INDOTECH
Indonesian Journal of Education And Computer Science
Vol. 1, No. 3, Desember 2023
Hal 127-135
E-ISSN : 2987-2650
P-ISSN : 2987-7644
Site : https://jurnal.intekom.id/index.php/indotech

Keefektifan Metode Proteksi Data dalam Mengatasi Ancaman *Cybersecurity*

Arfan Dwi Madya[1], Bagas Djoko Haryanto[2], Devi Putri Ningsih[3], Fried Sinlae[4]
[1,2,3,4]Fakultas Ilmu Komputer, Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia

Article Info

Article history:

Received June 17, 2023
Revised October 28, 2023
Accepted Desember 28, 2023

Kata Kunci*:*

Proteksi data,
Ancaman *Cyber*,
Cybersecurity

Keywords:
Data protection,
Cyber threats,
Cybersecurity

ABSTRAK

Keamanan informasi menjadi perhatian utama di era digital saat ini di mana ancaman serangan *cyber* semakin meningkat. Artikel ini membahas pertumbuhan pengguna internet yang signifikan dan dampaknya terhadap meningkatnya serangan *cyber*, dengan fokus pada situasi di Indonesia. Data menunjukkan bahwa serangan *cyber* di Indonesia mengalami peningkatan drastis, mencapai sekitar 190 juta percobaan pada tahun 2020. Melihat pentingnya strategi keamanan *cyber* nasional, penelitian ini bertujuan untuk mengevaluasi keefektifan metode proteksi data dalam mengatasi ancaman *cybersecurity*. Metode penelitian menggunakan pendekatan deskriptif kualitatif untuk mengeksplorasi dan memahami keefektifan metode proteksi data. Analisis data dilakukan secara holistik untuk memahami konteks dan dinamika yang mempengaruhi keberhasilan metode proteksi data dalam menghadapi ancaman *cybersecurity*. Hasil penelitian menekankan pentingnya keamanan *cyber* dalam menjaga data, privasi, dan kelancaran layanan. Ancaman *cyber* mencakup berbagai jenis, seperti fisik, logikal, dan operasional. Faktor manusia juga menjadi ancaman serius, termasuk kesalahan pengguna dan teknik social engineering. Proteksi data diidentifikasi sebagai strategi kunci dalam mengatasi ancaman *cybersecurity*. Langkah-langkah seperti deteksi *malware*, perlindungan terhadap serangan DoS dan *phishing*, keamanan basis data, enkripsi data, monitoring dan respons terhadap serangan, serta pendidikan dan pelatihan menjadi fokus utama untuk sektor perbankan.

ABSTRACT

Information security has become a primary concern in the current digital era, where the threat of cyber attacks is on the rise. This article discusses the significant growth of internet users and its impact on the increasing incidence of cyber attacks, with a focus on the situation in Indonesia. Data indicates a drastic surge in cyber attacks in Indonesia, reaching approximately 190 million attempts in 2020. Recognizing the importance of a national cyber security strategy, this research aims to evaluate the effectiveness of data protection methods in addressing cybersecurity threats. The research methodology employs *a qualitative descriptive approach to explore and understand the effectiveness of data protection methods. Data analysis is conducted holistically to comprehend the context and dynamics influencing the success of data protection methods in facing cybersecurity threats. The research findings emphasize the crucial role of cyber security in safeguarding data, privacy, and the smooth operation of services. Cyber threats encompass various types, including physical, logical, and operational threats. Human factors also pose a serious threat, including user errors and social engineering techniques. Data protection is identified as a key strategy in tackling cybersecurity threats. Measures such as malware detection, defense against DoS and phishing attacks, database security, data encryption,*

monitoring and response to attacks, as well as education and training, are highlighted as primary focuses for the banking sector

Corresponding Author:

Fried Sinlae
Fakultas Ilmu Komputer, Universitas Bhayangkara Jakarta Raya,
Bekasi, Indonesia
Email: fried.sinlae@dsn.ubharajaya.ac.id

1. PENDAHULUAN

Keamanan informasi merupakan aspek yang krusial dalam era digital saat ini, di mana teknologi informasi memainkan peran sentral dalam berbagai aspek kehidupan masyarakat. Seiring dengan berkembangnya teknologi, ancaman terhadap keamanan informasi juga semakin meningkat, terutama dalam bentuk serangan *cyber*. Serangan *cyber* dapat berdampak besar terhadap individu, perusahaan, dan bahkan negara. White dalam [1] telah menjelaskan bahwa istilah serangan *cyber* yang didefinisikan oleh Biro Investigasi Federal Amerika Serikat adalah serangan yang terlibat secara politis terhadap sistem komputer, informasi, program, dan data yang mengakibatkan kekerasan terhadap target non-militer oleh kelompok sub-nasional. Kemajuan dalam teknologi juga menyebabkan peningkatan ancaman *cyber* yang memerlukan pengembangan langkah pencegahan baru. Huang et al dalam [1] telah mengindikasikan bahwa serangan *cyber* semakin meningkat di bidang industri yang mengakibatkan kerusakan fisik pada fasilitas yang dapat menyebabkan kerugian jutaan dolar. Alasan di balik peningkatan serangan *cyber* di antara perusahaan terutama karena ketergantungan yang semakin meningkat pada teknologi digital yang menyebabkan informasi keuangan dan pribadi disimpan. Oleh karena itu, ini dianggap sebagai tantangan paling penting dalam situasi saat ini karena tidak hanya menyebabkan kerugian keuangan tetapi juga menyebabkan bocornya informasi sensitif. Menurut [2], serangan *cyber* bervariasi mulai dari peretasan, penolakan layanan, perangkat lunak mata-mata, dan infeksi *malware* yang dapat berdampak pada semua orang di negara tersebut. Serangan *cyber* juga dapat menyebabkan efek psikologis utama di antara individu yang mengakibatkan frustrasi, stres, dan kecemasan.

Menurut informasi dari World Bank yang dilaporkan oleh infokomputer Cakrawala, pada tahun 2017 sekitar 49% dari total populasi dunia menggunakan internet. Angka ini jauh lebih tinggi dibandingkan dengan hanya sekitar 6,7% pada tahun 2000. Sumber lain seperti Internet World Stats juga memperkirakan bahwa pada kuartal pertama tahun 2021, sekitar 64,2% dari total populasi dunia telah menggunakan internet, dengan jumlah pengguna internet diperkirakan lebih dari 5 miliar. Hal ini menandakan peningkatan yang sangat signifikan sebesar 1.300% dari tahun 2000. Namun, seiring dengan peningkatan pengguna internet, jumlah serangan juga meningkat secara dramatis. Menurut laporan dari Deep Instinct, serangan *cyber* menggunakan *malware* mengalami peningkatan sebesar 358% pada tahun 2020 dibandingkan dengan tahun sebelumnya. Khususnya, serangan ransomware meningkat sebanyak 435% pada tahun yang sama dibandingkan dengan tahun sebelumnya. Data tersebut

disediakan oleh Deep Instinct yang mengumpulkan informasi dari berbagai sumber, termasuk pihak ketiga dan konsumen mereka, dengan klaim bahwa data tersebut merefleksikan ratusan juta kejadian pada tahun 2020 [3].

Berdasarkan data dari Badan *Cyber* dan Sandi Negara (BSSN), Indonesia mengalami hampir 190 juta percobaan serangan *cyber* dari Januari hingga Agustus 2020, yang lebih dari empat kali lipat dari periode yang sama pada tahun sebelumnya, sekitar 39 juta percobaan. Proyeksi untuk tahun 2021 menunjukkan bahwa serangan *cyber* masih akan terjadi karena pandemi COVID-19 dapat meningkatkan kasus kemiskinan yang mungkin mendorong peningkatan kejahatan, termasuk serangan *cyber*. Oleh karena itu, Indonesia sangat membutuhkan strategi keamanan *cyber* nasional saat ini. Keamanan *cyber*, yang berarti bebas dari ancaman atau bahaya di dunia maya, menjadi hal yang sangat krusial dalam menjaga keamanan secara keseluruhan. Memahami ancaman di ruang *cyber* dan menemukan solusi yang tepat sangat penting untuk mengatasi masalah keamanan *cyber*. Jika langkah-langkah keamanan *cyber* tidak memadai, kemungkinan ancaman akan terus meningkat [3]

Penelitian ini bertujuan untuk mengetahui keefektifan metode proteksi data dalam mengatasi ancaman *cybersecurity*. Melalui pemahaman yang lebih mendalam terhadap berbagai metode proteksi data seperti enkripsi, keamanan jaringan, manajemen akses, dan aspek keamanan fisik, penelitian ini diharapkan dapat memberikan wawasan baru dalam merancang strategi keamanan informasi yang lebih efektif. Dengan demikian, hasil penelitian ini diharapkan dapat memberikan kontribusi signifikan terhadap pengembangan langkah-langkah preventif dan responsif terhadap ancaman *cyber* yang semakin kompleks di era digital ini.

2. METODE

Penelitian ini menggunakan pendekatan deskriptif kualitatif untuk mengeksplorasi dan memahami keefektifan metode proteksi data dalam mengatasi ancaman *cybersecurity*. Selain itu, pendekatan kualitatif memungkinkan peneliti untuk memahami konteks dan dinamika yang mungkin mempengaruhi keberhasilan atau kegagalan metode proteksi data dalam situasi nyata. Analisis data akan dilakukan secara holistik untuk menghasilkan pemahaman mendalam tentang keefektifan metode proteksi data sebagai upaya mitigasi dalam melawan ancaman *cybersecurity.*

3. HASIL DAN PEMBAHASAN

1.1 Pentingnya *Cybersecurity*

Penting bagi setiap orang untuk memahami keamanan dalam berinternet atau yang dikenal sebagai *cyber* security. Ini membantu kita mengenali potensi ancaman yang mungkin timbul dan bagaimana cara menghadapinya. *Cyber* security melibatkan berbagai alat, kebijakan, dan teknologi yang bertujuan melindungi data dan aset organisasi dari risiko *cyber*. Dengan pemahaman mengenai ancaman ini, kita dapat belajar cara menjaga keamanan data pribadi dan mengurangi risiko saat melakukan transaksi online. Pengetahuan tentang internet, juga dikenal sebagai Internet Knowledge, membantu kita tumbuh dan berkembang seiring waktu berdasarkan pengalaman dalam menggunakan internet [4]

Cybersecurity juga bisa diartikan sebagai kegiatan, proses, kemampuan, atau keadaan di mana sistem informasi dan komunikasi serta informasi yang terkandung di dalamnya dilindungi dari kerusakan, penggunaan atau modifikasi yang tidak sah, atau eksploitasi. Internet tanpa ragu

meningkatkan pengetahuan seseorang. Misalnya, permainan komputer online membutuhkan pengguna yang sangat terampil dalam berbahasa Inggris, agar bisa memahami pengaturan dan prosedur permainan. Hal ini secara tidak langsung akan mendorong perkembangan keterampilan membaca, menulis, dan berbicara dalam bahasa Inggris. Namun, permainan komputer biasanya menyenangkan, dan memakan waktu lama bagi pengguna untuk menyelesaikannya. Hal ini dapat membuat remaja menjadi malas, atau terlalu fokus pada permainan dan perangkat. Remaja juga bisa menjadi kecanduan, dan kegiatan produktif, seperti meninjau pelajaran mereka, diabaikan [5]

Cybersecurity sangat penting karena melindungi semua jenis data dari pencurian dan kerusakan, termasuk informasi sensitif dan yang dapat diidentifikasi secara pribadi. Keterhubungan yang semakin meningkat dan ketergantungan pada layanan cloud telah meningkatkan risiko pelanggaran data dan serangan siber. Ancaman-ancaman ini tidak hanya terbatas pada perusahaan besar tetapi juga meluas ke bisnis kecil dan individu. Oleh karena itu, langkah-langkah *cybersecurity* yang komprehensif dan pelatihan kesadaran sangat penting untuk melawan ancaman siber yang terus berkembang. Pemerintah di seluruh dunia telah menyadari seriusnya *cyber*crime dan telah mengambil langkah-langkah untuk mengatasinya. Peraturan Perlindungan Data Umum (GDPR) di Eropa adalah contoh legislasi yang bertujuan untuk melindungi privasi data individu. Di Amerika Serikat, California telah menerapkan undang-undang pengungkapan pelanggaran data untuk memastikan bahwa bisnis secara cepat memberitahukan individu yang terkena dampak dalam kasus pelanggaran data [6].

Dapat disimpulkan bahwa *cybersecurity* sangat penting dalam lanskap digital saat ini dalam upaya melindungi data, melindungi privasi, dan memastikan kelancaran fungsi layanan-layanan penting. Keterhubungan yang semakin meningkat dan ketergantungan pada teknologi menyoroti perlunya langkah-langkah *cybersecurity* yang kokoh dan kewaspadaan konstan untuk efektif melawan ancaman siber.

1.2 Macam – Macam Ancaman *Cybersecurity*

Perkembangan aplikasi web menimbulkan tantangan dalam memperkuat keamanannya karena rentannya platform ini terhadap serangan peretas seperti *SQL Injection, Phising*, dan *Cross-Site Scripting* (XSS) [7]. Ancaman dapat muncul karena kurangnya kesadaran dan literasi keamanan informasi, baik dari individu maupun organisasi. Keamanan informasi memerlukan kesadaran akan potensi ancaman dan langkah-langkah pencegahan [8].

Terdapat berbagai macam ancaman *cybersecurity*, menurut [9], ancaman *cyber* dapat melalui ancaman fisik, ancaman logikal dan ancaman operasional.

1) Ancaman Fisik

   Ancaman fisik adalah potensi kerusakan atau kehilangan pada bagian fisik dari infrastruktur TI. Hal ini dapat berupa pencurian perangkat keras, kerusakan fisik, atau sabotase. Ancaman fisik dapat menyebabkan kerusakan pada perangkat keras, pusat data, atau fasilitas fisik lainnya, yang dapat mengakibatkan gangguan operasional, kehilangan data, atau bahkan gangguan pada layanan. Untuk mengurangi risiko dari ancaman fisik ini, langkah-langkah pencegahan dan perlindungan terhadap aset fisik seperti pusat data dan perangkat keras kritis menjadi sangat penting.
2) Ancaman Logikal

Serangan pada infrastruktur teknologi informasi melalui *malware* adalah ancaman serius. *Malware* adalah istilah yang mencakup berbagai jenis perangkat lunak berbahaya seperti virus, worm, dan trojan. Virus menempel pada file atau program dan menyebar saat dieksekusi. Worm menyebar sendiri melalui jaringan, sedangkan trojan menyamar sebagai program berguna untuk mengeksploitasi sistem. Memahami dan menghadapi ancaman ini membutuhkan langkah-langkah seperti deteksi dini, pencegahan, dan respons cepat guna mengurangi dampak yang mungkin terjadi. Selain merusak sistem, *malware* juga bisa mencuri data sensitif seperti informasi login atau keuangan.

3) Ancaman Operasional
Ancaman serius bagi keberlangsungan operasional seringkali muncul dari faktor-faktor internal di dalam sebuah organisasi. Kesalahan manusia, seperti konfigurasi sistem yang salah atau penghapusan data tidak sengaja, dapat menyebabkan gangguan yang merugikan. Pelatihan rutin bagi karyawan dan penggunaan otomatisasi dalam proses dapat menjadi solusi yang efektif untuk menghindari hal ini. Selain itu, kelalaian dalam menjalankan tugas-tugas operasional juga menjadi sumber ancaman yang signifikan. Dengan kebijakan keamanan yang jelas serta pemantauan aktivitas pengguna, risiko dari kelalaian ini dapat diminimalkan.

Beberapa ancamanan lainnya adalah [8]:

1) Ancaman Manusia (*Human Factor*)
Kesalahan manusia (*human error*) dapat menjadi ancaman serius terhadap keamanan informasi. Misalnya, pengguna yang tidak sadar menjaga keamanan data, tidak menggunakan kata sandi yang kuat, atau mengklik iklan yang dapat mengandung *malware*.
2) Ancaman *Social Engineering*
Social engineering merupakan teknik manipulasi psikologis terhadap individu untuk mendapatkan informasi rahasia. Ancaman ini bisa muncul dalam bentuk upaya tipu daya untuk mencuri informasi yang seharusnya tidak diketahui oleh pihak yang tidak berwenang.
3) Ancaman pada Pengguna *Smartphone* dan Internet
Dalam konteks pengguna *smartphone,* terdapat ancaman yang berhubungan dengan penggunaan akun dan internet, seperti kurangnya kesadaran pengguna terhadap aspek keamanan informasi seperti kerahasiaan, ketersediaan, dan integritas data. Pengguna internet dapat menghadapi risiko seperti serangan *phishing*, pencurian data, dan serangan siber lainnya. Contoh dalam tulisan mencakup kasus pengaksesan situs pendidikan dengan risiko mengklik iklan berbahaya.

Berdasarkan penelitian [10] terdapat beberapa ancaman *cybersecurity* antara lain:

1) *Denial-of-*Service (DoS): Serangan ini bertujuan untuk mencegah pengguna yang dituju dari mengakses suatu mesin atau sumber daya jaringan. Hal ini dapat menyebabkan gangguan atau bahkan kegagalan dalam menjalankan fungsi yang diinginkan.
2) *Malware*: Artikel membahas tentang serangan *malware* yang menggunakan perangkat lunak berbahaya untuk mendapatkan akses tidak sah ke sistem komputer. *Malware*

dapat merusak, mencuri data, atau mengganggu operasi normal dari sistem yang terinfeksi.

3) *Phishing*: Serangan *phishing* melibatkan upaya untuk mendapatkan informasi sensitif dari pengguna internet dengan menggunakan teknik rekayasa sosial dan teknologi. Hal ini dapat mengakibatkan pencurian identitas dan kebocoran data pribadi.
4) *SQL Injection*: Serangan ini melibatkan penyisipan string input ke dalam aplikasi untuk memanipulasi perintah SQL yang dieksekusi oleh database. Hal ini dapat mengakibatkan akses tidak sah ke data sensitif atau bahkan kerusakan pada basis data.
5) *Man-in-the-Middle Attacks*: Serangan ini terjadi ketika pihak ketiga yang tidak sah menyusup ke dalam komunikasi antara dua pihak yang sah. Hal ini dapat mengakibatkan pencurian data atau manipulasi informasi yang dikirim antara kedua pihak.

Dari penjelasan di atas, dapat disimpulkan bahwa berbagai ancaman *cybersecurity* dapat mengancam keamanan sistem dan data, terutama dalam konteks sektor perbankan. Memahami ancaman-ancaman ini penting untuk merancang strategi proteksi data yang efektif dan melindungi informasi sensitif dari serangan siber.

1.3 Proteksi Data dalam Mengatasi Ancaman *Cybersecurity*

Proteksi data merupakan aspek krusial dalam menghadapi ancaman *cybersecurity* yang semakin kompleks dan sofistikatif. Seiring dengan kemajuan teknologi informasi, telah dilakukan berbagai kajian dan penelitian yang secara intensif mengeksplorasi strategi dan mekanisme untuk melindungi data dari serangan *cyber.* Para peneliti telah menyelidiki berbagai metode enkripsi, pengelolaan identitas digital, serta teknologi keamanan jaringan yang dapat mengurangi risiko peretasan dan kebocoran data. Selain itu, penelitian juga fokus pada pemahaman mendalam terhadap taktik dan teknik yang digunakan oleh pelaku kejahatan *cyber*, sehingga dapat dikembangkan solusi proaktif untuk mencegah serangan yang belum terdeteksi. Keberhasilan perlindungan data tidak hanya bergantung pada inovasi teknologi semata, tetapi juga melibatkan aspek kebijakan, kesadaran pengguna, dan kerjasama lintas sektor untuk menciptakan ekosistem keamanan informasi yang kokoh dan berkelanjutan.

Proteksi data dalam mengatasi ancaman *cybersecurity* dalam konteks smart grid dideskripsikan dalam [11] sebagai salah satu aspek penting dari keamanan smart grid. [11] menyebutkan bahwa kerahasiaan (confidentiality) data sangat penting untuk mencegah akses tidak sah terhadap informasi. Ancaman kerahasiaan data dalam smart grid mencakup upaya pencurian informasi yang seharusnya dibagikan atau dijaga kerahasiaannya di antara pihak-pihak yang aman. Beberapa contoh serangan yang disebutkan dalam artikel tersebut termasuk pembacaan memori perangkat secara ilegal, pemalsuan payload, serangan replay, dan perubahan program kontrol smart meter. Untuk melindungi kerahasiaan data dalam smart grid, [11] menyebutkan bahwa pengkodean jaringan (network coding) digunakan untuk menjaga privasi data. Hal ini memberikan kerahasiaan dalam smart grid. Selain itu, artikel juga menyoroti pentingnya penggunaan teknik enkripsi, deteksi serangan (IDS), dan pencegahan serangan (IPS) untuk melindungi kerahasiaan data dalam smart grid. Dengan demikian, proteksi data dalam mengatasi ancaman *cybersecurity* dalam konteks smart grid melibatkan

penggunaan teknik pengkodean jaringan, enkripsi, IDS, dan IPS untuk menjaga kerahasiaan data dan mencegah akses tidak sah serta modifikasi yang tidak diizinkan terhadap data dalam infrastruktur smart grid.

[12] membahas analisis perspektif ekonomi dalam proteksi keamanan dan privasi big data. Dalam konteks proteksi data untuk mengatasi ancaman keamanan *cyber*, [12] menyoroti beberapa poin penting:

1. Ancaman Keamanan dan Privasi Big Data; big data menjadi semakin rentan terhadap serangan *cyber*, terutama karena data yang terkonsolidasi dapat menarik perhatian para penjahat *cyber*. Ancaman tersebut mencakup pencurian data, kerentanan terhadap kerusakan infrastruktur kritis, dan potensi keuntungan finansial dari data yang diretas.
2. Investasi dalam Proteksi Data; pentingnya investasi dalam proteksi data, terutama dalam industri keuangan dan farmasi/kesehatan. Hal ini menyoroti bahwa organisasi perlu mengalokasikan dana untuk melindungi data mereka dari serangan *cyber*, dan memberikan contoh solusi keamanan data yang digunakan dalam industri keuangan.
3. Asuransi *Cyber*crime; pentingnya asuransi *cyber*crime sebagai langkah proteksi tambahan. Asuransi ini membantu perusahaan dan individu melindungi diri dari dampak finansial pencurian data.
4. Regulasi Pemerintah; pentingnya regulasi pemerintah dalam mengatur proteksi data. Hal ini menunjukkan bahwa regulasi pemerintah dapat memainkan peran penting dalam memastikan bahwa organisasi melindungi data mereka dengan benar.

Proteksi data dapat menjadi strategi yang efektif dalam mengatasi ancaman keamanan *cyber* karena data yang terlindungi dapat mengurangi potensi kerugian finansial yang disebabkan oleh pelanggaran keamanan. [12] menyatakan bahwa risiko pelanggaran data atau pengumpulan data yang terganggu seringkali disukai oleh manfaat finansial potensial seperti pemerasan, penipuan, pencurian kekayaan intelektual, dan persaingan bisnis. Dengan demikian, melindungi data dengan cara yang efektif dapat membantu mencegah kerugian finansial yang disebabkan oleh kejahatan *cyber*. Selain itu, [12] juga menyebutkan bahwa pelanggaran keamanan data besar dapat mengakibatkan konsekuensi hukum yang serius dan kerusakan reputasi bagi perusahaan, seringkali lebih parah daripada pelanggaran data tradisional. Dengan demikian, proteksi data yang efektif dapat membantu mengurangi risiko keuangan, konsekuensi hukum, dan kerusakan reputasi yang disebabkan oleh ancaman keamanan *cyber*, sehingga menjadi strategi yang penting dalam mengatasi ancaman keamanan *cyber*.

Berdasarkan penelitian [10] disebutkan bahwa proteksi data dalam mengatasi ancaman *cybersecurity* sangat penting dalam menjaga keamanan informasi, terutama dalam sektor perbankan. [10] membahas tentang pentingnya melindungi data dari intrusi dan serangan siber yang dapat mengancam keamanan informasi perbankan. Berdasarkan penelitian [10] terdapat beberapa langkah proteksi data yang dapat diambil untuk mengatasi ancaman *cybersecurity*, terutama dalam konteks sektor perbankan. Beberapa langkah tersebut antara lain:

1. Deteksi *Malware*: Menggunakan teknologi deteksi *malware* yang canggih dan sistem proteksi data yang mampu mengidentifikasi dan mengatasi serangan *malware*.

2. Proteksi Terhadap Serangan Denial-of-Service (DoS): Menerapkan sistem proteksi yang dapat mengidentifikasi dan merespons serangan DoS untuk mencegah gangguan atau kegagalan dalam operasi sistem.
3. Perlindungan Terhadap Serangan *Phishing*: Melakukan pelatihan dan pendidikan kepada karyawan dan pengguna untuk mengenali dan menghindari serangan *phishing*. Selain itu, penerapan teknologi keamanan seperti filter email dan firewall juga dapat membantu melindungi data dari serangan *phishing*.
4. Keamanan Basis Data: Melakukan langkah-langkah keamanan yang kuat untuk melindungi basis data dari serangan SQL injection, seperti menggunakan parameterized queries, validasi input, dan penerapan prinsip keamanan yang ketat.
5. Enkripsi Data: Mengenkripsi data sensitif untuk melindungi informasi dari akses yang tidak sah. Enkripsi data dapat membantu melindungi data bahkan jika terjadi pelanggaran keamanan.
6. Monitoring dan Respons Terhadap Serangan: Menerapkan sistem monitoring yang canggih untuk mendeteksi serangan siber dan merespons dengan cepat untuk mengurangi dampak dari serangan tersebut.
7. Pembaruan Sistem: Memastikan bahwa sistem dan perangkat lunak selalu diperbarui dengan patch keamanan terbaru untuk mengatasi kerentanan yang ditemukan.
8. Pendidikan dan Pelatihan: Melakukan pendidikan dan pelatihan secara teratur kepada karyawan dan pengguna untuk meningkatkan kesadaran akan ancaman siber dan praktik keamanan yang baik.

Dengan menerapkan langkah-langkah proteksi data ini, sektor perbankan dapat meningkatkan keamanan informasi dan melindungi data sensitif dari berbagai ancaman *cybersecurity*.

4. KESIMPULAN

Keamanan informasi merupakan aspek krusial dalam era digital, terutama di tengah meningkatnya ancaman serangan *cyber* yang dapat merugikan individu, perusahaan, dan negara. Peningkatan ketergantungan pada teknologi digital, seperti yang diindikasikan oleh pertumbuhan pengguna internet, juga memperbesar potensi risiko. Indonesia sendiri menghadapi lonjakan percobaan serangan *cyber*, menyoroti urgensi pengembangan strategi keamanan *cyber* nasional. Dalam menghadapi ancaman keamanan *cyber* yang semakin kompleks, diperlukan upaya yang komprehensif. Pentingnya pemahaman mengenai keamanan *cyber*, terutama dalam konteks proteksi data, menunjukkan perlunya strategi yang efektif. Ancaman *cyber* mencakup berbagai jenis, mulai dari serangan fisik, logikal, hingga operasional. Kesadaran pengguna, regulasi pemerintah, dan investasi dalam proteksi data menjadi kunci untuk melawan ancaman tersebut.

REFERENSI

[1] B. Alhayani, H. J. Mohammed, I. Z. Chaloob, and J. S. Ahmed, “Effectiveness of artificial intelligence techniques against *cyber* security risks apply of IT industry,” in *Materials Today: Proceedings*, Elsevier BV, Mar. 2021, pp. 1–6. doi: 10.1016/j.matpr.2021.02.531.

[2] M. Bada and J. R. C. Nurse, "The social and psychological impact of *cyber*attacks," in *Emerging Cyber Threats and Cognitive Vulnerabilities*, Elsevier, 2019, pp. 73–92. doi: 10.1016/B978-0-12-816203-3.00004-6.
[3] E. Budi, D. Wira, and A. Infantono, "Strategi Penguatan *Cyber* Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0," in *Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia (SENASTINDO)*, Akademi Angkatan Udara, Dec. 2021, pp. 223–234. doi: 10.54706/senastindo.v3.2021.141.
[4] P. I. D. C. Wulan, D. P. Perdana, A. A. Kurniawan, and R. Fauzi, "Sosialisasi *Cyber* Security Awareness untuk meningkatkan literasi digital di SMK N 2 Salatiga," *KACANEGARA Jurnal Pengabdian pada Masyarakat*, vol. 5, no. 2, pp. 213–218, May 2022, doi: 10.28989/kacanegara.v5i2.1204.
[5] N. A. A. Rahman, I. H. Sairi, N. A. M. Zizi, and F. Khalid, "The importance of *cybersecurity* education in school," *International Journal of Information and Education Technology*, vol. 10, no. 5, pp. 378–382, May 2020, doi: 10.18178/ijiet.2020.10.5.1393.
[6] A. T. Tunggal, "Why is *Cybersecurity* Important?" Accessed: Dec. 26, 2023. [Online]. Available: https://www.upguard.com/blog/*cybersecurity*-important
[7] Y. Samudra, A. Hidayat, and M. F. Wahyu, "Pengenalan *Cyber* Security Sebagai Fundamental Keamanan Data Pada Era Digital," *AMMA : Jurnal Pengabdian Masyarakat*, vol. 1, no. 12, pp. 1594–1601, 2023, [Online]. Available: https://journal.mediapublikasi.id/index.php/amma
[8] K. N. Isnaini, D. F. Sulistiyani, and M. Sutrisno, "Data Security Awareness sebagai Upaya Peningkatan Literasi Tentang *Cyber* Attacks dan Threats," *JPMB: Jurnal Pemberdayaan Masyarakat Berkarakter* , vol. 3, no. 2, pp. 121–132, 2020.
[9] M. O. Hoshmand and S. Ratnawati, "Analisis Keamanan Infrastruktur Teknologi Informasi dalam Menghadapi Ancaman *Cybersecurity*," *AICOMS: Applied Information Technology and Computer Science*, vol. 2, no. 2, pp. 9–18, 2023, [Online]. Available: https://jurnal.politap.ac.id/index.php/aicoms
[10] D. Ghelani, T. Kian Hua, S. Kumar, and R. Koduru, "*Cyber* Security Threats, Vulnerabilities, and Security Solutions Models in Banking," *American Journal of Computer Science and Technology*, pp. 1–10, 2022, doi: 10.22541/au.166385206.63311335/v1.
[11] M. Z. Gunduz and R. Das, "*Cyber*-security on smart grid: Threats and potential solutions," *Elsevier - Computer Networks*, vol. 169, Mar. 2020, doi: 10.1016/j.comnet.2019.107094.
[12] H. Tao *et al.*, "Economic perspective analysis of protecting big data security and privacy," *Future Generation Computer Systems*, vol. 98, pp. 660–671, Sep. 2019, doi: 10.1016/j.future.2019.03.042