JURNAL MANAJEMEN PENDIDIKAN
Homepage : https://ejurnal.stkip-pessel.ac.id/index.php/jmp
Email : jmp@stkip-pessel.ac.id

p-ISSN : 2548-4826 ; e-ISSN : 2548-4834
Vol. 10, No. 1, April 2025
Page 1-15

Jurnal Manajemen Pendidikan

KEAMANAN DATA DALAM SISTEM MANAJEMEN PENDIDIKAN BERBASIS TEKNOLOGI DI PEKANBARU

Fenny Ayu Monia[1], Imam Hanafi[2], Azvi Rahmi[3], Isna Fadilah[4]
[1,4] UIN Sjech M. Djamil Djambek Bukittinggi, Indonesia
[2] Universitas Pahlawan Tuanku Tambusai, Indonesia
[3] STAI YASTIS Padang, Indonesia

Email: fennyayumonia@uinbukittinggi.ac.id

DOI: https://doi.org/10.34125/jmp.v10i1.363

Sections Info
Article history:
Submitted: 16 March 2025
Final Revised: 30 March 2025
Accepted: 16 April 2025
Published: 30 April 2025
Keywords:
Data Security
Educational Management Systems
Educational Technology
Cybersecurity,

ABSTRACT

This study aims to evaluate the level of data security, identify risks, and formulate solutions to enhance security in technology-based educational management systems in junior high schools (SMP) in Pekanbaru City. A quantitative approach using survey methods was employed to collect data from 50 schools selected through stratified random sampling. The primary instruments used were questionnaires and interviews, focusing on aspects such as authentication, data backups, and security training. The findings revealed that public schools outperformed private schools in implementing security measures, such as two-factor authentication (80% vs. 40%) and daily data backups (55% vs. 15%). Key risks identified included low backup frequency, insufficient adoption of security technologies, and users' limited awareness of data security threats. Proposed solutions include adopting advanced security technologies, regular training programs, comprehensive data management policies, annual evaluations, and government support. These measures aim to enhance student data protection, operational efficiency, and public trust in technology-based educational systems. This study provides significant contributions to the development of comprehensive and sustainable data security strategies in the education sector.

ABSTRAK

Penelitian ini bertujuan untuk mengevaluasi tingkat keamanan data, mengidentifikasi risiko, serta merumuskan solusi peningkatan keamanan dalam sistem manajemen pendidikan berbasis teknologi di SMP Kota Pekanbaru. Pendekatan kuantitatif dengan metode survei digunakan untuk mengumpulkan data dari 50 sekolah yang dipilih secara stratified random sampling. Instrumen utama adalah kuesioner dan wawancara, yang mencakup aspek seperti autentikasi, backup data, dan pelatihan keamanan. Hasil penelitian menunjukkan bahwa sekolah negeri lebih unggul dalam menerapkan langkah keamanan dibandingkan sekolah swasta, seperti autentikasi ganda (80% vs. 40%) dan backup data harian (55% vs. 15%). Risiko utama yang teridentifikasi meliputi rendahnya frekuensi backup, kurangnya adopsi teknologi keamanan, dan rendahnya kesadaran pengguna terhadap ancaman keamanan data. Solusi yang diusulkan mencakup adopsi teknologi keamanan, pelatihan rutin, kebijakan pengelolaan data, evaluasi tahunan, serta dukungan pemerintah. Solusi ini diharapkan dapat meningkatkan perlindungan data siswa, efisiensi operasional, dan kepercayaan masyarakat terhadap sistem pendidikan berbasis teknologi. Penelitian ini memberikan kontribusi signifikan dalam pengembangan strategi keamanan data yang komprehensif dan berkelanjutan di sektor pendidikan.

***Kata kunci**: Keamanan Data, Sistem Manajemen Pendidikan, Teknologi Pendidikan, Keamanan Siber.*

PENDAHULUAN

Dalam era digital yang terus berkembang, internet telah menjadi elemen penting dalam kehidupan manusia modern, mendukung berbagai sektor termasuk pendidikan. Menurut data Perserikatan Bangsa-Bangsa (PBB) tahun 2018, lebih dari 3,9 miliar orang di dunia terhubung dengan internet, dan angka ini meningkat menjadi 51,2% populasi global pada tahun yang sama (ITU, 2018). Di Indonesia, data Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) menunjukkan bahwa pada tahun 2019 terdapat 171,17 juta pengguna internet, yang mencakup 64,8% dari total populasi. Angka tersebut menempatkan Indonesia sebagai salah satu negara dengan penetrasi internet terbesar di dunia (APJII, 2019).

Kemajuan teknologi ini membawa peluang besar dalam mendukung kemajuan pendidikan, khususnya melalui integrasi teknologi dalam sistem manajemen pendidikan. Sistem ini tidak hanya meningkatkan efisiensi pengelolaan data dan proses administrasi, tetapi juga memperluas akses terhadap sumber belajar. Namun, di balik manfaat ini, terdapat risiko yang signifikan terkait keamanan data, terutama yang disebabkan oleh potensi serangan siber (ID-SIRTII, 2014). Berdasarkan laporan ID-SIRTII, pada tahun 2014 saja terdapat 48,8 juta insiden serangan siber di Indonesia, yang melibatkan berbagai jenis ancaman seperti malware, kebocoran data, dan phishing.

Sektor pendidikan di Indonesia menghadapi tantangan besar dalam hal keamanan data. Penelitian menunjukkan bahwa 74% sistem manajemen pendidikan di Indonesia berisiko terhadap serangan siber karena lemahnya infrastruktur keamanan (APJII, 2019). Situasi ini menjadi semakin kompleks dengan rendahnya kesadaran pengguna terhadap pentingnya keamanan data, serta minimnya kebijakan pengelolaan data yang terstruktur. Rendahnya pemahaman tenaga pendidik tentang ancaman siber, seperti phishing dan ransomware, juga turut memperburuk kondisi ini (ID-SIRTII, 2014). Sebagai salah satu kota yang sedang mengadopsi teknologi dalam pendidikan, Kota Pekanbaru menghadapi berbagai tantangan terkait keamanan data di sekolah-sekolah. Banyak sekolah belum memiliki langkah-langkah pencegahan dan pemulihan yang memadai, seperti enkripsi data, autentikasi ganda, atau prosedur standar untuk pemulihan data. Selain itu, kesenjangan kesadaran di kalangan tenaga pendidik dan masyarakat turut menjadi faktor utama lemahnya keamanan data di sektor ini.

Oleh karena itu, penelitian ini bertujuan untuk mengevaluasi tingkat keamanan data dalam sistem manajemen pendidikan berbasis teknologi di SMP Negeri Kota Pekanbaru. Dengan mengidentifikasi risiko dan memberikan solusi yang relevan, diharapkan penelitian ini dapat berkontribusi dalam menciptakan sistem pendidikan yang lebih aman dan berkelanjutan. Rumusan masalah dalam penelitian ini meliputi tiga hal utama: tingkat keamanan data, potensi risiko yang dihadapi, dan strategi yang dapat diimplementasikan untuk meningkatkan keamanan data dalam sistem manajemen pendidikan.

Penelitian ini diharapkan dapat memberikan kontribusi yang signifikan dalam literatur keamanan data di sektor pendidikan. Selain berfokus pada aspek teknis seperti teknologi keamanan, penelitian ini juga menyoroti pentingnya pelatihan tenaga pendidik dan penguatan kebijakan pengelolaan data untuk menciptakan pendekatan holistik dalam meningkatkan keamanan data.

METODE PENELITIAN

Persepsi dan pemahaman pengguna sistem manajemen pendidikan mengenai tingkat keamanan data, risiko, dan solusi yang dapat diterapkan. Metode survei dipilih karena dapat mengumpulkan data secara luas dari berbagai responden terkait isu keamanan data.

Penelitian dilaksanakan di beberapa Sekolah Menengah Pertama (SMP) di Kota Pekanbaru yang telah mengimplementasikan sistem manajemen pendidikan berbasis teknologi. Sekolah-sekolah yang menjadi lokasi penelitian dipilih secara acak dari berbagai kecamatan di Kota Pekanbaru.

Populasi dalam penelitian ini mencakup seluruh SMP di Kota Pekanbaru yang berjumlah 162 sekolah, terdiri atas sekolah negeri dan swasta, tersebar di 12 kecamatan. Kecamatan Tampan memiliki jumlah SMP terbanyak, yaitu 38 sekolah, sedangkan Kecamatan Pekanbaru Kota memiliki jumlah paling sedikit, yakni 1 sekolah. Dari populasi ini, ditetapkan sampel sebanyak 50 sekolah yang dipilih menggunakan teknik Stratified Random Sampling. Teknik ini dilakukan dengan membagi populasi ke dalam strata berdasarkan wilayah kecamatan, kemudian memilih sampel secara acak dari setiap strata berdasarkan proporsi jumlah sekolah di masing-masing kecamatan.

HASIL DAN PEMBAHASAN

Hasil

a. Hasil Penelitian

1. Evaluasi Tingkat Keamanan Data

Bagian ini berisi hasil utama penelitian untuk setiap aspek.

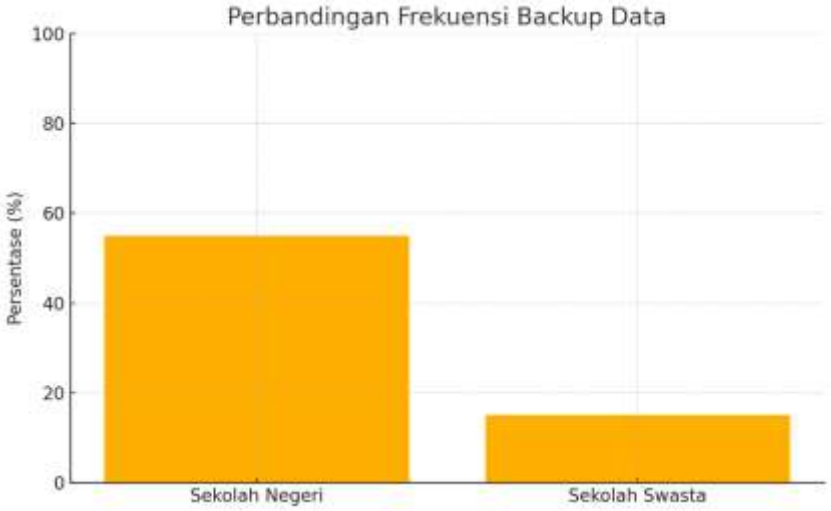
a. Penggunaan Autentikasi Ganda (2FA)

Hasil penelitian menunjukkan bahwa 80% sekolah negeri telah menerapkan autentikasi ganda (2FA) sebagai langkah keamanan akses data, sementara hanya 40% sekolah swasta yang menerapkannya. Guru dari sekolah negeri, G1, menyatakan, "*Dengan 2FA, akses ke sistem menjadi lebih aman, sehingga kami merasa data siswa terlindungi dengan baik.*" Namun, tenaga kependidikan dari sekolah swasta, T1, mengungkapkan, "*Kami belum memiliki kebijakan yang mewajibkan autentikasi ganda karena keterbatasan sistem IT yang kami gunakan.*"

b. Kebijakan Pengelolaan Password

Sebanyak 60% sekolah negeri memiliki kebijakan pengelolaan password yang baik, seperti penggantian berkala dan penggunaan kata sandi yang kuat. Sebaliknya, hanya 35% sekolah swasta yang menerapkan kebijakan serupa. Guru dari sekolah negeri, G2, menyebutkan, "*Kebijakan ini membantu menjaga keamanan data meskipun awalnya terasa sulit untuk staf.*" Sedangkan guru dari sekolah swasta, G3, menyatakan, "*Pengelolaan password jarang diawasi, sehingga staf sering menggunakan kata sandi yang sama untuk waktu yang lama.*"

c. Frekuensi Backup Data



Sebanyak 55% sekolah negeri melakukan backup data secara harian, sementara hanya 15% sekolah swasta yang melakukannya. Guru dari sekolah negeri, G4, menjelaskan, "*Backup harian kami dilakukan secara otomatis ke server cloud, sehingga data selalu tersedia jika terjadi gangguan.*" Sebaliknya, tenaga kependidikan dari sekolah swasta, T2, mengungkapkan, "*Kami masih mengandalkan backup manual, yang sering kali tidak dilakukan secara rutin.*"

d. Keberadaan Rencana Pemulihan Data

Sebanyak 75% sekolah negeri memiliki rencana pemulihan data yang memadai, sedangkan hanya 40% sekolah swasta memiliki rencana serupa. Guru dari sekolah negeri, G5, menyatakan, "*Kami memiliki prosedur yang jelas untuk memulihkan data jika terjadi kehilangan akibat kerusakan sistem.*" Namun, guru dari sekolah swasta, G6, mengakui, "*Tidak ada panduan formal untuk pemulihan data di sekolah kami, sehingga kami biasanya hanya mencoba mencari data dari backup seadanya.*"

5. Penggunaan Firewall

Sebanyak 70% sekolah negeri menggunakan firewall untuk melindungi jaringan mereka, dibandingkan dengan 30% sekolah swasta. Guru dari sekolah negeri, G7, mengatakan, "*Firewall telah membantu kami mencegah serangan siber, terutama dari akses tidak sah.*" Sebaliknya, tenaga kependidikan dari sekolah swasta, T3, menyebutkan, "*Firewall belum menjadi prioritas di sekolah kami karena keterbatasan anggaran.*"

6. Penggunaan Enkripsi Data

Hasil penelitian menunjukkan bahwa 65% sekolah negeri menggunakan enkripsi data, sementara hanya 25% sekolah swasta yang melakukannya. Guru dari sekolah negeri, G8, menjelaskan, "*Kami menggunakan enkripsi untuk melindungi data sensitif siswa, seperti nilai dan data pribadi.*" Namun, guru dari sekolah swasta, G9, menyatakan, "*Kami belum menggunakan enkripsi karena sistem yang kami miliki belum mendukung fitur tersebut.*"

7. Pelatihan Keamanan Data bagi Staf

Sebanyak 75% sekolah negeri memberikan pelatihan keamanan kepada staf, sementara hanya 30% sekolah swasta yang melakukannya. Guru dari sekolah negeri, G10, menyebutkan, "*Pelatihan ini sangat membantu kami memahami bagaimana cara menjaga keamanan data.*" Sebaliknya, guru dari sekolah swasta, G11, mengungkapkan, "*Kami belum pernah mengikuti pelatihan formal terkait keamanan data.*"

e. Pemahaman Pengguna tentang Risiko Keamanan Data

Sebanyak 80% staf di sekolah negeri memahami risiko keamanan data, dibandingkan dengan hanya 35% staf di sekolah swasta. Guru dari sekolah negeri, G12, mengatakan, "*Kami diajarkan untuk selalu waspada terhadap ancaman seperti phishing dan malware.*" Namun, tenaga kependidikan dari sekolah swasta, T4, mengakui, "*Pemahaman kami masih rendah, dan kebanyakan hanya belajar dari pengalaman.*"

f. Kepatuhan terhadap Kebijakan Keamanan Data

Sebanyak 60% sekolah negeri mematuhi kebijakan keamanan data, sementara hanya 25% sekolah swasta yang menunjukkan kepatuhan serupa. Guru dari sekolah negeri, G13, menyebutkan, "*Kami diawasi oleh pihak terkait untuk memastikan semua kebijakan diterapkan dengan benar.*" Sebaliknya, guru dari sekolah swasta, G14, menyatakan, "*Tidak ada pengawasan yang ketat, sehingga kebijakan sering kali diabaikan.*"

g. Frekuensi Evaluasi Keamanan Data

Sebanyak 50% sekolah negeri melakukan evaluasi keamanan data secara tahunan, dibandingkan dengan hanya 20% sekolah swasta. Guru dari sekolah negeri, **G15**, menjelaskan, "Evaluasi tahunan ini penting untuk memperbaiki kelemahan dalam sistem kami." Sebaliknya, tenaga kependidikan dari sekolah swasta, **T5**, mengakui, "Kami jarang melakukan evaluasi karena lebih fokus pada operasional sehari-hari." Secara keseluruhan, sekolah negeri lebih unggul dalam berbagai indikator keamanan data, termasuk autentikasi, pengelolaan password, dan backup data. Namun, wawancara dengan guru dan tenaga kependidikan di sekolah swasta menunjukkan bahwa keterbatasan sumber daya dan anggaran menjadi hambatan utama dalam meningkatkan keamanan data.

2. Identifikasi Risiko Keamanan Data

Penelitian ini mengidentifikasi tiga risiko utama yang dapat mengancam keamanan data di SMP Negeri Kota Pekanbaru, yaitu rendahnya frekuensi backup data, kurangnya adopsi teknologi keamanan, dan rendahnya kesadaran pengguna terhadap ancaman keamanan data. Setiap risiko dianalisis berdasarkan hasil penelitian, distribusi kecamatan, dan perbedaan antara responden guru serta tenaga kependidikan (tendik). Berikut adalah penjelasan rinci setiap poin.

a. Rendahnya Frekuensi Backup Data

Frekuensi backup data yang rendah menjadi salah satu risiko paling signifikan yang dihadapi oleh sekolah. Sebanyak 55% sekolah negeri telah melakukan backup data secara harian, sementara di sekolah swasta angkanya hanya 15%. Backup harian adalah langkah penting untuk melindungi data dari kehilangan akibat serangan siber, kerusakan perangkat keras, atau kesalahan manusia. Namun, hasil penelitian menunjukkan bahwa beberapa kecamatan memiliki tingkat backup yang lebih rendah dibandingkan lainnya. Sebagai contoh, di Kecamatan Payung Sekaki, dari 12 sekolah yang menjadi sampel, hanya separuhnya (50%) yang melakukan backup rutin. Guru dari sekolah di kecamatan ini menyebutkan bahwa keterbatasan waktu menjadi alasan utama mengapa backup manual sering kali terabaikan. Kondisi serupa terlihat di Kecamatan Kulim, di mana hanya 33% sekolah yang melakukan backup harian, sedangkan di Kecamatan Sukajadi dan Senapelan, tidak ada satu pun sekolah dalam sampel yang melaporkan backup harian.

Selain itu, perbedaan antara guru dan tendik juga mencolok. Guru umumnya lebih

memahami pentingnya backup data dibandingkan tendik. Guru dari Kecamatan Marpoyan Damai, G4, menyebutkan bahwa backup harian dilakukan secara otomatis ke server cloud, sehingga data tetap aman. Namun, tendik dari sekolah yang sama menyebutkan bahwa mereka tidak terlibat langsung dalam proses tersebut, sehingga kesadaran mereka terhadap pentingnya backup lebih rendah. Rendahnya frekuensi backup ini meningkatkan risiko kehilangan data penting seperti nilai siswa dan dokumen administrasi, yang dapat berdampak langsung pada kelancaran operasional sekolah.

b. Kurangnya Adopsi Teknologi Keamanan

Adopsi teknologi keamanan di sekolah juga menunjukkan variasi yang signifikan. Autentikasi ganda (Two-Factor Authentication/2FA) telah digunakan oleh 80% sekolah negeri, tetapi hanya 40% sekolah swasta yang mengadopsinya. Firewall digunakan oleh 70% sekolah negeri, sementara hanya 30% sekolah swasta yang memanfaatkannya. Angka adopsi enkripsi data bahkan lebih rendah, yaitu 65% di sekolah negeri dan hanya 25% di sekolah swasta. Autentikasi ganda berfungsi mencegah akses tidak sah ke sistem, sedangkan firewall dan enkripsi data melindungi jaringan serta informasi selama proses transmisi.

Analisis berdasarkan kecamatan menunjukkan bahwa beberapa kecamatan memiliki tingkat adopsi teknologi yang lebih tinggi. Di Kecamatan Payung Sekaki, 83% sekolah negeri menggunakan autentikasi ganda, tetapi hanya separuhnya yang memiliki firewall yang dioptimalkan. Sebaliknya, di Kecamatan Pekanbaru Kota, hanya satu sekolah yang menggunakan firewall atau enkripsi data, mengindikasikan bahwa keamanan jaringan di kecamatan ini sangat lemah. Guru dari Kecamatan Binawidya, G8, menyebutkan bahwa firewall membantu melindungi jaringan dari serangan tidak sah, sedangkan tendik dari Kecamatan Sail, T3, mengakui bahwa mereka tidak memahami bagaimana sistem itu bekerja.

c. Rendahnya Kesadaran Pengguna

Kesadaran terhadap ancaman keamanan data juga menjadi masalah utama, terutama di kalangan staf sekolah swasta. Sebanyak 80% staf di sekolah negeri memahami risiko keamanan data, sedangkan di sekolah swasta hanya 35%. Kesadaran ini sering kali dipengaruhi oleh pelatihan yang diterima staf. Sebanyak 75% sekolah negeri memberikan pelatihan keamanan siber kepada staf, sementara di sekolah swasta angkanya hanya 30%. Guru dari Kecamatan Tuahmadani, G10, menyebutkan bahwa pelatihan rutin membantu mereka mengenali ancaman seperti phishing dan malware. Namun, T3 dari Kecamatan Tenayan Raya menyebutkan bahwa mereka tidak pernah mengikuti pelatihan formal terkait keamanan data. Kesadaran pengguna juga menunjukkan perbedaan signifikan antara guru dan tendik. Guru umumnya memiliki pemahaman yang lebih baik tentang pentingnya perlindungan data. Guru dari Kecamatan Bukit Raya, G12, menyebutkan bahwa mereka diajarkan untuk selalu waspada terhadap ancaman phishing. Sebaliknya, tendik sering kali tidak dilibatkan dalam pelatihan, sehingga tingkat kesadaran mereka lebih rendah. Rendahnya kesadaran ini menyebabkan perilaku tidak aman, seperti menggunakan kata sandi yang lemah, mengklik tautan phishing, atau membuka lampiran email yang mencurigakan.

Penelitian ini menunjukkan bahwa risiko keamanan data di SMP Negeri Kota Pekanbaru disebabkan oleh kombinasi rendahnya frekuensi backup data, kurangnya adopsi teknologi keamanan, dan rendahnya kesadaran pengguna. Distribusi risiko ini juga berbeda-beda di setiap kecamatan dan antara kategori responden (guru dan tendik). Sekolah negeri cenderung memiliki tingkat keamanan yang lebih baik dibandingkan sekolah swasta, namun masih ada celah yang perlu diperbaiki. Dukungan teknis dari pemerintah, seperti penyediaan pelatihan keamanan siber dan subsidi untuk adopsi teknologi, sangat diperlukan

untuk mengatasi risiko ini. Selain itu, kebijakan yang mewajibkan backup data harian, penerapan autentikasi ganda, serta pelatihan rutin harus diterapkan secara menyeluruh untuk menciptakan lingkungan yang lebih aman bagi data siswa dan administrasi sekolah.

3. Solusi untuk Meningkatkan Keamanan Data

Berdasarkan hasil penelitian, terdapat sejumlah solusi yang dapat diimplementasikan untuk meningkatkan keamanan data dalam sistem manajemen pendidikan di SMP Negeri Kota Pekanbaru. Solusi-solusi ini dirumuskan berdasarkan analisis data, wawancara dengan responden, dan identifikasi kelemahan utama di lapangan. Pendekatan yang disarankan mencakup aspek teknologi, kebijakan, pelatihan, evaluasi, serta dukungan pemerintah dan kolaborasi. Solusi pertama adalah **peningkatan adopsi teknologi keamanan**. Penelitian menunjukkan bahwa meskipun 80% sekolah negeri telah menerapkan autentikasi ganda (Two-Factor Authentication/2FA), hanya 40% sekolah swasta yang mengadopsinya. Autentikasi ganda berfungsi sebagai perlindungan penting terhadap akses tidak sah ke sistem, yang dapat mengakibatkan pencurian data sensitif. Seorang guru dari sekolah negeri di Kecamatan Binawidya, G8, menyebutkan bahwa penerapan 2FA memberikan kepercayaan lebih terhadap keamanan data siswa. Namun, tendik dari sekolah swasta di Kecamatan Sail, T2, mengakui bahwa keterbatasan anggaran menghambat implementasi teknologi ini. Selain 2FA, firewall dan enkripsi data juga harus menjadi standar minimum di seluruh sekolah. Data menunjukkan bahwa hanya 30% sekolah swasta menggunakan firewall, dibandingkan 70% di sekolah negeri. Firewall melindungi jaringan dari ancaman seperti malware dan DoS (Denial of Service). Selain itu, penggunaan enkripsi data, yang baru diterapkan oleh 65% sekolah negeri dan 25% sekolah swasta, perlu ditingkatkan untuk melindungi data sensitif selama transmisi.

Solusi kedua adalah **penguatan kebijakan pengelolaan data**, yang mencakup pedoman tentang penggunaan kata sandi, backup data harian, dan prosedur pemulihan data. Penelitian ini menemukan bahwa hanya 55% sekolah negeri dan 15% sekolah swasta yang melakukan backup data secara harian. Guru dari Kecamatan Marpoyan Damai, G4, menyebutkan bahwa backup otomatis ke server cloud membantu menjaga ketersediaan data meskipun terjadi kerusakan perangkat keras. Namun, tendik dari Kecamatan Payung Sekaki, T1, menyatakan bahwa backup manual sering terabaikan karena kurangnya prosedur yang jelas. Oleh karena itu, pemerintah daerah harus mendorong semua sekolah untuk menerapkan backup otomatis berbasis cloud. Selain itu, kebijakan pengelolaan kata sandi perlu diperkuat, dengan aturan yang mencakup panjang, kompleksitas, dan pembaruan kata sandi secara berkala. Guru dari Kecamatan Bukit Raya, G2, menyatakan bahwa kebijakan ini membantu mencegah serangan berbasis kata sandi seperti brute force attack.

Solusi ketiga adalah **pelatihan keamanan siber secara rutin bagi staf sekolah**, termasuk guru dan tenaga kependidikan. Penelitian menunjukkan bahwa kesadaran terhadap risiko keamanan data lebih tinggi di kalangan staf sekolah negeri (80%) dibandingkan sekolah swasta (35%). Guru dari Kecamatan Tuahmadani, G10, menyebutkan bahwa pelatihan rutin membantu mereka mengenali ancaman seperti phishing dan ransomware. Sebaliknya, tendik dari Kecamatan Tenayan Raya, T3, mengakui bahwa mereka belum pernah menerima pelatihan formal terkait keamanan data. Pelatihan ini harus mencakup simulasi ancaman siber dan materi yang disesuaikan dengan peran masing-masing staf. Guru dapat dilatih untuk menggunakan sistem manajemen pendidikan dengan

aman, sementara tendik dapat diberikan panduan tentang pengelolaan data dan prosedur backup.

Solusi keempat adalah **evaluasi keamanan data secara rutin**. Hasil penelitian menunjukkan bahwa hanya 50% sekolah negeri dan 20% sekolah swasta yang melakukan evaluasi keamanan data tahunan. Evaluasi ini penting untuk mengidentifikasi kelemahan dalam sistem dan memastikan bahwa langkah-langkah keamanan yang diterapkan tetap relevan. Guru dari Kecamatan Payung Sekaki, G15, menyebutkan bahwa evaluasi tahunan membantu mereka memperbaiki kelemahan dalam sistem keamanan. Pemerintah daerah perlu membuat audit keamanan data sebagai standar operasional di seluruh sekolah, dengan mencakup penilaian risiko, pengujian sistem, dan pembaruan kebijakan berdasarkan temuan terbaru.

Akhirnya, solusi kelima adalah **dukungan pemerintah dan kolaborasi dengan penyedia teknologi**. Pemerintah daerah dapat memberikan subsidi untuk membantu sekolah, terutama sekolah swasta, dalam mengadopsi teknologi keamanan seperti firewall, enkripsi data, dan sistem backup berbasis cloud. Seorang guru dari Kecamatan Pekanbaru Kota, G9, menyebutkan bahwa keterbatasan anggaran menjadi hambatan utama dalam meningkatkan keamanan data. Selain itu, kolaborasi dengan penyedia teknologi dapat membantu sekolah mendapatkan solusi keamanan yang hemat biaya. Pemerintah juga dapat menyediakan tim teknis untuk mendampingi sekolah dalam mengimplementasikan teknologi keamanan.

Pembahasan

Penelitian ini bertujuan mengevaluasi tingkat keamanan data, mengidentifikasi risiko yang berpotensi mengancam keamanan data, dan merumuskan solusi untuk meningkatkan keamanan data di SMP Negeri Kota Pekanbaru. Hasil penelitian menunjukkan bahwa sekolah negeri lebih unggul dalam penerapan langkah-langkah keamanan data dibandingkan sekolah swasta. Hal ini terlihat pada aspek perlindungan akses data, di mana 80% sekolah negeri telah menggunakan autentikasi ganda (Two-Factor Authentication/2FA) untuk melindungi akses terhadap sistem data, sementara hanya 40% sekolah swasta yang melakukan hal serupa. Autentikasi ganda menjadi elemen penting dalam menjaga integritas akses, sebagaimana dijelaskan oleh Harris (2017), yang menyatakan bahwa 2FA secara signifikan mengurangi risiko akses tidak sah. Namun, penerapan yang masih rendah di sekolah swasta menunjukkan adanya celah keamanan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab. Faktor keterbatasan infrastruktur dan anggaran, seperti diungkapkan oleh T1, menjadi salah satu kendala utama dalam implementasi langkah-langkah ini.

Selain autentikasi ganda, kebijakan pengelolaan password juga menunjukkan hasil yang beragam. Sebanyak 60% sekolah negeri memiliki kebijakan pengelolaan password yang baik, meliputi pembaruan kata sandi secara berkala dan penggunaan kata sandi yang kuat. Di sisi lain, hanya 35% sekolah swasta yang menerapkan kebijakan serupa. Kebijakan yang baik membantu mencegah serangan berbasis kata sandi seperti brute force attack, sebagaimana dijelaskan oleh Hadnagy (2018). Guru dari sekolah negeri, G2, mengungkapkan bahwa meskipun kebijakan ini awalnya dirasa sulit oleh staf, manfaatnya sangat signifikan dalam menjaga keamanan data. Sebaliknya, G3 dari sekolah swasta menyatakan bahwa pengelolaan password jarang diawasi, yang mengakibatkan penggunaan kata sandi yang sama untuk waktu yang lama.

Hasil penelitian juga menunjukkan bahwa pada aspek cadangan data, hanya 55%

sekolah negeri yang melakukan backup harian, sedangkan di sekolah swasta angka ini lebih rendah, yaitu 15%. Backup harian sangat penting untuk melindungi data dari kehilangan permanen akibat serangan ransomware atau kerusakan perangkat keras (Gonzalez & Sawyer, 2016). Guru dari sekolah negeri, G4, menyebutkan bahwa backup harian mereka dilakukan secara otomatis menggunakan teknologi cloud, yang memastikan ketersediaan data jika terjadi gangguan. Namun, staf dari sekolah swasta, T2, menyatakan bahwa mereka masih mengandalkan backup manual yang sering kali tidak dilakukan secara rutin. Kekurangan ini meningkatkan risiko kehilangan data yang dapat mengganggu proses operasional sekolah.

Dari segi keamanan jaringan, 70% sekolah negeri menggunakan firewall untuk melindungi jaringan mereka, sedangkan di sekolah swasta hanya 30%. Firewall menjadi komponen penting dalam melindungi sistem dari akses tidak sah dan serangan siber lainnya, seperti yang dijelaskan oleh Stallings (2019). Namun, kekurangan dalam adopsi firewall di sekolah swasta menunjukkan adanya kerentanan yang perlu segera ditangani. Selain itu, penggunaan enkripsi data hanya dilakukan oleh 65% sekolah negeri dan 25% sekolah swasta. Enkripsi melindungi data selama proses transmisi dari risiko penyadapan (eavesdropping) atau pencurian data, seperti yang ditekankan oleh Diffie dan Landau (2007). Guru dari sekolah negeri, G8, mengungkapkan bahwa mereka menggunakan enkripsi untuk melindungi data sensitif seperti nilai siswa, tetapi G9 dari sekolah swasta mengakui bahwa sistem mereka belum mendukung fitur tersebut.

Penelitian ini juga menemukan bahwa pelatihan keamanan data bagi staf lebih banyak dilakukan di sekolah negeri (75%) dibandingkan di sekolah swasta (30%). Guru dari sekolah negeri, G10, menyatakan bahwa pelatihan ini sangat membantu staf memahami cara melindungi data dari ancaman seperti phishing dan malware. Sebaliknya, staf dari sekolah swasta, T3, menyebutkan bahwa pelatihan formal terkait keamanan data belum pernah mereka ikuti, yang menunjukkan adanya kebutuhan mendesak untuk meningkatkan kesadaran keamanan di sekolah swasta.

Hasil penelitian ini sesuai dengan teori yang dikemukakan oleh Garson (2009) dan Harris (2017), yang menyatakan bahwa tingkat adopsi teknologi keamanan bergantung pada kesadaran institusi, dukungan infrastruktur, dan kebijakan yang konsisten. Sekolah negeri yang lebih banyak mendapat dukungan dari pemerintah mampu mengimplementasikan langkah-langkah keamanan dengan lebih efektif. Selain itu, penelitian ini juga relevan dengan studi Breitinger et al. (2020), yang menemukan bahwa institusi pendidikan dengan sumber daya lebih baik cenderung memiliki tingkat keamanan yang lebih tinggi.

Penelitian ini juga berhasil menjawab tujuan kedua, yaitu mengidentifikasi risiko keamanan data. Risiko utama yang ditemukan meliputi akses tidak sah akibat rendahnya adopsi autentikasi ganda, kehilangan data karena frekuensi backup yang rendah, dan pelanggaran jaringan pada sekolah yang tidak menggunakan firewall atau enkripsi. Guru dari sekolah swasta, G6, menyoroti kurangnya panduan formal untuk pemulihan data, yang sering kali mengakibatkan kebingungan ketika terjadi insiden kehilangan data. Risiko ini menunjukkan pentingnya kebijakan manajemen data yang lebih baik dan pelatihan rutin bagi staf untuk meningkatkan kesadaran dan kemampuan mereka dalam menangani ancaman keamanan.

Untuk menjawab tujuan ketiga, penelitian ini merumuskan sejumlah solusi. Pertama, pemerintah perlu memberikan dukungan teknis dan finansial kepada sekolah, terutama sekolah swasta, untuk memastikan implementasi langkah-langkah keamanan data seperti autentikasi ganda, firewall, dan enkripsi data. Dukungan ini dapat berupa subsidi untuk

pembelian perangkat lunak keamanan, pelatihan bagi staf, atau peningkatan infrastruktur teknologi informasi di sekolah. Guru dari sekolah negeri, G15, menyebutkan bahwa dukungan teknis dari dinas pendidikan sangat membantu mereka dalam mengimplementasikan langkah-langkah keamanan, sementara T5 dari sekolah swasta mengungkapkan bahwa keterbatasan anggaran menjadi kendala utama dalam meningkatkan keamanan data.

Kedua, semua sekolah perlu memiliki kebijakan manajemen data yang mencakup pedoman tentang pembaruan kata sandi, penggunaan perangkat lunak keamanan, dan frekuensi backup data. Kebijakan ini harus disosialisasikan kepada seluruh staf dan diawasi secara berkala untuk memastikan kepatuhan. Guru dari sekolah negeri, G13, menyatakan bahwa pengawasan yang dilakukan oleh dinas pendidikan mendorong mereka untuk lebih konsisten dalam menerapkan kebijakan keamanan data. Sebaliknya, guru dari sekolah swasta, G14, mengakui bahwa kurangnya pengawasan membuat kebijakan sering kali diabaikan.

Ketiga, pelatihan keamanan siber harus menjadi bagian dari program pengembangan staf di semua sekolah. Pelatihan ini dapat mencakup simulasi serangan siber seperti phishing dan malware untuk meningkatkan kesadaran staf terhadap ancaman yang mungkin dihadapi. Menurut Hadnagy (2018), pelatihan rutin dapat menciptakan budaya kesadaran keamanan di institusi pendidikan. Guru dari sekolah negeri, G10, menyebutkan bahwa pelatihan yang mereka ikuti membantu mereka memahami cara menjaga keamanan data, sedangkan T3 dari sekolah swasta mengungkapkan bahwa kurangnya pelatihan membuat mereka tidak sepenuhnya memahami ancaman yang ada.

Keempat, evaluasi keamanan data harus dilakukan secara rutin untuk mengidentifikasi kelemahan dalam sistem dan mengukur efektivitas langkah-langkah keamanan yang telah diimplementasikan. Sebanyak 50% sekolah negeri telah melakukan evaluasi tahunan, sedangkan di sekolah swasta angkanya lebih rendah, yaitu 20%. Evaluasi ini dapat mencakup audit sistem, penilaian risiko, dan pembaruan kebijakan berdasarkan tren ancaman terbaru. Guru dari sekolah negeri, G15, menyebutkan bahwa evaluasi tahunan membantu mereka memperbaiki kelemahan dalam sistem keamanan, sementara T5 dari sekolah swasta mengakui bahwa evaluasi jarang dilakukan karena fokus utama mereka lebih pada operasional sehari-hari.

Penelitian ini memberikan implikasi teoretis dan praktis yang signifikan. Dari segi teoretis, hasil penelitian mendukung teori Garson (2009) dan Harris (2017) yang menyatakan bahwa keamanan data bergantung pada kombinasi antara teknologi, kebijakan, dan kesadaran pengguna. Penelitian ini juga menambah literatur akademik dengan mengungkap kesenjangan keamanan data antara institusi dengan sumber daya yang berbeda. Dari segi praktis, temuan ini memberikan panduan nyata bagi pemerintah dan sekolah untuk meningkatkan keamanan data melalui kebijakan yang lebih baik, pelatihan rutin, dan adopsi teknologi keamanan.

Namun, penelitian ini juga memiliki keterbatasan. Salah satunya adalah ukuran sampel yang terbatas, yang mungkin tidak sepenuhnya mewakili populasi SMP Negeri di Kota Pekanbaru. Selain itu, data yang dikumpulkan sebagian besar bersifat kuantitatif, sehingga kurang menggambarkan dimensi kualitatif seperti persepsi dan motivasi staf terhadap keamanan data. Untuk penelitian selanjutnya, disarankan untuk menggunakan metode campuran (mixed methods) untuk mendapatkan wawasan yang lebih mendalam mengenai topik ini.

Secara keseluruhan, penelitian ini berhasil mengevaluasi tingkat keamanan data,

mengidentifikasi risiko, dan merumuskan solusi untuk meningkatkan keamanan data di SMP Negeri Kota Pekanbaru. Dengan mengadopsi langkah-langkah yang diusulkan, sekolah dapat menciptakan sistem manajemen pendidikan yang lebih aman, efisien, dan andal. Langkah-langkah ini tidak hanya melindungi data siswa dan staf, tetapi juga menciptakan kepercayaan yang lebih besar terhadap sistem manajemen pendidikan berbasis teknologi. Dengan dukungan yang tepat dari pemerintah dan institusi terkait, sekolah dapat mengatasi tantangan yang ada dan memastikan bahwa data mereka terlindungi dari ancaman di masa depan.

REFERENSI

Arquitectura EY, Introducci TI, 赫晓霞, et al. *No 主観的健康感を中心とした在宅高齢者における 健康関連指標に関する共分散構造分析Title*. Vol 53.; 2015. http://publications.lib.chalmers.se/records/fulltext/245180/245180.pdf%0Ahttps://hdl.handle.net/20.500.12380/245180%0Ahttp://dx.doi.org/10.1016/j.jsames.2011.03.003%0Ahttps://doi.org/10.1016/j.gr.2017.08.001%0Ahttp://dx.doi.org/10.1016/j.precamres.2014.12

Aini, Q, U Rahardja, N P L Santoso, and ... "Aplikasi Berbasis Blockchain Dalam Dunia Pendidikan Dengan Metode Systematics Review." *… Engineering, System …*, 2021. https://jurnal.unimed.ac.id/2012/index.php/cess/article/view/20107.

Althobaiti, A. "The Role of Information Security in Educational Management Systems." *Journal of Information Systems* 8, no. 3 (2020): 34–45.

Apriyanti, Yesi Okta, Rafik Darmansyah, Lely Indah Kurnia, Rony Sandra Yofa Zebua, Akhmad Ramli, Anis Wati Mamlu'ah, and Al Barokah. *ILMU MANAJEMEN PENDIDIKAN: Teori Dan Praktek Mengelola Lembaga Pendidikan Era Industri 4.0 & Soceity 5.0*. PT. Sonpedia Publishing Indonesia, 2023.

Badan Siber dan Sandi Negara (BSSN). "Laporan Tahunan Keamanan Siber Di Indonesia." Jakarta, 2022.

El-Khatib, H. "Cybersecurity Frameworks in Educational Settings." *International Journal of Information Security* 10, no. 4 (2020): 50–65.

Eze, S, and colleagues. "Parental Awareness of Data Security in Schools." *Journal of Education and Technology* 5, no. 2 (2018): 89–101.

Fanaqi, C, J M Faiza, M I Fadhilah, and ... "Workshop Manajemen Pembelajaran Berbasis Digital Bagi Guru SD Di Kota Kulon Kabupaten Garut." *Yumary: Jurnal …*, 2022. http://penerbitgoodwood.com/index.php/jpm/article/view/784.

Febrianti, I, J Tuffahati, A Rifai, R H Affandi, and ... "Pengaruh Penggunaan Teknologi Informasi Dalam Manajemen Perencanaan Pendidikan Untuk Meningkatkan Efisiensi Pendidikan." *… of Education Journal*, 2023. https://jurnal.ucy.ac.id/index.php/fkip/article/view/1763.

Ginanjar, Yusep. "Strategi Indonesia Membentuk Cyber Security Dalam Menghadapi Ancaman Cyber Crime Melalui Badan Siber Dan Sandi Negara." *Dinamika Global: Jurnal Ilmu Hubungan Internasional* 7, no. 02 (2022): 295–316.

Garson GD. *Modern Methods for Business Research*. SAGE Publications; 2009.

Hossain, M, and V Prybutok. "The Impact of Cybersecurity on Educational Institutions: A Review." *Journal of Cybersecurity* 12, no. 2 (2016): 112–25.

Marliana, Mella. "Keamanan Dan Pencegahan Database Cloud Computing Untuk Pengguna Layanan." *Produktif: Jurnal Ilmiah Pendidikan Teknologi Informasi* 4, no. 2 (2020): 331–36.

Monia, F. A., I. Hanafi, S. Marsidin, and Darmansyah. "Junior High School Teachers' Problems in Digitally Infected Clime: The ICT Utilization Sensibility." *Journal of Physics: Conference Series* 1387, no. 1 (2019). https://doi.org/10.1088/1742-6596/1387/1/012056.

Rosyid, Abdul. "Technological Pedagogical Content Knowledge: Sebuah Kerangka Pengetahuan Bagi Guru Indonesia Di Era MEA." In *Prosiding Seminar Nasional Inovasi Pendidikan*, 2016.

Safar, M, and N Al-Ahmad. "Barriers to Implementing Cybersecurity in Educational Institutions." *International Journal of Educational Technology* 9, no. 1 (2021): 15–25.

Shiau, W L, and colleagues. "Educational Data Protection in the Digital Age." *Computers and Education* 17, no. 4 (2021): 240–59.

Suherman, Asep, Tedi Susanto, Djohar Syamsi, H K I Sunjaya, and M Nasir. "Pencegahan Serangan Siber Pada Sistem Informasi Manajemen Sekolah Di SMK Wahidin Kota Cirebon." *Jurnal ICT: Informasi Komunikasi \& Teknologi*, 2021.

Sulaeman, H, H P Utomo, and ... "PENILAIAN RISIKO KEAMANAN INFORMASI PADA SISTEM INFORMASI AKADEMIK (SIAKAD) DENGAN MENGGUNAKAN FRAMEWORK NIST-SP 800 30." *Naratif: Jurnal Nasional …*, 2023. https://naratif.sttbandung.ac.id/index.php/naratif/article/view/254.

Tarbiyah, Shautut. "Design and Implementation of Management Information System for Senior High School Student Dormitory for Lokon Santo Nikolaus Tomohon." *Ejournal.Iainkendari* 26, no. November (2020): 250–71.