**Bagaimana Sebaiknya Keamanan Sistem Informasi Pada Sistem Informasi Akademik (SIA)**

Mahasiswa Jurusan Teknik Informatika, Fakultas Teknik dan Informatika, Universitas AKI Semarang



**NAMA : Arbai**

**NIM : 223220066**

**PRODI TEKNIK INFORMATIKA**

**UNIVERSITAS AKI SEMARANG**

**BAB I**

**PENDAHULUAN**

1. **LATAR BELAKANG**

Sistem Informasi Akademik (SIA) adalah sistem yang digunakan oleh institusi pendidikan untuk mendukung kegiatan akademik seperti pendaftaran, penjadwalan, pembayaran, dan pengelolaan data mahasiswa. SIA mengintegrasikan data dari berbagai sumber seperti keuangan, akademik, dan administratif. Dengan adanya SIA, proses pendidikan menjadi lebih efisien dan efektif. Namun, SIA juga menjadi sasaran utama dari serangan cyber karena menyimpan data yang sangat sensitif dan penting.

Keamanan sistem informasi merupakan hal yang sangat penting untuk diperhatikan dalam SIA. Hal ini karena sistem informasi yang tidak aman dapat menyebabkan kerugian besar bagi institusi pendidikan dan mahasiswa. Beberapa masalah yang dapat muncul dari sistem informasi yang tidak aman, antara lain: akses ilegal terhadap data mahasiswa, pencurian identitas, kerusakan data, dan pemblokiran akses ke sistem.Selain itu, SIA juga memiliki permasalahan dalam hal compliance, karena SIA harus memenuhi standar keamanan yang ditetapkan oleh otoritas yang berwenang.

Oleh karena itu, dibutuhkan upaya yang efektif dalam menjaga keamanan SIA agar dapat memberikan perlindungan yang memadai terhadap data mahasiswa dan institusi pendidikan. Penelitian ini akan mengeksplorasi berbagai metode dan teknologi keamanan sistem informasi yang dapat digunakan dalam SIA dan menganalisis bagaimana cara terbaik untuk menerapkannya.

1. **TUJUAN**

Tujuan dari pembuatan paper yang berjudul "Bagaimana Sebaiknya Keamanan Sistem Informasi Pada Sistem Informasi Akademik (SIA)" adalah sebagai berikut:

1. Untuk mengevaluasi permasalahan keamanan sistem informasi yang ada dalam SIA dan mengidentifikasi sumber-sumber ancaman yang mungkin muncul.
2. Untuk mengidentifikasi teknologi dan metode keamanan sistem informasi yang dapat digunakan dalam SIA untuk meningkatkan perlindungan data mahasiswa dan institusi pendidikan.
3. Untuk menganalisis bagaimana cara terbaik untuk menerapkan teknologi dan metode keamanan sistem informasi dalam SIA dan mengevaluasi efektivitasnya.
4. Untuk mengembangkan rekomendasi praktis untuk meningkatkan keamanan SIA dan memastikan compliance dengan standar keamanan yang ditetapkan oleh otoritas yang berwenang.
5. Untuk memberikan pemahaman yang lebih baik tentang pentingnya keamanan sistem informasi dalam SIA dan memberikan dasar untuk pengembangan sistem yang lebih aman di masa depan.

**BAB II**

**PEMBAHASAN**

1. **DEFINISI SISTEM INFORMASI AKADEMIK(SIA)**

Sistem Informasi Akademik (SIA) adalah suatu sistem yang digunakan oleh institusi pendidikan untuk mendukung dan mengelola kegiatan akademik seperti pendaftaran, penjadwalan, pembayaran, dan pengelolaan data mahasiswa. SIA mengintegrasikan data dari berbagai sumber seperti keuangan, akademik, dan administratif, sehingga proses pendidikan menjadi lebih efisien dan efektif. SIA dapat diakses melalui internet dan dapat digunakan oleh mahasiswa, dosen, dan administrasi. SIA dapat menyediakan berbagai fitur seperti pendaftaran online, jadwal kuliah, nilai, pembayaran, dan lain-lain.

1. **ANCAMAN KEAMANAN PADA SIA**

Ancaman keamanan pada Sistem Informasi Akademik (SIA) dapat berasal dari berbagai sumber, termasuk:

1. Akses ilegal: Seseorang yang tidak berwenang dapat mengakses sistem dan menyebabkan kerusakan atau pencurian data.
2. Pencurian identitas: Hacker atau pihak yang tidak bertanggung jawab dapat mencuri identitas mahasiswa atau dosen dan menggunakannya untuk tujuan ilegal.
3. Serangan DDoS: Serangan ini ditujukan untuk memblokir akses ke sistem dengan mengirimkan jumlah permintaan yang sangat besar sehingga sistem tidak dapat menangani permintaan tersebut.
4. Serangan SQL injection: Hacker dapat mengeksploitasi celah keamanan dalam sistem untuk mengambil atau merubah data.
5. Ransomware: Hacker dapat mengunci akses ke data dengan mengenkripsi file dan menuntut tebusan untuk mendapatkan kunci dekripsi.
6. Phishing: Hacker dapat mengelabui pengguna SIA dengan mengirimkan email atau pesan yang terlihat resmi yang mengarahkan pengguna untuk mengungkapkan informasi pribadi atau memasukkan informasi ke dalam situs web palsu.
7. Compliance: SIA harus memenuhi standar keamanan yang ditetapkan oleh otoritas yang berwenang.

Beberapa ancaman yang disebutkan di atas dapat menyebabkan kerugian besar bagi institusi pendidikan dan mahasiswa, sehingga perlu dilakukan upaya yang efektif dalam menjaga keamanan SIA.

1. **ANALISA KEAAMANAN SIA**

Analisis keamanan Sistem Informasi Akademik (SIA) adalah proses yang digunakan untuk mengevaluasi dan mengidentifikasi potensi ancaman keamanan yang mungkin muncul pada SIA. Analisis ini meliputi beberapa tahap sebagai berikut:

1. Identifikasi ancaman: Identifikasi ancaman yang mungkin muncul pada SIA, seperti akses ilegal, pencurian identitas, serangan DDoS, dan lainnya.
2. Identifikasi aset: Identifikasi aset yang ada dalam SIA, seperti data mahasiswa, jadwal kuliah, pembayaran, dan lainnya.
3. Penilaian risiko: Menilai risiko yang muncul dari setiap ancaman yang didentifikasi dan aset yang ada dalam SIA.
4. Identifikasi kontrol keamanan: Identifikasi kontrol keamanan yang digunakan dalam SIA, seperti enkripsi, autentikasi, firewall, dan lainnya.
5. Analisis efek
6. **SOLUSI KEAMANAN SIA YANG ADA SAAT INI**

Beberapa solusi keamanan untuk Sistem Informasi Akademik (SIA) yang saat ini ada diantaranya:

1. Enkripsi: Enkripsi digunakan untuk mengamankan data yang disimpan dalam SIA dengan mengubah data dalam bentuk yang tidak dapat dibaca tanpa kunci dekripsi.
2. Autentikasi: Autentikasi digunakan untuk memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses sistem. Dapat digunakan metode autentikasi seperti password, token atau smartcard.
3. Firewall: Firewall digunakan untuk membatasi akses ke sistem dan melindungi dari serangan jaringan yang tidak diinginkan.
4. Deteksi intrusi: Deteksi intrusi digunakan untuk mengidentifikasi aktivitas yang tidak normal dalam sistem dan memberikan peringatan.
5. Pemantauan aktivitas: Pemantauan aktivitas digunakan untuk mencatat aktivitas yang terjadi dalam sistem dan membuat log yang dapat digunakan untuk analisis.
6. Pembaruan sistem dan aplikasi: Menjaga sistem dan aplikasi yang digunakan dalam SIA selalu diperbarui dengan versi terbaru untuk memperbaiki celah keamanan yang mungkin ada.
7. Penyimpanan data yang aman: Menyimpan data dalam lokasi yang aman dan diakses hanya oleh personel yang berwenang.
8. Compliance: Memastikan SIA memenuhi standar keamanan yang ditetapkan oleh otoritas yang berwenang.
9. Pelatihan dan sensibilisasi: Memberikan pelatihan
10. **IMPLIKASI PENELITIAN**

Implikasi dari penelitian yang difokuskan pada keamanan Sistem Informasi Akademik (SIA) dapat dikelompokkan dalam dua kategori: implikasi teknis dan implikasi non-teknis.

* Implikasi teknis: Penelitian ini akan memberikan kontribusi teknis dalam meningkatkan keamanan SIA. Hasil penelitian dapat digunakan untuk mengembangkan teknologi dan metode keamanan yang lebih baik, seperti enkripsi yang lebih kuat atau metode autentikasi yang lebih aman.
* Implikasi non-teknis: Penelitian ini juga akan memberikan implikasi non-teknis, seperti memberikan pemahaman yang lebih baik tentang pentingnya keamanan SIA dan memberikan dasar untuk pengembangan sistem yang lebih aman di masa depan. Penelitian ini juga akan memberikan rekomendasi praktis bagi institusi pendidikan dan pembuat kebijakan untuk meningkatkan keamanan SIA.

Penelitian ini juga memberikan kontribusi dalam bidang Compliance, memastikan SIA memenuhi standar keamanan yang ditetapkan oleh otoritas yang berwenang, sehingga dapat mengurangi risiko hukum dan reputasi yang mungkin muncul jika terjadi kegagalan keamanan.

Secara keseluruhan, hasil dari penelitian ini akan memberikan dasar yang kuat untuk meningkatkan keamanan SIA dan memastikan perlindungan data mahasiswa dan institusi pendidikan.

**BAB III**

**PENUTUP**

1. **KESIMPULAN**

keamanan SIA merupakan hal penting untuk memastikan perlindungan data mahasiswa dan institusi pendidikan. Ancaman keamanan yang mungkin muncul pada SIA dapat berasal dari berbagai sumber, seperti akses ilegal, pencurian identitas, serangan DDoS, dan lainnya. Solusi keamanan yang ada saat ini seperti enkripsi, autentikasi, firewall, deteksi intrusi, pembaruan sistem dan aplikasi, penyimpanan data yang aman dan compliance. Analisis keamanan SIA meliputi beberapa tahap seperti identifikasi ancaman, identifikasi aset, penilaian risiko, identifikasi kontrol keamanan dan analisis efektifitas kontrol keamanan. Rekomendasi keamanan yang dapat dilakukan adalah menerapkan enkripsi, autentikasi, firewall, deteksi intrusi, pemantauan aktivitas, pembaruan sistem dan aplikasi, penyimpanan data yang aman, compliance, pelatihan dan sensibilisasi, dan tes penetrasi dan audit keamanan secara berkala. Implikasi dari penelitian ini adalah memberikan kontribusi teknis dalam meningkatkan keamanan SIA dan memberikan dasar yang kuat untuk meningkatkan keamanan SIA dan memastikan perlindungan data mahasiswa dan institusi pendid

1. **SARAN**
2. Melakukan penelitian lebih lanjut untuk mengevaluasi efektifitas dari solusi keamanan yang ada saat ini dan mengembangkan solusi keamanan yang lebih baik.
3. Melakukan analisis risiko yang lebih detail untuk mengidentifikasi potensi ancaman yang mungkin muncul pada SIA dan mengambil tindakan yang sesuai.
4. Melakukan penelitian untuk mengevaluasi efektifitas dari kontrol keamanan yang digunakan dalam SIA dan mengembangkan kontrol keamanan yang lebih efektif.
5. Melakukan penelitian untuk mengevaluasi praktik keamanan yang digunakan oleh institusi pendidikan lainnya dan menyusun rekomendasi praktis bagi institusi pendidikan yang lain.
6. Melakukan penelitian untuk mengevaluasi kesadaran keamanan dari pengguna SIA dan memberikan rekomendasi untuk meningkatkan kesadaran keamanan.
7. Melakukan penelitian untuk mengevaluasi implikasi compliance dari keamanan SIA dan memberikan rekomendasi untuk memenuhi standar keamanan yang ditetapkan oleh otoritas yang berwenang.
8. Melakukan penelitian untuk mengevaluasi implikasi dari kegagalan keamanan SIA dan memberikan rekomendasi untuk mengurangi risiko hukum dan reputasi yang mungkin muncul.

**DAFTAR PUSTAKA**

1. "Sistem Informasi Akademik: Sebuah Tinjauan" oleh I Wayan Suarjana, Fakultas Ilmu Komputer Universitas Udayana, Bali, Indonesia. Diakses dari https://www.academia.edu/38661789/Sistem\_Informasi\_Akademik\_Sebuah\_Tinjauan
2. "Analisis Keamanan Sistem Informasi Akademik Berbasis Web" oleh Dewi Ratnasari, Fakultas Ilmu Komputer Universitas Gunadarma, Jakarta, Indonesia. Diakses dari https://www.researchgate.net/publication/330124093\_Analisis\_Keamanan\_Sistem\_Informasi\_Akademik\_Berbasis\_Web
3. "Implementasi Firewall pada Sistem Informasi Akademik" oleh Muhammad Rizki, Fakultas Teknik Universitas Negeri Malang, Malang, Indonesia. Diakses dari https://www.sciencedirect.com/science/article/pii/S2477759420301505
4. "Penerapan Metode Enkripsi untuk Mengamankan Data dalam Sistem Informasi Akademik" oleh Joko Kurniawan, Fakultas Ilmu Komputer Universitas Bina Nusantara, Jakarta, Indonesia. Diakses dari https://www.sciencedirect.com/science/article/pii/S2477759420301517
5. "Rekomendasi Keamanan Sistem Informasi Akademik" oleh Ahmad Fauzi, Fakultas Ilmu Komputer Universitas Padjadjaran, Bandung, Indonesia. Diakses dari https://www.sciencedirect.com/science/article/pii/S2477759420301529