Copyright © September 2023

CYBERSECURITY MASA DEPAN KITA

PERTEMUAN 5

Bab ini membahas masalah hukum dan etika yang muncul saat bekerja di keamanan siber. Ini juga membahas jalur pendidikan dan karir untuk keamanan siber. Ada jalur pendidikan menuju sertifikasi yang mungkin ingin Anda kejar dengan Cisco Networking Academy. Beberapa dari sertifikasi ini merupakan prasyarat untuk Sertifikat Spesialisasi di banyak bidang jaringan, termasuk keamanan siber. Halaman Jembatan Bakat Akademi Jaringan (netacad.com di bawah Sumberdaya) memberikan informasi yang baik untuk membantu Anda menulis resume yang bagus dan mempersiapkan diri untuk wawancara kerja. Ini juga berisi daftar untuk pekerjaan Cisco dan Mitra Cisco. Tiga mesin pencari pekerjaan Internet eksternal disajikan untuk Anda jelajahi.

1.1. HUKUM DAN ETIKA CYBERSECURITY, PENDIDIKAN DAN KARIR

1.1.1. Masalah Hukum dan Etika dalam Karir Cybersecurity

1. Masalah Hukum Dalam Keamanan Cyber

Profesional keamanan siber harus memiliki keterampilan yang sama dengan peretas, terutama peretas topi hitam, untuk melindungi dari serangan. Satu perbedaan antara peretas dan profesional keamanan siber adalah bahwa profesional keamanan siber harus bekerja dalam batasan hukum.

a. Masalah Hukum Pribadi

Anda bahkan tidak perlu menjadi karyawan untuk tunduk pada undang-undang keamanan siber. Dalam kehidupan pribadi Anda, Anda mungkin memiliki kesempatan dan keterampilan untuk meretas komputer atau jaringan orang lain. Ada pepatah lama,

Copyright © September 2023

"Just because you can does not mean you should." Ingatlah ini. Sebagian besar peretas meninggalkan jejak, baik disadari atau tidak, dan jejak ini dapat diikuti kembali ke peretas. Profesional keamanan siber mengembangkan banyak keterampilan yang dapat digunakan untuk kebaikan atau kejahatan. Mereka yang menggunakan keahlian mereka dalam sistem hukum, untuk melindungi infrastruktur, jaringan, dan privasi selalu sangat dibutuhkan.

b. Masalah Hukum Perusahaan

Sebagian besar negara memiliki beberapa undang-undang keamanan siber. Mereka mungkin ada hubungannya dengan infrastruktur penting, jaringan, dan privasi perusahaan dan individu. Bisnis diwajibkan untuk mematuhi undang-undang ini. Dalam beberapa kasus, jika Anda melanggar undang-undang keamanan siber saat melakukan pekerjaan Anda, perusahaanlah yang mungkin dihukum dan Anda bisa kehilangan pekerjaan. Dalam kasus lain, Anda bisa dituntut, didenda, dan mungkin dihukum. Secara umum, jika Anda bingung apakah suatu tindakan atau perilaku mungkin ilegal, anggap itu ilegal dan jangan lakukan. Perusahaan Anda mungkin memiliki departemen hukum atau seseorang di departemen sumber daya manusia yang dapat menjawab pertanyaan Anda sebelum Anda melakukan sesuatu yang ilegal.

c. Hukum Internasional dan Keamanan Siber

Bidang hukum keamanan siber jauh lebih baru daripada keamanan siber itu sendiri. Seperti disebutkan sebelumnya, sebagian besar negara memiliki beberapa undang-undang, dan akan ada lebih banyak undang-undang yang akan datang.

Copyright © September 2023

2. Etika dalam Cybersecurity

Selain bekerja dalam batas-batas hukum, profesional keamanan siber juga harus menunjukkan perilaku etis.

a. Masalah Etika Pribadi

Seseorang dapat bertindak tidak etis dan tidak dapat dituntut, didenda, atau dipenjara. Ini karena tindakan tersebut mungkin secara teknis tidak ilegal. Namun bukan berarti perilaku tersebut dapat diterima. Perilaku etis cukup mudah dipastikan. Mustahil untuk membuat daftar semua berbagai perilaku tidak etis yang dapat ditunjukkan oleh seseorang dengan keterampilan keamanan siber. Di bawah ini hanya dua. Bertanya pada diri sendiri:

- Apakah saya ingin mengetahui bahwa seseorang telah meretas komputer saya dan mengubah gambar di situs jejaring sosial saya?
- Apakah saya ingin mengetahui bahwa teknisi TI yang saya percayai untuk memperbaiki jaringan saya, memberi tahu rekan informasi pribadi tentang saya yang diperoleh saat bekerja di jaringan saya?

Jika jawaban Anda untuk salah satu pertanyaan ini adalah 'tidak', maka jangan lakukan hal seperti itu kepada orang lain.

b. Masalah Etika Perusahaan

Etika adalah kode perilaku yang kadang-kadang ditegakkan oleh hukum. Ada banyak area dalam keamanan siber yang tidak tercakup dalam undang-undang. Ini berarti

Copyright © September 2023

bahwa melakukan sesuatu yang secara teknis legal belum tentu merupakan hal yang etis untuk dilakukan. Karena begitu banyak bidang keamanan siber yang tidak (atau belum) dicakup oleh undang-undang, banyak organisasi profesional TI telah menciptakan kode etik untuk orang-orang di industri. Di bawah ini adalah daftar tiga organisasi dengan Kode Etik:

- CyberSecurity Institute (CSI) telah menerbitkan kode etik
- Information Systems Security Association (ISSA) memiliki kode etik
- Association of Information Technology Professionals (AITP) memiliki kode etik dan standar perilaku

3. Pekerjaan Cybersecurity

Banyak bisnis dan industri lain mempekerjakan profesional keamanan siber. Ada beberapa mesin pencari online untuk membantu Anda menemukan pekerjaan yang tepat di bidang keamanan siber:

- ITJobMatch –Mesin pencari ITJobMatch mengkhususkan diri dalam segala jenis pekerjaan TI, di seluruh dunia.
- Monster –Monster adalah mesin pencari untuk semua jenis pekerjaan. Tautan yang diberikan langsung menuju ke pekerjaan keamanan siber.
- CareerBuilder –CareerBuilder juga merupakan mesin pencari untuk semua jenis pekerjaan. Tautan yang diberikan langsung menuju ke pekerjaan keamanan siber.

Copyright © September 2023

1.2. Seni dalam Menjaga Kerahasiaan

Prinsip-prinsip kriptologi menjelaskan bagaimana protokol dan algoritma modern mengamankan komunikasi. Kriptologi adalah ilmu membuat dan memecahkan kode rahasia. Pengembangan dan penggunaan kode adalah kriptografi. Mempelajari dan memecahkan kode adalah kriptanalisis. Masyarakat telah menggunakan kriptografi selama berabad-abad untuk melindungi dokumen rahasia. Misalnya, Julius Caesar menggunakan sandi alfabet sederhana untuk mengenkripsi pesan ke jenderalnya di lapangan. Jenderalnya akan memiliki pengetahuan tentang kunci sandi yang diperlukan untuk mendekripsi pesan. Saat ini, metode kriptografi modern memastikan komunikasi yang aman. Kontrol akses adalah, seperti namanya, cara mengontrol akses ke gedung, ruangan, sistem, database, file, dan informasi. Organisasi menggunakan berbagai teknik kontrol akses untuk melindungi kerahasiaan. Bab ini akan membahas empat langkah dalam proses kontrol akses: 1) identifikasi, 2) otentikasi, 3) otorisasi, dan 4) akuntabilitas. Selain itu, bab ini menjelaskan berbagai model kontrol akses dan jenis kontrol akses. Bab ini diakhiri dengan membahas berbagai cara pengguna menyembunyikan data. Data obfuscation dan steganography adalah dua teknik yang digunakan untuk menyelesaikan data masking.

1.2.1. Kriptografi

1. Padangan Umum Kriptobrafi

Copyright © September 2023

Kriptologi adalah ilmu membuat dan memecahkan kode rahasia. Kriptografi adalah cara menyimpan dan mengirimkan data sehingga hanya penerima yang dituju yang dapat membaca atau memprosesnya. Kriptografi modern menggunakan algoritma komputasi yang aman untuk memastikan bahwa penjahat cyber tidak dapat dengan mudah mengkompromikan informasi yang dilindungi. Kerahasiaan data memastikan privasi sehingga hanya penerima yang dituju yang dapat membaca pesan. Pihak mencapai ini melalui enkripsi. Enkripsi adalah proses mengacak data sehingga pihak yang tidak berhak tidak dapat dengan mudah membacanya. Saat mengaktifkan enkripsi, data yang dapat dibaca adalah plaintext, atau cleartext, sedangkan versi terenkripsi adalah teks terenkripsi atau ciphertext. Enkripsi mengubah pesan teks biasa yang dapat dibaca menjadi teks sandi, yang merupakan pesan tersamar yang tidak dapat dibaca. Dekripsi membalikkan proses. Enkripsi juga memerlukan kunci, yang memainkan peran penting dalam mengenkripsi dan mendekripsi pesan. Orang yang memiliki kunci dapat mendekripsi ciphertext menjadi plaintext. Secara historis, pihak telah menggunakan berbagai algoritma dan metode enkripsi. Algoritma adalah proses atau rumus yang digunakan untuk memecahkan suatu masalah. Julius Caesar dikatakan telah mengamankan pesan dengan meletakkan dua set alfabet, berdampingan, dan kemudian menggeser salah satunya dengan sejumlah tempat tertentu. Jumlah tempat dalam shift berfungsi sebagai kuncinya. Dia mengubah plaintext menjadi ciphertext menggunakan kunci ini, dan hanya jenderalnya, yang juga memiliki kunci tersebut, yang tahu cara menguraikan pesan. Metode ini adalah sandi Caesar. Angka tersebut menunjukkan pesan rahasia menggunakan sandi Caesar.

Sejarah kriptografi dimulai dalam lingkaran diplomatik ribuan tahun yang lalu. Utusan dari istana raja membawa pesan terenkripsi ke pengadilan lain. Kadang-kadang, pengadilan lain yang tidak terlibat dalam komunikasi, berusaha mencuri pesan yang dikirim ke kerajaan yang mereka

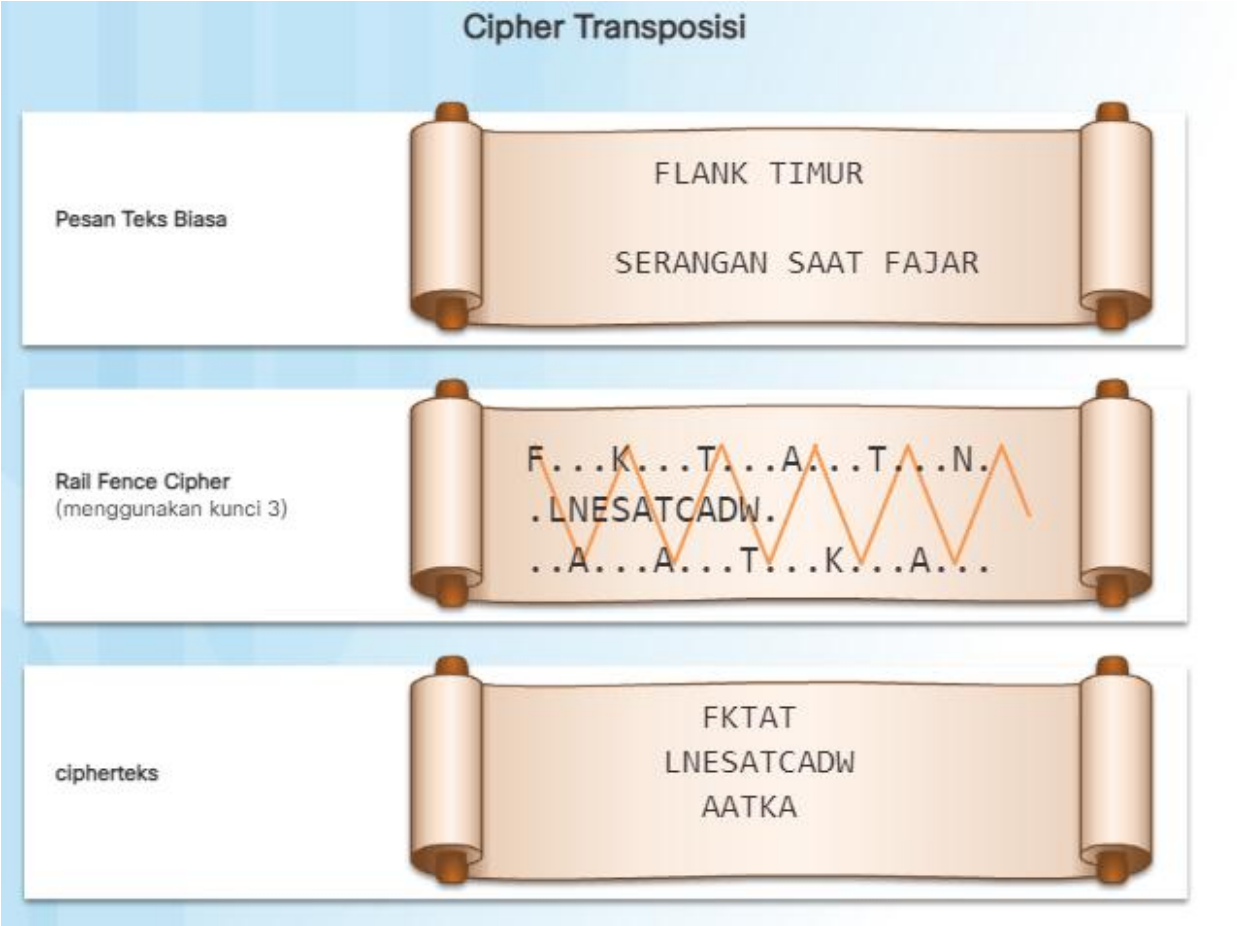
Copyright © September 2023

anggap musuh. Tidak lama kemudian, komandan militer mulai menggunakan enkripsi untuk mengamankan pesan. Selama berabad-abad, berbagai metode sandi, perangkat fisik, dan bantuan teks terenkripsi dan dekripsi , Semua metode cipher menggunakan kunci untuk mengenkripsi atau mendekripsi pesan. Kunci merupakan komponen penting dalam algoritma enkripsi. Sebuah algoritma enkripsi hanya sebaik kunci yang digunakan. Semakin banyak kompleksitas yang terlibat, semakin aman algoritmanya. Manajemen kunci adalah bagian penting dalam proses.

MEMBUAT CIPHERTEXT

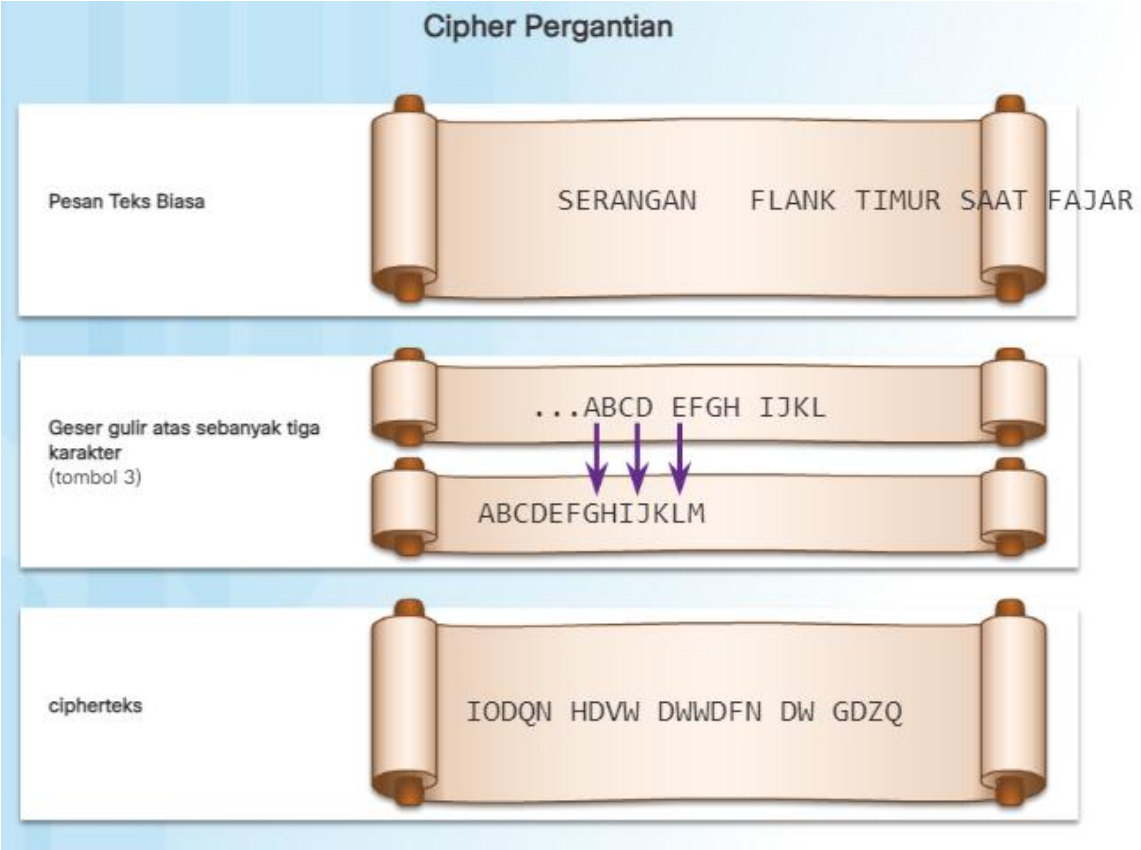
Setiap metode enkripsi menggunakan algoritma tertentu, yang disebut cipher, untuk mengenkripsi dan mendekripsi pesan. Cipher adalah serangkaian langkah yang terdefinisi dengan baik yang digunakan untuk mengenkripsi dan mendekripsi pesan. Ada beberapa metode untuk membuat ciphertext:

- Transposisi – huruf disusun ulang (Gambar 1)



Gambar 1. Transposisi

- Substitusi – huruf diganti (Gambar 2)



Gambar 2. Cipher substitusi

- One-time pad – plaintext yang digabungkan dengan kunci rahasia menciptakan karakter baru, yang kemudian digabungkan dengan plaintext untuk menghasilkan ciphertext (Gambar 3)

Gambar 3. One Time pad

DUA JENIS ENKRIPSI

Enkripsi kriptografi dapat memberikan kerahasiaan dengan menggabungkan berbagai alat dan protokol. Ada dua pendekatan untuk memastikan keamanan data saat menggunakan enkripsi. Yang pertama adalah untuk melindungi algoritma. Jika keamanan sistem enkripsi bergantung pada kerahasiaan algoritme itu sendiri, aspek terpenting adalah menjaga algoritme dengan cara apa pun. Setiap kali seseorang mengetahui detail algoritme, setiap pihak yang terlibat perlu mengubah algoritme. Pendekatan itu tidak terdengar sangat aman atau mudah dikelola. Pendekatan kedua adalah untuk melindungi kunci. Dengan kriptografi modern, algoritme bersifat publik. Kunci kriptografi memastikan kerahasiaan data. Kunci kriptografi adalah kata sandi yang

Copyright © September 2023

merupakan bagian dari input ke dalam algoritma enkripsi bersama dengan data yang membutuhkan enkripsi. Ada dua kelas algoritma enkripsi:

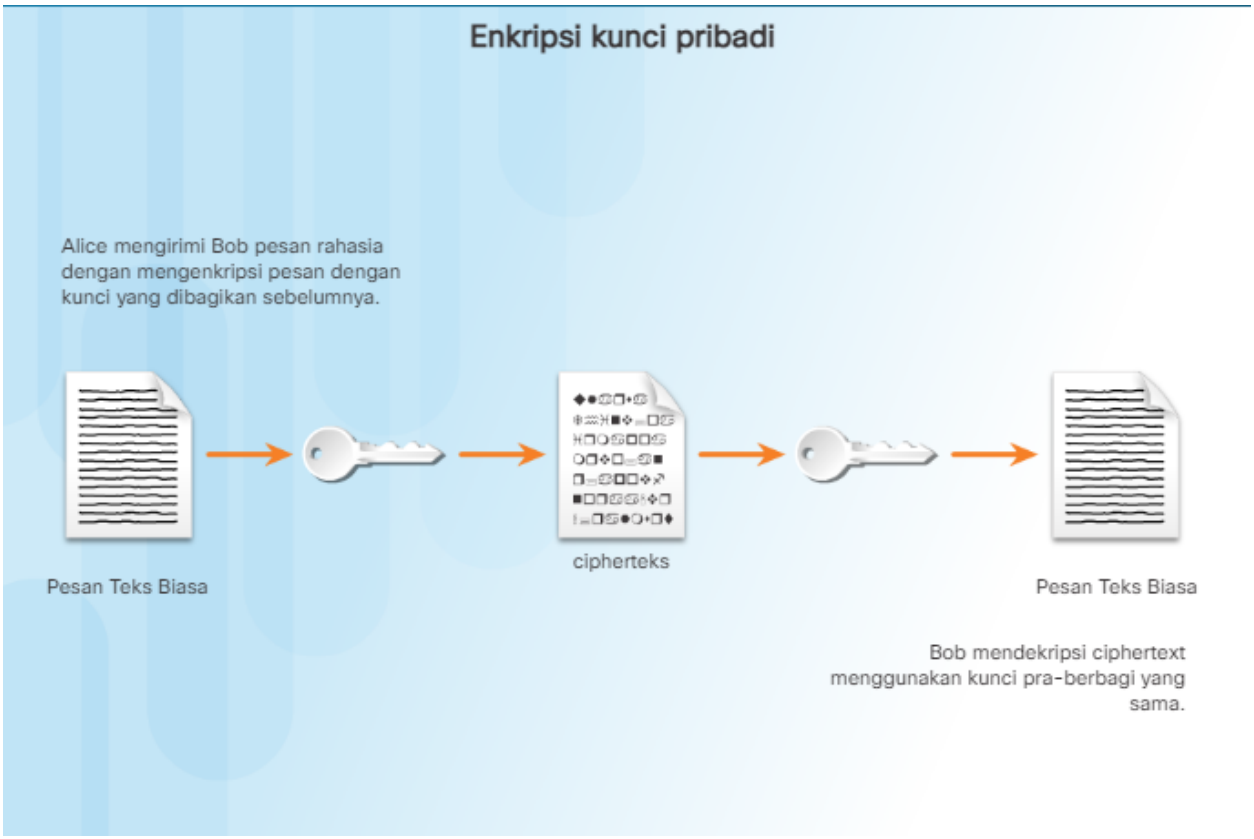
- Algoritme simetris - Algoritme ini menggunakan kunci yang dibagikan sebelumnya yang sama, terkadang disebut pasangan kunci rahasia, untuk mengenkripsi dan mendekripsi data. Baik pengirim dan penerima mengetahui kunci yang dibagikan sebelumnya sebelum komunikasi terenkripsi dimulai. Seperti yang ditunjukkan pada Gambar 1, algoritma simetris menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi plaintext. Algoritma enkripsi yang menggunakan kunci umum lebih sederhana dan membutuhkan lebih sedikit daya komputasi.
- Algoritma asimetris - Algoritma enkripsi asimetris menggunakan satu kunci untuk mengenkripsi data dan kunci yang berbeda untuk mendekripsi data. Satu kunci bersifat publik dan yang lainnya bersifat pribadi. Dalam sistem enkripsi kunci publik, setiap orang dapat mengenkripsi pesan menggunakan kunci publik penerima, dan penerima adalah satu-satunya yang dapat mendekripsi menggunakan kunci pribadinya. Pihak bertukar pesan aman tanpa memerlukan kunci yang dibagikan sebelumnya, seperti yang ditunjukkan pada Gambar 2. Algoritma asimetris lebih kompleks. Algoritma ini intensif sumber daya dan lebih lambat untuk dieksekusi.

A. Enkripsi Kunci Pribadi

PROSES ENKRIPSI SIMETRIS

Algoritme simetris menggunakan kunci yang dibagikan sebelumnya yang sama untuk mengenkripsi dan mendekripsi data, metode yang juga dikenal sebagai enkripsi kunci pribadi. Misalnya, Alice dan Bob tinggal di lokasi yang berbeda dan ingin bertukar pesan rahasia satu sama lain melalui sistem surat. Alice ingin mengirim pesan rahasia ke Bob. Enkripsi kunci

pribadi menggunakan algoritma simetris. Seperti yang diilustrasikan oleh kunci pada gambar, Alice dan Bob memiliki kunci yang identik untuk satu gembok. Pertukaran kunci terjadi sebelum mengirim pesan rahasia apa pun. Alice menulis pesan rahasia dan memasukkannya ke dalam kotak kecil yang dia kunci menggunakan gembok. Dia mengirimkan kotak itu ke Bob. Pesan itu aman di dalam kotak karena kotak itu melewati sistem kantor pos. Ketika Bob menerima kotak itu, dia menggunakan kuncinya untuk membuka gembok dan mengambil pesannya. Bob dapat menggunakan kotak dan gembok yang sama untuk mengirim balasan rahasia kembali ke Alice. Jika Bob ingin berbicara dengan Carol, dia memerlukan kunci pra-berbagi baru untuk komunikasi itu untuk merahasiakannya dari Alice. Semakin banyak orang yang ingin diajak berkomunikasi dengan aman oleh Bob, semakin banyak kunci yang perlu dia kelola.



Gambar 4. Proses Enkripsi

Copyright © September 2023

JENIS KRIPTOGRAFI

Jenis kriptografi yang paling umum adalah block cipher dan stream cipher. Setiap metode berbeda dalam cara mengelompokkan bit data untuk mengenkripsinya.

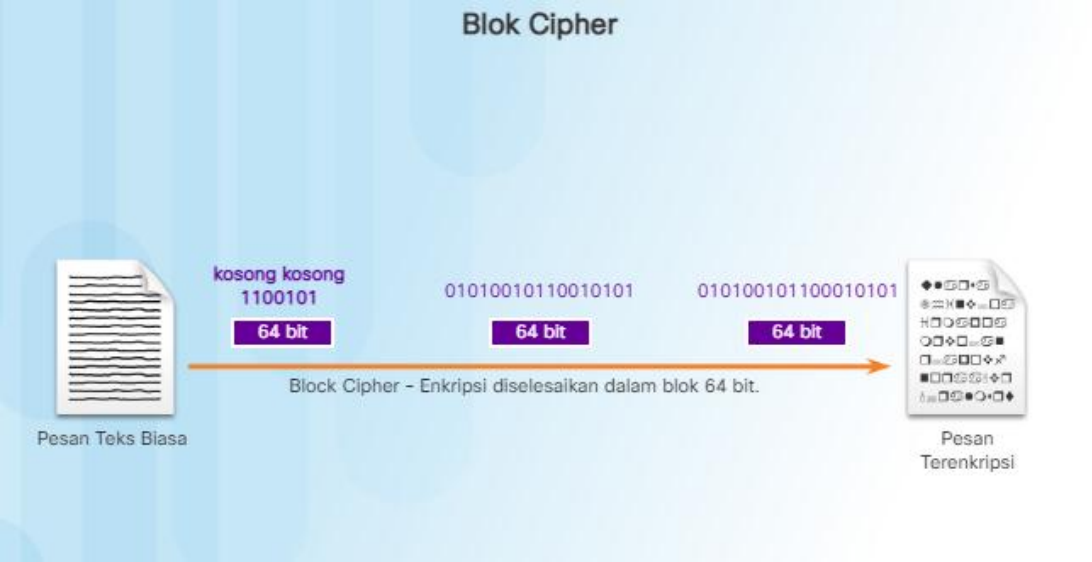
- Block Ciphers

  Block cipher mengubah blok plainteks dengan panjang tetap menjadi blok cipherteks umum 64 atau 128 bit. Ukuran blok adalah jumlah data yang dienkripsi pada satu waktu. Untuk mendekripsi ciphertext ini, terapkan transformasi terbalik ke blok ciphertext, menggunakan kunci rahasia yang sama. Block cipher biasanya menghasilkan data keluaran yang lebih besar dari data masukan, karena ciphertext harus kelipatan dari ukuran blok. Misalnya, Data Encryption Standard (DES) adalah algoritma simetris yang mengenkripsi blok dalam potongan 64-bit menggunakan kunci 56-bit. Untuk mencapai hal ini, algoritma blok mengambil data satu potongan pada satu waktu, misalnya, 8 byte per potongan, sampai seluruh blok penuh. Jika ada data masukan kurang dari satu blok penuh, algoritma menambahkan data buatan, atau kosong, sampai menggunakan 64 bit penuh, seperti yang ditunjukkan pada Gambar 1 untuk 64 bit di sebelah kiri.

- Stream Ciphers

  Tidak seperti block cipher, stream cipher mengenkripsi plaintext satu byte atau satu bit pada satu waktu, seperti yang ditunjukkan pada Gambar 2. Pikirkan stream cipher sebagai block cipher dengan ukuran blok satu bit. Dengan stream cipher, transformasi unit plaintext yang lebih kecil ini bervariasi, tergantung pada saat mereka ditemui selama proses enkripsi. Stream cipher bisa lebih cepat daripada block cipher, dan umumnya tidak menambah ukuran pesan, karena mereka dapat

mengenkripsi sejumlah bit yang berubah-ubah. A5 adalah stream cipher yang menyediakan privasi suara dan mengenkripsi komunikasi ponsel. Dimungkinkan juga untuk menggunakan DES dalam mode stream cipher. Sistem kriptografi yang kompleks dapat menggabungkan blok dan aliran dalam proses yang sama.



Gambar 5. Blok Cipher

- Algoritma Enkripsi Simetris

Banyak sistem enkripsi menggunakan enkripsi simetris. Beberapa standar enkripsi umum yang menggunakan enkripsi simetris meliputi:

3DES (Triple DES)

Digital Encryption Standard (DES) adalah cipher blok simetris dengan ukuran blok 64-bit yang menggunakan kunci 56-bit. Dibutuhkan blok plaintext 64-bit sebagai input dan mengeluarkan blok ciphertext 64-bit. Itu selalu beroperasi pada blok dengan ukuran yang sama dan menggunakan permutasi dan substitusi dalam algoritma. Permutasi adalah cara mengatur semua elemen dari suatu himpunan. Triple DES mengenkripsi data tiga kali dan menggunakan kunci yang berbeda untuk

Copyright © September 2023

setidaknya satu dari tiga lintasan, memberikan ukuran kunci kumulatif 112-168 bit. 3DES tahan terhadap serangan, tetapi jauh lebih lambat dari DES. Siklus enkripsi 3DES adalah sebagai berikut:

1) Data dienkripsi oleh DES pertama
2) Data didekripsi oleh DES kedua
3) Data dienkripsi ulang oleh DES ketiga

Proses sebaliknya mendekripsi ciphertext

IDE:

Algoritma Enkripsi Data Internasional (IDEA) menggunakan blok 64-bit dan kunci 128-bit. IDEA melakukan delapan putaran transformasi pada masing-masing dari 16 blok yang dihasilkan dari membagi setiap blok 64-bit. IDEA adalah pengganti DES, dan sekarang PGP (Pretty Good Privacy) menggunakannya. PGP adalah program yang menyediakan privasi dan otentikasi untuk komunikasi data. GNU Privacy Guard (GPG) adalah versi PGP yang berlisensi dan gratis.

AES:

Advanced Encryption Standard (AES) memiliki ukuran blok tetap 128-bit dengan ukuran kunci 128, 192, atau 256 bit. Institut Nasional Standar dan Teknologi (NIST) menyetujui algoritma AES pada bulan Desember 2001. Pemerintah AS menggunakan AES untuk melindungi informasi rahasia. AES adalah algoritma kuat yang menggunakan panjang kunci yang lebih panjang. AES lebih cepat daripada DES dan 3DES, sehingga memberikan solusi baik untuk aplikasi perangkat lunak

maupun penggunaan perangkat keras di firewall dan router. Sandi blok lainnya termasuk Skipjack (dikembangkan oleh NSA), Blowfish, dan Twofish.

B. Kontrol Akses

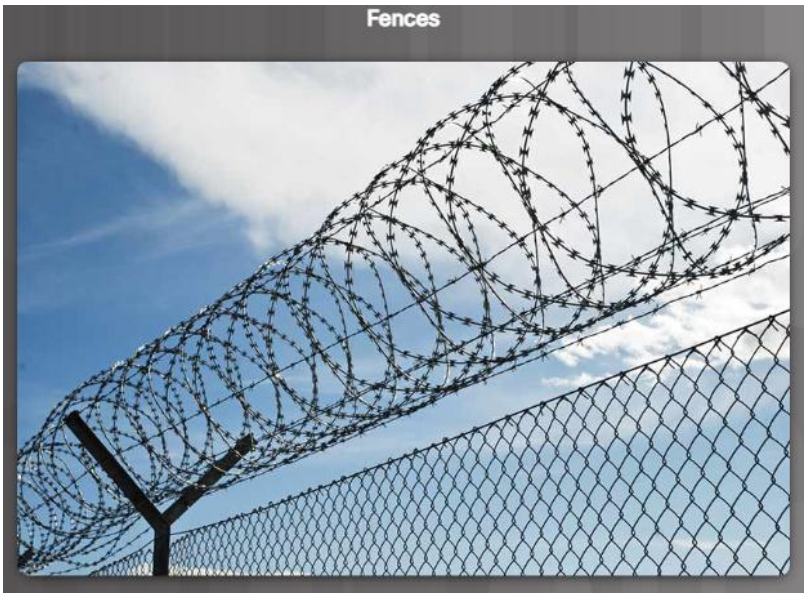
Jenis Kontrol Akses

Kontrol Akses Fisik, adalah penghalang aktual yang digunakan untuk mencegah kontak langsung dengan sistem. Tujuannya adalah untuk mencegah pengguna yang tidak berwenang mendapatkan akses fisik ke fasilitas, peralatan, dan aset organisasi lainnya. Kontrol akses fisik menentukan siapa yang bisa masuk (atau keluar), di mana mereka bisa masuk (atau keluar), dan kapan mereka bisa masuk (atau keluar). Contoh kontrol akses fisik meliputi:

- Penjaga (Gambar 6) memantau fasilitas

Gambar 6. Penjaga

- Pagar (Gambar 7) melindungi perimeter



Gambar 7. Pagar

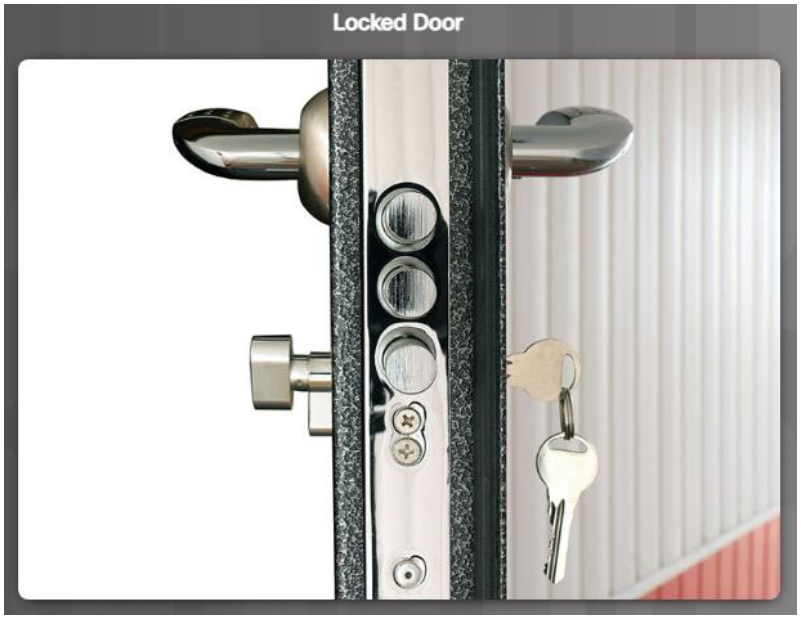
- Detektor gerak (Gambar 8) mendeteksi objek bergerak

Gambar 9. Detektor gerak

- Kunci laptop (Gambar 10) melindungi peralatan portable

Gambar 10. Kunci Laptop Portable

- Pintu terkunci (Gambar 11) mencegah akses yang tidak sah



Gambar 11. Kunci Pintu

Copyright © September 2023

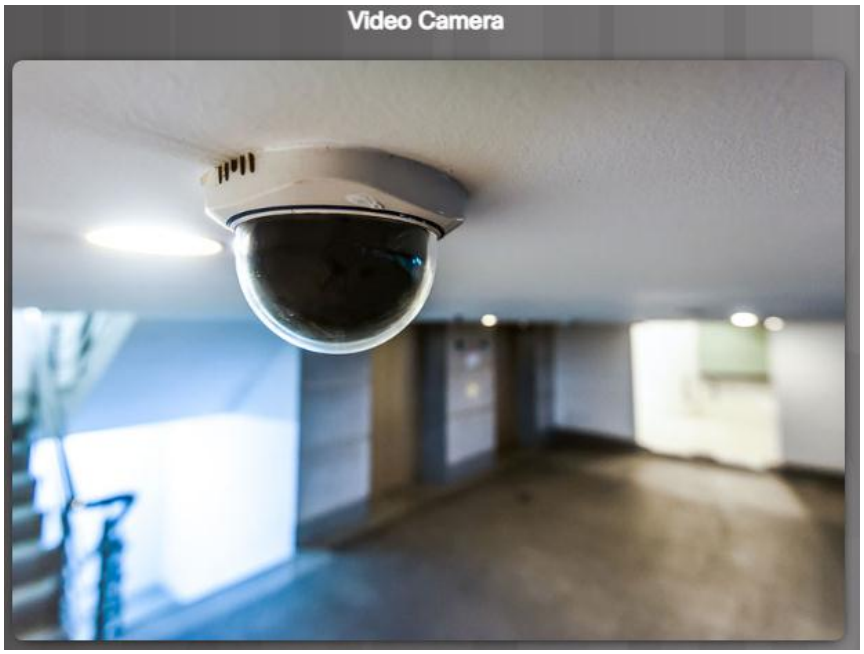
- Kartu gesek (Gambar 12) memungkinkan akses ke area terlarang

Gambar 12. Kartu Kunci

- Anjing penjaga (Gambar 13) melindungi fasilitas

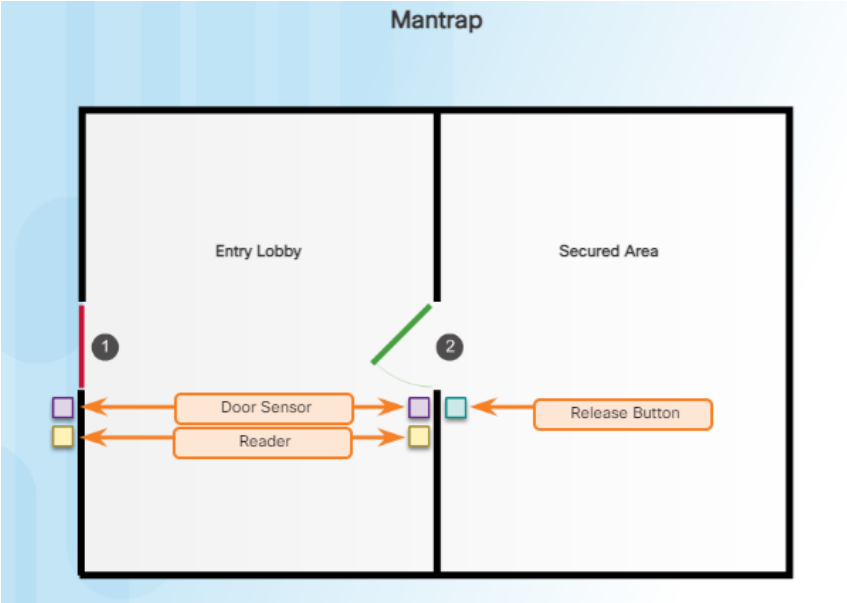
Gambar 13. Anjing Penjaga

- Kamera video (Gambar 14) memantau fasilitas dengan mengumpulkan dan merekam gambar



Gambar 14. Kamera Video

- Mantraps (Gambar 15) memungkinkan akses ke area aman setelah pintu 1 ditutup



Gambar 15. Mantrap

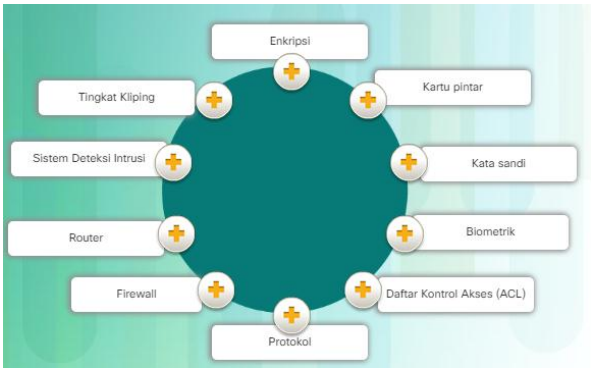
- Alarm (Gambar 16) mendeteksi intrusi

Gambar 16. Alaram

KONTROL AKSES LOGIS

Kontrol akses logis adalah solusi perangkat keras dan perangkat lunak yang digunakan untuk mengelola akses ke sumber daya dan sistem. Solusi berbasis teknologi ini mencakup alat dan protokol yang digunakan sistem komputer untuk identifikasi, otentikasi, otorisasi, dan akuntabilitas.

Kontrol akses logis mencakup hal-hal berikut:



Gambar 17 Kontrol Akses Logis

- Enkripsi adalah proses mengambil plaintext dan membuat ciphertext
- Kartu pintar memiliki microchip tertanam
- Kata sandi dilindungi string karakter
- Biometrik adalah karakteristik fisik pengguna
- Access Control Lists (ACL) menentukan jenis lalu lintas yang diizinkan di jaringan
- Protokol adalah seperangkat aturan yang mengatur pertukaran data antar perangkat
- Firewall mencegah lalu lintas jaringan yang tidak diinginkan
- Router menghubungkan setidaknya dua jaringan
- Sistem Deteksi Intrusi memantau jaringan untuk aktivitas yang mencurigakan
- Level Kliping adalah ambang batas tertentu yang diizinkan untuk kesalahan sebelum memicu tanda bahaya

KONTROL AKSES ADMINISTRATIF

Kontrol akses administratif adalah kebijakan dan prosedur yang ditetapkan oleh organisasi untuk menerapkan dan menegakkan semua aspek pengendalian akses yang tidak sah. Kontrol administratif berfokus pada personel dan praktik bisnis. Kontrol administratif mencakup hal-hal berikut:

Copyright © September 2023

Gambar 18. Kontrol akses administrative

- Kebijakan adalah pernyataan niat
- Prosedur adalah langkah-langkah rinci yang diperlukan untuk melakukan suatu kegiatan
- Praktik perekrutan melibatkan langkah-langkah yang diambil organisasi untuk menemukan karyawan yang memenuhi syarat
- Pemeriksaan latar belakang adalah penyaringan pekerjaan yang mencakup informasi verifikasi pekerjaan masa lalu, riwayat kredit, dan riwayat criminal
- Klasifikasi data mengkategorikan data berdasarkan sensitivitasnya
- Pelatihan keamanan mendidik karyawan tentang kebijakan keamanan di sebuah organisasi
- Ulasan mengevaluasi kinerja pekerjaan karyawan

STRATEGI AKSES KONTROL

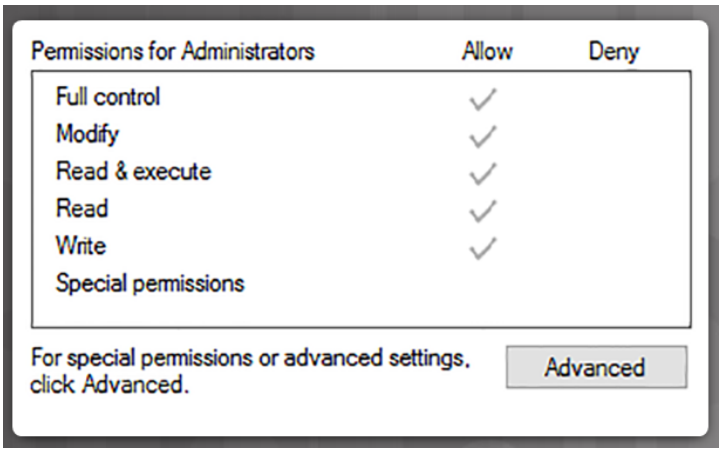
Mandatory Access Control (MAC) membatasi tindakan yang dapat dilakukan subjek pada objek. Subjek dapat berupa pengguna atau proses. Objek dapat berupa file, port, atau perangkat input/output. Aturan otorisasi memberlakukan apakah subjek dapat mengakses objek atau tidak. Organisasi menggunakan MAC di mana terdapat tingkat klasifikasi keamanan yang berbeda. Setiap objek memiliki label dan setiap subjek memiliki izin. Sistem MAC membatasi subjek berdasarkan klasifikasi keamanan objek dan label yang dilampirkan ke pengguna. Sebagai contoh, ambil klasifikasi keamanan militer Secret dan Top Secret. Jika sebuah file (sebuah objek) dianggap sangat rahasia, maka diklasifikasikan (diberi label) Top Secret. Satu-satunya orang (subjek) yang dapat melihat file (objek) adalah mereka yang memiliki izin Top Secret.

Copyright © September 2023

Terserah mekanisme kontrol akses untuk memastikan bahwa individu (subjek) hanya dengan izin Rahasia, tidak pernah mendapatkan akses ke file berlabel Top Secret. Demikian pula, seorang pengguna (subjek) yang diizinkan untuk akses Top Secret tidak dapat mengubah klasifikasi file (objek) berlabel Top Secret menjadi Secret. Selain itu, pengguna Top Secret tidak dapat mengirim file Top Secret ke pengguna yang dihapus hanya untuk melihat informasi Rahasia.

DISCRETIONARY ACCESS CONTROL

Pemilik objek menentukan apakah akan mengizinkan akses ke objek dengan kontrol akses diskresioner (DAC). DAC memberikan atau membatasi akses objek yang ditentukan oleh pemilik objek. Sesuai dengan namanya, kontrol bersifat diskresioner karena pemilik objek dengan izin akses tertentu dapat meneruskan izin tersebut ke subjek lain. Dalam sistem yang menggunakan kontrol akses diskresioner, pemilik objek dapat memutuskan subjek mana yang dapat mengakses objek itu dan akses spesifik apa yang mungkin mereka miliki. Salah satu metode umum untuk mencapai ini adalah dengan izin, seperti yang ditunjukkan pada gambar. Pemilik file dapat menentukan izin apa (baca/tulis/eksekusi) yang mungkin dimiliki pengguna lain. Daftar kontrol akses adalah mekanisme umum lainnya yang digunakan untuk menerapkan kontrol akses diskresioner. Daftar kontrol akses menggunakan aturan untuk menentukan lalu lintas apa yang dapat masuk atau keluar dari jaringan.



Gambar 19 Akses Kontrol

ROLE-BASED ACCESS CONTROL

Role-based access control (RBAC) tergantung pada peran subjek. Peran adalah fungsi pekerjaan dalam sebuah organisasi. Peran tertentu memerlukan izin untuk melakukan operasi tertentu. Pengguna memperoleh izin melalui peran mereka. RBAC dapat bekerja dalam kombinasi dengan DAC atau MAC dengan menerapkan kebijakan salah satunya. RBAC membantu menerapkan administrasi keamanan di organisasi besar dengan ratusan pengguna dan ribuan kemungkinan izin. Organisasi secara luas menerima penggunaan RBAC untuk mengelola izin komputer dalam suatu sistem, atau aplikasi, sebagai praktik terbaik.

RULE-BASED ACCESS CONTROL

Rule-Based Access Control menggunakan access control lists (ACLs) untuk membantu menentukan apakah akan memberikan akses. Serangkaian aturan terkandung dalam ACL, seperti yang ditunjukkan pada gambar. Penentuan apakah akan memberikan akses tergantung pada aturan ini. Contoh aturan semacam itu adalah aturan yang menyatakan bahwa tidak ada karyawan yang boleh memiliki akses ke file penggajian setelah jam kerja atau pada akhir pekan.

Copyright © September 2023

Seperti halnya MAC, pengguna tidak dapat mengubah aturan akses. Organisasi dapat menggabungkan kontrol akses berbasis aturan dengan strategi lain untuk menerapkan pembatasan akses. Misalnya, metode MAC dapat menggunakan pendekatan berbasis aturan untuk implementasi.

IDENTIFIKASI

Identifikasi memberlakukan aturan yang ditetapkan oleh kebijakan otorisasi. Subjek meminta akses ke sumber daya sistem. Setiap kali subjek meminta akses ke sumber daya, kontrol akses menentukan apakah akan memberikan atau menolak akses. Misalnya, kebijakan otorisasi menentukan aktivitas apa yang dapat dilakukan pengguna pada sumber daya. Pengidentifikasi unik memastikan hubungan yang tepat antara aktivitas dan subjek yang diizinkan. Nama pengguna adalah metode yang paling umum digunakan untuk mengidentifikasi pengguna. Nama pengguna dapat berupa kombinasi alfanumerik, nomor identifikasi pribadi (PIN), kartu pintar, atau biometrik, seperti sidik jari, pemindaian retina, atau pengenalan suara. Pengidentifikasi unik memastikan bahwa sistem dapat mengidentifikasi setiap pengguna secara individual; oleh karena itu, memungkinkan pengguna yang berwenang untuk melakukan tindakan yang sesuai pada sumber daya tertentu.

Gambar 20. Identifikasi user dan password

Kebijakan keamanan siber menentukan kontrol identifikasi mana yang harus digunakan. Sensitivitas sistem informasi dan informasi menentukan seberapa ketat pengendaliannya. Peningkatan pelanggaran data telah memaksa banyak organisasi untuk memperkuat kontrol identifikasi mereka. Misalnya, industri kartu kredit di Amerika Serikat mengharuskan semua vendor untuk beralih ke sistem identifikasi kartu pintar.