JURNAL RISET SISTEM INFORMASI
Halaman Jurnal: https://journal.smartpublisher.id/index.php/jissi
Halaman UTAMA Jurnal : https://journal.smartpublisher.id

DOI: https://doi.org/10.69714/qgnbgv11

KEAMANAN JARINGAN PADA PERGURUAN TINGGI

Muhammad Alfian [a*], Rakhmadi Rahman [b]
[a] Sistem Informasi, alfiaan8@gmail.com , Institut Teknologi Bacharuddin Jusuf Habibie, Parepare Sulawesi Selatan
[b] Information System Department, rakhmadi.rahman@ith.ac.id , Institut Teknologi Bacharuddin Jusuf Habibie, Parepare Sulawesi Selatan
[*] Korespondensi

ABSTRACT

This research analyzes the role of network security in higher education in the face of increasingly complex cyber threats. Using a literature study methodology, this research identified challenges such as malware attacks, phishing, DDoS, and hacking, as well as vulnerabilities such as resource limitations and lack of user awareness. Recommended preventive practices include the implementation of multifactor authentication systems, data encryption, and increased user awareness. The use of firewalls was also highlighted as an important component in protecting the college's digital assets. This research provides guidance for educational institutions to improve their network security infrastructure.

Keywords: network security, universities, firewalls.

Abstrak

Penelitian ini menganalisis peran keamanan jaringan di perguruan tinggi dalam menghadapi ancaman cyber yang semakin kompleks. Dengan menggunakan metodologi studi literatur, penelitian ini mengidentifikasi tantangan seperti serangan malware, phishing, DDoS, dan hacking, serta kerentanan seperti keterbatasan sumber daya dan kurangnya kesadaran pengguna. Rekomendasi praktik pencegahan termasuk implementasi sistem autentikasi multifaktor, enkripsi data, dan kesadaran pengguna yang ditingkatkan. Penggunaan firewall juga disorot sebagai komponen penting dalam melindungi aset digital perguruan tinggi. Penelitian ini memberikan panduan bagi institusi pendidikan untuk meningkatkan infrastruktur keamanan jaringan mereka.

Kata Kunci: keamanan jaringan, perguruan tinggi, firewall.

1. PENDAHULUAN

Di dunia saat ini, informasi telah menjadi sumber daya yang berharga. Semua jenis organisasi, termasuk lembaga pemerintah, universitas, perusahaan, dan individu, harus dapat memperoleh dan menyediakan informasi secara akurat dan cepat. Dengan kondisi perkembangan teknologi komputer dan telekomunikasi yang sangat cepat saat ini, penting untuk mempertimbangkan risiko dan bahaya penyalahgunaan layanan jaringan lokal dan aplikasi berbasis Internet[1].

Perguruan tinggi sebagai institusi pendidikan tinggi memiliki peran penting dalam meningkatkan kualitas pendidikan dan penelitian. Dalam era digital, jaringan menjadi salah satu infrastruktur yang sangat penting dalam mendukung aktivitas akademis dan penelitian. Namun, jaringan juga sering menjadi sasaran ancaman keamanan, seperti serangan malware, phishing, dan hacking. Ancaman-ancaman ini dapat menyebabkan kerusakan pada sistem, kehilangan data, dan bahkan mengganggu kualitas pendidikan dan penelitian.

Received Juni 5, 2024; Revised Juni 11, 2024; Accepted Juli 22, 2024; Published Juli 24, 2024

Contohnya terjadi pada tahun 2012 ketika serangan peretasan sistem informasi terjadi di Universitas Yale. Para peretas mendapatkan akses ke 1.200 akun data mahasiswa dan personel melalui pelanggaran tersebut. Kata sandi, alamat email, dan nama pengguna yang digunakan pada sistem termasuk di antara data yang dicuri. Setelah mencuri jaringan LAN, para peretas menargetkan sistem database. Hal ini merupakan akibat dari lemahnya infrastruktur sistem keamanan. Penghapusan infrastruktur sistem keamanan yang tidak memadai perlu dibarengi dengan langkah-langkah untuk mengurangi ancaman saat ini. Di antaranya adalah keamanan jaringan, yang perlu mempertimbangkan faktor arsitektur [2].

Sistem informasi, penelitian yang telah selesai, mahasiswa, staf, dosen, dan transfer data antardepartemen merupakan beberapa aset yang harus dijaga oleh universitas. Administrator sistem harus berpengalaman dalam menangani kesulitan yang muncul di dalam universitas selain jaringan. Ide keamanan ini termasuk dalam layanan yang dapat digunakan kembali secara cerdas dan aspek keamanan.

Oleh karena itu, perlu adanya pengembangan desain keamanan jaringan yang digunakan di perguruan tinggi. Konsep keamanan jaringan ini diharapkan dapat memperkuat infrastruktur keamanan TI universitas tanpa menimbulkan kesulitan bagi pengguna.

2. TINJAUAN PUSTAKA

2.1. Keamanan Jaringan

Keamanan jaringan menurut Mariusz Stawowski dalam jurnalnya “The principles of network security design”, adalah Keamanan jaringan yang utama sebagai perlindungan sumber daya sistem terhadap ancaman yang berasal dari luar jaringan. Keamanan komputer digunakan untuk mengontrol resiko yang berhubungan dengan penggunaan komputer. Keamanan komputer yang dimaksud adalah keamanan sebuah komputer yang terhubung ke dalam sebuah jaringan (Internet) [3].

2.2. Jaringan Komputer

Konsep asli jaringan komputer adalah proses komputer dimana komputer lain terhubung dan bekerja sama atau berkomunikasi. Pada awalnya hanya ada 2 komputer yang terhubung ke komputer lain, sehingga disebut point-to-point. Setelah berkembang pesatnya teknologi, tidak hanya 2 komputer yang saling terhubung, tetapi bisa lebih dari dua atau lebih, yang disebut jaringan komputer .

3. METODOLOGI PENELITIAN

Penelitian ini mengkaji fungsi, risiko, kelemahan, dan arsitektur arsitektur keamanan jaringan pada perguruan tinggi dengan menggunakan metodologi studi literatur. Mencari, mengkaji, dan menganalisis berbagai sumber literatur terkait yang telah diterbitkan dalam 5 tahun terakhir adalah cara penelitian ini dilakukan. Jurnal ilmiah, buku, makalah penelitian, artikel konferensi, dan disertasi adalah beberapa contoh literatur ini.

Setelah analisis, informasi dari literatur dikumpulkan dan digabungkan untuk menyajikan gambaran menyeluruh tentang keamanan jaringan di pendidikan tinggi beserta saran untuk meningkatkannya. Penelitian ini memungkinkan peneliti memperoleh pemahaman menyeluruh tanpa perlu mengumpulkan data primer dengan menggunakan metode studi literatur.

4. HASIL DAN PEMBAHASAN

4.1 Peran Penting Keamanan Jaringan

Universitas sangat penting untuk kemajuan teknologi dan peningkatan standar pendidikan. Dalam upaya ini, keamanan jaringan menjadi krusial karena berbagai data dan informasi sensitif disimpan dalam sistem jaringan mereka. Keamanan jaringan yang kuat tidak hanya menjaga integritas institusi, tetapi juga melindungi privasi mahasiswa, staf, dan informasi penting lainnya.

4.1.1. Faktor – Faktor Yang Mempengaruhi Keamanan Jaringan Perguruan Tinggi

a. Penggunaan Teknologi yang Aman
   Perguruan tinggi harus memilih dan mengimplementasikan teknologi yang terbaru dan aman. Sistem autentikasi yang kuat dan enkripsi data menjadi contoh teknologi yang efektif dalam mencegah serangan keamanan.

b. Pengawasan dan Pemantauan Rutin
   Pengawasan dan pemantauan sistem jaringan secara rutin sangat penting. Dengan melakukan pemantauan secara teratur, perguruan tinggi dapat mendeteksi dan menghentikan serangan keamanan

sebelum menyebabkan kerusakan yang signifikan.

c. Pendidikan dan Keterampilan
Memberikan pendidikan dan pelatihan yang tepat kepada staf dan mahasiswa tentang keamanan jaringan sangat penting. Meningkatkan kesadaran akan ancaman keamanan dan mengajarkan praktik-praktik yang aman akan membantu mengurangi risiko serangan.

d. Koordinasi dan Kerjasama
Tantangan keamanan jaringan seringkali melintasi batas institusi. Kerjasama dengan pemerintah, lembaga keamanan, dan mitra industri adalah langkah penting untuk menghadapi ancaman yang semakin kompleks dan canggih.

4.1.2. Implementasi Praktik Keamanan Jaringan Perguruan Tinggi

a. **Sistem Autentikasi Multifaktor**: Mengimplementasikan sistem autentikasi yang memerlukan lebih dari satu metode verifikasi memberikan lapisan perlindungan tambahan. Ini bisa melibatkan kombinasi kata sandi, token, atau biometrik.
b. **Enkripsi Data**: Melindungi data sensitif dengan enkripsi saat istirahat atau berpindah tangan merupakan langkah yang penting. Dengan demikian, bahkan jika data tersebut direbut, akan sulit bagi penyerang untuk membacanya.
c. **Penggunaan Alat Pemantauan dan Analisis**: Melalui penggunaan perangkat lunak pemantauan jaringan dan analisis log, perguruan tinggi dapat mendeteksi aktivitas mencurigakan dan meresponsnya dengan cepat. Dengan memantau lalu lintas jaringan secara terus-menerus, serangan dapat dihentikan sebelum menyebabkan kerusakan yang signifikan.

4.2 Ancaman dan Kerentanan Sistem Informasi Dan Jaringan Komputer Pada Perguruan Tinggi

Perubahan dinamis dalam teknologi informasi terjadi di perguruan tinggi karena mereka adalah tempat pendidikan dan penelitian yang mengelola banyak data sensitif. Karena teknologi telah masuk ke hampir semua aspek kehidupan akademik dan administratif, perguruan tinggi menjadi sasaran potensial untuk serangan cyber. Seiring dengan kemajuan teknologi, ancaman ini terus meningkat, menambah kompleksitas masalah yang dihadapi oleh lembaga-lembaga ini.

Perguruan tinggi memiliki tanggung jawab besar untuk melindungi aset digital mereka dari serangan cyber karena mereka menjaga data sensitif seperti informasi pribadi siswa, hasil penelitian, dan kebijakan akademis. Namun, mereka juga memiliki beberapa masalah dengan sistem informasi dan jaringan komputer mereka. Ada banyak titik masuk yang mungkin bagi penyerang, seperti kolaborasi penelitian dan administrasi akademis dan keuangan.

4.2.1. Ancaman

a. Serangan Malware
Serangan malware membahayakan perguruan tinggi. Virus, worm, dan ransomware adalah beberapa jenis malware yang dapat menyebabkan kerusakan yang signifikan pada sistem informasi dan jaringan komputer. Virus dan worm dapat merusak atau menghapus data, mengganggu operasi sistem, atau bahkan membuat sistem tidak dapat digunakan sama sekali. Ransomware, di sisi lain, dapat mengenkripsi data penting perguruan tinggi dan menuntut pembayaran sebagai imbalan untuk memulihkan data tersebut. Perguruan tinggi harus rutin memperbarui dan memperkuat sistem pertahanan mereka untuk menghadapi malware yang terus berkembang dan berubah.

b. Serangan Phising
Serangan phishing biasanya menjadi jalan menuju serangan cyber yang lebih besar. Penipu dapat menggunakan email atau situs web palsu, membuat orang tidak curiga saat memberikan informasi pribadi atau kredensial login mereka. Serangan phishing dapat menargetkan karyawan, mahasiswa, atau bahkan fakultas di perguruan tinggi. Sebuah email palsu yang mengaku berasal dari administrasi dengan permintaan untuk memperbarui informasi akun dapat mengakibatkan pengungkapan data pribadi atau bahkan peretasan sistem.

c. Serangan DDoS (Distrubuted Denial of Service)
Serangan DDoS adalah serangan yang membanjiri server dengan lalu lintas internet yang tidak perlu untuk membuat jaringan tidak tersedia bagi pengguna. Serangan DDoS dapat mengganggu layanan penting perguruan tinggi, seperti portal siswa, sistem pendaftaran, atau situs web institusi. Serangan ini juga dapat mengganggu aktivitas akademik dan administratif, serta merusak reputasi perguruan tinggi

di mata siswa, karyawan, dan masyarakat umum.

d. Serangan Hacking
Serangan hacking adalah upaya untuk menembus keamanan sistem dengan tujuan mencuri data, merusak infrastruktur jaringan, atau mengganggu layanan. Hacker dapat memanfaatkan bug perangkat lunak atau sistem operasi untuk mendapatkan akses yang tidak sah ke jaringan perguruan tinggi. Serangan semacam ini dapat merusak reputasi institusi, mencuri data sensitif seperti informasi pribadi siswa atau hasil penelitian, dan mengganggu kelancaran operasi.

e. Pelanggaran Data
Pelanggaran data adalah bahaya besar yang dapat menyebabkan kehilangan finansial, reputasi, dan kepercayaan masyarakat. Pengungkapan atau kebocoran data sensitif seperti identitas, catatan akademik, atau informasi penelitian rahasia dapat merusak reputasi perguruan tinggi dan mengakibatkan kerugian finansial. Lebih dari itu, pelanggaran data juga dapat berdampak pada orang-orang yang terkena dampaknya, seperti siswa atau karyawan. Oleh karena itu, perguruan tinggi harus memprioritaskan perlindungan data sensitif.

4.2.2. Kerentanan

a. Keterbatasan Sumber Daya
Perguruan tinggi sering menghadapi kesulitan dalam mengelola keamanan jaringan karena kekurangan sumber daya manusia dan dana. Universitas mungkin tidak memiliki infrastruktur dan peralatan yang diperlukan untuk mendeteksi, mencegah, dan merespons serangan dengan cepat dan efektif jika anggaran dan staf keamanan tidak cukup. Dengan demikian, kelemahan pertahanan dapat muncul, meningkatkan kemungkinan serangan cyber yang berhasil.

b. Ketergantungan pada Teknologi Terbaru
Perguruan Tinggi sering bergantung pada sistem atau perangkat lunak tertentu untuk beroperasi. Namun, jika terdapat celah keamanan dalam teknologi tersebut, ketergantungan ini juga dapat menjadi sumber risiko. Terutama dalam kasus di mana pembaruan dan perbaikan tidak dilakukan secara konsisten, celah ini dapat dimanfaatkan oleh pencuri untuk mengakses sistem atau mencuri data. Oleh karena itu, sangat penting bagi institusi pendidikan tinggi untuk memantau dan memelihara sistem dan perangkat lunak yang digunakan secara teratur.

c. Kurangnya Kesadaran Pengguna
Karena kurangnya kesadaran tentang praktik keamanan yang aman, pengguna, termasuk karyawan dan mahasiswa, sering kali menjadi titik lemah dalam pertahanan jaringan. Serangan phishing atau pembuatan kerentanan dengan menggunakan kata sandi yang lemah atau mengklik tautan yang mencurigakan dapat dengan mudah terjadi pada pengguna yang tidak waspada terhadap ancaman cyber. Untuk mengatasi masalah ini, perguruan tinggi harus meningkatkan kesadaran pengguna dengan memberikan instruksi dan pelatihan rutin tentang praktik keamanan data.

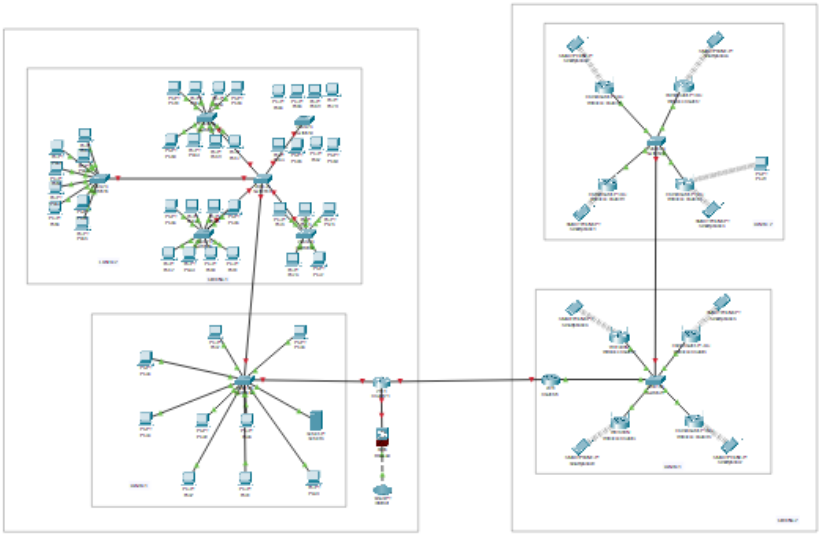
d. Kerentanan dalam Peringkat IoT (Internet of Things)
Untuk meningkatkan efisiensi operasional, institusi pendidikan tinggi telah mulai menggunakan perangkat Internet of Things (IoT), seperti kamera pengawas atau sistem kontrol pintu. Karena kurangnya keamanan yang terintegrasi, perangkat IoT sering menjadi sasaran serangan. Perangkat Internet of Things dapat digunakan oleh pencuri untuk mengakses jaringan institusi jika tidak dilindungi dengan baik. Akibatnya, institusi pendidikan tinggi harus mematuhi peraturan yang ketat tentang penggunaan dan pengamanan perangkat IoT, seperti memperbarui perangkat lunak, mengenkripsi data, dan membatasi akses.

e. Pencegahan Ancaman Keamanan Pada Jaringan
Firewall adalah jenis perangkat keamanan jaringan yang melindungi dari bahaya online untuk PC dan koneksi jaringan lainnya. Firewall meningkatkan keamanan jaringan komputer dengan mengatur dan melacak lalu lintas jaringan. Mengatur dan menyaring paket data yang masuk dan keluar dari jaringan untuk memastikan mereka mematuhi kebijakan keamanan yang ditetapkan adalah salah satu dari banyak tugas firewall.

Lebih jauh lagi, setiap usaha untuk mengakses akan diautentikasi oleh firewall, menjamin bahwa hanya pengguna yang berwenang yang dapat mengakses jaringan. Selain itu, firewall mencatat setiap peristiwa transaksi yang terjadi di dalamnya, sehingga memungkinkan deteksi dini masalah keamanan.

Firewall dapat mengidentifikasi perilaku yang tidak wajar pada setiap aktivitas dan bertindak cepat untuk mencegah serangan. Firewall berperan penting dalam mencegah akses yang tidak sah dan serangan siber yang dapat merusak atau merusak data dan sistem karena mereka mengatur dan mengontrol alur lalu lintas jaringan.

Berikut merupakan topologi keamanan jaringan yang menggunakan firewall.



Gambar 1. Topologi jaringan menggunakan firewall

Firewall adalah komponen penting dalam melindungi jaringan perguruan tinggi dari ancaman digital. Tugas utama firewall adalah mengawasi dan mengontrol aliran informasi yang masuk dan keluar dari jaringan, termasuk paket-paket yang dikirim dan diterima oleh perangkat jaringan. Firewall melakukan ini dengan mengikuti protokol, alamat IP, dan port yang digunakan.

Salah satu fungsi utama firewall adalah melindungi terhadap serangan siber dengan menghalangi akses ke sumber yang tidak dikenal dan mencegah ancaman seperti virus, worm, dan Trojan horse. Firewall juga aktif memantau lalu lintas jaringan dan memberikan laporan tentang aktivitas yang mencurigakan. Jika mereka menemukan aktivitas yang mencurigakan, seperti serangan siber, firewall memberikan peringatan dan mengambil tindakan untuk memblokir akses ke sumber tersebut.

5. KESIMPULAN DAN SARAN

Studi ini menemukan bahwa keamanan jaringan sangat penting untuk menjaga integritas dan kelangsungan institusi pendidikan tinggi di era digital yang penuh tantangan. Tindakan pencegahan yang kuat terhadap ancaman cyber yang semakin kompleks termasuk penerapan sistem autentikasi yang kuat, enkripsi data, dan pemantauan aktif terhadap aktivitas jaringan. Selain itu, dianggap penting bahwa lembaga pendidikan, pemerintah, dan mitra industri bekerja sama untuk menghadapi ancaman bersama. Sementara itu, perguruan tinggi harus meningkatkan kesadaran pengguna tentang praktik keamanan, memperkuat infrastruktur keamanan jaringan, dan terus memperbarui strategi pencegahan untuk mengantisipasi ancaman dan kemajuan teknologi. Langkah-langkah ini diharapkan akan membantu perguruan tinggi menjaga keberlangsungan aktivitas akademik dan administratif serta melindungi aset digital mereka.

DAFTAR PUSTAKA

[1] Asry, D. W., Siswanto, E., Kurniawan, D., & Huda, H. I. (2023). Deteksi Malware Statis Menggunakan Deep Neural Networks Pada Portable Executable. *Teknik: Jurnal Ilmu Teknik dan Informatika*, *3*(1), 19-34.

[2] R. Permana, D. Ramadhani, and I. Lestari, "Proteksi Keamanan Jaringan Komputer di Sekolah Menengah Kejuran Al-Madani Pontianak," *Int. J. Nat. Sci. Eng.*, vol. 3, no. 1, p. 37, 2019, doi:

10.23887/ijnse.v3i1.22175.

[3] F. A. Putra and J. Purwanto, "Perancangan pengamanan jaringan pada perguruan tinggi xyz," *Semin. Nas. Sist. Inf. Indones.*, no. November, pp. 2–4, 2015.

[4] j-sika, Zen Munawar, & Novianti Indah Putri. (2020). KEAMANAN JARINGAN KOMPUTER PADA ERA BIG DATA. *J-SIKA|Jurnal Sistem Informasi Karya Anak Bangsa*, *2*(01), 14–20.

[5] E. N. Hartiwati, "Keamanan Jaringan Dan Keamanan Sistem Komputer Yang Mempengaruhi Kualitas Pelayanan Warnet," *J. Ilm. Inform. Komput. Univ. Gunadarma*, vol. 19, no. 3, pp. 27–33, 2019.

[6] Permana, R., Ramadhani, D., & Lestari, I. (2019). Proteksi Keamanan Jaringan Komputer di Sekolah Menengah Kejuran Al-Madani Pontianak. *International Journal of Natural Science and Engineering*, *3*(1), 37–43.

[7] Yulhendri, Y., Simorangkir, H., Faridho, F., & Kurniawan, D. (2022). Implementasi Digital Dashboard Untuk Mengontrol Wilayah Rt/Rw. *Jurnal Informatika Dan Tekonologi Komputer (JITEK)*, *2*(1), 43-54.