Maliki Interdisciplinary Journal (MIJ) eISSN: 3024-8140
Volume 2, Issue 6, 2024 pp. 965-971 http://urj.uin-malang.ac.id/index.php/mij/index

Keamanan informasi dalam konteks teknologi komunikasi modern

Alifiyah Nur Habibah
Program Studi Teknik Informatika, Universitas Islam Negeri Maulana Malik Ibrahim Malang;
e-mail: alifiyahnur356@gmail.com

Kata Kunci:
keamanan informasi; teknologi modern; keamanan siber; keamanan jaringan; teknologi

Keywords:
information security; modern technology; cyber security; network security; technology

A B S T R A K

Perkembangan pesat teknologi komunikasi modern telah mengubah cara kita berinteraksi, bekerja, dan berbagi informasi. Artikel ini membahas berbagai aspek keamanan informasi dalam konteks teknologi komunikasi modern, termasuk ancaman yang dihadapi, bentuk ancaman keamanan informasi, metode perlindungan, dan praktik terbaik. Masalah penelitian berfokus pada semakin pentingnya keamanan informasi di era transformasi digital dan kebutuhan individu, kelompok, dan pemerintah untuk menerapkan langkah-langkah keamanan yang efektif untuk melindungi informasi pribadi. Metodologi yang digunakan melibatkan ulasan literatur untuk memahami lanskap saat ini dari ancaman keamanan informasi, kerentanan, dan praktik terbaik. Peserta termasuk individu, organisasi, dan entitas pemerintah yang terlibat dalam praktik keamanan informasi.

A B S T R A C T

The rapid development of modern communication technology has changed the way we interact, work, and share information. This article deals with various aspects of information security in the context of modern communication technology, including threats faced, forms of security threats, methods of protection, and best practices. The research issue focuses on the increasing importance of information security in the era of digital transformation and the need for individuals, groups, and governments to implement effective security measures to protect personal information. The methodology used involves reviewing literature to understand the current landscape from information security threats, vulnerabilities, and best practices. Participants include individuals, organizations, and governmental entities involved in information security practices.

Pendahuluan

Dalam era digital yang terus berkembang pesat, teknologi komunikasi modern telah mengubah cara kita berinteraksi, bekerja, dan berbagi informasi. Meningkatnya aksesibilitas dan konektivitas di seluruh dunia telah membawa banyak manfaat, termasuk kemudahan dalam berkomunikasi, peningkatan efisiensi operasional, dan peningkatan tingkat produktivitas di berbagai industri (Ariani, 2022). Namun, di balik manfaat ini, terdapat tantangan besar yang harus dihadapi, yaitu isu keamanan informasi. Dalam teknologi komunikasi modern, keamanan informasi merujuk pada perlindungan data dari ancaman yang dapat menyebabkan kebocoran, kerugian, atau

penyalahgunaan data. Ancaman ini dapat berasal dari berbagai sumber, seperti peretas (hacker), malware, phishing, serta ancaman dari dalam. Oleh karena itu, tidak dapat dipungkiri bahwa dampak terhadap perkembangan masyarakat Indonesia yang sedang berkembang di era reformasi saat ini adalah menghadapi berbagai krisis politik, ekonomi, dan sosial budaya, dan hal tersebut harus ditanggulangi sedemikian rupa (Habibi & Liviani, 2020).

Perkembangan teknologi informasi dan komunikasi terus berkembang pesat, kini teknologi informasi dan komunikasi sudah dapat dimanfaatkan melalui perangkat mobile (Habibi & Liviani, 2020). Teknologi informasi dan komunikasi (TIK) telah membawa dampak positif yang signifikan terhadap ekonomi global. Kemajuan TIK telah meningkatkan produktivitas, mendorong persaingan yang sehat, dan meningkatkan partisipasi masyarakat. Hal ini dimungkinkan oleh konektivitas yang lebih baik antar pemerintah, pengusaha, dan masyarakat di dunia maya. Namun, konektivitas global ini juga menghadirkan tantangan baru, yaitu ancaman keamanan siber. Meningkatnya interaksi online membuat pemerintah, pengusaha, dan individu rentan terhadap serangan siber. Oleh karena itu, diperlukan upaya yang lebih fokus untuk memperkuat keamanan siber demi melindungi ekonomi global dan menjaga kepercayaan masyarakat (Budi et al., 2021). Penting bagi setiap individu, kelompok, dan pemerintah untuk memahami dan menerapkan strategi keamanan yang efektif untuk melindungi data dan menjaga keutuhan sistem informasi.

Kemajuan teknologi seperti Internet of Things (IoT), cloud computing, dan big data analytics membawa manfaat yang luar biasa, namun juga menghadirkan kompleksitas baru dalam mengelola keamanan informasi. Sementara IoT menawarkan konektivitas yang luas dan integrasi sistem yang canggih, hal ini juga membuka peluang bagi potensi ancaman baru. Demikian pula, penggunaan cloud computing yang semakin populer membawa tantangan tersendiri terkait dengan keamanan data yang disimpan dan diproses di lingkungan cloud. Di era Society 5.0, di mana teknologi informasi dan komunikasi menjadi semakin terhubung dan canggih, Indonesia memerlukan strategi keamanan siber nasional yang kuat untuk melindungi infrastruktur digitalnya, data pribadi warga negaranya, dan stabilitas ekonominya (Budi et al., 2021). Di samping itu, peraturan dan kebijakan terkait keamanan informasi juga sangat penting untuk menjaga dan memastikan perlindungan data. Kebijakan ini mencakup kerangka kerja untuk respon terhadap insiden, pedoman untuk manajemen risiko dan peraturan keamanan.

Pembahasan

Di era digital ini, cara kita berinteraksi dan berbagi informasi telah mengalami transformasi besar dengan kemunculan teknologi komunikasi modern seperti internet, perangkat mobile, dan media sosial. Karena banyaknya data yang dikirim melalui berbagai platform seperti internet, telepon, dan jaringan komputer, keamanan informasi menjadi sangat penting. Namun, perkembangan ini juga membawa tantangan besar dalam hal keamanan informasi. Artikel ini membahas berbagai aspek keamanan informasi dalam konteks teknologi komunikasi modern, termasuk ancaman yang dihadapi, bentuk ancaman keamanan informasi, metode perlindungan, dan praktik terbaik yang dapat diterapkan.

Ancaman Keamanan Informasi

Di era digital yang serba terhubung dan penuh kecanggihan ini, informasi menjelma menjadi aset berharga. Kemudahan pertukaran informasi dan data melalui internet dan perangkat digital membawa manfaat luar biasa, namun juga membuka celah bagi berbagai ancaman terhadap keamanan informasi. Keamanan informasi merupakan upaya terstruktur untuk mencegah dan menangkal tindakan kriminal yang berkaitan dengan informasi, serta meminimalkan dampak yang ditimbulkannya. Hal ini penting untuk menjaga integritas, kerahasiaan, dan ketersediaan informasi. Modernisasi teknologi, yang sering disebut "era digital", ditandai dengan kemunculan internet dan komputer. Kehidupan digital yang serba cepat dan terkoneksi ini menghadirkan ketergantungan pada perangkat seperti komputer tablet dan smartphone. Kemudahan akses informasi di era digital turut memicu munculnya ancaman terhadap keamanan informasi. Pihak-pihak yang tidak bertanggung jawab melakukan tindakan ilegal untuk mendapatkan informasi yang diinginkan. Hal ini meningkatkan risiko serangan sistem informasi seperti hacking, cybercrime, skimming, dan lainnya.

Di era digital yang serba terhubung ini, keamanan informasi menjadi semakin penting. Berbagai jenis malware, seperti ransomware, phishing, dan social engineering, mengintai para pengguna internet, mengancam data pribadi dan aset digital mereka. Ransomware adalah jenis malware yang menggunakan metode cryptovirology untuk mengenkripsi data korban. Para pelaku kemudian menuntut tebusan dalam bentuk mata uang digital seperti Bitcoin untuk membuka enkripsi dan memulihkan akses ke data. Phishing adalah teknik penipuan online yang bertujuan untuk mencuri informasi sensitif seperti password, nomor kartu kredit, atau data pribadi lainnya. Para pelaku biasanya membuat situs web palsu yang menyerupai situs web asli, seperti bank atau toko online, dan mengirim email phishing yang tampak meyakinkan untuk memancing korban memasukkan informasi mereka. Social Engineering adalah teknik manipulasi psikologis yang digunakan untuk mendapatkan informasi sensitif dari korban. Para pelaku biasanya berpura-pura menjadi orang lain yang terpercaya, seperti karyawan bank atau administrator IT, untuk mendapatkan informasi penting seperti password atau akses ke sistem komputer. Media sosial menjadi sumber informasi berharga bagi para peretas. Dengan mempelajari profil media sosial korban, mereka dapat mengumpulkan data pribadi seperti hobi, tempat tinggal, dan bahkan informasi keluarga untuk melancarkan aksi mereka.

Faktor keamanan informasi telah menjadi topik yang sangat penting yang tidak boleh diabaikan. Penerapan keamanan data dimulai dari diri kita sendiri dan diterapkan pada perangkat yang sering kita gunakan seperti komputer dan perangkat. Untuk menjaga proteksi komputer digunakan untuk mengakses komputer dengan password, menginstal anti virus, selalu menggunakan software berlisensi, tidak menggunakan media data yang ditransfer oleh orang yang tidak dikenal (harddisk eksternal, flash memory) dan selalu menyimpan data. secara teratur Perlindungan kata sandi sangat penting untuk keamanan data. Selalu gunakan kata sandi yang panjangnya minimal delapan karakter, terdiri dari huruf besar, huruf kecil, karakter khusus, dan angka, serta ubah kata sandi anda secara berkala hingga 180 hari. Keamanan informasi juga didukung oleh penggunaan internet, intranet, email, Wi-Fi yang cerdas dan ketaatan pada etika

dalam penggunaan media sosial, karena pergerakan informasi yang cepat dapat menimbulkan konsekuensi negatif. Beberapa cara tersebut dapat digunakan untuk meningkatkan keamanan data. Kesadaran akan keamanan informasi semakin meningkat dan melahirkan budaya keamanan informasi dalam kehidupan sehari-hari, yang tidak hanya melindungi kita, namun meluas ke bidang yang lebih luas (Kurniawan, 2021).

Kriptografi dan Enkripsi Data

Kriptografi berasal dari gabungan dua kata yaitu "Crypto" yang berarti rahasia dan "graphia" yang berarti tulisan. Dalam komputasi, kriptografi diartikan sebagai ilmu dan seni menjaga keamanan data. Komponen kriptografi yang paling penting adalah algoritma kriptografi, biasanya berupa persamaan matematika yang digunakan sebagai dasar sistem kerahasiaan data, dan kunci yang merupakan alat kerahasiaan data (Sutarno, 2007). Dalam teknologi komunikasi kontemporer, kriptografi dan enkripsi data adalah dua konsep penting untuk menjaga keamanan data. Kriptografi sebagian besar digunakan untuk melindungi data sensitif dari orang yang tidak berhak mengetahuinya.

Pengoperasian kriptografi didasarkan pada tiga fungsi algoritma kriptografi, yaitu enkripsi, dekripsi, dan kunci. Enkripsi mengubah plaintext menjadi ciphertext, sedangkan dekripsi memahami data dari ciphertext ke plaintext. Dan kunci digunakan sebagai parameter enskripsi dan dekripsi (Sutarno, 2007). Dengan menggunakan algoritma kriptografi, data sensitif seperti pesan teks, file, atau informasi transaksi dienkripsi sebelum ditransmisikan melalui internet atau disimpan di dalam penyimpanan digital. Dengan menerapkan enkripsi data, informasi sensitif akan terlindungi dari akses tidak sah atau perubahan oleh pihak yang tidak berwenang. Penerapan Enkripsi data penting untuk melindungi kerahasiaan dan integritas data jika perangkat fisik seperti laptop atau ponsel pintar hilang atau dicuri.

Keamanan Jaringan

Keamanan jaringan merupakan bagian penting dalam industri teknologi informasi yang bertujuan untuk melindungi infrastruktur jaringan komputer dari ancaman yang dapat merusak, mencuri atau membahayakan integritas data. Upaya untuk menjaga keamanan jaringan menjadi semakin penting, seiring dengan meningkatnya serangan *cyber* lintas sektoral, dan karena jaringan Internet publik dan global pada dasarnya tidak aman, keamanan sistem informasi Internet menjadi sangat penting. Ketika informasi dikirim dari satu komputer ke komputer lain di Internet, informasi tersebut berpindah melalui beberapa komputer lain, yang berarti akan memberi kesempatan pada pengguna tersebut untuk mengambil alih satu atau lebih komputer.

Kejahatan cyber atau lebih dikenal dengan cyber crime adalah suatu bentuk kejahatan virtual yang memanfaatkan media komputer yang terhubung ke internet, dan mengekploitasi komputer lain yang terhubung internet juga. Jika sistem operasi memiliki celah pencurian informasi data maka keamanan, peretas, cracker, dan script kiddies dapat mengeksploitasinya untuk mendapatkan akses ke komputer. Karena biasanya hanya memerlukan verifikasi identitas, biasanya dengan username dan password.

Ada beberapa poin yang harus di pahami dalam pembahasan keamanan jaringan diantaranya:

1. Firewall: salah satu mekanisme pertahanan pertama dalam sebuah jaringan. Firewall berfungsi sebagai penghalang antara jaringan internal dan eksternal. Firewall juga memiliki kemampuan untuk mengawasi dan mengatur lalu lintas data dari yang masuk dan keluar jaringan.
2. Pemantauan Jaringan (Network Monitoring): Pemantauan jaringan secara aktif membantu mendeteksi adanya anomali atau aktivitas mencurigakan yang mungkin merupakan tanda serangan terhadap jaringan. Dengan pemantauan yang efektif, administrator jaringan dapat menanggapi ancaman tersebut sebelum menyebabkan kerusakan yang lebih besar.
3. Enkripsi Data: Seperti yang telah kita bahas sebelumnya, enkripsi data adalah teknik yang efektif untuk melindungi informasi yang dipertukarkan melalui jaringan agar tidak mudah disusupi oleh pihak yang tidak berwenang.
4. Patching dan Update: Melakukan patching sistem dan aplikasi yang digunakan dalam jaringan dan update perangkat lunak keamanan yang ada sangat penting untuk mengatasi bug atau celah keamanan yang dapat dieksploitasi oleh hacker.
5. Kebijakan Keamanan: Menyusun kebijakan keamanan yang jelas dan diterapkan secara konsisten di seluruh jaringan merupakan landasan dalam memastikan bahwa aspek keamanan dijaga dengan baik.

Kerentanan IoT (Internet of Things)

Definisi Internet of Things adalah konsep yang memiliki kemampuan untuk mengirimkan informasi data melalui jaringan. Hal ini tentu saja mendorong banyak perusahaan menawarkan berbagai program untuk membantu pengembang dalam pengembangan produk berbasis IoT ini. Adapun arti singkat dari Internet of Things adalah Internet dari peralatan / perangkat-perangkat. Sehingga secara singkat memiliki arti seberapa sering perangkat yang digunakan terhubung ke internet (Van den Akker, 1999).

Internet of Things (IoT) adalah sebuah konsep di mana objek fisik seperti perangkat elektronik, kendaraan, dan peralatan rumah tangga, dilengkapi dengan sensor, perangkat lunak, dan koneksi internet, yang memungkinkan objek tersebut berkomunikasi satu sama lain dan berbagi informasi. Meskipun IoT membawa banyak manfaat dalam kehidupan sehari-hari, namun juga membawa risiko keamanan yang meningkat karena kerentanan yang melekat pada teknologi ini. Salah satu risiko penggunaan Internet of Things ini adalah kurangnya standar keamanan, yang membuat perangkat IoT rentan terhadap serangan cyber. Selain itu, data yang dikirim antara perangkat IoT dan server seringkali tidak dienkripsi dengan baik, yang membuat perangkat IoT rentan terhadap penyadapan data oleh pihak yang tidak berwenang.

Perangkat IoT dapat menjadi sasaran serangan hacker yang menemukan celah keamanan untuk mengakses data sensitif atau merusak sistem. Produsen perangkat, pengguna, dan para pemangku kepentingan lainnya dapat bekerja sama untuk meningkatkan keamanan IoT dengan menerapkan standar keamanan yang ketat,

pembaruan perangkat lunak yang sering, dan enkripsi data. Kesadaran menjadi titik awal bagi seluruh karyawan suatu organisasi atau pengguna media digital ketika mencari atau memahami keamanan teknologi informasi.

Kesadaran Keamanan Informasi

Kesadaran menjadi titik awal bagi seluruh karyawan suatu organisasi atau pengguna media digital ketika mencari atau memahami keamanan teknologi informasi. Dengan kesadaran keamanan informasi, seorang karyawan atau pengguna dapat fokus pada satu atau lebih potensi masalah atau ancaman (Kurniawan, n.d.). Kesadaran keamanan informasi adalah ketika seseorang atau organisasi menyadari betapa pentingnya menjaga kerahasiaan, integritas, dan ketersediaan informasi yang mereka miliki. Sangat penting untuk memahami keamanan informasi untuk melindungi data pribadi dan sensitif dari ancaman keamanan seperti pencurian data, serangan malware, dan penyusupan. Dengan meningkatkan kesadaran pengguna, kita dapat membentuk lapisan pertahanan tambahan dalam melindungi sistem informasi. Kesadaran pengguna merupakan langkah pertama dalam menghadapi ancaman keamanan dan dasar yang kuat untuk perlindungan menyeluruh.

Kesimpulan dan Saran

Perkembangan teknologi komunikasi modern telah membawa dampak positif yang besar bagi masyarakat dunia. Namun, kita juga harus menyadari bahwa semakin canggihnya teknologi, semakin kompleks pula tantangan yang dihadapi dalam menjaga keamanan informasi. Ancaman keamanan informasi dapat menyebabkan kerugian yang besar bagi individu, organisasi, bahkan negara. Oleh karena itu, penting bagi kita untuk meningkatkan kesadaran tentang pentingnya keamanan informasi dan mengambil langkah yang tepat untuk mengatasi ancaman tersebut.

Salah satu langkah yang dapat dilakukan adalah dengan meningkatkan literasi digital, yaitu kemampuan individu untuk memahami dan menggunakan teknologi informasi secara aman dan bertanggung jawab. Selain itu, pemerintah dan perusahaan juga perlu mengambil tindakan yang lebih serius dalam memperkuat sistem keamanan informasi, seperti melalui penggunaan sistem enkripsi, perlindungan data, dan pemantauan yang ketat terhadap akses informasi.

Daftar Pustaka

Ariani, N. (2022). Peran teknologi dalam inovasi pendidikan.

Budi, E., Wira, D., & Infantono, A. (2021). Strategi penguatan cyber security guna mewujudkan keamanan nasional di era society 5.0. *Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia (SENASTINDO)*, *3*, 223–234. https://doi.org/10.54706/senastindo.v3.2021.141

Habibi, M. R., & Liviani, I. (2020). Kejahatan teknologi informasi (cyber crime) dan penanggulangannya dalam sistem hukum Indonesia. *Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam*, *23*(2), 400–426. https://doi.org/10.15642/alqanun.2020.23.2.400-426

Kurniawan, R. (2021). Analisis keamanan fasilitas jaringan (wifi) terhadap serangan packet sniffing pada protocol http dan https. *Universitas Islam Riau.*

Kurniawan, R. (n.d.). Pengantar keamanan data.

Sutarno, H. (2007). Enkripsi data sistem kriptografi kunci publik menggunakan algoritma diophantine. *FPMIPA Universitas Pendidikan Indonesia*. *10*(2), 8–20.

Van den Akker, J. (1999). Principles and methods of development research. *Design approaches and tools in education and training*, 1-14.