JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 3, Oktober 2023
ISSN 3025-0919 (media online)
Hal 999-999

Keamanan Jaringan Melindungi Sistem dari Serangan Luar

Agung Wijoyo[1*], Ade Rosadi[1], Fadhil Is Hakim[1], Muhamad Hanafi[1], Rizal Sidik[1]

[1]Fakultas Ilmu Komputer, Program Studi Teknik Informatika, Universitas Pamulang, Tangerang Selatan, Banten, Indonesia

Email: [1*]dosen1671@unpam.ac.id, [2]aderosadi222@gmail.com, [3]fadhilishakim@gmail.com, [4]muhamadhanafi319@gmail.com, [5]rizalsidikrosyadi46@gmail.com

AbstrakPentingnya keamanan jaringan dalam era digital yang berkembang disoroti dalam pembahasan ini. Jaringan komputer digunakan secara luas untuk berkomunikasi, berbagi informasi, dan menjalankan bisnis online, tetapi dengan konektivitas tersebut datang risiko serangan siber yang dapat merusak, mencuri, atau menghancurkan data dan sistem. Keamanan jaringan melibatkan serangkaian tindakan dan praktik untuk melindungi integritas, kerahasiaan, dan ketersediaan data dan sistem. Metode kuantitatif digunakan dalam penelitian ini untuk mengumpulkan dan menganalisis data terkait keamanan jaringan, seperti jumlah serangan siber, kerugian yang ditimbulkan, dan tingkat kesadaran pengguna terhadap risiko keamanan. Hasil penelitian ini membantu organisasi untuk meningkatkan keamanan jaringan mereka dengan bukti kuat. Dalam pembahasan, juga dijelaskan berbagai jenis serangan siber, prinsip dasar keamanan jaringan, peran teknologi seperti firewall dan IDS, serta pentingnya pencegahan serangan untuk menjaga keamanan jaringan.

Kata Kunci: Jaringan; Keamanan jaringan; Era digital; Serangan siber; Data dan sistem

AbstractThe importance of network security in the evolving digital era is highlighted in this discussion. Computer networks are widely used for communication, information sharing, and conducting online businesses, but with this connectivity comes the risk of cyberattacks that can damage, steal, or disrupt data and systems. Network security involves a series of actions and practices to protect the integrity, confidentiality, and availability of data and systems. Quantitative methods are used in this research to gather and analyze data related to network security, such as the number of cyberattacks, the losses incurred, and user awareness of security risks. The results of this research assist organizations in enhancing their network security with strong evidence. The discussion also explains various types of cyberattacks, the basic principles of network security, the role of technologies like firewalls and IDS, and the importance of preventing attacks to maintain network security.

Keywords: Network; Network security; Digital era; Cyber attacks; Data and systems

1. PENDAHULUAN

Dalam era digital yang semakin berkembang, jaringan komputer telah menjadi tulang punggung dari hampir semua aspek kehidupan kita. Baik dalam skala individu maupun korporat, jaringan komputer digunakan untuk berbagai keperluan, mulai dari berkomunikasi dan berbagi informasi hingga menjalankan bisnis secara online. Namun, dengan kemudahan dan kenyamanan yang ditawarkan oleh konektivitas ini, datanglah risiko besar yang harus dihadapi, yaitu serangan dari luar yang dapat merusak, mencuri, atau bahkan menghancurkan data dan sistem yang ada. Oleh karena itu, keamanan jaringan menjadi sangat penting.

Keamanan jaringan adalah serangkaian tindakan dan praktik yang dirancang untuk melindungi sistem komputer dan data dari serangan yang dapat membahayakan integritas, kerahasiaan, dan ketersediaan mereka. Ancaman-ancaman ini dapat berupa serangan siber, seperti malware, serangan phishing, serangan Denial of Service (DoS), dan banyak lagi. Keamanan jaringan juga melibatkan perlindungan terhadap akses yang tidak sah, pemantauan aktivitas jaringan, serta implementasi kebijakan keamanan yang tepat.

2. METODE

Dalam penelitian yang berfokus pada "Keamanan Jaringan: Melindungi Sistem dari Serangan Luar," metode kuantitatif digunakan sebagai pendekatan utama untuk mengumpulkan, menganalisis, dan

menginterpretasikan data dalam bentuk angka atau statistik. Melalui pengumpulan data kuantitatif, peneliti dapat mengukur faktor-faktor terkait keamanan jaringan, seperti jumlah serangan siber, kerugian yang ditimbulkan, atau tingkat kesadaran pengguna terhadap risiko keamanan. Analisis statistik digunakan untuk mengidentifikasi pola dan tren yang relevan, seperti peningkatan serangan tertentu selama periode waktu tertentu atau efektivitas tindakan keamanan yang diimplementasikan. Data kuantitatif juga memungkinkan penilaian kinerja teknologi keamanan, seperti firewall atau sistem deteksi ancaman, serta pengukuran efektivitas tindakan pencegahan seperti pembaruan perangkat lunak dan pelatihan pengguna.

Hasil dari penelitian ini dapat membantu organisasi dalam mengambil keputusan berdasarkan bukti kuat untuk meningkatkan keamanan jaringan mereka, menjaga integritas, kerahasiaan, dan ketersediaan data dan sistem yang digunakan dalam era digital yang semakin berkembang.

3. ANALISA DAN PEMBAHASAN

Dalam upaya untuk menjaga keamanan jaringan, pemahaman tentang berbagai jenis serangan siber sangat penting. Beberapa serangan siber yang paling umum meliputi malware, serangan phishing, DoS, DDoS, serangan Man-in-the-Middle, serangan Zero-Day, dan serangan melalui jaringan nirkabel. Malware adalah ancaman berbahaya yang dapat merusak sistem dan mencuri data, sementara serangan phishing mencoba mendapatkan informasi sensitif dengan menyamar sebagai entitas tepercaya. Serangan DoS dan DDoS bertujuan menghentikan layanan jaringan dengan banjiran lalu lintas, dan serangan Man-in-the-Middle dapat menyusup dalam komunikasi. Serangan Zero-Day memanfaatkan kerentanan yang belum diketahui, dan serangan melalui jaringan nirkabel bisa menjadi pintu masuk ke dalam jaringan.

Untuk melindungi jaringan dari serangan tersebut, prinsip dasar keamanan jaringan seperti kepercayaan, kerahasiaan, integritas, ketersediaan, dan keandalan harus diterapkan. Kepercayaan memastikan bahwa hanya entitas yang sah yang dapat mengakses jaringan, kerahasiaan menjaga informasi sensitif dari akses yang tidak sah, integritas melindungi data dari perubahan yang tidak sah, ketersediaan menjaga jaringan aktif, dan keandalan menjaga konsistensi kebijakan keamanan.

Untuk mendeteksi dan merespons serangan siber, organisasi dapat menggunakan teknologi seperti firewall, IDS, sistem deteksi ancaman, dan pemantauan lalu lintas jaringan secara real-time. Namun, pencegahan adalah kunci dalam menjaga keamanan jaringan. Ini termasuk pemutusan kerentanan, pemantauan terus-menerus, pembaruan perangkat lunak berkala, dan pelatihan pengguna. Pemutusan kerentanan melibatkan identifikasi dan perbaikan kerentanan keamanan, pemantauan terus-menerus membantu mendeteksi serangan lebih awal, pembaruan perangkat lunak mengatasi kerentanan yang ditemukan, dan pelatihan pengguna meningkatkan kesadaran tentang risiko. Melalui kombinasi upaya ini, jaringan dapat menjadi lebih aman dan terlindungi dari serangan siber.

4. KESIMPULAN

Melalui penelitian ini, kami telah memahami bahwa keamanan jaringan merupakan elemen kunci dalam menjaga integritas, kerahasiaan, dan ketersediaan data dan sistem komputer. Ancaman siber yang berkembang pesat, seperti malware, serangan phishing, DDoS, dan lainnya, menunjukkan betapa pentingnya pemahaman dan perlindungan yang efektif terhadap jaringan dan sistem.

Kami juga telah membahas berbagai jenis serangan dan teknik yang digunakan oleh penyerang, serta prinsip dasar keamanan jaringan yang harus diterapkan. Kami telah menyoroti peran teknologi, seperti firewall, IDS, dan sistem deteksi ancaman, dalam mendeteksi dan merespons serangan siber.

REFERENCES

Badrul, mohammad. Dedi sugiarto, febi dan dodi. 2018. Teknik Jaringan (Sistem Operasi dan Jaringan). Jakarta: Inti Prima Promosindo.

Gutters. Joko dan Erna. 2019. Perancangan dan pengembangan jaringan Vlan pada Dili *Institute of technology* (DIT). ISSN:2338-612. Jurnal Jarkom. Vol. 1 No. 2 Januari 2016.

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 3, Oktober 2023
ISSN 3025-0919 (media online)
Hal 999-999

Herdina, Yana.2017. Evaluasi Implementasi Keamanan Jaringan Virtual Private Network (VPN) (Study kasus pada CV. Pangestu Jaya). Yogyakarta. Jurnal teknologi, volume 5 Nomor 2 Desember 2017.

Nugroho, Iwan,. Bebas dan Kustanto. 2012. Perbandingan Performa di Jaringan VPN Metode Point to Point Tunneling Protocol. SSN : 2338-4018. Jurnal TikomSin. 2017

Rudol, 2017. Implementasi Keamanan Jaringan Komputer Pada VPN Menggunakan IP sec. ISSN 2502-6968. Jurnal Infotec. Vol : Vol 2, No 1, Februari 2017.