime (studi kasus phising sebagai ancaman keamanan digital)," *Jurnal Hukum Legalita*, vol. 5, no. 2, pp. 143–155, 2023.

[8] J. Pendidikan and D. Konseling, "Kejahatan Phising dalam Dunia Cyber Crime dan Sistem Hukum di Indonesia."

[9] M. O. Hoshmand, S. Ratnawati, and E. P. Korespondensi, "Analisis Keamanan Infrastruktur Teknologi Informasi dalam Menghadapi Ancaman Cybersecurity," *Jurnal Sains dan Teknologi*, vol. 5, no. 2, pp. 679–686, 2023.

[10] Aprelia Windarni, V., Ferdita Nugraha, A., Tri Atmaja Ramadhani, S., Anisa Istiqomah, D., Mahananing Puri, F., & Setiawan, A. (2023). DETEKSI WEBSITE PHISHING MENGGUNAKAN TEKNIK FILTER PADA MODEL MACHINE LEARNING. In Information System Journal (INFOS) | (Vol. 6, Issue 1).