PERAN DAN STRATEGI KEAMANAN JARINGAN KOMPUTER DALAM MENGATASI SERANGAN SIBER DI WEBSITE INSTITUSI PENDIDIKAN

Lusi Rahma Amelia Putri[1], Moch. Bil Barokah Ilmi[2], Rudianto[3], Leyo Bayu Maruli Batubara[4], Adiba Naufal Ubaid[5], Imam Wahyudi[6], Muhammad Rinov Cuhanazriansyah[7]

[1,2,3,4,5,6,7]Pendidikan Teknologi Informasi, IKIP PGRI Bojonegoro,
Jl.Panglima Polim No. 46 , Pacul, Kec, Bojonegoro, Kab. Bojonegoro
E-mail: lusirahmaamelia@gmail.com, Telp: 0895-3963-43711

Abstrak

Di era digital, institusi pendidikan semakin mengandalkan teknologi informasi untuk mendukung proses pembelajaran, administrasi, dan komunikasi. Namun, ketergantungan ini juga meningkatkan risiko terhadap serangan siber yang dapat mengancam integritas, ketersediaan, dan kerahasiaan data. Artikel ini membahas peran penting keamanan jaringan komputer dalam melindungi website institusi pendidikan dari berbagai ancaman siber seperti peretasan, dan malware. Penelitian ini menggunakan metode studi literatur dengan menganalisis berbagai sumber ilmiah dan praktik terbaik dalam keamanan siber. Hasil kajian menunjukkan bahwa penerapan strategi keamanan yang komprehensif—termasuk firewall, enkripsi data, autentikasi ganda, serta pelatihan keamanan bagi staf IT—berperan signifikan dalam mencegah dan menangani insiden siber. Selain itu, pentingnya kebijakan keamanan yang berkelanjutan dan evaluasi sistem secara berkala juga menjadi faktor kunci dalam menjaga keamanan website institusi pendidikan. Artikel ini diharapkan dapat menjadi referensi bagi pengelola sistem informasi di institusi pendidikan dalam mengembangkan strategi pertahanan yang efektif terhadap serangan siber.

Kata kunci: keamanan jaringan, serangan siber, website pendidikan, firewall, strategi keamanan

Abstract

In the digital era, educational institutions increasingly rely on information technology to support learning, administration, and communication. However, this reliance also increases the risk of cyberattacks that can threaten data integrity, availability and confidentiality. This article discusses the important role of computer network security in protecting educational institution websites from various cyber threats such as hacking, and malware. This research uses the literature study method by analyzing various scientific sources and best practices in cybersecurity. The results show that implementing a comprehensive security strategy-including firewalls, data encryption, double authentication, and security training for IT staff-plays a significant role in preventing and handling cyber incidents. In addition, the importance of ongoing security policies and regular system evaluations are also key factors in maintaining the security of educational institution websites. This article is expected to be a reference for information system managers in educational institutions in developing effective defense strategies against cyberattacks.

Keywords : network security, cyberattack, educational website, firewall, security strategy

PENDAHULUAN

Perkembangan pesat teknologi informasi telah mendorong lembaga pendidikan untuk menggunakan teknologi digital dalam berbagai bagian operasional mereka. Salah satu hal yang langsung terpengaruh adalah kemajuan pada situs web institusi pendidikan. Situs web institusi pendidikan yang berfungsi dengan baik adalah alat penting untuk memastikan bahwa siswa menerima informasi, layanan, dan kesempatan pendidikan terbaik (Cuhanazriansyah, 2023:217). Hal ini termasuk sistem pembelajaran, administrasi, layanan informasi berbasis web, dan komunikasi. Salah satu cara utama untuk memberikan informasi kepada masyarakat umum, dosen, dan siswa

adalah situs web institusi pendidikan. Akan tetapi, kemajuan dalam perkembangan teknologi informasi ini juga diimbangi dengan meningkatnya potensi ancaman siber yang dapat mengganggu proses pendidikan, mencuri data, dan merusak sistem (Monia, 2025:2).

Serangan siber seperti pencurian data (data breach), defacing (perusakan tampilan website), Distributed Denial of Service (DDoS), penyebaran malware, hingga teknik rekayasa sosial seperti phishing semakin sering terjadi pada sebuah website Institusi. Ancaman-ancaman ini sangat merugikan, karena dapat menghambat operasional layanan digital dan juga berdampak pada menurunnya reputasi dan tingkat kepercayaan masyarakat terhadap institusi yang bersangkutan, hingga menimbulkan kerugian finansial dan hukum (Muharam dalam Laksana, 2024:109). Oleh sebab itu, strategi keamanan jaringan komputer yang efektif diperlukan untuk mencegah, mendeteksi, dan menanggapi berbagai jenis serangan siber tersebut (Alfian, 2024:59).

Keamanan jaringan komputer tak hanya mengenai pemasangan firewall atau antivirus. Keamanan jaringan adalah sistem yang mencakup semua aspek teknis, prosedural, dan kebijakan. Ini mencakup penerapan sistem otentikasi dan enkripsi yang kuat, pembaruan perangkat lunak rutin, dan pemantauan lalu lintas jaringan secara real-time. Institusi pendidikan juga harus membuat rencana pelestarian yang proaktif, seperti menerapkan sistem deteksi intrusi, melakukan audit keamanan rutin, dan membentuk tim tanggap kejadian siber(Alfian, 2024:60).

Tantangan keamanan siber di sektor pendidikan diperparah oleh pengguna yang tidak menyadari pentingnya menjaga keamanan digital mereka. Banyak pelajar yang tidak memahami prinsip keamanan dasar, seperti menggunakan kata sandi yang kuat, waspada terhadap email mencurigakan, dan menghindari jaringan publik yang tidak aman. Selain itu, anggaran dan infrastruktur teknologi sering menjadi hambatan untuk menerapkan sistem keamanan yang ideal. Oleh karena itu, budaya keamanan siber yang kuat bergantung pada tim informasi teknologi , pimpinan institusi, dan seluruh sistem pengguna bekerja sama (Monia, 2025:2).

Dalam penelitian ini akan membahas secara menyeluruh bagaimana keamanan jaringan komputer sangat penting untuk melindungi website institusi pendidikan dari serangan siber. Dan juga akan membahas berbagai pendekatan yang dapat digunakan untuk membangun sistem keamanan yang kuat dan berkelanjutan. Dan diharapkan lembaga pendidikan memiliki kemampuan untuk membangun ekosistem digital yang aman, terpercaya, dan mendukung kelancaran proses pendidikan di era modern.

METODE

Metode penelitian yang digunakan dalam kajian ini bersifat deskriptif kualitatif. Tujuan utamanya adalah menggali data yang disajikan dalam bentuk narasi, baik melalui tuturan lisan, tulisan, maupun pengamatan terhadap perilaku, tanpa mengandalkan angka atau analisis statistik. Penelitian kualitatif sendiri merupakan pendekatan dalam ilmu sosial yang menekankan pentingnya memahami pengalaman manusia dalam konteks aslinya. Peneliti berusaha menangkap makna dari interaksi sosial melalui bahasa dan istilah yang digunakan oleh para partisipan, dengan mengedepankan sudut pandang mereka secara alami dan mendalam.(Syahrizal 2023 : 7). Penulisan artikel ini menggunakan metode studi literatur atau studi kepustakaan, Metode ini mencakup beberapa tahapan yang saling berkaitan, mulai dari menelusuri dan mengumpulkan data dari berbagai sumber literatur, membaca secara cermat, mencatat informasi yang dianggap penting, hingga mengorganisasi bahan-bahan tersebut agar mendukung proses analisis dalam penelitian (Athiyah 2021 : 2). Penelitian ini menggunakan teknik studi pustaka sebagai metode pengumpulan data, yakni dengan mengumpulkan informasi dari berbagai sumber literatur yang relevan. Teknik ini dilakukan untuk memperoleh pemahaman yang lebih mendalam terkait permasalahan yang diteliti.

HASIL DAN PEMBAHASAN

A. Jenis Ancaman Siber pada Website Institusi Pendidikan

Institut pendidikan adalah tempat pendidikan dan penelitian yang mengelola banyak data sensitif, sehingga mereka mengalami perubahan dinamis dalam informasi teknologi. Institut pendidikan menjadi sasaran potensial untuk serangan siber karena teknologi telah memasuki hampir seluruh aspek kehidupan akademik dan administratif. Ancaman ini terus meningkat karena kompleksitas masalah yang dihadapi lembaga-lembaga ini. Karena mereka menyimpan data sensitif seperti informasi pribadi siswa, hasil penelitian, dan kebijakan akademis, perguruan tinggi memiliki tanggung jawab besar untuk melindungi aset digital mereka dari serangan cyber (Alfian, 2024: 59). Kolaborasi penelitian, administrasi akademis dan keuangan adalah beberapa hal yang menjadi sebuah titik masuk bagi penyerang. Serangan siber dapat berdampak serius terhadap keamanan dan privasi data, merusak reputasi, serta mengganggu stabilitas sistem secara menyeluruh. Oleh karena itu, untuk mencegahnya secara efektif, sangat penting memahami berbagai jenis serangan siber yang paling umum menyerang situs web milik institusi pendidikan (Laksana, 2024: 111).

1. Phishing dan Social Engineering

Teknik phishing adalah cara untuk mencuri data sensitif dengan menyamar sebagai pihak yang dapat dipercaya. Penipu dapat menggunakan email atau situs web palsu, membuat orang tidak curiga saat memberikan data login atau pribadi mereka. Serangan phishing dapat menargetkan mahasiswa, karyawan, atau bahkan dosen universitas. Sebuah email palsu yang mengaku berasal dari administrasi dengan permintaan untuk memperbarui informasi akun dapat mengakibatkan tersebarnya data pribadi atau bahkan peretasan sistem (Alfian, 2024: 61).

Social engineering merupakan metode yang memanfaatkan interaksi sosial secara langsung atau tidak langsung untuk mengumpulkan data dan informasi penting. Pengguna aktif media sosial adalah target utama rekayasa sosial, karena keinginan untuk tetap eksis dengan mengunggah aktivitas mereka dalam bentuk tulisan, foto, atau video, remaja cenderung lebih terbuka. Unggahan tersebut sering mengandung data pribadi, yang dapat menempatkan mereka dalam bahaya, seperti kemungkinan kehilangan privasi dan ancaman keamanan data pribadi (Ayu, 2025:8).

Untuk mendorong korban untuk memberikan informasi yang diinginkan, strategi ini sering digunakan bersama dengan metode social engineering. Pelaku dapat mengambil alih sistem internal kampus, menyalahgunakan akun, atau menyebarkan malware lebih lanjut jika upaya mereka berhasil.

2. Malware

Dalam ranah kejahatan siber, serangan malware merupakan salah satu ancaman yang paling berbahaya. Malware sendiri adalah jenis perangkat lunak berbahaya yang dirancang untuk merusak atau mengambil alih sistem komputer yang memiliki celah keamanan. Umumnya, serangan ini dilakukan melalui tautan atau lampiran mencurigakan yang disisipkan dalam email atau media sosial. Begitu pengguna mengkliknya, malware dapat menyusup ke dalam sistem, lalu menyebabkan kerusakan, mencuri informasi penting, atau bahkan mengendalikan perangkat tanpa sepengetahuan pemiliknya (Praptono, 2024:1532).

Malware memiliki beberapa jenis yaitu, virus, worm, dan ransomware, yang dapat merusak atau menghapus data, mengganggu sistem operasi, atau bahkan membuat sistem tidak dapat digunakan sama sekali (Ayu, 2025:6). Sebaliknya, ransomware dapat mengenkripsi data akademis penting dan kemudian menuntut pembayaran sebagai ketidakseimbangan untuk memulihkan data tersebut. Perguruan tinggi harus memperbaiki dan memperkuat sistem pertahanan mereka secara teratur untuk menangkal malware yang terus berkembang. Risiko penyebaran malware sangat tinggi di lingkungan kampus yang banyak berbagi dokumen dan tautan. Serangan ransomware di institusi pendidikan dapat menyebabkan pencurian data, pengambilan kendali sistem, atau penguncian data penting.

3. Serangan DDoS (Distributed Denial of Service)

Serangan yang menggunakan jaringan komputer yang tersebar secara geografis untuk mengirimkan lalu lintas data dalam jumlah besar ke target tertentu dengan tujuan mengganggu atau menghentikan layanan yang diberikan oleh target tersebut. Teknik ini menggunakan kelemahan infrastruktur jaringan, seperti keterbatasan bandwidth atau sumber daya komputasi, dan membanjiri target dengan permintaan lalu lintas yang melebihi. Kemajuan teknologi telah membuat serangan DDoS lebih sulit dan lebih mematikan. Serangan DDoS dapat menyebabkan kerugian finansial besar bagi korbannya, selain menimbulkan masalah teknis. Layanan downtime yang tak terduga seringkali menyebabkan kerugian besar bagi perusahaan, seperti hilangnya reputasi dan kepercayaan pelanggan. Industri keamanan siber terus mengembangkan teknologi dan strategi mitigasi yang lebih baik untuk menangani ancaman ini. Penggunaan sistem deteksi dini yang lebih canggih, metode kreatif untuk mengelola lalu lintas serangan , dan layanan perlindungan DDoS yang disediakan oleh penyedia keamanan atau Content Delivery Network (CDN) adalah bagian dari upaya tersebut (Ayu, 2025:8).

4. Web defacement

Web Defacement adalah jenis serangan siber di mana penyerang berhasil mengakses situs web dan mengganti isi halaman dengan pesan atau iklan yang sering kali berisi pandangan politik, isu agama, atau konten yang kasar dan tidak layak. Hal ini dapat merusak reputasi situs tersebut secara signifikan. Salah satu tujuan dari web defacement adalah untuk mencuri data atau informasi pribadi, yang kemudian dapat disalahgunakan.Web defacement biasanya terjadi ketika situs web sedang lemah atau memiliki celah keamanan yang dapat digunakan oleh peretas. Ada beberapa metode yang umum diterapkan oleh peretas dalam melakukan pelanggaran tampilan web.Contoh dari web defacement adalah saat seorang peretas memodifikasi halaman utama dari sebuah website dengan mengubah desain, jenis huruf, serta menampilkan gambar atau pemberitahuan yang tidak pantas. Serangan dari peretas ini jelas sangat merugikan pengunjung dan membahayakan keamanan data yang ada di dalamnya (Hendarto, 2024:1548).

5. Cross-Site Scripting (XXS)

Serangan Cross-Site Scripting (XSS) merupakan tipe injeksi, di mana kode berbahaya ditempatkan di situs web yang dianggap aman dan terpercaya. Serangan XSS terjadi ketika penyerang memanfaatkan aplikasi web untuk mengirimkan kode yang merugikan, biasanya berupa skrip yang dieksekusi di sisi klien, kepada pengguna lain. Kerentanan yang memungkinkan terjadinya serangan ini cukup umum dan dapat ditemukan di berbagai aplikasi web yang menggunakan masukan dari pengguna dalam output yang dihasilkan tanpa melakukan validasi atau pengkodean (Kuswara, 2025:2700).

Seorang penyerang bisa memanfaatkan XSS untuk mengirimkan kode jahat kepada pengguna yang tidak curiga. Peramban pengguna tidak mampu mendeteksi bahwa kode itu tidak terpercaya, sehingga akan menjalankannya. Dengan menganggap kode tersebut berasal dari sumber yang dapat diandalkan, kode jahat ini bisa mengakses cookie, token sesi, atau data sensitif lainnya yang tersimpan di peramban dan digunakan dengan situs tersebut. Kode ini bahkan mampu mengubah isi halaman HTML.

B. Peran Keamanan Jaringan Komputer

Keamanan jaringan komputer memiliki peran krusial dalam mencegah, mendeteksi, dan merespons berbagai ancaman tersebut. Beberapa peran utama yang teridentifikasi adalah:

1. Deteksi Dini Ancaman Dengan menggunakan sistem Intrusion Detection System (IDS)

Menurut Ariyus dalam Fauzi (2018:12) Intrusion Detection System (IDS) merupakan kombinasi perangkat keras dan perangkat lunak yang dirancang untuk mengidentifikasi serta melaporkan aktivitas mencurigakan dalam jaringan komputer. Sistem ini berfungsi sebagai alat bantu yang mampu menganalisis lalu lintas data secara real-time guna mendeteksi potensi ancaman, mencatat kejadian (log), serta mencegah upaya penyalahgunaan atau serangan terhadap sistem.

Intrusion Detection System (IDS) adalah salah satu perangkat keamanan yang berfungsi untuk menghadapi upaya peretasan. Sistem ini mampu mendeteksi dan memberikan peringatan ketika terdapat aktivitas mencurigakan di dalam jaringan. Meski demikian, IDS hanya berperan dalam mendeteksi, bukan mencegah secara langsung terjadinya serangan atau penyusupan (Fauzi, 2018:13).

2. Enkripsi dan perannya dalam Keamanan Informasi Perusahaan

Enkripsi merupakan salah satu bentuk kontrol pencegahan yang digunakan untuk menjaga kerahasiaan dan privasi data. Teknik ini berfungsi sebagai lapisan perlindungan terakhir yang harus dihadapi oleh pihak yang mencoba menyusup, terutama saat data dikirim melalui internet atau ketika mereka berhasil memperoleh akses tidak sah terhadap data yang tersimpan. Enkripsi sendiri adalah proses mengubah teks biasa menjadi format yang tidak dapat dibaca tanpa kunci khusus (Wulandari & Hwihanus, 2023:16).

Faktor yang mempengaruhi kekuatan enkripsi. Ini membuat sulit untuk melakukan upaya untuk menampilkan pola ciphertext yang mencerminkan pola plaintext asli. Dalam bahasa Inggris, 8 bit mewakili semua huruf, membuatnya lebih mudah untuk menggunakan informasi tentang frekuensi kata. Oleh karena itu, sebagian besar kunci enkripsi setidaknya 256 bit (sesuai dengan 2 karakter bahasa Inggris), sering mencapai lebih dari 1.02 bit.

3. Faktor-Faktor Yang Mempengaruhi kekuatan Enkripsi

a) Algoritma Enkripsi

Jenis algoritma yang digunakan untuk menghubungkan tombol dan teks biasa sangat penting. Algoritma yang kompleks dan kuat tidak dapat dengan mudah diretas dengan teknologi brute force. Kekuatan algoritma tidak ada dalam kerahasiaannya,

tetapi dalam kenyataan bahwa ia diuji dengan cermat dan terbukti tahan terhadap serangan.

b) Pedoman untuk Mengelola Kunci Enkripsi

Manajemen kunci enkripsi sering kali menjadi titik paling rentan dalam sistem enkripsi. Ketika seorang karyawan keluar dari perusahaan, atau ada dugaan bahwa kunci telah disusupi, penting bagi organisasi untuk segera mengambil tindakan. Salah satu langkah krusial adalah mencabut kunci tersebut secepat mungkin, terutama jika ada pihak lain yang bergantung pada kunci tersebut, guna mencegah potensi penyalahgunaan data.

c) Kebijakan untuk mengolah kunci kriptografi

Sistem Kriptografi Ada dua jenis dasar dari Sistem Enkripsi Simetris (Sistem Enkripsi Simetris) dengan kunci yang sama dengan. Contoh: AES Sistem Enkryption Asymmetric) Sistem. Anda dapat melihatnya menggunakan salah satu tombol ini, tetapi hanya pasangan Anda yang dapat mendekripsi ciphertext. Contoh: RSA dan PGP.

Salah satu kelemahan utama dari sistem enkripsi asimetris adalah kecepatannya yang relatif lambat dibandingkan dengan enkripsi simetris. Karena alasan ini, enkripsi asimetris dianggap kurang efisien untuk pertukaran data dalam jumlah besar melalui internet. Oleh karena itu, dalam praktik e-bisnis, biasanya digunakan kombinasi dari kedua metode. Enkripsi simetris digunakan untuk mengenkripsi sebagian besar data karena kecepatannya lebih tinggi, sementara enkripsi asimetris dimanfaatkan untuk mengamankan kunci enkripsi simetris tersebut—misalnya dengan mengirimkan kunci melalui email menggunakan kunci publik milik penerima. Hanya penerima yang memiliki kunci privat yang sesuai yang dapat membuka kunci simetris tersebut. Setiap bisnis tentu memiliki informasi yang bersifat rahasia atau sensitif. Maka dari itu, penting untuk menerapkan sejumlah langkah strategis guna meningkatkan perlindungan terhadap data dan menjaga keamanan informasi perusahaan secara keseluruhan.

Membuat Kebijakan Informasi Perusahaan memerlukan arahan data yang jelas untuk membedakan antara informasi rahasia dan tidak mengidentifikasi dan untuk mengatur proses yang ketat untuk identifikasi, manajemen, dan perlindungan data. Gunakan enkripsi untuk transmisi data enkripsi penting untuk melindungi data yang digunakan dalam sistem informasi dan jaringan perusahaan dari akses yang tidak valid. Data harus dilindungi selama penggunaan dan pengiriman. Pilih Perangkat Lunak Aman Gunakan perangkat lunak yang direkomendasikan oleh para ahli keamanan informasi dan orang -orang yang mematuhi standar keamanan. Perangkat lunak yang tidak aman dapat membuka celah peretasan. Kata Sandi (Kata Sandi) Jika kata sandi yang meningkatkan keamanan lemah, ada risiko besar. Anda dapat meningkatkan keamanan dengan menggunakan pelatihan dan aplikasi untuk manajemen kata sandi. Sebagian besar pelanggaran keamanan terjadi karena kelalaian dalam menggunakan kata sandi Anda. Standar ini adalah metode yang diakui secara internasional dan terstruktur untuk melindungi informasi. ISO/IEC 27001 memberikan instruksi organisasi untuk menilai, mengimplementasikan, dan mempertahankan keamanan informasi berdasarkan praktik terbaik.

4. Isolasi Dan Pemulihan sistem

a) Pentingnya Perlindungan Informasi

Peran Sistem Informasi Akuntansi dalam Enkripsi Teknologi Informasi menawarkan keuntungan besar, terutama dalam hal pengiriman, manajemen dan pelaporan keuangan. Sistem Informasi Akuntansi (SIA) adalah bagian penting dari ini. Data yang masuk pengguna diproses sesuai dengan langkah-langkah yang sesuai untuk membuat informasi akuntansi yang akurat dan meningkat. untuk menjadi data akuntansi yang berguna dan andal, semua komponen SIA harus terintegrasi dengan benar. Penggunaan enkripsi dalam sistem ini memainkan peran penting dalam menjaga keamanan dan integritas data pembukuan perusahaan. Isolasi dan Pemulihan Sistem: Keamanan jaringan memungkinkan isolasi bagian sistem yang terdampak serangan dan mempercepat proses pemulihan. Manajemen Insiden Cyber adalah proses yang melibatkan mengidentifikasi, menanggapi, pemulihan, dan pembelajaran dari insiden keamanan siber untuk meminimalkan dampak pada organisasi Anda. Insiden cyber meliputi berbagai peristiwa, seperti cedera data, serangan malware, ransomware, pencurian informasi pendaftaran atau penyakit layanan (DOS/DDOS) (Wulandari & Hwihanus, 2023: 14)

C. Strategi Keamanan Efektif yang Direkomendasikan

Strategi yang ditemukan dalam kajian literatur dan dinilai efektif untuk diterapkan di lingkungan institusi pendidikan meliputi:

1. Penerapan Firewall dan Sistem IDS/IPS

Menurut E. P. Nugroho oleh A. Bustami, Dengan melakukan konfigurasi dan menambahkan aturan tertentu, Snort dapat mengenali serangan berdasarkan pola-pola yang telah ditentukan dalam aturan tersebut. Melalui proses ini, sistem IDS berhasil mendeteksi adanya aktivitas mencurigakan atau serangan. Di sisi lain, terdapat juga NIDS (Network Intrusion Detection System), yakni sistem deteksi intrusi yang beroperasi pada tingkat jaringan. NIDS memiliki kemampuan untuk menerima lalu lintas data, menganalisisnya, dan memberikan respons berupa peringatan ketika terdeteksi ancaman.

Sementara itu, IPS atau sistem pencegahan intrusi berbasis jaringan—juga dikenal sebagai NIPS (Network Intrusion Prevention System)—digunakan dalam layanan Infrastruktur sebagai Layanan (IaaS) pada platform komputasi awan terbuka. Sistem ini berperan dalam memantau serta melindungi jaringan dari upaya penyusupan eksternal yang mencoba mengakses sistem. Jika terdapat serangan di dalam lingkungan cloud, sistem ini akan secara otomatis memberikan laporan kepada administrator jaringan untuk ditindaklanjuti.

2. Enkripsi dan Verifikasi Ganda

Enkripsi data adalah proses mengubah data menjadi bentuk yang tidak dapat dibaca atau dimengerti oleh siapa pun, kecuali oleh pihak yang memiliki akses atau kunci khusus. Teknik ini digunakan untuk menjaga kerahasiaan data saat dikirim atau disimpan di dalam jaringan komputer (Saputra, M. I. 2023 : 2).Untuk menjaga keamanan akses ke sistem digital kampus, seperti portal akademik dan platform e-learning, diperlukan perlindungan ganda yang tidak hanya mengandalkan kata sandi saja. Salah satu cara yang cukup efektif adalah dengan mengenkripsi data—baik saat dikirim maupun saat disimpan—agar tidak mudah dibaca oleh pihak yang tidak berwenang.

Selain itu, penggunaan autentikasi dua langkah (seperti kode OTP ke ponsel) juga sangat membantu menekan risiko akun diretas. Dalam dunia pendidikan, di mana data pribadi mahasiswa dan dosen tersimpan, pendekatan ini bisa jadi pelindung pertama yang mencegah penyalahgunaan akses. Tanpa sistem keamanan yang kuat di sisi pengguna, celah keamanan bisa sangat mudah dimanfaatkan oleh pihak yang tidak bertanggung jawab. Teknologi enkripsi merupakan salah satu cara untuk meningkatkan keamanan. Data yang dikirim dimodifikasi sedemikian rupa sehingga sangat sulit untuk dicegat (Putri, N. C. R, 2024 : 57).

3. Cadangan Data dan Rencana Pemulihan Jika Terjadi Gangguan

Tidak cukup hanya mencegah serangan, institusi pendidikan juga harus siap jika serangan benar-benar terjadi. Oleh sebab itu, pencadangan data secara teratur menjadi keharusan. Data penting, seperti nilai, arsip akademik, dan dokumen administrasi, perlu disalin dan disimpan di tempat yang aman—baik itu dalam sistem cloud maupun perangkat terpisah. Disaster recovery merupakan serangkaian proses, kebijakan, dan langkah-langkah yang disusun untuk mempersiapkan pemulihan atau kelanjutan operasional infrastruktur teknologi penting suatu organisasi setelah terjadinya bencana, baik yang disebabkan oleh faktor alam maupun ulah manusia (Efendi, I. M. R. N. 2017: 28). Selain itu, menyusun strategi pemulihan sangat penting ketika terjadi insiden besar, seperti peretasan atau serangan ransomware. Dengan memiliki rencana pemulihan bencana (disaster recovery), sebuah institusi dapat mempercepat proses pemulihan dan kembali beroperasi tanpa kehilangan data penting ataupun mengalami gangguan operasional yang berkepanjangan.

4. Peningkatan Kesadaran dan Evaluasi Keamanan Sistem Secara Berkala

Membangun budaya keamanan siber bukanlah hal yang mudah, karena hal ini memerlukan kesadaran kolektif dari semua pihak terhadap pentingnya ketahanan di dunia digital. (Khoironi, S. C. 2020 : 38). Keamanan siber dalam lingkungan institusi pendidikan tidak hanya bergantung pada kekuatan sistem teknologi yang digunakan, tetapi juga pada perilaku dan kesadaran para penggunanya. Ancaman siber bisa timbul bukan hanya dari luar, melainkan juga dari kelalaian internal seperti staf atau mahasiswa yang secara tidak sengaja membuka tautan berbahaya atau menggunakan kata sandi yang mudah ditebak. Oleh karena itu, penting bagi institusi untuk mengedukasi seluruh sivitas akademika mengenai praktik dasar keamanan digital, seperti mengenali phishing, menggunakan autentikasi yang kuat, serta menjaga kerahasiaan informasi pribadi.

Program pelatihan dan sosialisasi terkait keamanan siber perlu dilakukan secara rutin, baik dalam bentuk workshop, modul pembelajaran mandiri, hingga pengingat berkala melalui sistem kampus. Misalnya, setiap awal semester atau ketika ada perubahan kebijakan sistem informasi, pelatihan dasar keamanan dapat diberikan sebagai bagian dari orientasi digital. Langkah ini bertujuan untuk membentuk budaya sadar keamanan (security awareness culture) yang kuat di lingkungan kampus, sehingga setiap pengguna merasa bertanggung jawab atas keamanan informasi yang mereka kelola.

Namun, meningkatkan kesadaran saja tidak cukup. Sistem keamanan jaringan dan infrastruktur digital perlu dievaluasi secara berkala untuk memastikan bahwa tidak ada celah atau kelemahan yang dapat dimanfaatkan oleh pihak luar. Audit keamanan merupakan langkah penting yang dilakukan untuk menilai apakah sistem telah sesuai

dengan standar operasional dan apakah ada konfigurasi yang berisiko. Selain itu, pengujian penetrasi (penetration testing) dapat dilakukan sebagai simulasi serangan yang dikendalikan untuk mengetahui seberapa kuat sistem dalam menahan ancaman dunia nyata.

Untuk menjaga data tetap aman dari berbagai ancaman, organisasi perlu menerapkan strategi keamanan data yang menyeluruh. Beberapa langkah yang bisa dilakukan antara lain menetapkan kontrol akses yang ketat, mengenkripsi data penting, rutin melakukan pencadangan, memperbarui perangkat lunak secara berkala, memberikan pelatihan kesadaran keamanan kepada staf, serta melakukan pemantauan dan analisis sistem secara terus-menerus. Selain itu, pengujian penetrasi secara berkala juga penting untuk mengidentifikasi celah keamanan yang mungkin dimanfaatkan oleh pihak tak bertanggung jawab (Chic, S. A., & Bilqisthi, M. F. 2024 : 5135) . Dengan menggabungkan pendekatan edukatif dan teknis seperti ini, institusi pendidikan tidak hanya bersikap reaktif terhadap ancaman yang muncul, tetapi juga proaktif dalam mencegah potensi risiko di masa depan. Kombinasi antara kesadaran pengguna yang tinggi dan sistem yang terus dipantau dan diuji menjadikan keamanan siber sebagai tanggung jawab kolektif yang berkelanjutan. Hal ini menunjukkan bahwa institusi benar-benar serius dalam menjaga integritas, kerahasiaan, dan ketersediaan layanan digital yang menjadi tulang punggung aktivitas akademik dan administrasi.

SIMPULAN

Di era digital, institusi pendidikan sangat bergantung pada teknologi informasi untuk komunikasi, pembelajaran, dan administrasi. Karena ketergantungan ini, mereka menjadi sasaran potensial untuk berbagai jenis serangan siber, seperti phishing, malware, serangan DDoS, defacement web, dan cross-site scripting. Serangan ini mengganggu operasional dan mengancam kerahasiaan, integritas, dan ketersediaan data, serta reputasi institusi.

Keamanan jaringan komputer sangat penting dalam melindungi situs web institusi dari serangan siber. Keamanan digital sangat penting bagi seluruh organisasi, dan ini termasuk penerapan firewall, sistem deteksi intrusi (IDS), enkripsi data, autentikasi ganda, dan instruksi keamanan siber kepada pengguna dan karyawan IT. Selain itu, kebijakan keamanan yang berkelanjutan, evaluasi sistem berkala, dan kesadaran tentang keamanan digital sangat penting. Untuk mendukung proses pendidikan di era modern, lembaga pendidikan dapat membangun ekosistem digital yang aman, tangguh, dan terpercaya melalui pendekatan yang menyeluruh dan kolaboratif.

DAFTAR PUSTAKA

Alfian, M., & Rahman, R. (2024). KEAMANAN JARINGAN PADA PERGURUAN TINGGI. Jurnal Riset Sistem Informasi, 1(3), 59-64. DOI: https://doi.org/10.69714/qgnbgv11

Athiyah, U., Handayani, A. P., Aldean, M. Y., Putra, N. P., & Ramadhani, R. (2021). Sistem Inferensi Fuzzy: Pengertian, Penerapan, dan Manfaatnya. Journal of Dinda: Data Science, Information Technology, and Data Analytics, 1(2), 73-76. DOI: https://doi.org/10.20895/dinda.v1i2.201

Ayu, R. S., Rivai, M. M., Al Mubarak, N., & Pratama, D. (2025). KEAMANAN INFRASTRUKTUR TEKNOLOGI INFORMASI: ANALISIS ANCAMAN SIBER DAN PENDEKATAN

MITIGASI. *Jurnal Pendidikan Sosial dan Humaniora*, *4*(2), 2598-2609. https://publisherqu.com/index.php/pediaqu/article/view/1945

Cuhanazriansyah, M. R., & Cahyaningrum, Y. (2023). Optimalisasi pengembangan website program studi pendidikan teknologi informasi dengan integrasi data center. *JPGI (Jurnal Penelitian Guru Indonesia)*, *8*(2), 217-220. DOI : https://doi.org/10.29210/023472jpgi0005

Dar, M. H., & Harahap, S. Z. (2018). Implementasi snort intrusion detection system (IDS) pada sistem jaringan komputer. *Informatika*, *6*(3), 14-23. DOI: https://doi.org/10.36987/informatika.v6i3.1619

Fauzi, A. R., & Suartana, I. M. (2018). Monitoring Jaringan Wireless Terhadap Serangan Packet Sniffing Dengan Menggunakan Ids. J. Manaj. Inform, 8(2), 7. https://core.ac.uk/download/pdf/230785539.pdf

Hendarto, D. H., & Handayani, R. S. (2024). Pencegahan Kejahatan Siber Terkait Distribusi Perjudian Online di Indonesia dalam Rangka Mewujudkan Keamanan dan Ketertiban Masyarakat. *Jurnal Syntax Admiration*, *5*(5), 1542-1558. DOI: https://doi.org/10.46799/jsa.v5i5.1136

Kuswara, R., & Ami, F. (2025). ANALISIS KEAMANAN WEBSITE DI SMK WONGSOREJO GOMBONG TERHADAP SERANGAN CROSS-SITE SCRIPTING (XSS) MENGGUNAKAN PENETRATION TESTING. JATI (Jurnal Mahasiswa Teknik Informatika), 9(2), 2700-2707. DOI: https://doi.org/10.36040/jati.v9i2.13158

Laksana, T. G., & Mulyani, S. (2024). Pengetahuan dasar identifikasi dini deteksi serangan kejahatan siber untuk mencegah pembobolan data perusahaan. Jurnal Ilmiah Multidisiplin, 3(01), 109-122. DOI: https://doi.org/10.56127/jukim.v3i01.1143

Monia, F. A., Hanafi, I., Rahmi, A., & Fadilah, I. (2025). KEAMANAN DATA DALAM SISTEM MANAJEMEN PENDIDIKAN BERBASIS TEKNOLOGI DI PEKANBARU. Jurnal Manajemen Pendidikan, 10(1), 1-15. DOI: https://doi.org/10.34125/jmp.v10i1.363

Praptono, A., & Yusuf, H. (2024). Tinjauan Kriminologi Terhadap Pelaku Kejahatan Pemerasan Dengan Menggunakan Virus, Ransomware Wannacry Sebagai Suatu Kejahatan Modern. *Jurnal Intelek Dan Cendikiawan Nusantara*, *1*(2), 1660-1669.

Reyfaldi, A. N., & Rahmatulloh, A. (2024). Optimalisasi Konfigurasi Firewall MikroTik Menggunakan Metode Filter Rules Untuk Keamanan Jaringan. *Jurnal Informatika dan Riset*, *2*(2), 5-12. DOI: https://doi.org/10.36308/iris.v2i2.744

Saputra, M. I. (2023). Literature Review Network Security. Jurnal Jaringan Komputer Dan Keamanan, 04, 30–34. DOI: https://doi.org/10.61346/jjkk.v4i3.66

Suhendi, H., & Cahyo, W. D. (2021). Perancangan dan Implementasi Keamanan Jaringan Menggunakan Snort sebagai Intrusion Prevention System (IPS) pada Jaringan Internet STEI

ITB. *Naratif: Jurnal Nasional Riset, Aplikasi dan Teknik Informatika*, *3*(2), 60-68. DOI: https://doi.org/10.53580/naratif.v3i02.137

Syahrizal, H., & Jailani, M. S. (2023). Jenis-jenis penelitian dalam penelitian kuantitatif dan kualitatif. QOSIM: Jurnal Pendidikan, Sosial & Humaniora, 1(1), 13-23. DOI: https://doi.org/10.61104/jq.v1i1.49

Wulandari, I. W., & Hwihanus, H. (2023). *Peran Sistem Informasi Akuntansi Dalam Pengaplikasian Enkripsi Terhadap Peningkatan Keamanan Perusahaan*. Jurnal Kajian Dan Penalaran Ilmu Manajemen, 1(1), 11–25. DOI: https://doi.org/10.59031/jkpim.v1i1.46