Modul Pelatihan

JUNIOR CYBER SECURITY

Vocational School Graduate Academy
Digital Talent Scholarship
Tahun 2023

KATA PENGANTAR

Dunia saat ini berada pada era industri 4.0 yang lebih banyak menggunakan teknologi digital dan Indonesia telah mempersiapkan diri untuk masuk ke dalam tahap industri 4.0 tersebut melalui agenda percepatan transformasi digital. Salah satu langkah yang dilakukan dalam percepatan transformasi digital adalah penyiapan talenta digital. Laporan Bank Dunia tahun 2019 menyatakan bahwa Indonesia memiliki kekurangan 9 juta pekerja berketerampilan teknologi informasi dan komunikasi, sehingga perlu dilakukan penyiapan talenta digital untuk memenuhi kebutuhan tersebut dengan alokasi 600.000 orang setiap tahun. Upaya penyiapan talenta digital dilakukan oleh berbagai unsur baik pemerintah, institusi pendidikan, industri, komunitas masyarakat, maupun media publik.

Sejak tahun 2018, Kementerian Komunikasi dan Informatika melalui Badan Penelitian dan Pengembangan Sumber Daya Manusia menginisiasi Program Beasiswa Pelatihan Digital bernama *Digital Talent Scholarship* (DTS) yang telah berhasil dianugerahkan kepada lebih dari 300.000 penerima pelatihan bidang teknologi informasi dan komunikasi. Program *Digital Talent Scholarship* ini ditujukan untuk memberikan pelatihan dan sertifikasi berbagai tema pada bidang informatika, komunikasi, dan telekomunikasi, serta diharapkan melengkapi pemenuhan kebutuhan talenta digital Indonesia.

Program DTS tahun 2023 secara garis besar dibagi menjadi delapan akademi, salah satunya Vocational School Graduate Academy (VSGA). VSGA merupakan program pelatihan berbasis kompetensi kerja nasional bagi lulusan pendidikan vokasi SMK/sederajat dan diploma bidang *Science, Technology, Engineering, Mathematics* (STEM) yang belum mendapatkan pekerjaan atau sedang tidak bekerja. Tujuan Program VSGA adalah menyiapkan talenta digital dengan standar kompetensi sesuai Standar Kompetensi Kerja Nasional Indonesia (SKKNI). Oleh karena itu, penyusunan modul pelatihan untuk Program VSGA disusun dengan berbasis pada kompetensi (*Competency Based Training*). Kami berpesan agar modul pelatihan berbasis kompetensi yang telah disusun ini dapat menjadi referensi bagi peserta dan pengajar agar pelatihan berjalan efektif dan efisien.

Selamat mengikuti Pelatihan *Digital Talent Scholarship*, mari persiapkan diri kita menjadi talenta digital Indonesia yang kompeten.

Jakarta, April 2023
Kepala Badan Penelitian dan Pengembangan Sumber Daya Manusia
Kementerian Komunikasi dan Informatika Republik Indonesia

Dr. Hary Budiarto, M.Kom

Pendahuluan

Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam Menerapkan Kontrol Akses Berdasarkan Konsep/Metodologi yang telah Ditetapkan untuk menjaga keamanan sistem informasi dengan membatasi akses ke sumber daya informasi hanya pada orang-orang yang diizinkan dan memastikan bahwa informasi tersebut tidak disalahgunakan atau dirusak. Mengharuskan seseorang memiliki pengetahuan dasar tentang keamanan sistem informasi, seperti prinsip-prinsip dasar keamanan, risiko dan ancaman keamanan, kebijakan keamanan, manajemen identitas dan akses, dan teknologi keamanan seperti firewall, VPN, dan enkripsi.

A. Tujuan Umum

Setelah mempelajari modul ini peserta latih diharapkan mampu dalam Menerapkan Kontrol Akses Berdasarkan Konsep/Metodologi yang telah Ditetapkan benar.

B. Tujuan Khusus

Adapun tujuan mempelajari unit kompetensi melalui buku modul alam mengumpulkan data ini guna memfasilitasi peserta latih sehingga pada akhir pelatihan diharapkan memiliki kemampuan sebagai berikut:

1. Menerapkan Kontrol Akses Berdasarkan Konsep/Metodologi yang telah Ditetapkan mengharuskan seseorang memiliki pengetahuan dasar tentang keamanan sistem informasi, seperti prinsip-prinsip dasar keamanan, risiko dan ancaman keamanan, kebijakan keamanan, manajemen identitas dan akses, dan teknologi keamanan seperti firewall, VPN, dan enkripsi.
2. Selain pengetahuan, keterampilan teknis juga sangat penting dalam menerapkan kontrol akses. Seseorang harus memahami teknologi keamanan dan sistem operasi yang digunakan, seperti Windows, Linux, dan MacOS. Seseorang juga harus dapat memahami berbagai alat keamanan seperti sistem manajemen akses, sistem manajemen sandi, dan aplikasi pengelolaan identitas.
3. Selain pengetahuan dan keterampilan teknis, sikap kerja yang baik juga sangat penting dalam menerapkan kontrol akses. Seseorang harus memiliki kesadaran yang tinggi terhadap keamanan informasi dan memahami pentingnya menjaga kerahasiaan, integritas, dan ketersediaan data. Seseorang harus dapat berpikir kritis dan analitis dalam mengidentifikasi ancaman keamanan dan merancang strategi untuk mengatasi ancaman tersebut.
4. Keterampilan komunikasi dan kerja sama juga diperlukan dalam menerapkan kontrol akses. Seseorang harus dapat berkomunikasi dengan baik dengan anggota tim dan stakeholder lainnya, seperti manajer, pengguna, dan vendor keamanan. Seseorang juga harus dapat bekerja sama dengan tim untuk mengimplementasikan kontrol akses dan menjaga keamanan sistem informasi.

Latar belakang

Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mengumpulkan data untuk data science. Penilaian

dilakukan dengan mengacu kepada Kriteria Unjuk Kerja (KUK) dan dilaksanakan di Tempat Uji Kompetensi (TUK), ruang simulasi atau workshop dengan cara:

1.1 Lisan
1.2 Wawancara
1.3 Tes tertulis
1.4 Demonstrasi
1.5 Metode lain yang relevan.

Deskripsi Pelatihan

Materi Pelatihan ini memfasilitasi pembentukan kompetensi dalam menentukan kebutuhan teknis Mengelola Log.

Tujuan Pembelajaran

Setelah mengikuti pelatihan ini, peserta mampu menentukan kebutuhan teknis Menerapkan Kontrol Akses Berdasarkan Konsep/Metodologi yang telah Ditetapkan.

Kompetensi Dasar

Mampu menentukan kebutuhan teknis Menerapkan Kontrol Akses Berdasarkan Konsep/Metodologi yang telah Ditetapkan.

Indikator Hasil Belajar

Ketepatan dalam melakukan proses pengambilan data sesuai dengan tools yang telah disiapkan

INFORMASI PELATIHAN

INFORMASI PELATIHAN	
Akademi	VSGA untuk Junior Cyber Security
Mitra Pelatihan	
Tema Pelatihan	***Junior Cyber Security***
Sertifikasi	Sertifikasi kompetensi BNSP *Junior Cyber Security*
Deskripsi Pelatihan	Pelatihan ini menyiapkan peserta agar kompeten dalam melaksanakan pekerjaan *junior cyber security* yang dapat membantu pekerjaan praktisi *cyber security.* Kualifikasi pada jabatan ini menuntut seseorang memiliki kompetensi dalam menerapkan prinsip perlindungan informasi, menerapkan prinsip keamanan informasi untuk penggunaan jaringan internet, menerapkan prinsip keamanan informasi pada transaksi elektronik, melaksanakan kebijakan keamanan informasi, mengaplikasikan ketentuan/persyaratan keamanan informasi , mengelola log, dan menerapkan kontrol akses berdsarkan konsep/metodologi yang telah ditetapkan
Output Pelatihan	Setelah mengikuti pelatihan peserta akan mampu menganalisis dan memvisualisasikan data sehingga dapat digunakan dalam pengambilan keputusan
Durasi Pelatihan	24 JP (3 hari)

INFORMASI PELATIHAN	
Jenis Pelatihan	**Luring *Offline* (40% Pengetahuan - 60% Praktek)**
Persyaratan Peserta	● Warga Negara Indonesia ● Usia Maksimal 29 Tahun pada saat mendaftar ● Lulus Pendidikan D3 Bidang TIK/SMK Bidang (TKJ/TI/RPL) yang pernah bekerja minimal 3 tahun ● Belum Mendapatkan Pekerjaan Tetap/Pernah Bekerja tapi sedang tidak bekerja ● Lolos Seleksi Administrasi dan Tes Substansi
Persyaratan Sarana Peserta	Laptop/PC dengan spesifikasi: ● RAM minimal 4 GB ● 32/64-bit processor ● Operating System Windows 7,8,10, Linux, atau MAC OSX ● konektivitas WiFi ● Akses Internet Dedicated 256 kbps per peserta per perangkat
Kriteria Pengajar/*Trainer*/ Instruktur:	1. Minimal Lulusan S2 di bidang TIK; atau Memiliki kompetensi Okupasi Nasional "*Junior Cyber Security*". 2. Pengalaman Kerja diutamakan sebagai tenaga pengajar Pelatihan Bidang TIK minimal selama 2 tahun 3. Telah mengikuti pelatihan *training of trainner Junior Cyber Security*
Tim Penyusun:	1. Yan Hadynoer (BSSN) 2. Yoyok Darmanto (BSSN)

INFORMASI PEMBELAJARAN

RENCANA PELATIHAN		
Pertemuan	**Topik**	**Aktivitas**
Hari 1	● Pembukaan dan Penjelasan Rencana Pembelajaran ● Pre test	Pemaparan materi, diskusi dan *hands-on lab live class* 1 JP
	Pengantar *Junior Cyber Security* (Posisi dan peran *junior cyber security)*	Pemaparan materi, diskusi dan *hands-on*

		lab live class 1 JP
	Persiapan alat bantu (tools) pelatihan - Python (Jupiter) kenalkan dengan yang online; numpy, pandas, matplotl, seaborn, folium - MySql (XAMPP)	Pemaparan materi, diskusi dan *hands-on lab live class* 1 JP
	Menerapkan prinsip perlindungan informasi 1. Mendefinisikan prosedur keamanan informasi yang tepat untuk tiap klasifikasi 2. Mengidentifikasi kelemahan dari informasi dalam sistem komunikasi bisnis 3. Menerapkan akses kontrol lingkungan Komputasi yang sesuai 4. Mematuhi dan melaksanakan petunjuk yang terdapat pada dokumen yang diterbitkan khusus oleh pemerintah atau badan-badan resmi terkait untuk mengelola sistem operasi 5. Mengumpulkan dan memelihara data yang diperlukan untuk memenuhi persyaratan pelaporan keamanan sistem.	Pemaparan materi, diskusi dan *hands-on lab live class* 2 JP
	Menerapkan prinsip keamanan informasi untuk penggunaan jaringan internet 1. Mematuhi dan menerapkan kebijakan dan prosedur keamanan informasi yang terkait dengan penggunaan jaringan internet 2. Mengidentifikasi tipe kelemahan dan jenisjenis serangan dalam jaringan internet 3. Mengaplikasikan penggunaan jaringan internet secara aman	Pemaparan materi, diskusi dan *hands-on lab live class* 3 JP

Hari 2	**Menerapkan prinsip keamanan informasi pada transaksi elektronik** 1. Mengidentifikasikan dan memenuhi kebutuhan terkait kerahasiaan, integritas, bukti dari pengguna dokumen kunci dan kontrak yang diakui 2. Menetapkan aspek-aspek transaksi 3. Melaksanakan dan memantau perlindungan keamanan untuk sistem infrastruktur dan penggunaan teknologi informasi sesuai dengan rencana implementasi dan prosedur operasi standar	Pemaparan materi, diskusi dan *hands-on lab live class* 3 JP
	Melaksanakan kebijakan keamanan informasi 1. Mengidentifikasi aset penting dalam organisasi 2. Memproteksi aset penting dalam organisasi 3. Melakukan pemantauan terhadap aktivitas yang rentan ancaman	Pemaparan materi, diskusi dan *hands-on lab live class* 2 JP
	Mengaplikasikan ketentuan/persyaratan keamanan informasi 1. Mengaplikasikan persyaratan untuk program yang spesifik untuk keamanan lingkungan komputasi guna mengidentifikasi kelemahan/kerentanan 2. Menyediakan masukan tentang hal yang terkait dengan persyaratan keamanan untuk dimasukkan dalam laporan pekerjaan dan dokumen-dokumen pengadaan terkait 3. Mengumpulkan dan memelihara data yang diperlukan untuk memenuhi persyaratan pelaporan keamanan sistem 4. Mengindentifikasikan persyaratan keamanan dalam prosedur operasi di lingkungan komputasi 5. Menyusun persyaratan keamanan untuk perangkat keras, piranti lunak, dan penggunaan layanan yang spesifik	Pemaparan materi, diskusi dan *hands-on lab live class* 3 JP

	untuk program keamanan jaringan 6. Mengevaluasi dan/atau menyetujui persyaratan keamanan yang relevanterhadap kemampuan teknologi informasi yang baru	
Hari 3	**Mengelola *log*** 1. Menetapkan kebijakan pencatatan *log* untuk menyertakan peristiwa penting 2. Melakukan kontrol berkas *log* terhadap kemungkinan diubah atau dihapus 3. Melakukan kontrol tempat menyimpan media file pencatatan terhadap kemungkinan penuh sehingga terjadi kegagalan ketika mencatat kejadian yang terjadi	Pemaparan materi, diskusi dan *hands-on lab live class* 4 JP
	Menerapkan kontrol akses berdsarkan konsep/metodologi yang telah ditetapkan 1. Menerapkan kontrol akses lingkungan komputasi yang sesuai 2. Melaksanakan kebijakan organisasi dan kebijakan *password* organisasi 3. Mengelola akun hak jaringan dan hak akses ke sistem jaringan dan infrastrukturnya 4. Mengimplementasikan peringatan secara online untuk menginformasikan para pengguna atas peraturan akses dari seluruh infrastruktur dan penggunaan sistem teknologi informasi 5. Menyusun prosedur untuk memastikan pengguna sistem menyadari tanggung jawab keamanan mereka sebelum memberikan akses ke sistem informasi organisasi 6. Melakukan kontrol dan pengawasan pada setiap pengguna yang memiliki akses khusus menjalankan fungsi keamanan agar menerima pelatihan keamanan dasar dan berkelanjutan serta mendapatkan sertifikasi yang sesuai untuk melaksanakan tugas keamanan	Pemaparan materi, diskusi dan *hands-on lab live class* 4 JP

Materi Pokok
5.1 Menerapkan kontrol akses lingkungan komputasi yang sesuai 5.2 Melaksanakan kebijakan organisasi dan kebijakan password organisasi 5.3 Mengelola akun hak jaringan dan hak akses ke sistem jaringan dan infrastrukturnya 5.4 Mengimplementasikan peringatan secara online untuk menginformasikan para pengguna atas peraturan akses dari seluruh infrastruktur dan penggunaan sistem teknologi informasi 5.5 Menyusun prosedur untuk memastikan pengguna sistem menyadari tanggung jawab keamanan mereka sebelum memberikan akses ke sistem informasi organisasi 5.6 Melakukan kontrol dan pengawasan pada setiap pengguna yang memiliki akses khusus menjalankan fungsi keamanan agar menerima pelatihan keamanan dasar dan berkelanjutan serta mendapatkan sertifikasi yang sesuai untuk melaksanakan tugas keamanan

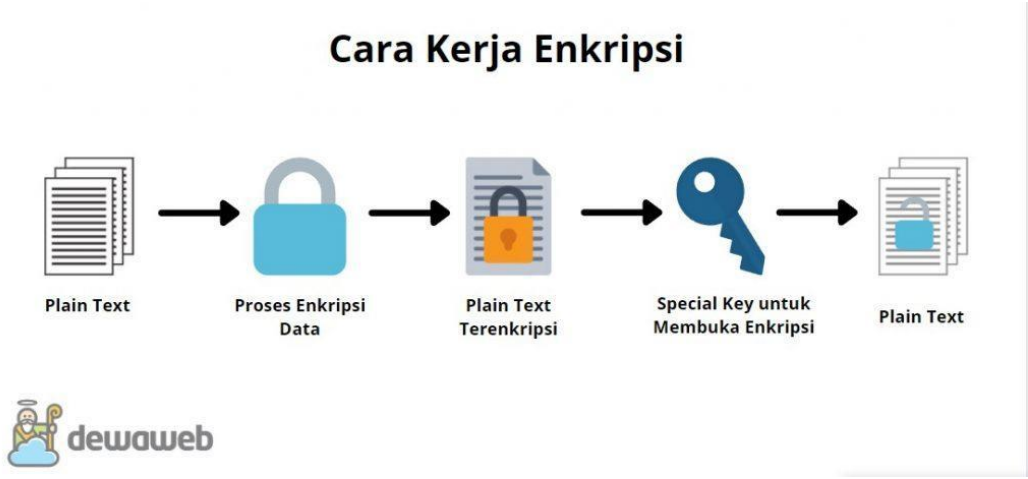
Sub Materi Pokok
1.1. Penetapan Sistem dan prosedur kontrol akses. 1.2. Pembuatan Log untuk setiap kegiatan akses 2.1. Dokumen kebijakan password dan penggunaannya 2.2. Laporan atas penerapan system password 3.1. pembuatan Daftar akun beserta hak akses ke dalam sistem. 3.2. Pendefinisian Daftar hak - hak penting yang diberikan kepada pengguna tertentu. 4.1. Penerapan Sistem online dari daftar peringatan yang telah terjadi selama akses penggunaan infrastruktur dan sistem teknologi informasi tersebut. 4.2. Laporan pelaksanaan peringatan secara online. 4.3. Catatan log dari daftar peringatan yang sudah terjadi dan kondisi terakhir masing-masing peringatan tersebut. 5.1. Prosedur tentang tanggung jawab keamanan bagi setiap pengguna telah disusun. 5.2. Hasil audit/rekomendasi pelaksanaan pemberian akses ke pengguna. 6.1. Pelatihan keamanan dasar dan berkelanjutan dilaksanakan untuk SDM yang memiliki akses khusus menjalankan fungsi keamanan. 6.2. Sertifikasi keamanan yang dikeluarkan oleh badan/lembaga terkait dimiliki oleh SDM yang memiliki akses khusus menjalankan fungsi keamanan

5.1 MENERAPKAN KONTROL AKSES LINGKUNGAN KOMPUTASI YANG SESUAI

Menerapkan kontrol akses lingkungan komputasi yang sesuai adalah suatu tindakan yang penting dalam menjaga keamanan sistem informasi dan memastikan bahwa sumber daya IT hanya digunakan oleh orang-orang yang memilik hak akses yang sesuai. Berikut adalah beberapa cara untuk menerapkan kontrol akses lingkungan komputasi yang sesuai:

1. Identifikasi pengguna dan hak akses: Identifikasi pengguna dan hak akses yang sesuai dengan setiap pengguna. Berikan akses yang cukup pada orang yang memerlukannya dan batasi akses pada orang yang tidak memerlukannya.

2. Gunakan password yang kuat: Pastikan bahwa pengguna menggunakan password yang kuat dan unik. Jangan menggunakan password yang mudah ditebak seperti tanggal lahir atau nama hewan peliharaan.
3. Mengaktifkan mekanisme otentikasi: Gunakan mekanisme otentikasi seperti login ganda atau verifikasi dua faktor untuk mengamankan akses ke sumber daya informasi.
4. Gunakan enkripsi: Gunakan enkripsi untuk mengamankan data sensitif seperti informasi klien atau karyawan, termasuk dalam penyimpanan atau saat transfer data.
   Untuk melakukan enkripsi pada suatu file, Anda dapat mengikuti langkah-langkah berikut:
   1. Pilih algoritma enkripsi yang akan digunakan. Ada banyak algoritma enkripsi yang tersedia, termasuk AES, RSA, dan Blowfish, masing-masing dengan kelebihan dan kekurangan. Pastikan untuk memilih algoritma enkripsi yang cocok untuk kebutuhan Anda.
   2. Instal software enkripsi pada komputer Anda. Ada banyak software enkripsi yang tersedia, seperti VeraCrypt, GnuPG, atau 7-Zip. Pilih software yang sesuai dengan algoritma enkripsi yang Anda pilih.
   3. Buka software enkripsi dan pilih file yang akan dienkripsi. Pilih opsi enkripsi pada software dan tentukan kata sandi atau kunci enkripsi yang akan digunakan.
   4. Tunggu hingga proses enkripsi selesai. Ini mungkin memakan waktu beberapa saat, tergantung pada ukuran file dan kecepatan komputer Anda.
   5. Simpan file yang dienkripsi di tempat yang aman dan jangan lupa kata sandi atau kunci enkripsi yang digunakan. Pastikan untuk membuat backup file yang dienkripsi dan menyimpannya di tempat yang aman juga.



   Dalam melakukan enkripsi pada file, pastikan untuk memilih kata sandi atau kunci enkripsi yang kuat dan aman. Gunakan kombinasi huruf, angka, dan karakter khusus, serta hindari kata sandi atau kunci yang mudah ditebak seperti tanggal lahir atau nama keluarga. Selain itu, pastikan untuk menggunakan software enkripsi yang tepercaya dan terkini, untuk memastikan keamanan file yang dienkripsi.

5. Menerapkan pengawasan akses: Gunakan perangkat lunak pengawasan akses untuk memantau dan merekam aktivitas pengguna. Hal ini dapat membantu mendeteksi aktivitas mencurigakan dan mencegah akses yang tidak sah.
6. Jangan membagikan informasi akun: Pastikan informasi akun tidak dibagikan dengan siapa pun kecuali orang yang sah untuk mengakses sistem. Ini termasuk ID pengguna, password, dan kunci enkripsi.

7. Pelatihan dan kesadaran: Lakukan pelatihan dan pendidikan tentang praktik keamanan IT yang baik. Peningkatan kesadaran akan pentingnya keamanan dapat membantu mencegah serangan dan kesalahan manusia yang tidak disengaja.

Dengan menerapkan kontrol akses lingkungan komputasi yang sesuai, organisasi dapat meminimalkan risiko keamanan dan memastikan bahwa sumber daya IT hanya digunakan oleh orang-orang yang memerlukannya dan memiliki hak akses yang sesuai. Hal ini dapat membantu melindungi informasi sensitif, menjaga kepatuhan, dan memastikan keamanan dan integritas sistem informasi.

1.1 Penetapan Sistem dan Prosedur Kontrol Akses

Sistem dan prosedur kontrol akses adalah cara-cara yang ditetapkan oleh organisasi untuk mengontrol akses terhadap sumber daya informasi dan teknologi yang dimilikinya. Dalam sistem dan prosedur kontrol akses, terdapat beberapa hal yang harus diperhatikan, yaitu:

1. Identifikasi dan otorisasi pengguna: Setiap pengguna harus memiliki identifikasi unik dan otorisasi yang sesuai dengan tugas dan tanggung jawabnya.
2. Verifikasi identitas pengguna: Organisasi harus memiliki cara untuk memverifikasi identitas pengguna sebelum memberikan akses ke sistem atau sumber daya informasi.
3. Pembatasan akses: Organisasi harus membatasi akses ke sumber daya informasi yang sensitif hanya pada orang yang memerlukannya.
4. Pengawasan akses: Organisasi harus memantau akses ke sumber daya informasi dan merekam aktivitas pengguna.
5. Pengelolaan kata sandi: Organisasi harus memiliki kebijakan yang jelas dan prosedur untuk mengelola kata sandi, termasuk persyaratan kompleksitas dan siklus penggantian kata sandi.
6. Pembatasan akses jaringan: Organisasi harus membatasi akses jaringan hanya pada orang yang memerlukan akses.
7. Pemantauan dan inspeksi: Organisasi harus memantau dan memeriksa sistem dan aplikasi secara berkala untuk memastikan keamanan dan integritasnya.
8. Pendidikan dan pelatihan: Organisasi harus memberikan pelatihan dan pendidikan kepada pengguna dan staf tentang praktik keamanan yang baik.

Dalam sistem dan prosedur kontrol akses, organisasi harus menetapkan kebijakan dan prosedur yang jelas dan terukur untuk mengatur hak akses pengguna dan memastikan bahwa sumber daya informasi dan teknologi hanya dapat diakses oleh orang yang memerlukan akses. Proses ini melibatkan identifikasi, verifikasi, dan pengelolaan identitas pengguna, serta pembatasan akses dan pengawasan aktivitas pengguna untuk menjaga keamanan dan integritas sumber daya informasi dan teknologi organisasi.

Berikut adalah pengertian dari masing-masing model keamanan yang sering digunakan dalam kontrol akses:

1. Discretionary Access Control (DAC) adalah model keamanan di mana pemilik dari suatu sumber daya dapat menentukan siapa yang dapat mengakses sumber daya tersebut dan jenis akses yang diizinkan. Pemilik sumber daya bertanggung jawab untuk mengelola hak akses pada sumber daya mereka, yang dapat berupa file, folder, atau perangkat lunak. Dalam DAC, pengguna memiliki kontrol penuh atas hak akses yang diberikan pada sumber daya mereka.

2. Mandatory Access Control (MAC) adalah model keamanan di mana hak akses ditentukan oleh label keamanan yang terpasang pada objek dan subjek. Label keamanan ini menentukan level akses yang diizinkan untuk subjek tertentu pada objek tertentu. Label keamanan biasanya digunakan pada sistem operasi, firewall, dan perangkat keamanan jaringan.
3. Role-Based Access Control (RBAC) adalah model keamanan di mana hak akses ditentukan berdasarkan peran atau posisi pekerjaan pengguna. Setiap peran atau posisi memiliki hak akses tertentu pada sumber daya yang terkait dengan pekerjaan mereka. RBAC lebih mudah dikelola daripada DAC, karena pengguna tidak memiliki kontrol penuh atas hak akses mereka.
4. Attribute-Based Access Control (ABAC) adalah model keamanan di mana hak akses ditentukan berdasarkan atribut dari subjek, objek, atau lingkungan. Atribut ini termasuk informasi seperti waktu akses, lokasi, dan level keamanan. ABAC sangat fleksibel dan dapat disesuaikan dengan kebutuhan bisnis, tetapi dapat lebih sulit dikelola daripada model keamanan lainnya.

Semua model keamanan di atas memiliki kelebihan dan kelemahan masing-masing dan organisasi harus memilih model keamanan yang paling cocok untuk kebutuhan bisnis dan keamanan mereka.

1.2 Pembuatan Log untuk setiap kegiatan akses

Pembuatan log untuk setiap kegiatan akses secara rinci adalah salah satu aspek penting dari sistem dan prosedur kontrol akses. Log harus mencatat semua akses yang dilakukan pengguna ke sumber daya informasi dan teknologi organisasi, termasuk informasi seperti:

1. Nama pengguna atau identitas pengguna yang digunakan untuk mengakses sumber daya.
2. Waktu dan tanggal akses dilakukan.
3. Jenis sumber daya yang diakses, seperti aplikasi atau file.
4. Jenis aksi yang dilakukan oleh pengguna, seperti membaca, menulis, atau mengedit.
5. Hasil dari aksi yang dilakukan oleh pengguna, seperti file yang diubah atau data yang dimasukkan.
6. Informasi tambahan, seperti alamat IP pengguna atau jenis perangkat yang digunakan.

Log harus disimpan dengan aman dan terlindungi dari akses yang tidak sah atau modifikasi. Pengawasan log secara berkala dan pengujian untuk keaslian dan integritas penting untuk memastikan bahwa log tidak diubah atau dimanipulasi untuk mengelabui pengawasan keamanan.

Dengan membuat log yang rinci dan memastikan keaslian dan integritasnya, organisasi dapat mengidentifikasi aktivitas yang mencurigakan atau tidak sah dan memonitor penggunaan sumber daya informasi dan teknologi organisasi. Log juga dapat digunakan untuk audit dan pemenuhan persyaratan hukum dan peraturan keamanan informasi yang berlaku.

5.2 MELAKSANAKAN KEBIJAKAN ORGANISASI DAN KEBIJAKAN PASSWORD ORGANISASI

Melaksanakan kebijakan organisasi dan kebijakan password organisasi adalah bagian penting dari kontrol akses lingkungan komputasi. Kebijakan ini bertujuan untuk memastikan

bahwa pengguna hanya memiliki akses ke sumber daya informasi dan teknologi yang sesuai dengan tugas dan tanggung jawab mereka, serta memastikan keamanan sistem informasi dan teknologi organisasi.

Kebijakan organisasi dapat mencakup:

1. Kebijakan identifikasi dan otentikasi pengguna, termasuk persyaratan untuk membuat akun pengguna, memverifikasi identitas, dan memberikan hak akses yang sesuai.
2. Kebijakan akses yang terkait dengan data dan aplikasi, termasuk persyaratan untuk melindungi data sensitif, membatasi akses ke aplikasi tertentu, dan mengendalikan penggunaan sumber daya informasi dan teknologi organisasi.
3. Kebijakan penanganan password, termasuk persyaratan untuk membuat password yang kuat, mengganti password secara berkala, dan melindungi password dari akses yang tidak sah.

Melaksanakan kebijakan password organisasi juga penting untuk memastikan keamanan sistem informasi dan teknologi organisasi. Beberapa tindakan yang dapat dilakukan untuk melaksanakan kebijakan password organisasi, antara lain:

1. Menetapkan persyaratan password yang kuat dan aman, seperti panjang minimal password, kombinasi huruf besar dan kecil, angka, dan karakter khusus.
2. Memastikan bahwa password yang digunakan tidak mudah ditebak atau dapat ditebak oleh orang lain, seperti nama atau tanggal lahir.
3. Menerapkan kebijakan penggantian password secara berkala untuk memastikan keamanan dan mencegah penggunaan password yang sama untuk waktu yang lama.
4. Menggunakan teknologi pengelolaan password yang aman dan efektif, seperti pengelolaan password yang terenkripsi dan teknologi autentikasi ganda.

Dengan melaksanakan kebijakan organisasi dan kebijakan password organisasi dengan benar, organisasi dapat memastikan bahwa pengguna hanya memiliki akses ke sumber daya informasi dan teknologi yang sesuai dengan tugas dan tanggung jawab mereka, serta memastikan keamanan sistem informasi dan teknologi organisasi.

2.1 Dokumen kebijakan password dan penggunaannya.

Berikut adalah contoh dokumen kebijakan password dan penggunaannya yang dapat ditetapkan dalam suatu organisasi:

1. Tujuan Tujuan dari kebijakan ini adalah untuk memastikan bahwa password yang digunakan oleh pengguna dalam lingkungan komputasi organisasi memenuhi standar keamanan dan privasi yang diperlukan.
2. Lingkup Kebijakan ini berlaku untuk semua pengguna yang memiliki akses ke lingkungan komputasi organisasi.
3. Kebijakan a. Password harus memiliki minimal 8 karakter. b. Password harus terdiri dari kombinasi huruf besar, huruf kecil, angka, dan karakter khusus. c. Password harus diubah setiap 90 hari sekali. d. Password lama tidak boleh digunakan kembali. e. Pengguna tidak boleh menggunakan password yang sama untuk akun yang berbeda. f. Pengguna harus mengunci perangkat mereka ketika meninggalkan tempat kerja.
4. Pengecualian Pengecualian atas kebijakan ini harus dilakukan oleh manajer atau administrator sistem, setelah mempertimbangkan faktor keamanan dan privasi yang terlibat.
5. Pelaksanaan a. Pengguna harus mendapatkan instruksi tentang penggunaan password yang aman. b. Administrator sistem harus memastikan bahwa

password pengguna memenuhi standar keamanan dan privasi yang ditetapkan. c. Jika ada pelanggaran terhadap kebijakan ini, tindakan yang sesuai akan diambil.

6. Evaluasi Kebijakan ini akan dievaluasi secara berkala oleh administrator sistem untuk memastikan bahwa masih sesuai dengan kebutuhan organisasi dan standar keamanan yang diperlukan.
7. Referensi Kebijakan ini merujuk pada standar keamanan dan privasi yang diperlukan untuk lingkungan komputasi organisasi.

2.2 Laporan atas penerapan system password

Berikut adalah contoh laporan atas penerapan sistem password yang ada:
Laporan Penerapan Sistem Password
Tanggal: 25 Maret 2023
Kepada: Manajer Keamanan Informasi
Dari: Tim IT
Subjek: Laporan Penerapan Sistem Password

1. Pendahuluan Laporan ini disusun untuk memberikan informasi tentang penerapan sistem password di lingkungan komputasi organisasi. Sistem password ini diterapkan untuk memastikan keamanan dan privasi data yang digunakan oleh pengguna.
2. Kebijakan Password Kebijakan password organisasi telah ditetapkan dan dipatuhi oleh seluruh pengguna. Kebijakan password meliputi persyaratan minimal 8 karakter, kombinasi huruf besar, huruf kecil, angka, dan karakter khusus. Pengguna diwajibkan mengubah password setiap 90 hari sekali dan tidak boleh menggunakan password lama yang telah digunakan sebelumnya. Pengguna juga dilarang menggunakan password yang sama untuk akun yang berbeda.
3. Penerapan Sistem Password Sistem password telah diimplementasikan pada semua sistem yang digunakan oleh pengguna. Sistem password memungkinkan pengguna untuk membuat password yang sesuai dengan kebijakan organisasi dan meminta pengguna untuk mengubah password secara berkala. Sistem password juga mencegah pengguna untuk menggunakan password yang sama untuk akun yang berbeda.
4. Evaluasi dan Peningkatan Kami melakukan evaluasi sistem password secara berkala untuk memastikan bahwa sistem tersebut berfungsi dengan baik dan sesuai dengan kebijakan organisasi. Kami juga terus melakukan peningkatan sistem password untuk meningkatkan keamanan dan privasi data organisasi.

Kesimpulan Dari laporan ini, dapat disimpulkan bahwa sistem password telah diimplementasikan dengan baik di lingkungan komputasi organisasi dan seluruh pengguna mematuhi kebijakan password yang telah ditetapkan. Kami akan terus melakukan evaluasi dan peningkatan sistem password untuk memastikan keamanan dan privasi data organisasi tetap terjaga.

5.3 MENGELOLA AKUN HAK JARINGAN DAN HAK AKSES KE SISTEM JARINGAN DAN INFRASTRUKTURNYA

Manajemen akun, hak akses jaringan, dan infrastruktur sistem sangat penting dalam mengelola keamanan jaringan. Beberapa tindakan yang dapat dilakukan untuk mengelola akun, hak akses jaringan, dan infrastruktur sistem adalah sebagai berikut:

1. Pembuatan akun pengguna: Setiap pengguna harus memiliki akun yang unik dan aman. Penggunaan nama pengguna dan kata sandi yang kuat dianjurkan untuk menghindari penggunaan yang tidak sah.
2. Membatasi hak akses: Setiap pengguna harus memiliki hak akses yang sesuai dengan tugas dan tanggung jawab mereka. Pengguna yang tidak perlu memiliki hak akses tertentu harus dibatasi.
3. Manajemen kata sandi: Aturan untuk panjang kata sandi dan kompleksitas harus ditetapkan dan diterapkan secara konsisten. Kata sandi harus diubah secara berkala dan pengguna harus diberi tahu untuk tidak menggunakan kata sandi yang sama untuk akun yang berbeda.
4. Peninjauan akun pengguna: Daftar akun pengguna harus diperbarui secara teratur dan dihapus jika pengguna tidak lagi memerlukan akses.
5. Logging dan monitoring: Log akses harus ditetapkan dan dipantau secara teratur untuk mendeteksi aktivitas mencurigakan atau tidak sah.
6. Membatasi akses jaringan: Jaringan harus dibatasi dan hanya diakses oleh pengguna yang membutuhkan akses. Perangkat lunak keamanan, seperti firewall dan antivirus, harus diterapkan dan diatur dengan benar.
7. Pemantauan infrastruktur sistem: Infrastruktur sistem harus dipantau secara teratur untuk mendeteksi dan mencegah serangan.

Laporan dapat dibuat untuk memeriksa dan mengevaluasi keamanan sistem, termasuk manajemen akun, hak akses jaringan, dan infrastruktur sistem. Hal ini membantu memastikan bahwa sistem berfungsi sebagaimana mestinya dan melindungi informasi sensitif dari akses yang tidak sah.

3.1 Pembuatan Daftar akun beserta hak akses ke dalam sistem.

Untuk membuat daftar akun beserta hak akses ke dalam sistem, dapat dilakukan langkah-langkah sebagai berikut:

1. Identifikasi semua akun pengguna yang terdaftar dalam sistem jaringan dan infrastruktur yang dikelola.
2. Analisis kebutuhan dan hak akses yang dibutuhkan oleh masing-masing akun pengguna sesuai dengan tugas dan tanggung jawabnya.
3. Tetapkan hak akses yang sesuai untuk setiap akun pengguna, termasuk hak akses ke sistem jaringan dan infrastruktur seperti akses ke server, akses ke database, dan sebagainya.
4. Buat daftar akun pengguna beserta hak aksesnya dalam sebuah dokumen yang mudah diakses dan dipahami oleh semua pihak terkait.
5. Perbarui daftar akun dan hak akses secara berkala, terutama saat ada perubahan dalam struktur organisasi atau perubahan tugas dan tanggung jawab pengguna.

Dengan adanya daftar akun beserta hak akses ke dalam sistem, pengelola sistem jaringan dan infrastruktur dapat memastikan bahwa setiap akun pengguna memiliki hak akses yang sesuai dengan tugas dan tanggung jawabnya, sehingga dapat mengurangi risiko penyalahgunaan hak akses yang dapat membahayakan keamanan sistem.

Berikut ini adalah contoh daftar akun beserta hak akses ke dalam sistem:

No.	Nama Pengguna	Hak Akses
1	admin	- Akses ke semua server - Akses ke semua database - Hak akses penuh dalam sistem
2	user1	- Akses ke server web - Akses ke database pelanggan - Hak akses pembaca dalam sistem
3	user2	- Akses ke server aplikasi - Akses ke database keuangan - Hak akses pembaca dan penulis dalam sistem
4	user3	- Akses ke server file - Hak akses pembaca dan penulis dalam sistem

Dalam contoh di atas, terdapat empat akun pengguna yang terdaftar dalam sistem. Setiap akun memiliki hak akses yang sesuai dengan tugas dan tanggung jawabnya. Akun admin memiliki hak akses penuh dalam sistem, sementara akun user1 memiliki hak akses ke server web dan database pelanggan dengan hak akses pembaca dalam sistem. Akun user2 memiliki hak akses ke server aplikasi dan database keuangan dengan hak akses pembaca dan penulis dalam sistem. Akun user3 hanya memiliki akses ke server file dengan hak akses pembaca dan penulis dalam sistem. Dengan daftar akun seperti ini, pengelola sistem dapat dengan mudah memantau dan mengatur hak akses setiap pengguna dalam sistem.

3.2 Pendefinisian Daftar hak - hak penting yang diberikan kepada pengguna tertentu.

Berikut adalah contoh daftar hak-hak penting yang diberikan kepada pengguna tertentu dalam suatu sistem jaringan:

1. Hak akses administratif: Pengguna dengan hak akses ini memiliki kemampuan penuh untuk mengelola sistem jaringan dan infrastruktur seperti mengelola pengguna, grup, dan kebijakan keamanan.
2. Hak akses keamanan: Pengguna dengan hak akses ini dapat mengelola kebijakan keamanan sistem dan infrastruktur, seperti mengelola firewall, antivirus, dan mekanisme deteksi intrusi.
3. Hak akses jaringan: Pengguna dengan hak akses ini dapat mengakses dan mengelola perangkat jaringan seperti switch, router, dan gateway.
4. Hak akses data: Pengguna dengan hak akses ini dapat mengakses dan mengelola data dalam sistem jaringan, seperti membuat, mengedit, dan menghapus file dan folder.
5. Hak akses aplikasi: Pengguna dengan hak akses ini dapat mengakses dan mengelola aplikasi dalam sistem jaringan, seperti menginstal, mengatur konfigurasi, dan memperbarui aplikasi.
6. Hak akses monitor: Pengguna dengan hak akses ini dapat mengakses dan mengelola alat pemantauan sistem jaringan dan infrastruktur, seperti perangkat pemantauan kinerja, log file, dan alat manajemen kapasitas.
7. Hak akses penyimpanan: Pengguna dengan hak akses ini dapat mengakses dan mengelola perangkat penyimpanan dalam sistem jaringan, seperti hard drive, storage area network (SAN), dan network-attached storage (NAS).

5.4 MENGIMPLEMENTASIKAN PERINGATAN SECARA ONLINE UNTUK MENGINFORMASIKAN PARA PENGGUNA ATAS PERATURAN AKSES DARI SELURUH INFRASTRUKTUR DAN PENGGUNAAN SISTEM TEKNOLOGI INFORMASI

Implementasi peringatan secara online dapat dilakukan dengan cara menampilkan pesan atau pop-up di layar komputer ketika pengguna mengakses infrastruktur atau sistem

teknologi informasi. Pesan tersebut dapat berisi informasi tentang peraturan akses yang harus diikuti oleh pengguna, serta sanksi atau konsekuensi yang akan diberikan apabila peraturan tersebut dilanggar.
Contoh peringatan online yang dapat diterapkan adalah sebagai berikut:

- Saat pengguna login ke sistem, tampilkan pesan yang mengingatkan pengguna untuk tidak membagikan password atau melakukan tindakan yang dapat membahayakan keamanan sistem.
- Ketika pengguna akan mengakses data yang sensitif atau mengubah pengaturan yang penting, tampilkan pesan peringatan untuk memastikan bahwa pengguna memahami risiko dari tindakan tersebut.
- Saat pengguna menggunakan aplikasi tertentu, tampilkan pesan peringatan jika aplikasi tersebut memiliki risiko keamanan yang tinggi atau apabila pengguna melakukan tindakan yang berpotensi merusak data atau sistem.

4.1. Penerapan **Sistem online dari daftar peringatan yang telah terjadi selama akses penggunaan infrastruktur dan sistem teknologi informasi tersebut.**
Berikut adalah contoh sistem online dari daftar peringatan yang telah terjadi selama akses penggunaan infrastruktur dan sistem teknologi informasi:

1. Pengguna dengan akun "userA" telah mencoba mengakses halaman "admin.php". Tindakan ini melanggar kebijakan akses dan akan direkam untuk keamanan.
2. Pengguna dengan akun "userB" telah memasukkan kata sandi yang salah tiga kali saat mencoba masuk ke akunnya. Akun tersebut akan terkunci sementara waktu untuk mencegah penyalahgunaan.
3. Ada percobaan login yang dicurigai dari alamat IP yang tidak diketahui. Ini mungkin merupakan tanda dari upaya hacking atau serangan phishing. Tindakan lebih lanjut akan dilakukan untuk memastikan keamanan sistem.
4. Pengguna dengan akun "userC" telah melakukan percobaan login dengan menggunakan kata sandi yang sama dengan yang digunakan pada akun email pribadinya. Ini merupakan pelanggaran kebijakan keamanan dan pengguna akan diberi peringatan untuk mengubah kata sandi yang tidak aman.
5. Pengguna dengan akun "userD" telah mengakses halaman yang hanya tersedia untuk administrator. Pengguna akan diberi peringatan dan aksesnya akan dicatat untuk audit.

Dengan sistem online seperti ini, para pengguna akan diberi peringatan secara langsung ketika melanggar kebijakan akses atau melakukan tindakan yang tidak aman. Hal ini akan meningkatkan kesadaran dan kepatuhan terhadap kebijakan keamanan dan membantu melindungi infrastruktur dan sistem teknologi informasi dari ancaman keamanan.

4.2. Laporan pelaksanaan peringatan secara online.
Berikut ini adalah contoh laporan pelaksanaan peringatan secara online:
Laporan Pelaksanaan Peringatan Online
Tanggal: 25 Maret 2023
Peringatan Hari Ini:

1. Harap diperhatikan bahwa penggunaan sistem jaringan hanya diperbolehkan untuk tujuan bisnis dan tidak untuk keperluan pribadi.
2. Dilarang mengunggah, mengunduh atau menyebarkan materi yang mengandung unsur pornografi atau kekerasan.
3. Pastikan bahwa password yang digunakan untuk mengakses sistem jaringan memiliki tingkat keamanan yang cukup.

4. Pastikan bahwa akses ke data sensitif hanya diberikan kepada pengguna yang berwenang.
5. Jangan meninggalkan perangkat elektronik yang terhubung ke sistem jaringan tanpa pengawasan.

Catatan:

- Peringatan online telah ditampilkan pada layar komputer pengguna sebanyak 3 kali selama periode kerja hari ini.
- Tidak ada pelanggaran aturan yang dilaporkan selama periode kerja hari ini.
- Seluruh pengguna diharapkan untuk mematuhi aturan dan regulasi yang berlaku terkait penggunaan sistem jaringan dan infrastruktur teknologi informasi.

Dibuat oleh:
Nama: [Nama Penanggung Jawab] Jabatan: [Jabatan Penanggung Jawab]

4.3. Catatan log dari daftar peringatan yang sudah terjadi dan kondisi terakhir masingmasing peringatan tersebut.

Berikut adalah contoh catatan log dari daftar peringatan yang telah terjadi beserta kondisi terakhir masing-masing peringatan:

No	Tanggal	Peringatan	Kondisi Terakhir	Tindakan
1	01/01/2022	Penggunaan password lemah	Diperbaiki dengan meminta pengguna untuk mengganti password dengan password yang lebih kuat	Meminta pengguna untuk mengganti password dengan password yang lebih kuat
2	05/02/2022	Upaya login yang tidak sah	Diidentifikasi dan ditindaklanjuti oleh administrator sistem untuk mencegah upaya login yang tidak sah di masa depan	Melaporkan upaya login yang tidak sah kepada administrator sistem
3	10/03/2022	Akses ke halaman yang tidak diizinkan	Diidentifikasi dan ditindaklanjuti oleh administrator jaringan dengan memblokir akses pengguna ke halaman yang tidak diizinkan	Meminta pengguna untuk tidak mengakses halaman yang tidak diizinkan dan memblokir akses pengguna ke halaman tersebut

Catatan log tersebut mencatat peringatan yang terjadi, tanggal peringatan terjadi, kondisi terakhir dari peringatan tersebut, serta tindakan yang dilakukan untuk menangani peringatan tersebut. Dengan adanya catatan log seperti ini, akan memudahkan pihak terkait untuk melakukan evaluasi terhadap peringatan-peringatan yang terjadi dan memastikan bahwa tindakan yang diambil tepat dan efektif dalam mencegah terjadinya peringatan yang sama di masa depan.

5.5 MENYUSUN PROSEDUR UNTUK MEMASTIKAN PENGGUNA SISTEM MENYADARI TANGGUNG JAWAB KEAMANAN MEREKA SEBELUM MEMBERIKAN AKSES KE SISTEM INFORMASI ORGANISASI

Langkah-langkah dalam menyusun prosedur untuk memastikan pengguna sistem menyadari tanggung jawab keamanan mereka sebelum diberikan akses ke sistem informasi organisasi antara lain:

1. Identifikasi risiko keamanan informasi yang berkaitan dengan sistem informasi organisasi dan informasikan kepada pengguna sistem.
2. Jelaskan kebijakan keamanan informasi organisasi kepada pengguna sistem, termasuk tentang tindakan yang harus dilakukan untuk menjaga keamanan informasi.
3. Sediakan panduan atau instruksi yang jelas tentang tindakan yang harus dilakukan oleh pengguna sistem untuk menjaga keamanan informasi.
4. Ajarkan pengguna sistem tentang tindakan yang harus dilakukan saat menghadapi situasi keamanan informasi yang tidak diinginkan, seperti kehilangan perangkat, serangan virus, atau upaya phishing.
5. Lakukan pelatihan secara berkala kepada pengguna sistem tentang kebijakan dan prosedur keamanan informasi organisasi, termasuk tentang penggunaan kata sandi yang aman.
6. Mintalah pengguna sistem untuk menandatangani pernyataan persetujuan yang menyatakan bahwa mereka telah memahami dan menyetujui kebijakan dan prosedur keamanan informasi organisasi sebelum diberikan akses ke sistem informasi organisasi.
7. Pantau dan evaluasi kepatuhan pengguna sistem terhadap kebijakan dan prosedur keamanan informasi organisasi secara berkala.

Contoh dokumen yang dapat digunakan untuk menyusun prosedur ini antara lain: kebijakan keamanan informasi organisasi, panduan penggunaan sistem informasi, formulir persetujuan keamanan informasi, dan laporan evaluasi kepatuhan pengguna sistem terhadap kebijakan keamanan informasi.

5.1. Prosedur tentang tanggung jawab keamanan bagi setiap pengguna telah disusun.

Berikut adalah contoh prosedur tentang tanggung jawab keamanan bagi tiap pengguna dalam sebuah organisasi:

1. Setiap pengguna wajib menjaga kerahasiaan username dan password mereka. Penggunaan akun oleh orang lain tidak diperbolehkan.
2. Pengguna harus melakukan penggantian password secara berkala dengan interval maksimal 90 hari sekali. Password harus terdiri dari kombinasi huruf, angka, dan karakter khusus serta memiliki panjang minimal 8 karakter.
3. Pengguna harus memastikan bahwa perangkat yang mereka gunakan untuk mengakses sistem informasi organisasi terlindungi oleh antivirus dan firewall yang terbaru. Perangkat harus diupdate secara berkala dengan patch terbaru untuk menghindari kerentanan keamanan.
4. Pengguna harus memastikan bahwa data yang mereka akses dan simpan di dalam sistem informasi organisasi tidak disebarkan kepada pihak yang tidak berwenang.
5. Pengguna tidak diperbolehkan mengakses sistem informasi organisasi menggunakan perangkat yang tidak sah atau tidak dikelola oleh organisasi.
6. Pengguna harus melaporkan setiap insiden keamanan yang mereka temukan dalam sistem informasi organisasi ke departemen keamanan informasi atau pihak yang bertanggung jawab atas keamanan informasi.
7. Setiap pengguna wajib memahami dan menaati kebijakan keamanan informasi organisasi.

Prosedur di atas harus dikomunikasikan secara jelas dan teratur kepada setiap pengguna dalam organisasi, baik melalui pelatihan, seminar, atau materi pelatihan lainnya. Selain itu, prosedur ini juga harus disematkan dalam kebijakan keamanan informasi organisasi dan setiap pengguna harus menandatanganinya sebagai bukti pemahaman dan kesediaan mereka untuk mematuhi prosedur tersebut.

5.2. Hasil audit/rekomendasi pelaksanaan pemberian akses ke pengguna.

Berikut ini adalah contoh hasil audit/rekomendasi pelaksanaan pemberian akses ke pengguna:

Setelah dilakukan audit keamanan sistem informasi, kami merekomendasikan beberapa perubahan dalam pelaksanaan pemberian akses ke pengguna. Beberapa rekomendasi kami adalah sebagai berikut:

1. Memastikan bahwa setiap pengguna memiliki hak akses sesuai dengan pekerjaannya dan tidak ada hak akses yang berlebihan atau tidak relevan dengan pekerjaannya.
2. Menetapkan prosedur untuk pemberian hak akses, termasuk pemeriksaan latar belakang, verifikasi identitas, dan persetujuan oleh atasan langsung.
3. Memperbarui dan mengelola daftar akun pengguna secara teratur, termasuk menghapus akun yang tidak aktif atau sudah tidak digunakan lagi.
4. Melakukan pelatihan keamanan informasi bagi pengguna sistem secara teratur, termasuk mengenai tanggung jawab keamanan masing-masing pengguna.
5. Memastikan bahwa pengguna sistem menyetujui kebijakan keamanan informasi organisasi sebelum diberikan akses ke sistem.

Kami menyarankan agar rekomendasi ini segera dilaksanakan untuk meningkatkan keamanan sistem informasi organisasi.

5.6 MELAKUKAN KONTROL DAN PENGAWASAN PADA SETIAP PENGGUNA YANG MEMILIKI AKSES KHUSUS MENJALANKAN FUNGSI KEAMANAN AGAR MENERIMA PELATIHAN KEAMANAN DASAR DAN BERKELANJUTAN SERTA MENDAPATKAN SERTIFIKASI YANG SESUAI UNTUK MELAKSANAKAN TUGAS KEAMANAN

Kontrol dan pengawasan pada setiap pengguna yang memiliki akses khusus menjalankan fungsi keamanan sangat penting untuk memastikan keamanan sistem informasi organisasi. Hal ini dapat dilakukan melalui beberapa langkah, antara lain:

1. Menyediakan pelatihan keamanan dasar dan berkelanjutan bagi setiap pengguna yang memiliki akses khusus menjalankan fungsi keamanan. Pelatihan ini dapat mencakup materi tentang praktik keamanan informasi, kebijakan dan prosedur keamanan organisasi, serta teknologi keamanan yang digunakan oleh organisasi.
2. Memberikan sertifikasi yang sesuai bagi setiap pengguna yang telah menerima pelatihan keamanan dasar dan berkelanjutan. Sertifikasi ini dapat menjadi bukti bahwa pengguna memiliki pemahaman yang memadai tentang keamanan informasi dan siap untuk melaksanakan tugas keamanan yang diamanahkan.
3. Melakukan pengawasan terhadap setiap pengguna yang memiliki akses khusus menjalankan fungsi keamanan. Pengawasan dapat dilakukan dengan memantau aktivitas pengguna, mengumpulkan catatan log, dan melakukan pemeriksaan berkala terhadap sistem keamanan organisasi.

4. Menegakkan disiplin dan tindakan hukuman bagi setiap pengguna yang melanggar kebijakan keamanan atau melakukan tindakan yang dapat membahayakan keamanan sistem informasi organisasi. Tindakan hukuman ini dapat berupa peringatan, pembatasan akses, atau bahkan pemutusan hubungan kerja.

Contoh hasil dari pelaksanaan kontrol dan pengawasan pada setiap pengguna yang memiliki akses khusus menjalankan fungsi keamanan adalah meningkatnya kesadaran dan keterampilan keamanan informasi di kalangan pengguna, peningkatan keamanan sistem informasi organisasi, serta pengurangan risiko keamanan yang dapat membahayakan organisasi.

6.1. **Pelatihan keamanan dasar dan berkelanjutan dilaksanakan untuk SDM yang memiliki akses khusus menjalankan fungsi keamanan.**

Pelatihan keamanan dasar dan berkelanjutan sangat penting dilaksanakan untuk SDM yang memiliki akses khusus menjalankan fungsi keamanan. Berikut ini adalah contoh prosedur pelaksanaan pelatihan keamanan dasar dan berkelanjutan:

1. Identifikasi SDM yang memiliki akses khusus menjalankan fungsi keamanan.
2. Tentukan materi pelatihan keamanan dasar dan berkelanjutan yang sesuai dengan kebutuhan dan tugas masing-masing SDM.
3. Siapkan jadwal pelatihan yang memungkinkan setiap SDM untuk mengikuti pelatihan.
4. Lakukan pelatihan keamanan dasar dan berkelanjutan, baik secara online maupun offline, dengan melibatkan narasumber yang ahli dalam bidang keamanan.
5. Evaluasi hasil pelatihan dan berikan sertifikasi yang sesuai dengan kinerja masing-masing SDM.
6. Lakukan pemantauan dan evaluasi secara berkala untuk memastikan bahwa SDM yang memiliki akses khusus menjalankan fungsi keamanan telah menerapkan pelatihan keamanan dasar dan berkelanjutan dalam tugas mereka secara efektif.
7. Pastikan bahwa SDM yang memiliki akses khusus menjalankan fungsi keamanan selalu diberikan pelatihan keamanan yang sesuai dengan perkembangan teknologi informasi dan kebutuhan organisasi.

Berikut adalah contoh pelatihan keamanan dasar dan berkelanjutan:

Pelatihan Keamanan Dasar:

1. Pengenalan tentang keamanan informasi dan peranannya dalam organisasi.
2. Jenis-jenis ancaman keamanan dan cara menghadapinya.
3. Pengenalan tentang enkripsi dan dekripsi.
4. Penggunaan password yang aman.
5. Penggunaan firewall dan antivirus.

Pelatihan Keamanan Berkelanjutan:

1. Mempelajari teknologi keamanan terbaru.
2. Pelatihan keterampilan keamanan seperti penanganan insiden keamanan dan investigasi keamanan.
3. Pemantauan dan evaluasi sistem keamanan organisasi.
4. Memahami dan mematuhi kebijakan keamanan organisasi.
5. Pelatihan dalam bidang keamanan khusus seperti keamanan jaringan, keamanan web, dan keamanan aplikasi.

6.2. **Sertifikasi keamanan yang dikeluarkan oleh badan/lembaga terkait dimiliki oleh SDM yang memiliki akses khusus menjalankan fungsi keamanan**

Contoh Sertifikasi keamanan yang dikeluarkan oleh badan/lembaga terkait dapat meliputi:

- Certified Information Systems Security Professional (CISSP) dari International Information System Security Certification Consortium (ISC)2
- Certified Information Security Manager (CISM) dari Information Systems Audit and Control Association (ISACA)
- CompTIA Security+ dari CompTIA
- Certified Ethical Hacker (CEH) dari International Council of Electronic Commerce Consultants (EC-Council)

Sertifikasi tersebut menunjukkan bahwa SDM yang memiliki akses khusus dalam menjalankan fungsi keamanan telah memenuhi standar pengetahuan dan keterampilan yang diakui secara internasional dalam bidang keamanan informasi.

Latihan Praktikum :

1. bagaimana membuat hak akses di db mysql ?
   Jawaban :

   Untuk membuat hak akses di MySQL, Anda perlu melakukan beberapa langkah sebagai berikut:
   1. Masuk ke dalam MySQL dengan menggunakan akun root.
   2. Buat sebuah user baru dengan perintah CREATE USER.
   3. Atur password untuk user baru tersebut dengan perintah SET PASSWORD.
   4. Berikan hak akses pada user tersebut dengan perintah GRANT.
   5. Pastikan untuk menyimpan perubahan dengan perintah FLUSH PRIVILEGES.

   Berikut adalah contoh perintah SQL yang dapat digunakan untuk membuat hak akses pada database "nama_database" untuk user "nama_user" dengan password "password_user" dan hak akses "SELECT", "INSERT", "UPDATE", dan "DELETE":

   ```
   CREATE USER 'nama_user'@'localhost' IDENTIFIED BY 'password_user';
   GRANT SELECT, INSERT, UPDATE, DELETE ON nama_database.* TO
   'nama_user'@'localhost';
   FLUSH PRIVILEGES;
   ```

   Perintah di atas akan membuat user baru dengan nama "nama_user" dan password "password_user", dan memberikan hak akses "SELECT", "INSERT", "UPDATE", dan "DELETE" pada database "nama_database". Anda dapat mengubah perintah tersebut sesuai dengan kebutuhan Anda.

2. Akses SSH Server menggunakan Kunci Publik dan Private ?
   Jawaban :

   Untuk menerapkan akses SSH ke server menggunakan kunci publik dan kunci privat, ikuti langkah-langkah berikut:
   1. Buat kunci publik dan kunci privat di komputer lokal Anda dengan menggunakan perintah "ssh-keygen" pada terminal. Anda dapat menggunakan algoritma enkripsi RSA atau Ed25519.

      ```
      ssh-keygen -t rsa -b 4096 -C "email@example.com"
      ```

Perintah di atas akan membuat kunci publik dan kunci privat dengan panjang bit 4096 menggunakan algoritma RSA, dan email Anda sebagai label. Jika Anda ingin menggunakan algoritma Ed25519, ganti "-t rsa" menjadi "-t ed25519".

2. Salin kunci publik Anda ke server dengan perintah "ssh-copy-id". Masukkan password untuk akun Anda pada server jika diminta.

```
ssh-copy-id username@server-ip
```

Perintah di atas akan menyalin kunci publik Anda ke server dan menambahkannya ke file authorized_keys.

3. Sekarang, coba masuk ke server dengan menggunakan kunci privat. Gunakan perintah "ssh" dan tambahkan argumen "-i" untuk menentukan lokasi kunci privat.

```
ssh -i /path/to/private/key username@server-ip
```

Perintah di atas akan membuka koneksi SSH ke server menggunakan kunci privat yang telah Anda buat.

4. Jika koneksi SSH berhasil, Anda dapat mengonfigurasi server untuk hanya menerima koneksi SSH dengan kunci publik dan kunci privat dengan mengedit file konfigurasi SSH pada server.

```
sudo nano /etc/ssh/sshd_config
```

Pastikan baris berikut tidak di-comment dan bernilai "yes":

```
PubkeyAuthentication yes
```

Setelah itu, simpan dan keluar dari file konfigurasi SSH, dan jalankan perintah "sudo systemctl restart sshd" untuk memulai ulang layanan SSH.

Sekarang Anda sudah dapat masuk ke server menggunakan kunci publik dan kunci privat tanpa memasukkan password. Pastikan untuk menjaga kunci privat Anda dengan aman, karena orang lain dapat menggunakan kunci privat Anda untuk masuk ke server tanpa memasukkan password.

3. Instalasi password manager dan bagaimana cara menggunakannya ?
Jawaban :

Ada banyak aplikasi manajemen kata sandi yang tersedia di pasar, di antaranya:

1. LastPass
2. 1Password
3. Dashlane

4. Keeper
5. Bitwarden

Berikut adalah contoh penggunaan LastPass, salah satu aplikasi manajemen kata sandi populer:

1. Unduh dan instal aplikasi LastPass pada perangkat Anda.
2. Buat akun LastPass dengan menggunakan email dan password yang kuat.
3. Setelah berhasil masuk, LastPass akan meminta Anda untuk menambahkan password yang sudah ada dan menyimpannya ke dalam aplikasi. Anda juga dapat membuat password baru melalui aplikasi dan menyimpannya secara otomatis.
4. LastPass akan mengenkripsi semua password Anda dan menyimpannya di cloud. Anda dapat mengakses password Anda dari perangkat mana saja dengan masuk ke akun LastPass Anda.
5. Anda dapat menggunakan LastPass untuk memasukkan password secara otomatis pada situs web dan aplikasi yang terhubung dengan LastPass. LastPass juga dapat menghasilkan kata sandi yang kuat secara otomatis untuk akun baru yang Anda buat.
6. LastPass juga dapat digunakan untuk menyimpan catatan penting, seperti nomor kartu kredit atau nomor paspor.
7. LastPass juga memiliki fitur keamanan tambahan, seperti dua faktor otentikasi, yang memerlukan kode unik saat Anda login ke LastPass dari perangkat baru.

Dalam penggunaan LastPass, pastikan untuk mengaktifkan dua faktor otentikasi dan memilih password yang kuat dan unik untuk akun LastPass Anda. Selain itu, jangan gunakan password yang sama untuk akun lain dan pastikan untuk memperbarui password secara berkala.

4. Bagaimana melakukan pembatasan akses hanya read di db mysql?
   Jawaban :
   Anda dapat membuat pengguna dengan hak akses "read-only" di MySQL dengan cara berikut:
   1. Login ke MySQL dengan akun root atau dengan akun pengguna yang memiliki hak akses untuk mengelola pengguna.
   2. Buat pengguna baru dengan perintah SQL berikut:

```
CREATE USER 'nama_pengguna'@'localhost' IDENTIFIED BY 'password_baru';
```

      Ganti 'nama_pengguna' dengan nama pengguna baru yang ingin Anda buat, dan 'password_baru' dengan password yang kuat.

   3. Berikan hak akses hanya untuk membaca data pada database tertentu dengan perintah SQL berikut:

```
GRANT SELECT ON nama_database.* TO 'nama_pengguna'@'localhost';
```

      Ganti 'nama_database' dengan nama database yang ingin Anda berikan hak akses "read-only", dan 'nama_pengguna' dengan nama pengguna yang baru Anda buat.

4. Anda dapat mengulangi langkah 3 untuk setiap database yang ingin diberikan hak akses "read-only".
5. Terakhir, simpan perubahan hak akses dengan perintah SQL berikut:

```
FLUSH PRIVILEGES;
```

Dengan mengikuti langkah-langkah di atas, pengguna baru yang dibuat hanya memiliki hak akses untuk membaca data di database yang telah ditentukan. Pengguna ini tidak dapat membuat, mengubah, atau menghapus data di database.

5. Bagaimana melakukan instalasi dan menggunakan gpg
Jawaban :

GPG (GNU Privacy Guard) adalah salah satu aplikasi enkripsi open source yang digunakan untuk mengenkripsi dan memverifikasi data. Berikut adalah langkah-langkah untuk menginstal dan menggunakan GPG:

Instalasi GPG:

1. Download GPG dari situs web resmi (https://gnupg.org/download/index.html) sesuai dengan sistem operasi Anda.
2. Ikuti petunjuk instalasi hingga selesai.
3. Setelah selesai instalasi, buka terminal atau command prompt.

Menggunakan GPG:

1. Buat kunci publik dan kunci privat menggunakan perintah: **gpg --gen-key**.
2. Ikuti instruksi untuk membuat kunci publik dan kunci privat Anda.
3. Setelah membuat kunci publik dan kunci privat, Anda dapat mengirimkan kunci publik Anda ke pihak lain untuk memverifikasi tanda tangan digital Anda.
4. Untuk mengenkripsi sebuah file, gunakan perintah: **gpg -e -r <nama pengguna> <nama file>**. Perintah ini akan mengenkripsi file menggunakan kunci publik pengguna yang ditentukan.
5. Untuk mendekripsi sebuah file yang telah dienkripsi, gunakan perintah: **gpg -d <nama file>.gpg**. Perintah ini akan meminta Anda memasukkan kata sandi untuk membuka file yang telah dienkripsi.
6. Anda juga dapat menandatangani sebuah file dengan menggunakan perintah: **gpg --sign <nama file>**. Perintah ini akan menandatangani file menggunakan kunci privat Anda.
7. Untuk memverifikasi sebuah tanda tangan digital pada sebuah file, gunakan perintah: **gpg --verify <nama file>.asc**. Perintah ini akan memverifikasi tanda tangan digital menggunakan kunci publik dari pengguna yang menandatangani file tersebut.

Pastikan untuk menjaga kunci privat Anda dengan aman, karena kunci privat adalah kunci untuk mengakses data yang telah dienkripsi dengan kunci publik Anda. Dengan mengikuti langkah-langkah ini, Anda dapat menginstal dan menggunakan GPG dengan aman dan efektif.

A. Pengetahuan yang diperlukan untuk menerapkan Kontrol akses berdasarkan konsep metodologi yang telah diterapkan

1. Model Keamanan: Anda harus memahami model keamanan yang digunakan dalam organisasi Anda, seperti model keamanan Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC), atau Attribute-Based Access Control (ABAC). Anda harus memahami kelebihan dan kelemahan dari masing-masing model keamanan ini dan memilih model keamanan yang tepat untuk organisasi Anda.
2. Identitas Pengguna: Anda harus memahami cara mengelola identitas pengguna, seperti cara membuat, mengubah, dan menghapus akun pengguna, serta cara menetapkan hak akses kepada pengguna berdasarkan peran atau pekerjaan mereka. Anda juga harus memahami cara mengotentikasi pengguna, seperti dengan menggunakan password atau metode otentikasi lainnya seperti kunci publik atau kartu pintar.
3. Kebijakan Akses: Anda harus memahami kebijakan akses organisasi Anda, seperti kebijakan password, kebijakan penggunaan internet, kebijakan privasi, dan kebijakan penggunaan perangkat seluler. Anda harus memastikan bahwa kebijakan ini diterapkan dengan benar dan bahwa pengguna mengetahuinya.
4. Sistem Manajemen Akses: Anda harus memahami sistem manajemen akses yang digunakan dalam organisasi Anda, seperti cara memberikan hak akses pada suatu file atau folder pada sistem operasi, cara mengkonfigurasi firewall untuk membatasi akses ke jaringan, dan cara mengelola hak akses pada database.
5. Audit: Anda harus memahami cara melakukan audit dan pemantauan sistem untuk memastikan bahwa hak akses dan kebijakan keamanan organisasi Anda telah diterapkan dengan benar. Anda juga harus memahami cara melaporkan pelanggaran keamanan dan cara menangani pelanggaran tersebut.
6. Dengan memahami konsep-konsep di atas, Anda dapat menerapkan kontrol akses dengan lebih efektif dan memastikan bahwa sistem keamanan organisasi Anda terlindungi dari ancaman keamanan.

B. Keterampilan yang diperlukan untuk menerapkan Kontrol akses berdasarkan konsep metodologi yang telah diterapkan

1. Untuk menerapkan kontrol akses berdasarkan konsep metodologi yang telah diterapkan, diperlukan keterampilan-keterampilan sebagai berikut:
2. Pengetahuan tentang model keamanan: Anda perlu memahami model keamanan yang tersedia seperti Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC), dan Attribute-Based Access Control (ABAC) dan kelebihan dan kelemahan masing-masing.
3. Pengetahuan tentang protokol keamanan: Anda perlu memahami protokol keamanan seperti Transport Layer Security (TLS), Secure Shell (SSH), dan Virtual Private Network

(VPN) dan bagaimana mengkonfigurasinya untuk melindungi data dan akses dari pengguna yang tidak sah.

4. Kemampuan administrasi sistem operasi: Anda perlu menguasai administrasi sistem operasi seperti Windows dan Linux, termasuk pengaturan hak akses, pembatasan akses, manajemen pengguna, dan konfigurasi keamanan.
5. Kemampuan administrasi basis data: Jika Anda bekerja dengan basis data, Anda perlu menguasai administrasi basis data seperti MySQL, Oracle, dan SQL Server, termasuk pengaturan hak akses, pembatasan akses, manajemen pengguna, dan konfigurasi keamanan.
6. Kemampuan programming: Jika Anda membangun aplikasi atau sistem keamanan, Anda perlu menguasai pemrograman untuk membangun fungsi keamanan seperti autentikasi dan otorisasi.
7. Kemampuan analisis risiko: Anda perlu mampu menganalisis risiko keamanan dan mengembangkan rencana mitigasi untuk mengatasi potensi ancaman keamanan.
8. Kemampuan manajemen proyek: Anda perlu mampu mengelola proyek keamanan, termasuk merencanakan, mengatur anggaran, mengawasi proyek, dan melaporkan kemajuan proyek kepada pemangku kepentingan.

Dengan menguasai keterampilan-keterampilan di atas, Anda dapat menerapkan kontrol akses berdasarkan konsep metodologi yang telah diterapkan dengan efektif dan efisien.

C. Sikap Kerja yang diperlukan dalam menerapkan Kontrol akses berdasarkan konsep metodologi yang telah diterapkan

1. Kepatuhan: Anda harus memiliki sikap patuh terhadap aturan dan kebijakan keamanan yang telah ditetapkan. Anda harus mematuhi prosedur keamanan yang ada dan menjaga kerahasiaan informasi penting.
2. Disiplin: Anda harus disiplin dalam mengelola akses dan memberikan izin kepada pengguna. Anda harus mengatur waktu dengan efektif dan memastikan bahwa tugas-tugas keamanan diprioritaskan dengan benar.
3. Kewaspadaan: Anda harus selalu waspada terhadap potensi ancaman keamanan dan memiliki keahlian dalam mengidentifikasi ancaman serta cara-cara melindungi sistem dan data dari serangan.
4. Kolaborasi: Anda harus memiliki kemampuan untuk bekerja sama dengan tim keamanan dan departemen IT lainnya untuk memastikan bahwa kebijakan keamanan yang telah ditetapkan diikuti dengan benar dan sistem keamanan bekerja dengan baik.

5. Kemampuan belajar: Anda harus terus belajar dan meningkatkan pengetahuan dan keterampilan keamanan untuk dapat memenuhi tantangan keamanan yang semakin kompleks dan terus berkembang.
6. Tanggung jawab: Anda harus memiliki rasa tanggung jawab terhadap sistem keamanan dan melindungi data sensitif dan privasi pengguna dengan cara yang efektif dan aman.
7. Etika: Anda harus memegang prinsip etika dalam pekerjaan Anda, termasuk menjaga kerahasiaan informasi dan tidak menyalahgunakan hak akses yang Anda miliki. Anda harus bertindak secara profesional dan berintegritas dalam menjalankan tugas keamanan.

Tugas Dan Proyek Pelatihan
1. Kerjakan Soal dan praktikum lab

Link Referensi Modul Ketiga
1. Video Pembelajaran 2. E-book 3. Link Youtube/Website rujukan

Link Pertanyaan Modul Ketiga
https://app.sli.do/ (bisa mengunakan aplikasi ini)

Bahan Tayang
Bisa berupa Link/ Screen Capture Slide pelatihan

Link room Pelatihan dan Jadwal live sesi bersama instruktur
Zoom, Meets

Penilaian

Komposisi penilaian Kuis 1 Mengumpulkan data: Nilai 10 (Range 0 -10)

Target Penyelesaian Modul Ketiga
1hari/sampai 6 JP

KOMINFO digitalent

VSGA Vocational School Graduate Academy

2023

#JadiJagoanDigital

digitalent.kominfo.go.id