JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 3, Oktober 2023
ISSN 3025-0919 (media online)
Hal 999-999

Penerapan CIS Control V8 dalam Manajemen Hak Akses

Pawit Wahib[1], Mia Audina[1], Arya Tunggal Narotama[1], Nur Muhamad Rijki[1], M. Firdaus Fitrananda[1], Agung Wijoyo[1*]

[1]Fakultas Ilmu Komputer, Program Studi Teknik Informatika, Universitas Pamulang, Tangerang Selatan, Banten, Indonesia

Email: [1]pawitwahib.wrk@gmail.com, [2]maudina847@gmail.com, [3]aryanrtm1337@gmail.com, [4]nurmrijki17@gmail.com, [4]daxuslite@gmail.com, [5*] dosen01671@unpam.ac.id

Abstrak – Dalam era digital yang terus berkembang pesat, peran komputer dan sistem informasi telah menjadi tak tergantikan dalam kehidupan sehari-hari, baik di organisasi besar maupun kecil. Namun, tingkat ketergantungan yang tinggi pada teknologi informasi juga membawa sejumlah tantangan serius terkait dengan keamanan komputer. Salah satu aspek utama dalam menjaga keamanan komputer yang krusial adalah manajemen hak akses. Sayangnya, masih banyak organisasi, terutama yang lebih kecil, yang kurang menyadari betapa pentingnya menerapkan langkah-langkah keamanan dalam operasi mereka. Hal ini dapat memiliki konsekuensi serius, termasuk potensi kerentanan terhadap serangan siber, kebocoran informasi sensitif, dan ancaman terhadap integritas data. Kesadaran akan urgensi perlindungan informasi dan sistem harus menjadi tanggung jawab bersama di seluruh organisasi, bukan hanya tugas departemen IT. Manajemen hak akses adalah pendekatan penting dalam menjaga keamanan komputer. Ini adalah sistem yang memungkinkan organisasi untuk mengatur, mengendalikan, dan memantau akses individu terhadap data dan sistem informasi. Proses ini melibatkan penentuan tingkat akses yang sesuai, pemberian izin berdasarkan peran dan tanggung jawab, serta pemastian bahwa akses tersebut selaras dengan peraturan dan kebijakan organisasi. Manajemen hak akses yang efektif dapat mencegah akses yang tidak sah dan penyalahgunaan sistem, menjaga keberlangsungan operasional, serta melindungi informasi organisasi. Salah satu solusi yang terbukti efektif untuk mengatasi tantangan ini adalah penerapan CIS Control V8. Kerangka kerja ini telah terbukti berhasil membantu organisasi mengidentifikasi, melindungi, dan mengelola risiko keamanan informasi dengan baik.

Kata Kunci: Keamanan Komputer; Manajemen Hak Akses

Abstract – In the rapidly evolving digital era, the role of computers and information systems has become indispensable in our daily lives, both in large and small organizations. However, the high level of dependence on information technology also brings several serious challenges related to computer security. One crucial aspect of maintaining computer security is access management. Unfortunately, many organizations, especially smaller ones, are often unaware of the importance of implementing security measures in their operations. This can have serious consequences, including potential vulnerabilities to cyberattacks, leakage of sensitive information, and threats to data integrity. Awareness of the urgency of information and system protection should be a collective responsibility throughout the organization, not just the task of the IT department. Access management is a vital approach to computer security. It is a system that allows organizations to control, regulate, and monitor individual access to data and information systems. This process involves determining appropriate access levels, granting permissions based on roles and responsibilities, and ensuring that access is in line with organizational regulations and policies. Effective access management can prevent unauthorized access and system misuse, maintain operational continuity, and safeguard organizational information. One proven solution to address these challenges is the implementation of CIS Control V8. This framework has been successful in helping organizations identify, protect, and manage information security risks effectively.An abstract is a brief summary of a paper to help readers quickly ascertain the purpose of the study and according to research needs. Abstracts must be clear and informative, provide a statement for the problem under study and the solution. The abstract length is between 90 and 230 words. Avoid unusual abbreviations and define all symbols used in abstracts. Using keywords related to research topics is recommended.

Keywords: Computer Security; Access Management

1. PENDAHULUAN

Era digital yang terus berkembang membawa perubahan mendasar dalam cara kita berinteraksi dengan teknologi. Komputer dan sistem informasi telah menjadi tulang punggung masyarakat modern, baik dalam skala individu maupun organisasi. Dalam lingkup bisnis, teknologi informasi tidak hanya menjadi alat pendukung, tetapi juga tulang punggung operasi sehari-hari. Namun, di

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 3, Oktober 2023
ISSN 3025-0919 (media online)
Hal 999-999

balik kenyamanan dan efisiensi yang diberikan oleh teknologi ini, kita juga dihadapkan pada tantangan serius terkait dengan keamanan komputer.

Manajemen hak akses adalah salah satu aspek penting dalam menjaga keamanan komputer dan data. Ini adalah konsep yang mendasar yang berkaitan dengan pengaturan, pengawasan, dan kontrol terhadap akses individu atau entitas ke dalam sistem dan data yang sensitif. Manajemen hak akses melibatkan pemberian hak akses yang sesuai kepada pengguna, memastikan bahwa hak akses tersebut konsisten dengan peraturan dan kebijakan, serta pemantauan terhadap aktivitas pengguna untuk mencegah akses yang tidak sah.

Namun, kesadaran akan pentingnya manajemen hak akses sering kali masih kurang di banyak organisasi. Terutama di kalangan organisasi yang lebih kecil, keamanan seringkali tidak menjadi prioritas utama. Ini membuka peluang bagi potensi kerentanan dan risiko keamanan yang dapat mengganggu integritas data dan sistem.

Ketidakpahaman tentang pentingnya manajemen hak akses di seluruh organisasi adalah tantangan yang perlu diatasi. Manajemen hak akses bukanlah tanggung jawab semata-mata departemen IT, melainkan merupakan tanggung jawab bersama yang harus dipahami oleh setiap anggota organisasi. Tanpa pemahaman ini, organisasi dapat menjadi target empuk bagi pelaku jahat yang mencari celah untuk mengakses informasi sensitif dan merusak operasional.

Dalam konteks inilah CIS *Control* V8 muncul sebagai solusi yang efektif. Kerangka kerja ini, yang dikembangkan oleh *Center for Internet Security* (CIS). CIS *Control* V8 menawarkan pendekatan yang terstruktur dan efektif untuk manajemen hak akses, membantu organisasi meminimalkan risiko pelanggaran keamanan, kebocoran data, dan penyalahgunaan hak akses.

2. METODE

Penelitian ini akan menggunakan pendekatan kualitatif. Pendekatan ini dipilih karena fokus penelitian adalah pada pemahaman yang mendalam tentang penerapan CIS *Control* V8 dalam konteks manajemen hak akses. Data akan diperoleh melalui wawancara, analisis dokumen, dan observasi.

2.1 Pengumpulan Data

1. Wawancara
   Peneliti melakukan wawancara dengan pemangku kepentingan dalam organisasi yang telah menerapkan CIS *Control* V8. Wawancara akan berfokus pada evaluasi efektivitas implementasi dan hambatan yang mereka hadapi.
2. Analisis Dokumen
   Dokumen-dokumen terkait dengan implementasi CIS *Control* V8 akan dianalisis, termasuk kebijakan, prosedur, dan laporan keamanan.
3. Observasi
   Peneliti mengamati praktik-praktik yang berkaitan dengan manajemen hak akses di dalam organisasi tersebut.

3. ANALISA DAN PEMBAHASAN

3.1 Manajemen Hak Akses

Manajemen hak akses adalah sistem penting untuk mengatur, mengendalikan, dan memantau akses individu atau entitas terhadap data dan sistem informasi. Proses ini melibatkan pengaturan tingkat akses yang sesuai, pemberian izin berdasarkan peran dan tanggung jawab, serta pemastian kesesuaian dengan peraturan dan kebijakan. Manajemen hak akses yang efektif adalah kunci untuk mencegah akses tidak sah dan menjaga keberlangsungan operasional serta melindungi informasi organisasi. Dalam konteks ini, terdapat dua pendekatan yang signifikan yang dapat digunakan dalam manajemen hak akses, yaitu *Role-Based Access Control* (RBAC) dan *Attribute-Based Access Control* (ABAC).

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 3, Oktober 2023
ISSN 3025-0919 (media online)
Hal 999-999

3.2 CIS Control V8 sebagai Solusi

Penerapan CIS Control V8 diperkenalkan sebagai solusi yang efektif untuk mengatasi tantangan dalam manajemen hak akses. Framework ini dikembangkan oleh *Center for Internet Security* (CIS) dan memiliki fokus pada identifikasi, perlindungan, dan manajemen risiko keamanan informasi. CIS *Control* V8 memberikan panduan konkret tentang praktik-praktik keamanan yang dapat membantu organisasi menghadapi potensi pelanggaran keamanan, kebocoran data, dan penyalahgunaan hak akses. Ini adalah langkah penting dalam memperkuat keamanan komputer dan menjaga integritas data.

3.3 *Role-Based Access Control* (RBAC) dan *Attribute-Based Access Control* (ABAC)

Dalam konteks manajemen hak akses, ada dua pendekatan utama yang dapat digunakan untuk mengontrol akses pengguna yaitu *Role-Based Access Control* (RBAC) dan *Attribute-Based Access Control* (ABAC).

1. RBAC (*Role-Based Access Control*)

   RBAC adalah pendekatan yang memungkinkan organisasi untuk memberikan hak akses berdasarkan peran atau posisi pengguna dalam organisasi. Ini berarti setiap pengguna diberikan hak akses sesuai dengan peran atau tanggung jawab mereka, seperti admin, pengguna biasa, atau manajer. RBAC membantu mengurangi risiko akses yang tidak sah dengan memastikan bahwa pengguna hanya memiliki akses ke informasi dan sistem yang sesuai dengan peran mereka.

2. ABAC (*Attribute-Based Access Control*)

   ABAC adalah pendekatan yang lebih fleksibel, di mana hak akses diberikan berdasarkan atribut-atribut pengguna, konteks, dan kebijakan. Misalnya, akses dapat diberikan berdasarkan atribut seperti usia, lokasi, atau tingkat keamanan. ABAC memungkinkan tingkat presisi yang lebih tinggi dalam mengatur hak akses dan lebih cocok untuk lingkungan di mana kebijakan akses kompleks.

Keduanya memiliki keunggulan dan kelemahan masing-masing, dan pemilihan antara RBAC dan ABAC harus disesuaikan dengan kebutuhan dan kompleksitas organisasi.

3.4 Analisis Data

Data hasil penelitian akan dianalisis untuk mengevaluasi efektivitas implementasi CIS *Control* V8, mengidentifikasi hambatan yang mungkin dihadapi oleh organisasi, dan memahami dampaknya terhadap keamanan komputer. Selain itu, analisis juga akan mempertimbangkan bagaimana RBAC dan ABAC dapat digunakan sebagai bagian dari strategi manajemen hak akses yang lebih luas dalam melindungi data dan sistem organisasi.

4. KESIMPULAN

Dalam era digital yang terus berkembang, manajemen hak akses memainkan peran krusial dalam menjaga keamanan komputer dan informasi organisasi. Penelitian ini telah mengidentifikasi sejumlah aspek penting terkait dengan manajemen hak akses dan penerapan CIS *Control* V8 sebagai solusinya.

Penerapan CIS Control V8, yang dikembangkan oleh *Center for Internet Security* (CIS), menjadi solusi efektif dalam mengatasi tantangan manajemen hak akses. Framework ini membantu organisasi mengidentifikasi, melindungi, dan mengelola risiko keamanan informasi. Ini memberikan panduan konkret tentang praktik keamanan yang dapat membantu menghadapi potensi pelanggaran keamanan, kebocoran data, dan penyalahgunaan hak akses.

Selain itu, dalam konteks manajemen hak akses, terdapat dua pendekatan utama yang perlu diperhatikan, yaitu *Role-Based Access Control* (RBAC) dan *Attribute-Based Access* Control (ABAC). RBAC mengizinkan pengaturan hak akses berdasarkan peran pengguna, sementara ABAC memungkinkan pengaturan berdasarkan atribut-atribut dan konteks yang lebih fleksibel. Pemilihan antara RBAC dan ABAC harus disesuaikan dengan kebutuhan dan kompleksitas organisasi.

.

REFERENCES

Fadila, V., Mutiah, N., & Sari, R. P. Cyber Security Audit using CIS CSC, NIST CSF and COBIT 2019 Framework. *CESS (Journal of Computer Engineering, System and Science)*, *8*(2), 271-283.

Learning dalam Pengendalian Akses Jaringan. Jurnal Keamanan Jaringan Komputer, 6(4), 394-407.

Setiawan, Budi. (2022). Tantangan Manajemen Hak Akses di Era Cloud Computing. Jurnal Teknologi Informasi dan Keamanan Komputer, 15(2), 112-125.

Susilo, Indra, & Kurniawan, Agus. (2020). Implementasi Sistem Deteksi Intrusi Berbasis Machine