Infotek : Jurnal Informatika dan Teknologi
Vol. 6 No. 2, Juli 2023
Hal. 01-08

e-ISSN 2614-8773

DOI : 10.29408/jit.v4i1.2999 Link : https://dx.doi.org/10.29408/jit.v4i1.2999

STRATEGI UNTUK MENJAMIN KEAMANAN JARINGAN YANG EFISIEN DAN EFEKTIF

Iyondiansyah Eka Cahyo[1]*, Imam Noor Arifin[2], Muhammad Alfahri Solehan[3], Hanif Rifqi Alkhafizh[4], Aiko Nur Hendry Yansyah[5],
[1,2,3,4,5] Teknik Komputer, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta
*iyondiansyahekacahyo@students.amikom.ac.id

Abstrak

Di dunia yang terhubung saat ini, memastikan keamanan jaringan sangat penting, dan memasang keamanan port adalah langkah yang diperhitungkan untuk melindungi jaringan dari akses yang tidak diinginkan dan potensi pelanggaran keamanan. Keamanan jaringan juga menjadi kunci untuk mengamankan semua data baik data pribadi atau data perusahaan. Topik bahasan utama dalam abstrak ini adalah bagaimana menggunakan teknik keamanan port untuk meningkatkan keamanan jaringan. Ini menekankan pentingnya menggunakan strategi menyeluruh yang menggabungkan segmentasi jaringan, kontrol akses, dan langkah-langkah otentikasi. Dengan memperhatikan strategi dan tahapan keamanan diharapkan dan menjadi peningkatan untuk menjaga keamanan jaringan komputer, Dengan mempraktikkan taktik ini, perusahaan dapat membuat kerangka kerja keamanan jaringan yang kuat yang melindungi data sensitif, mengurangi risiko, dan menjamin ketersediaan dan integritas sumber daya jaringan mereka. Abstrak ini berfungsi sebagai pengantar eksplorasi jurnal tentang berbagai strategi untuk memanfaatkan keamanan port secara efektif untuk memastikan keamanan jaringan. Selain itu, mengurangi dari resiko yang akan terjadi pada keamanan jaringan.

Kata kunci: Keamanan port, Teknik keamanan port, Pengurangan risiko.

Abstract

In the connected world of today, ensuring network security is essential, and installing port security is a calculated move to safeguard networks from unwanted access and potential security breaches. Network security is also the key to securing all data, both personal data and company data The main topic of discussion in this abstract is how to use port security techniques to improve network security. It emphasizes the significance of using a thorough strategy that incorporates network segmentation, access controls, and authentication measures. By putting these tactics into practice, companies may create a strong network security framework that protects sensitive data, reduces risks, and guarantees the availability and integrity of their network resources. This abstract serves as an introduction to the journal's exploration of various strategies for effectively utilizing port security to ensure network security. In addition, reducing the risks that will occur in network security.

Keywords: Port security, Port security techniques, Risk reduction.

1. Pendahuluan

Keamanan jaringan adalah aspek yang sangat penting dalam lingkungan digital yang berkembang pesat. Di zaman yang semakin terhubung ini, organisasi dan individu menghadapi ancaman serius terhadap keamanan, integritas, dan ketersediaan data mereka. Oleh karena itu, sangat penting untuk mengembangkan strategi yang efektif dan efisien untuk menjaga keamanan jaringan[1].

Artikel ini bertujuan untuk menyajikan strategi yang dapat secara efektif dan efisien membantu organisasi dan individu menjaga keamanan jaringan mereka. Dalam konteks ini, efektif berarti strategi yang mampu memberikan perlindungan optimal dengan penggunaan sumber daya yang minimal, sedangkan efektif berarti strategi yang mampu mengatasi ancaman keamanan, keamanan yang muncul, dan perlindungan jaringan yang lengkap. Jurnal

Infotek : Jurnal Informatika dan Teknologi
Vol. 6 No. 2, Juli 2023
Hal. 01-08

e-ISSN 2614-8773

DOI : 10.29408/jit.v4i1.2999 Link : https://dx.doi.org/10.29408/jit.v4i1.2999

ini akan membahas tiga metode menerapkan konsep port security dalam keamanan jaringan yaitu shutdown, restrict, dan protect. Ini termasukmengidentifikasi kemungkinan risiko, mengembangkan kebijakan keamanan yang komprehensif, menerapkan tindakan teknis seperti menggunakan shutdown, restrict, dan protect.

Melalui pemahaman menyeluruh tentang strategi keamanan jaringan yang efektif dan efisien, kami berharap pembaca artikel ini dapat mengidentifikasi langkah-langkah yang tepat untuk melindungi jaringan mereka dari ancaman ancaman yang ada. Dengan menerapkan strategi ini, organisasi dan individu dapat mengurangi risiko serangan dan menjaga jaringan mereka tetap berjalan.

2. Tinjauan Pustaka

Keamanan jaringan menjadi kebutuhan yang semakin mendesak dalam era digital yang terus berkembang. Ancaman serangan siber yang kompleks dan serbuan ancaman membutuhkan strategi yang efisien dan efektif untuk menjaga keamanan jaringan dengan baik. Dalam tinjauan pustaka ini, kami akan mengkaji beberapa penelitian terkait strategi untuk menjamin keamanan jaringan yang efisien dan efektif, dengan fokus pada evaluasi risiko, kebijakan keamanan, pemantauan, pemulihan, dan pelatihan pengguna. Untuk memulai strategi keamanan jaringan yang efisien, evaluasi risiko yang menyeluruh diperlukan. Menurut Jones dan Brinson (2018), evaluasi risiko melibatkan identifikasi ancaman potensial, penilaian kerentanan jaringan, dan penentuan dampak yang mungkin terjadi. Hasil dari evaluasi risiko ini dapat membantu organisasi dan perusahaan mengidentifikasi area yang rentan dan memprioritaskan langkah-langkah keamanan yang harus diambil. Kemudian, Penetapan kebijakan keamanan yang tepat merupakan langkah penting dalam strategi keamanan jaringan yang efisien dan efektif[2]. Menurut Fung dan Pun (2020), kebijakan keamanan yang ketat harus mencakup aspek-aspek seperti akses jaringan, otentikasi pengguna, enkripsi data, dan kebijakan penggunaan yang jelas. Kebijakan ini harus disusun dengan mempertimbangkan kebutuhan unik organisasi serta standar keamanan yang relevan[3].

Selain itu, Pemantauan aktif jaringan merupakan langkah penting dalam mendeteksi dan mencegah serangan yang mungkin terjadi. Menurut Li et al. (2021), implementasi sistem pemantauan yang canggih dapat membantu mengidentifikasi aktivitas mencurigakan, serangan berbasis malware, atau upaya penetrasi yang tidak sah[4]. Pemantauan yang berkelanjutan dan respons cepat terhadap insiden dapat membantu mengurangi dampak serangan serta memperkuat keamanan jaringan. Kesiapan pemulihan setelah serangan adalah aspek penting dalam strategi keamanan jaringan yang efisien. Menurut Hasan et al. (2023), langkah-langkah pemulihan yang efektif melibatkan pencadangan data secara teratur, pemulihan sistem yang handal, dan pemulihan aktivitas bisnis yang cepat. Proses pemulihan harus diuji secara berkala untuk memastikan keandalan dan kesiapan dalam menghadapi serangan atau kejadian yang tidak diinginkan[5]. Lalu Aspek pelatihan dan kesadaran pengguna juga penting dalam strategi keamanan jaringan yang efisien dan efektif. Menurut Elbendak et al. (2020), pelatihan yang terus-menerus dan kampanye kesadaran pengguna dapat membantu mengurangi kesalahan manusia yang dapat menyebabkan kerentanan jaringan[6]. Pengguna yang terlatih akan lebih sadar akan praktik keamanan, seperti penggunaan kata sandi yang kuat, pengenalan serangan phishing, dan langkah-langkah pencegahan yang penting.

Melalui tinjauan pustaka ini, dapat disimpulkan bahwa strategi untuk menjamin keamanan jaringan yang efisien dan efektif melibatkan evaluasi risiko yang menyeluruh, penetapan kebijakan keamanan yang ketat, pemantauan jaringan yang aktif, kesiapan pemulihan yang baik, serta pelatihan dan kesadaran pengguna yang terus-menerus ditingkatkan. Implementasi strategi ini dapat

Infotek : Jurnal Informatika dan Teknologi
Vol. 6 No. 2, Juli 2023
Hal. 01-08

e-ISSN 2614-8773

DOI : 10.29408/jit.v4i1.2999 Link : https://dx.doi.org/10.29408/jit.v4i1.2999

membantu organisasi dan perusahaan melindungi jaringan mereka dari serangan siber dan menjaga keamanan dengan baik di tengah ancaman yang terus berkembang.

3. Metode Penelitian

Penelitian yang dilakukan dengan menggunakan pengumpulan data yang kami kembangkan sebagai bahan referensi untuk menjawab bagaimana strategi menjamin keamanan jaringan dengan efisien dan efektif. Adapun metode yang kami lakukan untuk melakukan strategi untuk menjamin keamanan jaringan dengan cara melakukan shutdown, restrict, dan protect pada jaringan.

a. Pengumpulan data

Untuk menjawab pertanyaan penelitian ini, data akan dikumpulkan dari berbagai sumber. Berikut adalah sumber data yang akan digunakan dalam penelitian ini:

- Studi literatur tentang keamanan jaringan dan strategi yang digunakan untuk melindungi data dan informasi sensitif.
- Pengumpulan data dari berbagai jurnal port security yang kami gunakan untuk menjawab penelitian ini.
- Pengamatan lapangan yang menerapkan kebijakan keamanan yang efektif dan efisien dalam melindungi data dan informasi sensitif.

b. Identifikasi Kemungkinan Risiko

Setelah data telah dianalisis, kemungkinan risiko yang dihadapi oleh organisasi dan individu dalam menjaga keamanan jaringan mereka akan diidentifikasi. Risiko ini mencakup serangan siber, ancaman keamanan, dan kehilangan data dan informasi sensitif.

c. Pengembangan Kebijakan Keamanan yang Komprehensif

Setelah risiko telah diidentifikasi, kebijakan keamanan yang komprehensif akan dikembangkan untuk mengatasi risiko yang ditemukan. Kebijakan ini akan mencakup penggunaan tindakan teknis seperti shutdown, restrict, dan protect untuk memastikan keamanan jaringan.Implementasi Tindakan Teknis

Setelah kebijakan keamanan yang komprehensif telah dikembangkan, tindakan teknis seperti shutdown, restrict, dan protect akan diimplementasikan untuk memastikan keamanan jaringan. Tindakan ini akan disesuaikan dengan kebutuhan masing-masing organisasi dan individu.

d. Presentasi

Setelah kebijakan implementasi tindakan teknis sudah dilakukan kita melakukan presentasi atau pembuktian pada strategi keamanan jaringan.

Menggunakan metode penelitian ini akan memungkinkan penyusunan strategi yang efektif dan efisien untuk membantu organisasi dan individu menjaga keamanan jaringan mereka. Strategi ini dapat dicapai dengan mengidentifikasi kemungkinan risiko, mengembangkan kebijakan keamanan yang komprehensif, menerapkan tindakan teknis seperti shutdown, restrict, dan protect, dan memberikan pelatihan dan pengawasan yang baik kepada pengguna.Metode penelitian yang digunakan dalam penelitian ini dapat dilihat pada gambar 1.

4. Hasil dan Pembahasan

a. Pengumpulan data

Keamanan jaringan dan perlindungan data dan informasi sensitif merupakan topik penting dalam dunia teknologi informasi. Untuk melindungi data dan informasi sensitif, banyak organisasi dan perusahaan menggunakan strategi keamanan jaringan. Dalam melaksanakan pencarian data yang dilakukan sebaiknya ditentukan terlebih dahulu sumber data yang akan digunakan dan diidentifikasi juga kredibilitas atau mutu sumber data yang dikumpulkan. Dengan demikian, pengumpulan data dapat menjawab tujuan penelitian secara optimal. Terdapat 16 referensi jurnal sebagai salah satu tahapan untuk menyelesainkan

Infotek : Jurnal Informatika dan Teknologi
Vol. 6 No. 2, Juli 2023
Hal. 01-08

e-ISSN 2614-8773

DOI : 10.29408/jit.v4i1.2999 Link : https://dx.doi.org/10.29408/jit.v4i1.2999

penelitian ini. Kemudian kita melakukan pengamatan lapangan atas kebijakan keamanan yang diterapkan, akan membantu mengidentifikasi kemungkinan celah dan masalah yang muncul pada sistem keamanan yang diterapkan untuk memproteksi data dan informasi sensitif. Dengan begitu, seluruh hak dalam privasi dan confidentiality terjaga dengan baik tanpa adanya potensi terbocornya dan berbagai kejahatan siber lainnya.

b. Identifikasi Kemungkinan Risiko

Hasil dari identifikasi kemungkinan resiko yang akan terjadi pada pembobolan data melalui jaringan . Pada tahap ini kita mendapatkan beberapa resiko yang dapat terjadi :

1. Kemungkinan serangan virus atau malware pada sistem:Untuk mengatasi risiko ini, perlu dilakukan instalasi perangkat lunak antivirus dan firewalls yang dapat memantau dan mencegah situs web yang mengandung virus dan malware.
2. Ancaman DDoS: Salah satu cara untuk meminimalkan risiko serangan DDoS adalah dengan memperkuat infrastruktur jaringan dengan menggunakan firewall, load balancer, dan mengaktifkan layanan CDN (Content Delivery Network) untuk mengalihkan lalu lintas dari server utama ke server lain.
3. Ancaman hacking: Untuk mengatasi kemungkinan risiko hacking, dianjurkan untuk melakukan pentesting secara teratur, melaksanakan pengamanan dengan menggunakan password yang kuat dan mengenkripsi data.[8]
4. Kemungkinan kebocoran data: Untuk meminimalkan kemungkinan kebocoran data, perlu dilakukan kriptografi untuk mengenkripsi data, penanganan keamanan yang ketat terhadap pelanggaran privasi, dan mengambil tindakan pencegahan khusus untuk mengurangi kemungkinan kebocoran data.
5. Dana keamanan: Untuk menjaga keamanan jaringan yang efektif dan efisien, harus diinvestasikan dana untuk ketersediaan dan pemeliharaan perangkat keras, perangkat lunak keamanan dan untuk memastikan keandalan sistem.[9]

c. Pengembangan Kebijakan Keamanan yang Komprehensif

Pengembangan kebijakan keamanan yang komprehensif merupakan proses pengaturan dan pengorganisasian dari berbagai aspek keamanan yang terkait dengan suatu organisasi atau lingkungan, baik itu skala kecil seperti individu, keluarga, maupun skala besar seperti negara. Kebijakan keamanan yang komprehensif harus mempertimbangkan dan mengatasi berbagai ancaman dan risiko yang mungkin terjadi.

1. Shutdown

Pengembangan dari fitur Shutdown pada jaringan adalah dengan menambahkan fitur Violation Detection. Fitur ini akan memantau setiap trafik yang masuk ke dalam jaringan dan melihat apakah ada aktifitas yang mencurigakan atau melanggar aturan jaringan.Dengan adanya fitur ini, administrator jaringan tidak perlu khawatir jika terjadi pelanggaran aturan pada jaringan. Langkah tindakan yang tepat sudah otomatis diterapkan oleh sistem sehingga jaringan bisa tetap berjalan dengan aman dan lancar[10]. Setelah itu Switch akan mengirim notifikasi (SNMP).Notifikasi SNMP tersebut akan memberikan informasi tentang port yang telah dimatikan, alasan matinya port tersebut (Violation), dan tanggal serta waktu ketika pelanggaran terjadi. Informasi ini akan sangat berguna bagi administrator jaringan untuk mengetahui dan memecahkan masalah yang terjadi, serta mengambil langkah-langkah pencegahan agar pelanggaran semacam itu tidak terulang kembali di masa depan[11].

2. Restrict

Pengembangan dari Restrict dapat dilakukan dengan menambahkan fitur yang dapat mendeteksi adanya violation dan menghentikan penggunaan port tersebut namun tetap menjaga port tersebut dalam kondisi aktif. Dengan begitu, pengguna masih dapat melihat port yang tersedia namun tidak akan dapat menggunakannya jika terdapat violation. Pengembangan lainnya adalah dengan

Infotek : Jurnal Informatika dan Teknologi
Vol. 6 No. 2, Juli 2023
Hal. 01-08

e-ISSN 2614-8773

DOI : 10.29408/jit.v4i1.2999 Link : https://dx.doi.org/10.29408/jit.v4i1.2999

menambahkan fitur notifikasi yang dapat memberitahu administrator apabila terjadi violation pada salah satu port. Dengan begitu, administrator dapat mengambil tindakan yang diperlukan untuk mengatasi pelanggaran yang terjad[12]. Selain itu, fitur "Restrict" ini juga dapat menambahkan lapisan keamanan tambahan pada Switch sehingga bahaya dari pelanggaran keamanan jaringan dapat diminimalkan. Dengan menggunakan fitur ini, pengguna jaringan dapat merasa lebih aman dan terlindungi dari ancaman jaringan yang tidak diinginkan[13].

3. Protect

Ketika terjadi pelanggaran maka sistem akan secara otomatis mengirimkan notifikasi ke administrator agar dapat mengambil tindakan yang diperlukan. Misalnya dengan meminta keterangan dari pihak yang terlibat atau melakukan investigasi lebih lanjut untuk mengetahui penyebab pelanggaran tersebut.Selain itu, dapat juga ditambahkan fitur pembatasan waktu dalam penggunaan port sehingga jika penggunaan port sudah melebihi batas waktu yang ditentukan maka port tersebut akan otomatis dihentikan penggunaannya atau diberikan batasan akses pada jam tertentu.[14]Jika pelanggaran terjadi terus-menerus pada suatu port, switch dapat memblokir port tersebut sepenuhnya untuk mencegah serangan lebih lanjut. Administrator jaringan dapat melakukan investigasi lebih lanjut pada port yang diblokir untuk menemukan dan memperbaiki kerentanan atau kelemahan pada sistem.

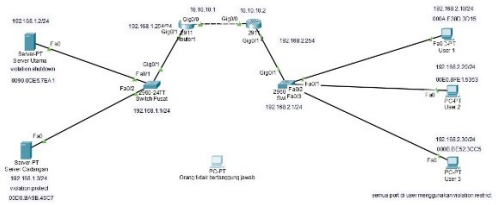
d. Implementasi Tindakan Teknis

Hasil dari implementasi ini adalah topologi strategi keamanan jaringan dengan format .img dan tabel.Tools yang digunakan untuk melakukan proses pengimplementasian ini adalah pada cisco paket tracer. Cisco Packet Tracer menyediakan platform simulasi jaringan yang memungkinkan pengguna untuk membuat dan menguji jaringan yang kompleks menggunakan berbagai jenis perangkat jaringan. Dengan Cisco Packet Tracer, pengguna dapat merancang topologi jaringan yang kompleks dan mensimulasikan berbagai jenis perangkat jaringan dalam satu topologi. Ini membantu pengguna memahami bagaimana beberapa perangkat jaringan berinteraksi di dalam jaringan[15]. Tabel 1 menunjukan, perangkat, port yang digunakan, ip address pada masing masing perangkat , subnet mask yang digunakan dan didaftarkan, dan default gateway.

Tabel 1. Perangkat dan ip address

Device	Port	Ip Address	Subnet Mask
Router 1	G0/0	192.168.1.254	255.255.255.0
	G0/1	10.10.10.1	255.255.255.0
Router 2	G0/0	10.10.10.2	255.255.255.1
	G0/1	192.168.2.254	255.255.255.2
Swicth 1	Vlan 1	192.168.1.1	255.255.255.3
Swicth 1	Vlan 1	192.168.2.1	255.255.255.4
Server Utama	F0/0	192.168.1.2	255.255.255.5
Server Cadangan	F0/0	192.168.1.3	255.255.255.6
User 1	F0/1	192.168.2.10	255.255.255.7
User 2	F0/2	192.168.2.20	255.255.255.8
User 3	F0/2	192.168.2.30	255.255.255.9

Setelah identifikasi pada ip address dan perangkat yang digunakan selesai kemudian kita lakukan perancangan topologi sederhana sebagai implementasi tindakan teknis terhadap strategi menjamin keamanan jaringan yang efisien. Gambar 1 merupakan topologi pada cisco paket tracer.



Gambar 1 Topologi Strategi Keamanan Jaringan

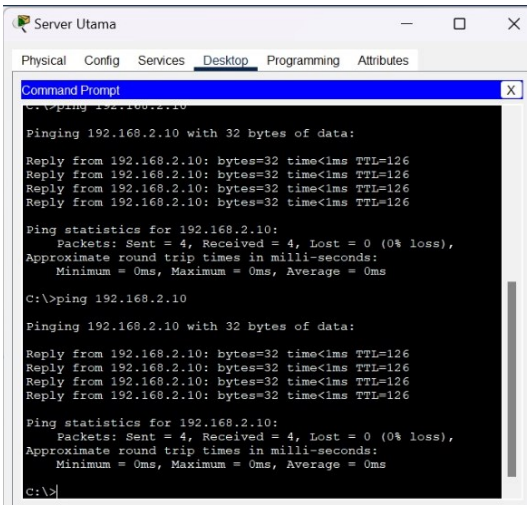
Infotek : Jurnal Informatika dan Teknologi
Vol. 6 No. 2, Juli 2023
Hal. 01-08

e-ISSN 2614-8773

DOI : 10.29408/jit.v4i1.2999 Link : https://dx.doi.org/10.29408/jit.v4i1.2999

e. Presentasi

Hasil dari penerapan fitur Violation Detection, administrator jaringan dapat menggunakan perangkat lunak keamanan jaringan yang terintegrasi dengan fitur ini atau dapat memilih untuk menginstal aplikasi khusus yang dapat melakukan pemantauan trafik di jaringan. Setelah dipasang, fitur ini dapat dikonfigurasi dengan menentukan aturan yang harus dipatuhi oleh setiap perangkat dalam jaringan. Dengan adanya fitur Violation Detection, jaringan dapat terus berjalan dengan aman dan lancar tanpa khawatir akan pelanggaran aturan yang dapat membahayakan keselamatan data dan kinerja jaringan[16]. Gambar 2. merupakan porses ping pada server sebelum dilakukan rekayasa penyerangan.



Gambar 2 Proses ping pada server sebelum dilakuakn rekayasa penyerangan

Shutdown: Shutdown adalah proses mematikan sistem secara aman dan benar.

- Dalam proses shutdown, sistem akan menutup semua aplikasi dan proses yang sedang berjalan.
- Sistem kemudian akan menjalankan proses pengaturan akhir sebelum mematikan komputer sepenuhnya.
- Akhirnya, sistem akan mati sepenuhnya dan tidak dapat dioperasikan sampai dihidupkan kembali.

Restrict: Restrict adalah proses mengatur batasan atau pembatasan pada penggunaan sistem.

- Dalam proses restrict, pengguna diberi akses terhadap sistem dan aplikasi hanya pada level yang tertentu.
- Proses ini dapat terdiri dari mengubah hak akses pengguna untuk mengakses file dan aplikasi tertentu, atau membatasi penggunaan sistem hanya pada waktu-waktu tertentu.
- Tujuannya adalah untuk meminimalkan risiko kerusakan atau kebocoran data pada sistem.

Protect: Protect adalah proses melindungi sistem dari serangan luar atau pengguna yang tidak berwenang.

- Dalam proses protect, sistem dilindungi dengan firewall dan antivirus untuk memastikan tidak adanya serangan virus atau malware.
- Selain itu, sistem juga dilindungi melalui enkripsi data untuk meminimalkan risiko kehilangan atau pencurian data.
- Tujuannya adalah untuk memaksimalkan keamanan sistem dan melindungi data dari kebocoran atau hilang.

Hasil dari rekayasa serangan pada server yang telah kami konfigurasi yaitu sebuah penyerangan yang mencoba menyerang dan kemudian ada tindakan shutdown, restrict dan protect. Adanya proses penutupan semua aplikasi dan proses yang sedang berjalan. Kemudian terdapat proses restrict dimana pengguna diberikan hak akses untuk mengakses file dan aplikasi tertentu atau dengan membatasi penggunaan sistem hanya pada waktu-waktu tertentu saja. Selain itu terdapat proses protect yaitu sistem dilindungi dengan firewall dan antivirus untuk memastikan tidak adanya serangan virus atau malware. Gambar 3. adalah rekayasa penyerangn pada suatu jaringan.

Infotek : Jurnal Informatika dan Teknologi
Vol. 6 No. 2, Juli 2023
Hal. 01-08

e-ISSN 2614-8773

DOI : 10.29408/jit.v4i1.2999 Link : https://dx.doi.org/10.29408/jit.v4i1.2999

5. Kesimpulan

Kesimpulan dari penelitian ini adalah bahwa strategi terpadu yang mencakup evaluasi risiko, kebijakan keamanan, pemantauan dan pemulihan, serta pelatihan pengguna merupakan pendekatan yang efisien dan efektif untuk menjamin keamanan jaringan yang optimal. Implementasi strategi ini dapat membantu organisasi dan perusahaan melindungi jaringan mereka dari serangan siber, mengurangi kerentanan, dan meminimalkan kerugian yang mungkin terjadi.

Dalam dunia yang terhubung saat ini, keamanan jaringan sangat penting. Menggunakan teknik keamanan port dapat meningkatkan keamanan jaringan dengan strategi menyeluruh yang mencakup segmentasi jaringan, kontrol akses, dan otentikasi. Dengan menerapkan taktik ini, perusahaan dapat membuat kerangka kerja keamanan jaringan yang kuat untuk melindungi data sensitif, mengurangi risiko, dan menjamin ketersediaan dan integritas sumber daya jaringan mereka. Abstrak ini membahas tentang strategi yang berbeda untuk memanfaatkan keamanan port secara efektif untuk memastikan keamanan jaringan. Oleh karena itu, penting bagi organisasi untuk memahami pentingnya keamanan jaringan dan menggunakan teknik yang tepat untuk melindungi sumber daya mereka.

6. Daftar Pustaka

[1] Gi-Tae Yeo, Ji-Yeong Pak and Zaili Yang, “Analysis of dynamic effects on seaports adopting ports security policy,”Policy and Practice., vol. 49, March 2019. page 285-301.

[2] Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2018). A Review Of Cyber Security Risk Assessment Methods For SCADA Systems. Computers & Security, 56, 1–27. Https://Doi.Org/10.1016/J.Cose.2015.09.009

[3] L. K. Lee, Y. C. Fung, Y. W. Pun, K. K. Wong, M. T. Y. Yu, and N. I. Wu. (2020). A Review Of Using a multiplatform chatbot as an online tutor in a university course. In Proceedings of the 6th International Symposium on Educational Technology (ISET), pp. 53-56, IEEE, 2020. https://ieeexplore.ieee.org/document/9215528

[4] Liu et al. (2021). Contrastive Context-Aware Learning for 3D High-Fidelity Mask Face Presentation Attack Detection, IEEE, 2021. https://arxiv.org/abs/2104.06148

[5] Mohammad Kamrul Hasan, AKM Ahasan Habib, Zarina Shukur , Fazil Ibrahim , Shayla Islam , Md Abdur Razzaque. (2022). Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations, IEEE, 2022. https://doi.org/10.1016/j.jnca.2022.103540

[6] Z. A. Rahman and H. M. Taha, "Secure Data Transmission Through Virtual Private Network," Journal of Telecommunication, Electronic and Computer Engineering, vol. 10, no. 1-13, pp. 1-5, 2018.

[7] R. M. Barts, “The Stub Loaded Helix: A Reduced Size Helical Antenna,” Doctoral Dissertation, 2003. [Online]. Available: http://hdl.handle.net/10919/29728.

[8] A. Asyhar, R. Gusti, and W. Adi, "Network Security on Small Business: Risks and Solutions," in 2020 International Conference on Computer, Control, Informatics and its Applications (IC3INA), 2020, pp. 1-6

[9] Pouyan Ahmadi, Khondkar Islam, Trevor Maco,Manilya Katam. (2018). A Survey on Internet of Things Security Issues and Applications, 2018. https://www.computer.org/csdl/proceedings-

Infotek : Jurnal Informatika dan Teknologi
Vol. 6 No. 2, Juli 2023
Hal. 01-08

e-ISSN 2614-8773

DOI : 10.29408/jit.v4i1.2999 Link : https://dx.doi.org/10.29408/jit.v4i1.2999

article/csci/2018/136000a925/1gjRulKhMiI

[10] S. V. Ganti, K. V. Ramana, and M. K. Jena, "Real time network violation detection and port shutdown using sdn," International Journal of Electrical and Computer Engineering (IJECE), vol. 11, no. 6, pp. 4961-4970, Dec. 2021.

[11] T. N. Rizky and A. M. Azmy, "Detection of MAC Spoofing Attacks Using SNMP Traps," International Journal of Computer Networks and Communications Security, vol. 6, no. 11, pp. 216-224, 2018.

[12] Jiang, C., & Liu, L. (2018). Vulnerability analysis of network port restriction and improvement method. Journal of Physics: Conference Series, 1149(1), 012042. doi: 10.1088/1742-6596/1149/1/012042

[13] Al-Faqih, A., & Zahran, M. (2019). High availability for software-defined networks using OpenStack and SDN controllers. Journal of Network and Computer Applications, 141, 1-10. https://doi.org/10.1016/j.jnca.2019.04.008

[14] A. D. Dewi and S. Wijayanto, "Development of a network security system using software-defined networking (SDN) approach," 2018 International Conference on Information and Communications Technology (ICOIACT), Yogyakarta, 2018, pp. 387-392.

[15] B. Gültekin, "The Effectiveness of Using Cisco Packet Tracer on the Acquisition of Packet-Switching Concepts," International Journal of Engineering Research and Application, vol. 10, no. 1, 2020, pp. 34-40.

[16] Finardi, E. R., Junior, P. R., Pereira, F. C., & Silva, F. R. (2019). Intrusion detection in internet of things (IoT) networks: A survey. Computer Communications, 132, 172-190. ipv6 network," in 2016 International Conference on Informatics and Computing (ICIC), 2016, pp. 111–116.