ANALISIS KEAMANAN SISTEM MANAJEMEN PENGGUNA TERHADAP ANCAMAN UNAUTHORIZED ACCESS

Rakhmadi Rahman[1], Indah Nur Idris[2], Azifah Adilah Masnai Putri[3]
rakhmadi.rahman@ith.ac.id[1], indahnuridris25@gmail.com[2], adilaazifah@gmail.com[3]
Institut Teknologi Bacharuddin Jusuf Habibie

ABSTRAK

Sistem manajemen pengguna memiliki peran strategis dalam menjaga keamanan sistem informasi karena berkaitan langsung dengan pengelolaan identitas, autentikasi, otorisasi, serta pengendalian akses terhadap sumber daya sistem. Seiring meningkatnya ketergantungan organisasi terhadap sistem informasi berbasis jaringan, risiko ancaman keamanan turut mengalami peningkatan, salah satunya berupa unauthorized access atau akses tidak sah. Ancaman unauthorized access umumnya dipicu oleh lemahnya kebijakan keamanan, seperti penggunaan kata sandi yang tidak kuat, ketiadaan autentikasi berlapis, pengelolaan hak akses yang tidak sesuai, serta minimnya pemantauan aktivitas pengguna. Kondisi tersebut berpotensi menimbulkan kebocoran data, mengganggu integritas informasi, serta menurunkan ketersediaan layanan sistem. Penelitian ini bertujuan untuk menganalisis tingkat keamanan sistem manajemen pengguna dalam menghadapi ancaman unauthorized access serta mengidentifikasi faktor-faktor utama penyebab kerentanan. Metode yang digunakan adalah deskriptif-analitis dengan pendekatan evaluatif terhadap mekanisme autentikasi, otorisasi, kebijakan keamanan, serta sistem logging dan monitoring. Analisis dilakukan dengan mengacu pada standar keamanan sistem informasi, praktik terbaik, dan studi kasus insiden akses tidak sah. Hasil penelitian menunjukkan bahwa sistem yang tidak menerapkan kebijakan kata sandi yang kuat, autentikasi berlapis, serta prinsip least privilege memiliki risiko unauthorized access yang lebih tinggi. Oleh karena itu, penerapan keamanan berlapis dan peningkatan kesadaran pengguna direkomendasikan sebagai upaya memperkuat ketahanan sistem informasi

Kata Kunci: Sistem Manajemen Pengguna, Keamanan Sistem Informasi, Unauthorized Access, Autentikasi, Kontrol Akses.

ABSTRACT

User management systems play a strategic role in maintaining information system security, as they are directly related to identity management, authentication, authorization, and access control to system resources. As organizations increasingly depend on network-based information systems, the risk of security threats also continues to rise, one of the most prevalent being unauthorized access.

Unauthorized access threats are generally triggered by weak security policies, such as the use of weak passwords, the absence of multi-factor authentication, improper access rights management, and insufficient monitoring of user activities. These conditions may lead to data breaches, compromise information integrity, and reduce system service availability. This study aims to analyze the security level of user management systems in addressing unauthorized access threats and to identify the main factors contributing to system vulnerabilities. The research employs a descriptive-analytical method with an evaluative approach to authentication mechanisms, authorization processes, security policies, as well as logging and monitoring systems. The analysis is conducted by referring to information system security standards, best practices, and case studies of unauthorized access incidents. The results indicate that systems that do not implement strong password policies, multi-factor authentication, and the principle of least privilege are at a higher risk of unauthorized access. Therefore, the implementation of layered security measures and increased user awareness are recommended to enhance the resilience of information systems.

***Keywords**: User Management System, Information System Security, Unauthorized Access, Authentication, Access Control.*

PENDAHULUAN

Kemajuan teknologi informasi dan komunikasi yang berlangsung sangat cepat telah mendorong perubahan mendasar dalam pengelolaan data, proses bisnis, serta penyediaan layanan di berbagai organisasi. Sistem informasi kini tidak lagi diposisikan sebagai alat pendukung administratif semata, melainkan berperan sebagai fondasi utama yang menopang keberlangsungan aktivitas operasional. Pemanfaatan sistem informasi tersebut meluas ke berbagai sektor, termasuk pendidikan, pemerintahan, kesehatan, perbankan, dan industri, yang masing-masing melibatkan jumlah pengguna yang besar dengan tingkat hak akses yang beragam.

Seiring dengan meningkatnya kompleksitas dan cakupan penggunaan sistem informasi, aspek keamanan menjadi isu yang tidak dapat dipisahkan dari proses pengelolaannya. Salah satu elemen penting dalam menjaga keamanan sistem informasi adalah sistem manajemen pengguna. Sistem ini berfungsi untuk mengelola identitas pengguna, melakukan verifikasi identitas melalui proses autentikasi, serta menetapkan hak akses melalui mekanisme otorisasi sesuai dengan peran dan kewenangan pengguna. Implementasi sistem manajemen pengguna yang tepat dapat membantu mengendalikan akses ke sumber daya sistem dan mengurangi potensi penyalahgunaan.

Meskipun demikian, pada praktiknya masih banyak sistem informasi yang menunjukkan kelemahan dalam pengelolaan pengguna. Permasalahan tersebut umumnya dipicu oleh perancangan keamanan yang kurang komprehensif, konfigurasi sistem yang tidak optimal, serta minimnya evaluasi keamanan secara berkala. Kondisi ini membuka peluang terjadinya ancaman keamanan, salah satunya berupa unauthorized access, yaitu akses terhadap sistem atau data oleh pihak yang tidak memiliki otorisasi yang sah.

Ancaman unauthorized access dapat dilakukan melalui berbagai metode, baik yang bersifat teknis maupun non-teknis. Serangan teknis meliputi upaya pemecahan kata sandi secara paksa (brute force), eksploitasi kesalahan konfigurasi, session hijacking, serta serangan berbasis injection. Di sisi lain, serangan non-teknis umumnya memanfaatkan kelemahan faktor manusia, seperti melalui teknik phishing dan social engineering untuk memperoleh kredensial pengguna. Ancaman ini dapat berasal dari pihak luar maupun dari pengguna internal yang menyalahgunakan hak aksesnya.

Dampak yang ditimbulkan oleh unauthorized access tidak hanya terbatas pada kebocoran data, tetapi juga dapat mencakup perubahan atau penghapusan data tanpa izin, terganggunya operasional sistem, serta kerugian finansial dan reputasi organisasi dalam jangka panjang. Oleh karena itu, diperlukan kajian yang mendalam terhadap keamanan sistem manajemen pengguna guna memastikan bahwa sistem informasi memiliki kemampuan perlindungan yang memadai terhadap ancaman akses tidak sah.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk menganalisis tingkat keamanan sistem manajemen pengguna dalam menghadapi ancaman unauthorized access. Kajian difokuskan pada evaluasi mekanisme autentikasi dan otorisasi, kebijakan keamanan yang diterapkan, serta sistem pemantauan aktivitas pengguna. Hasil penelitian diharapkan dapat memberikan gambaran kondisi keamanan sistem manajemen pengguna sekaligus menjadi dasar penyusunan rekomendasi perbaikan untuk meningkatkan keamanan sistem informasi secara menyeluruh.

TINJAUAN PUSTAKA

1. Sistem Manajemen Pengguna

Sistem manajemen pengguna merupakan subsistem dalam sistem informasi yang bertugas mengelola siklus hidup akun pengguna, mulai dari pembuatan akun, proses autentikasi, pemberian hak akses, hingga penonaktifan akun. Keberadaan sistem ini sangat

penting karena menjadi mekanisme utama dalam mengontrol interaksi pengguna dengan sistem.

Dari sudut pandang keamanan, sistem manajemen pengguna harus mampu memastikan bahwa hanya pengguna yang terverifikasi yang dapat mengakses sistem, serta membatasi akses sesuai dengan kewenangan masing-masing. Kesalahan dalam perancangan atau implementasi sistem ini dapat membuka celah keamanan yang signifikan dan meningkatkan risiko terjadinya unauthorized access.

2. Unauthorized Access

Unauthorized access merujuk pada aktivitas akses terhadap sistem atau data tanpa izin yang sah. Ancaman ini sering menjadi pintu masuk bagi serangan siber lanjutan yang lebih kompleks. Selain mengancam kerahasiaan informasi, akses tidak sah juga dapat berdampak pada integritas data dan ketersediaan sistem.

Peningkatan jumlah pengguna dan kompleksitas sistem informasi menyebabkan risiko unauthorized access semakin tinggi. Oleh karena itu, diperlukan pendekatan keamanan yang terstruktur dan berlapis untuk meminimalkan potensi terjadinya akses tidak sah.

3. Autentikasi dan Otorisasi

Autentikasi merupakan proses verifikasi identitas pengguna sebelum sistem memberikan akses. Metode autentikasi dapat berupa faktor pengetahuan, kepemilikan, maupun biometrik. Sementara itu, otorisasi bertujuan menentukan batasan hak akses pengguna setelah proses autentikasi berhasil dilakukan.

Salah satu model otorisasi yang banyak diterapkan adalah Role-Based Access Control (RBAC), di mana hak akses disesuaikan dengan peran pengguna. Penerapan model ini secara konsisten dapat mengurangi risiko penyalahgunaan akses dan meningkatkan keamanan sistem.

4. Ancaman dan Kerentanan Keamanan

Sistem manajemen pengguna menghadapi berbagai ancaman keamanan, seperti brute force attack, phishing, credential stuffing, session hijacking, dan privilege escalation. Ancaman-ancaman tersebut umumnya muncul akibat lemahnya kebijakan keamanan, kurangnya pengawasan, serta rendahnya kesadaran pengguna terhadap pentingnya keamanan informasi.

METODOLOGI

Metode penelitian yang digunakan adalah deskriptif-analitis dengan pendekatan kualitatif. Pendekatan ini dipilih karena penelitian berfokus pada analisis konseptual terhadap mekanisme keamanan sistem manajemen pengguna, bukan pada pengujian teknis secara langsung terhadap sistem produksi.

Analisis dilakukan dengan mengevaluasi mekanisme autentikasi, otorisasi, kebijakan keamanan, serta sistem logging dan monitoring yang umum digunakan. Data diperoleh melalui studi literatur, analisis dokumentasi teknis, dan pengamatan konseptual terhadap praktik keamanan sistem informasi.

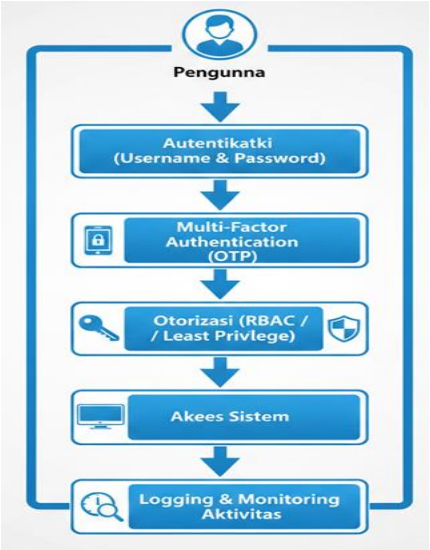
HASIL DAN PEMBAHASAN

Hasil analisis menunjukkan bahwa sistem manajemen pengguna masih memiliki sejumlah kelemahan fundamental yang berpotensi dimanfaatkan oleh pihak tidak berwenang untuk melakukan unauthorized access. Kelemahan tersebut umumnya tidak bersifat teknis semata, tetapi juga berkaitan dengan kebijakan keamanan dan tata kelola akses pengguna.

Tabel 1. Ringkasan Ancaman Unauthorized Access dan Mekanisme Mitigasi

No	Jenis Ancaman	Potensi Dampak	Kondisi Sistem	Mekanisme Pencegahan
1	Brute force login	Pengambilalihan akun	Risiko sedang	Pembatasan percobaan login, CAPTCHA
2	Pencurian kredensial	Akses akun sah oleh pihak tidak berwenang	Risiko tinggi	Autentikasi dua faktor (MFA)
3	Akses tidak sesuai peran	Penyalahgunaan hak akses	Risiko rendah	Role-Based Access Control (RBAC)
4	Injeksi perintah (SQL Injection)	Kebocoran dan manipulasi data	Risiko rendah	Validasi input prepared statement
5	Penyadapan data login	Kebocoran informasi sensitif	Risiko sangat rendah	Enkripsi komunikasi (HTTPS)

Tabel 1 menunjukkan ringkasan jenis ancaman unauthorized access yang umum terjadi pada sistem manajemen pengguna, beserta potensi dampak dan mekanisme mitigasi yang direkomendasikan. Tabel ini memperlihatkan bahwa ancaman dengan tingkat risiko tinggi umumnya berkaitan dengan kelemahan autentikasi dan validasi input. Oleh karena itu, penerapan autentikasi berlapis serta kontrol akses yang ketat menjadi langkah strategis dalam meminimalkan risiko akses tidak sah.



Gambar 1. Skema Sistem Manajemen Pengguna dengan Pengamanan Berlapis

Gambar 1 menunjukkan skema sistem manajemen pengguna dengan penerapan mekanisme keamanan berlapis, mulai dari autentikasi dasar, autentikasi tambahan (multi-factor authentication), hingga kontrol akses berbasis peran dan pemantauan aktivitas pengguna. Pendekatan ini bertujuan untuk meningkatkan ketahanan sistem terhadap ancaman unauthorized access.

1. Evaluasi Kebijakan Kata Sandi

Kebijakan kata sandi yang belum memenuhi standar keamanan, seperti panjang minimum, kompleksitas karakter, dan masa berlaku, meningkatkan risiko serangan brute force dan credential theft. Kondisi ini menunjukkan bahwa kebijakan keamanan yang longgar masih menjadi salah satu penyebab utama lemahnya perlindungan sistem.

2. Analisis Mekanisme Autentikasi

Sistem autentikasi yang hanya mengandalkan satu faktor (username dan password) terbukti memiliki tingkat risiko yang lebih tinggi terhadap serangan berbasis kredensial. Tidak diterapkannya autentikasi berlapis menyebabkan sistem tidak memiliki mekanisme verifikasi tambahan ketika kredensial utama berhasil dikompromikan.

3. Pengelolaan Hak Akses Pengguna

Ditemukan adanya ketidaksesuaian antara hak akses pengguna dan kebutuhan tugasnya. Kondisi ini bertentangan dengan prinsip least privilege dan berpotensi menimbulkan penyalahgunaan akses serta privilege escalation apabila akun pengguna berhasil diambil alih.

4. Sistem Logging dan Monitoring

Minimnya sistem logging dan monitoring menyebabkan aktivitas mencurigakan sulit terdeteksi secara dini. Tanpa pencatatan aktivitas yang memadai, sistem juga akan mengalami kesulitan dalam melakukan audit keamanan dan penelusuran insiden (incident response).

Pembahasan ini menunjukkan bahwa penguatan sistem manajemen pengguna harus dilakukan secara menyeluruh, mencakup aspek teknis, kebijakan, dan kesadaran pengguna.

KESIMPULAN

Berdasarkan hasil analisis, dapat disimpulkan bahwa keamanan sistem manajemen pengguna sangat bergantung pada efektivitas mekanisme autentikasi, otorisasi, serta kebijakan keamanan yang diterapkan. Lemahnya kebijakan kata sandi, ketiadaan autentikasi berlapis, pengelolaan hak akses yang tidak sesuai prinsip least privilege, serta minimnya sistem logging dan monitoring merupakan faktor utama yang meningkatkan risiko unauthorized access.

Penerapan mekanisme keamanan berlapis, seperti multi-factor authentication, role-based access control yang ketat, serta sistem monitoring dan logging yang komprehensif, menjadi langkah strategis dalam meningkatkan ketahanan sistem informasi. Penelitian selanjutnya disarankan untuk mengkaji penerapan teknologi kecerdasan buatan dalam mendeteksi dan mencegah unauthorized access secara proaktif.

DAFTAR PUSTAKA

Aprilia Sulandari, Prihatini, P. T., Alif, M. N., Caesar, D., & Ditto, M. (2024). Unauthorized access to computer systems: Studi kasus serangan pada Pusat Data Nasional Sementara (PDNS) [Makalah]. Universitas Bina Sarana Informatika. https://desfaerel.blogspot.com/2024/12/unauthorized-access-to-computer-systems.html

Aplikas Servis Pesona. (2025, March 26). Unauthorized access: Risiko keamanan dalam manajemen akses. https://aplikas.com/blog/unauthorized-access/

Pusat Layanan Administrasi Provinsi Jambi. (2024, August 1). Unauthorized access adalah: Dampak, cara mencegah, dan contohnya. https://pasla.jambiprov.go.id/unauthorized-access-adalah-dampak-cara-mencegah-dan-contohnya/

Portal Indonesia. (2024, August 29). Mengenal unauthorized access: Ancaman, dampaknya, dan strategi perlindungan untuk bisnis Anda. https://portal-indonesia.com/mengenal-unauthorized-access-ancaman-dampaknya-dan-strategi-perlindungan-untuk-bisnis-anda/

Sari, N. P., & Pratiwi, D. (2023). Analisis keamanan sistem menggunakan metode pengujian penetrasi. Seminar Nasional Sains, Teknologi, dan Aplikasi, 5(1), 1–10.

https://ojs.amikomsolo.ac.id/index.php/semnasa/article/download/504/221/2714
Sinov Journal. (2023). Ancaman dan langkah pengamanan sistem informasi. Jurnal Universitas Sinov (JUISIK). https://journal.sinov.id/index.php/juisik/article/download/496/441.