BAHAN E-LEARNING

Keamanan Jaringan Komputer

UNIVERSITAS BINA SARANA INFORMATIKA

www.bsi.ac.id

Copyright © September 2023

PERTEMUAN 1

PENGENALAN KEAMANA JARINGAN

1.1. DATA PRIBADI

1.1.1. Pengantar Data Pribadi

1. Apa itu Keamanan Jaringan?

Jaringan informasi elektronik yang terhubung telah menjadi bagian integral dari kehidupan kita sehari-hari. Semua jenis organisasi, seperti lembaga medis, keuangan, dan pendidikan, menggunakan jaringan ini untuk beroperasi secara efektif. Mereka memanfaatkan jaringan dengan mengumpulkan, memproses, menyimpan, dan berbagi sejumlah besar informasi digital. Karena semakin banyak informasi digital dikumpulkan dan dibagikan, perlindungan informasi ini menjadi semakin penting bagi keamanan nasional dan stabilitas ekonomi kita. Keamanan siber adalah upaya berkelanjutan untuk melindungi sistem jaringan ini dan semua data dari penggunaan atau bahaya yang tidak sah. Pada tingkat pribadi, Anda perlu melindungi identitas Anda, data Anda, dan perangkat komputasi Anda. Di tingkat korporat, merupakan tanggung jawab setiap orang untuk melindungi reputasi, data, dan pelanggan organisasi. Di tingkat negara bagian, keamanan nasional, serta keselamatan dan kesejahteraan warga dipertaruhkan.

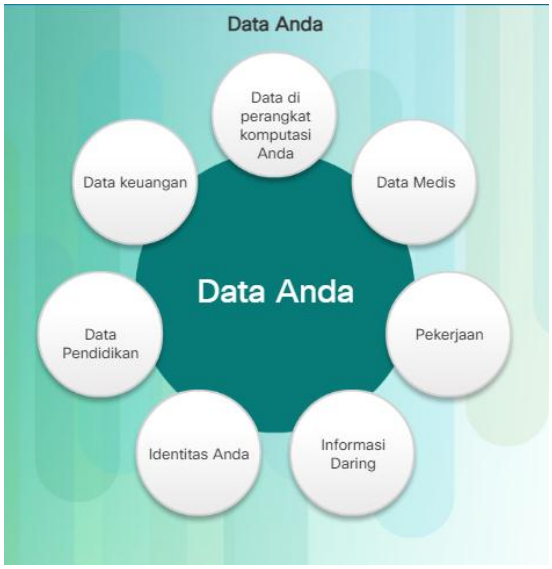
2. Status Identitas Seorang Saat Online dan Offline

Semakin banyak waktu yang dihabiskan untuk online, identitas Anda, baik online maupun offline, dapat memengaruhi hidup Anda. Identitas offline Anda adalah orang yang berinteraksi dengan teman dan keluarga Anda setiap hari di rumah, di sekolah, atau di tempat kerja. Mereka mengetahui informasi pribadi Anda, seperti nama, usia, atau tempat tinggal Anda. Identitas online Anda adalah siapa Anda di dunia maya. Identitas online Anda adalah bagaimana Anda menampilkan diri Anda kepada orang lain secara online. Identitas online

ini seharusnya hanya mengungkapkan sedikit informasi tentang Anda. Anda harus berhati-hati saat memilih nama pengguna atau alias untuk identitas online Anda. Nama pengguna tidak boleh menyertakan informasi pribadi apa pun. Itu harus sesuatu yang pantas dan terhormat. Nama pengguna ini tidak boleh membuat orang asing berpikir bahwa Anda adalah sasaran empuk kejahatan dunia maya atau perhatian yang tidak diinginkan.

3. Data Anda

Setiap informasi tentang Anda dapat dianggap sebagai data Anda. Informasi pribadi ini dapat secara unik mengidentifikasi Anda sebagai individu. Data ini mencakup gambar dan pesan yang Anda tukarkan dengan keluarga dan teman Anda secara online. Informasi lain, seperti nama, nomor jaminan sosial, tanggal dan tempat lahir, atau nama gadis ibu, diketahui oleh Anda dan digunakan untuk mengidentifikasi Anda. Informasi seperti informasi medis, pendidikan, keuangan, dan pekerjaan, juga dapat digunakan untuk mengidentifikasi Anda secara online.



Gambar 1. Data anda tersimpan

a. Rekam medis

Copyright © September 2023

Setiap kali Anda pergi ke kantor dokter, lebih banyak informasi ditambahkan ke catatan kesehatan elektronik (EHR) Anda. Resep dari dokter keluarga Anda menjadi bagian dari EHR Anda. EHR Anda mencakup kesehatan fisik, kesehatan mental, dan informasi pribadi lainnya yang mungkin tidak terkait secara medis. Misalnya, jika Anda memiliki konseling sebagai seorang anak ketika ada perubahan besar dalam keluarga, ini akan berada di suatu tempat dalam catatan medis Anda. Selain riwayat kesehatan dan informasi pribadi Anda, EHR juga dapat menyertakan informasi tentang keluarga Anda. Perangkat medis, seperti gelang kebugaran, menggunakan platform cloud untuk memungkinkan transfer nirkabel, penyimpanan, dan tampilan data klinis seperti detak jantung, tekanan darah, dan gula darah. Perangkat ini dapat menghasilkan sejumlah besar data klinis yang dapat menjadi bagian dari catatan medis Anda.

b. Catatan Pendidikan

Saat Anda maju melalui pendidikan Anda, informasi tentang nilai dan nilai ujian Anda, kehadiran Anda, kursus yang diambil, penghargaan dan gelar yang diberikan, dan laporan disipliner apa pun mungkin ada dalam catatan pendidikan Anda. Catatan ini juga dapat mencakup informasi kontak, catatan kesehatan dan imunisasi, dan catatan pendidikan khusus termasuk program pendidikan individual (IEPs).

c. Catatan Ketenagakerjaan dan Keuangan

Catatan keuangan Anda mungkin termasuk informasi tentang pendapatan dan pengeluaran Anda. Catatan pajak dapat mencakup slip gaji, laporan kartu kredit, peringkat kredit Anda, dan informasi perbankan lainnya. Informasi pekerjaan Anda dapat mencakup pekerjaan Anda sebelumnya dan kinerja Anda.

4. Dimana Data Anda?

Copyright © September 2023

Semua informasi ini tentang Anda. Ada berbagai undang-undang yang melindungi privasi dan data Anda di negara Anda. Tapi apakah Anda tahu di mana data Anda? Ketika Anda berada di kantor dokter, percakapan Anda dengan dokter dicatat dalam bagan medis Anda. Untuk tujuan penagihan, informasi ini dapat dibagikan dengan perusahaan asuransi untuk memastikan penagihan dan kualitas yang sesuai. Sekarang, bagian dari rekam medis Anda untuk kunjungan itu juga ada di perusahaan asuransi. Kartu loyalitas toko mungkin merupakan cara yang nyaman untuk menghemat uang untuk pembelian Anda. Namun, toko sedang menyusun profil pembelian Anda dan menggunakan informasi itu untuk penggunaannya sendiri. Profil menunjukkan pembeli membeli pasta gigi merek dan rasa tertentu secara teratur. Toko menggunakan informasi ini untuk menargetkan pembeli dengan penawaran khusus dari mitra pemasaran. Dengan menggunakan kartu loyalitas, toko dan mitra pemasaran memiliki profil untuk perilaku pembelian pelanggan. Ketika Anda membagikan foto Anda secara online dengan teman-teman Anda, apakah Anda tahu siapa yang mungkin memiliki salinan foto tersebut? Salinan gambar ada di perangkat Anda sendiri. Teman Anda mungkin memiliki salinan gambar yang diunduh ke perangkat mereka. Jika foto-foto itu dibagikan secara publik, orang asing mungkin juga memiliki salinannya. Mereka dapat mengunduh gambar-gambar itu atau mengambil tangkapan layar dari gambar-gambar itu. Karena gambar-gambar tersebut diposting secara online, mereka juga disimpan di server yang berlokasi di berbagai belahan dunia. Sekarang gambar tidak lagi hanya ditemukan di perangkat komputasi Anda.

5. Perangkat Komputasi

Copyright © September 2023

Perangkat komputasi Anda tidak hanya menyimpan data Anda. Sekarang perangkat ini telah menjadi portal ke data Anda dan menghasilkan informasi tentang Anda. Kecuali Anda telah memilih untuk menerima laporan tertulis untuk semua akun Anda, Anda menggunakan perangkat komputasi Anda untuk mengakses data. Jika Anda menginginkan salinan digital dari laporan kartu kredit terbaru, Anda menggunakan perangkat komputasi Anda untuk mengakses situs web penerbit kartu kredit. Jika Anda ingin membayar tagihan kartu kredit Anda secara online, Anda mengakses situs web bank Anda untuk mentransfer dana menggunakan perangkat komputasi Anda. Selain memungkinkan Anda untuk mengakses informasi Anda, perangkat komputasi juga dapat menghasilkan informasi tentang Anda. Dengan semua informasi tentang Anda ini tersedia secara online, data pribadi Anda menjadi menguntungkan bagi hackers.

1.1.2. Data Pribadi Sebagai Target

1. Mereka Menginginkan Uang Anda

Jika Anda memiliki sesuatu yang berharga, para penjahat menginginkannya. Kredensial online Anda sangat berharga. Kredensial ini memberi pencuri akses ke akun Anda. Anda mungkin berpikir bahwa frequent flyer miles yang Anda peroleh tidak berharga bagi penjahat dunia maya. Pikirkan lagi. Setelah sekitar 10.000 akun American Airlines dan United diretas, penjahat dunia maya memesan penerbangan gratis dan upgrade menggunakan kredensial yang dicuri ini. Meskipun miles frequent flyer dikembalikan ke pelanggan oleh maskapai, ini menunjukkan nilai kredensial login. Seorang penjahat juga bisa memanfaatkan hubungan Anda. Mereka dapat mengakses akun online Anda dan reputasi Anda untuk menipu Anda agar mengirimkan uang ke teman atau keluarga Anda. Penjahat dapat mengirim pesan yang menyatakan bahwa keluarga atau teman Anda membutuhkan Anda untuk mengirim uang kepada mereka sehingga mereka dapat pulang dari luar negeri setelah kehilangan dompet mereka. Para penjahat sangat imajinatif ketika mereka mencoba menipu

Copyright © September 2023

Anda untuk memberi mereka uang. Mereka tidak hanya mencuri uang Anda; mereka juga bisa mencuri identitas Anda dan menghancurkan hidup Anda.

2. Mereka Menginginkan Identitas Anda

Selain mencuri uang Anda untuk keuntungan moneter jangka pendek, para penjahat menginginkan keuntungan jangka panjang dengan mencuri identitas Anda. Ketika biaya medis meningkat, pencurian identitas medis juga meningkat. Pencuri identitas dapat mencuri asuransi kesehatan Anda dan menggunakan manfaat medis Anda untuk diri mereka sendiri, dan prosedur medis ini sekarang ada dalam catatan medis Anda. Prosedur pengajuan pajak tahunan dapat bervariasi dari satu negara ke negara lain; Namun, penjahat dunia maya melihat waktu ini sebagai peluang. Misalnya, rakyat Amerika Serikat harus mengajukan pajak mereka paling lambat tanggal 15 April setiap tahun. Internal Revenue Service (IRS) tidak memeriksa pengembalian pajak terhadap informasi dari majikan sampai Juli. Pencuri identitas dapat mengajukan pengembalian pajak palsu dan mengumpulkan pengembalian dana. Pelapor yang sah akan melihat ketika pengembalian mereka ditolak oleh IRS. Dengan identitas yang dicuri, mereka juga dapat membuka rekening kartu kredit dan membayar hutang atas nama Anda. Ini akan menyebabkan kerusakan pada peringkat kredit Anda dan membuat Anda lebih sulit untuk mendapatkan pinjaman. Kredensial pribadi juga dapat mengarah ke data perusahaan dan akses data pemerintah.

1.2. DATA ORGANISASI

Copyright © September 2023

1.2.1. Pengantar Data Organisasi

1. Jenis Data Organisasi

a. Data Tradisional

Data perusahaan mencakup informasi personalia, kekayaan intelektual, dan data keuangan. Informasi kepegawaian mencakup materi aplikasi, penggajian, surat penawaran, perjanjian karyawan, dan informasi apa pun yang digunakan dalam membuat keputusan ketenagakerjaan. Kekayaan intelektual, seperti paten, merek dagang, dan rencana produk baru, memungkinkan bisnis memperoleh keuntungan ekonomi atas para pesaingnya. Kekayaan intelektual ini dapat dianggap sebagai rahasia dagang; kehilangan informasi ini dapat menjadi bencana bagi masa depan perusahaan. Data keuangan, seperti laporan laba rugi, neraca, dan laporan arus kas suatu perusahaan memberikan wawasan tentang kesehatan perusahaan.

b. Internet of Things dan Big Data

Dengan munculnya Internet of Things (IoT), ada lebih banyak data untuk dikelola dan diamankan. IoT adalah jaringan besar objek fisik, seperti sensor dan peralatan yang melampaui jaringan komputer tradisional. Semua koneksi ini, ditambah fakta bahwa kami telah memperluas kapasitas penyimpanan dan layanan penyimpanan melalui cloud dan virtualisasi, mengarah pada pertumbuhan data yang eksponensial. Data ini telah menciptakan bidang minat baru dalam teknologi dan bisnis yang disebut "Big Data". Dengan kecepatan, volume, dan variasi data yang dihasilkan oleh IoT dan operasi bisnis sehari-hari, kerahasiaan, integritas, dan ketersediaan data ini sangat penting. penting bagi kelangsungan hidup organisasi.

2. Confidentiality, Integrity, and Availability

Confidentiality, integrity and availability yang dikenal sebagai triad adalah pedoman untuk keamanan informasi bagi suatu organisasi. Kerahasiaan memastikan privasi data

Copyright © September 2023

dengan membatasi akses melalui enkripsi otentikasi. Integritas memastikan bahwa informasi tersebut akurat dan dapat dipercaya. Ketersediaan memastikan bahwa informasi dapat diakses oleh orang yang berwenang.

a. Confidentiality

Istilah lain untuk kerahasiaan adalah privasi. Kebijakan perusahaan harus membatasi akses ke informasi untuk personel yang berwenang dan memastikan bahwa hanya individu yang berwenang yang melihat data ini. Data dapat dikotak-kotakkan sesuai dengan tingkat keamanan atau sensitivitas informasi. Misalnya, pengembang program Java tidak harus mengakses informasi pribadi semua karyawan. Selanjutnya, karyawan harus menerima pelatihan untuk memahami praktik terbaik dalam menjaga informasi sensitif untuk melindungi diri mereka sendiri dan perusahaan dari serangan. Metode untuk memastikan kerahasiaan termasuk enkripsi data, ID nama pengguna dan kata sandi, otentikasi dua faktor, dan meminimalkan paparan informasi sensitif.

b. Integrity

Integritas adalah akurasi, konsistensi, dan kepercayaan data selama seluruh siklus hidupnya. Data tidak boleh diubah selama transit dan tidak diubah oleh entitas yang tidak berwenang. Izin file dan kontrol akses pengguna dapat mencegah akses yang tidak sah. Kontrol versi dapat digunakan untuk mencegah perubahan yang tidak disengaja oleh pengguna yang berwenang. Cadangan harus tersedia untuk memulihkan data yang rusak, dan hashing checksum dapat digunakan untuk memverifikasi integritas data selama transfer.

Checksum digunakan untuk memverifikasi integritas file, atau string karakter, setelah ditransfer dari satu perangkat ke perangkat lain melalui jaringan lokal Anda atau Internet. Checksum dihitung dengan fungsi hash. Beberapa checksum yang umum

adalah MD5, SHA-1, SHA-256, dan SHA-512. Fungsi hash menggunakan algoritma matematika untuk mengubah data menjadi nilai panjang tetap yang mewakili data, seperti yang ditunjukkan pada Gambar 2. Nilai hash hanya ada untuk perbandingan. Dari nilai hash, data asli tidak dapat diambil secara langsung. Misalnya, jika Anda lupa kata sandi, kata sandi Anda tidak dapat dipulihkan dari nilai hash. Kata sandi harus diatur ulang.

Setelah file diunduh, Anda dapat memverifikasi integritasnya dengan memverifikasi nilai hash dari sumber dengan yang Anda buat menggunakan kalkulator hash apa pun. Dengan membandingkan nilai hash, Anda dapat memastikan bahwa file tidak dirusak atau rusak selama transfer.

c. Availability

Memelihara peralatan, melakukan perbaikan perangkat keras, memperbarui sistem operasi dan perangkat lunak, dan membuat cadangan memastikan ketersediaan jaringan dan data kepada pengguna yang berwenang. Harus ada rencana untuk segera pulih dari bencana alam atau bencana buatan manusia. Peralatan atau perangkat lunak keamanan, seperti firewall, menjaga dari waktu henti akibat serangan seperti penolakan layanan (DoS). Penolakan layanan terjadi ketika penyerang mencoba membanjiri sumber daya sehingga layanan tidak tersedia bagi pengguna.

3. LAB PRAKTIKUM – Membandingkan data dengan Aplikasi HASH

Tujuan :

Gunakan program hashing untuk memverifikasi integritas data.

Latar Belakang / Skenario:

Copyright © September 2023

Penting untuk dipahami ketika data telah rusak atau telah dirusak. Program hashing dapat digunakan untuk memverifikasi apakah data telah berubah, atau apakah tetap sama. Program hashing melakukan fungsi hash pada data atau file, yang mengembalikan nilai (biasanya jauh lebih pendek). Ada banyak fungsi hash yang berbeda, beberapa sangat sederhana dan beberapa sangat kompleks. Ketika hash yang sama dilakukan pada data yang sama, nilai yang dikembalikan selalu sama. Jika ada perubahan yang dilakukan pada data, nilai hash yang dikembalikan akan berbeda.

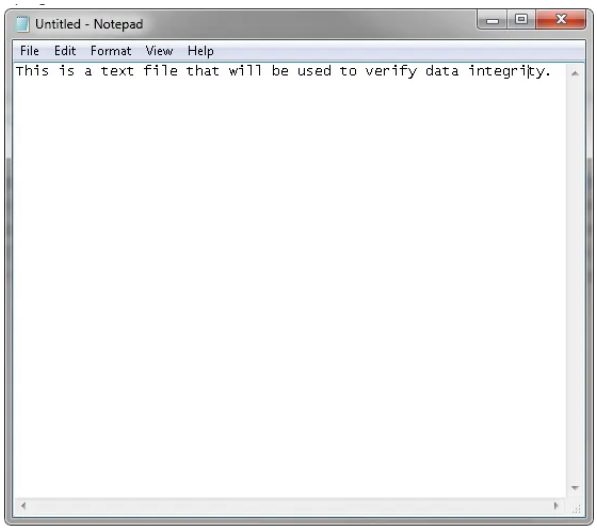
Catatan : Anda akan memerlukan hak instalasi dan beberapa pengetahuan tentang proses untuk menginstal program Windows.

Sumber Daya yang Diperlukan:

PC dengan akses Internet

Langkah 1: Buat file Teks

a. Buka Aplikasi Notepad
b. Ketik beberapa kata dalam Notepad tersebut



Gambar 2. Ketik beberapa kata dalam aplikasi notepad

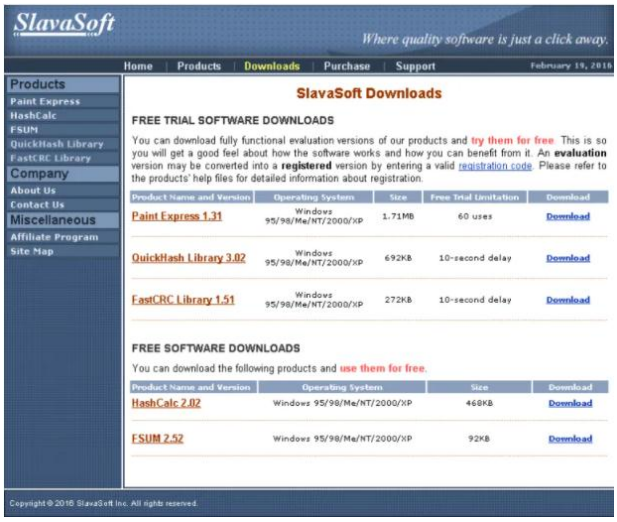
c. Pilih File > save

d. Simpan pada penyimpanan Desktop

e. Dengan nama File " Hash" lalu simpan

Langkah 2: Instal HashCalc

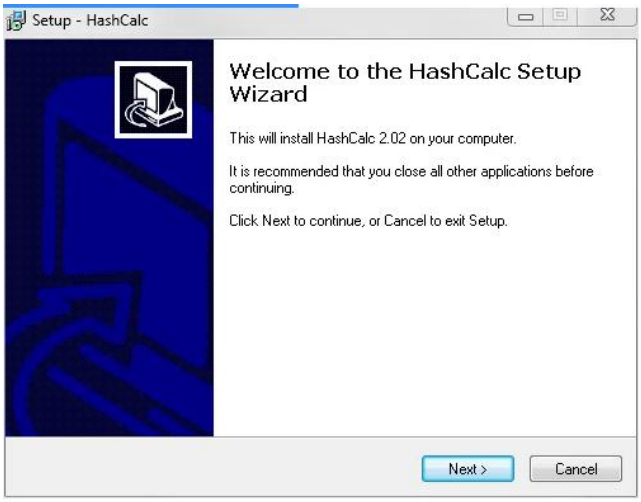
a. Buka browser web dan navigasikan ke http://www.slavasoft.com/download.htm



Gambar 3. Tampilan download Hash

b. Klik download pada baris HashCalc 2.02

c. Buka file hashcalc.zip dan jalankan file setup.exe di dalamnya.



Gambar 4. Install HashCalc

d. Ikuti wizard penginstalan untuk menginstal HashCalc.

e. Klik Finish pada layar terakhir, dan tutup file README jika dibuka. Anda dapat membaca file tersebut jika Anda mau.

f. HashCalc sekarang diinstal dan berjalan.

Gambar 5. Tampilan aplikasi HashCalc

<u>Langkah 3: Hitung hash dari file Hash.txt</u>

a. Perhatikan pemilihan menu dalam Hashcalc

1) Data Format : File
2) Data : klik button … selanjutkan ambil data notepad yang sudah dibuat sebelumnya pada Desktop dengan nama file Hast.txt
3) Hilangkan tanda cheklist pada HMAC
4) Hilangkan semua tanda cheklist pada aplikasi Kecuali MD5

b. Klik tombol Button Calculate

1) Berapa nilai di sebelah MD5 ? -Jawaban silakan diisi-
2) Buka file Hash.txt pada penyimpanan Dekstop
3) Buat perubahan kecil pada teks, seperti menghapus huruf, atau menambahkan spasi atau titik.
4) Klik File > Save , dan tutup Notepad .

Langkah 5: Hitung hash baru dari file Hash.txt

a. Klik tombol Button Calculate pada HashCalc lagi.

Berapa nilai di sebelah MD5 ? -Jawaban silakan diisi-

Apakah nilainya berbeda dengan nilai yang tercatat di Langkah 3? -Jawaban silakan diisi-

b. Beri tanda ceklist di semua jenis hash.

c. Klik tombol Button Calculate

d. Perhatikan bahwa banyak tipe hash membuat hash dengan panjang yang berbeda.

Mengapa? -Jawaban silakan diisi-

Dalam peraktikum mandiri yang kita lakukan pada aplikasi Hash menjelakan bahwa sebuah data memiliki sebuat nilai bit yang dapat dikonveriskan berdasarkan isi yang terdapat dalam data tersebut, bila nilai bit sudah tidak sesuai dengan versi original yang

kita miliki sudah dijamin bahwa data tersebut sudah mengalami perubahan isi dan perlu di curigai terkait perubahan data yang tidak dapat dilakukan oleh orang lain selain diri anda yang memang sebagai pemilik hak penuh atas data tersebut.

1.2.2. Dampak Pelanggaran Keamanan

1. Konsekuensi dari Pelanggaran Keamanan

Untuk melindungi organisasi dari setiap kemungkinan serangan siber tidak mungkin dilakukan, karena beberapa alasan. Keahlian yang diperlukan untuk menyiapkan dan memelihara jaringan yang aman bisa mahal. Penyerang akan selalu terus mencari cara baru untuk menargetkan jaringan. Akhirnya, serangan siber yang canggih dan tepat sasaran akan berhasil. Prioritas selanjutnya adalah seberapa cepat tim keamanan Anda dapat merespons serangan tersebut untuk meminimalkan hilangnya data, waktu henti, dan pendapatan. Sekarang Anda tahu bahwa apa pun yang diposting online dapat hidup online selamanya, bahkan jika Anda dapat menghapus semua salinan yang Anda miliki. Jika server Anda diretas, informasi personel rahasia dapat dipublikasikan. Seorang peretas (atau grup peretas) dapat merusak situs web perusahaan dengan memposting informasi yang tidak benar dan merusak reputasi perusahaan yang membutuhkan waktu bertahun-tahun untuk dibangun. Peretas juga dapat menghapus situs web perusahaan yang menyebabkan perusahaan kehilangan pendapatan. Jika situs web tidak aktif untuk jangka waktu yang lebih lama, perusahaan mungkin tampak tidak dapat diandalkan dan mungkin kehilangan kredibilitas. Jika situs web atau jaringan perusahaan telah dilanggar, hal ini dapat menyebabkan kebocoran dokumen rahasia, pengungkapan rahasia dagang, dan pencurian kekayaan intelektual. Hilangnya semua informasi ini dapat menghambat pertumbuhan dan ekspansi perusahaan. Biaya moneter dari pelanggaran jauh lebih tinggi daripada hanya mengganti perangkat yang hilang atau dicuri, berinvestasi dalam keamanan yang ada dan memperkuat keamanan fisik bangunan. Perusahaan mungkin bertanggung jawab untuk menghubungi

Copyright © September 2023

semua pelanggan yang terkena dampak tentang pelanggaran tersebut dan mungkin harus bersiap untuk proses pengadilan. Dengan semua gejolak ini, karyawan dapat memilih untuk meninggalkan perusahaan. Perusahaan mungkin perlu kurang fokus pada pertumbuhan dan lebih banyak pada perbaikan reputasinya.

2. Contoh Pelanggaran Keamanan 1

Pengelola kata sandi online, LastPass, mendeteksi aktivitas yang tidak biasa di jaringannya pada Juli 2015. Ternyata peretas telah mencuri alamat email pengguna, pengingat kata sandi, dan hash otentikasi. Untungnya bagi para pengguna, para peretas tidak dapat memperoleh brankas kata sandi terenkripsi siapa pun. Meskipun terjadi pelanggaran keamanan, LastPass tetap dapat mengamankan informasi akun pengguna. LastPass memerlukan verifikasi email atau otentikasi multi-faktor setiap kali ada login baru dari perangkat atau alamat IP yang tidak dikenal. Peretas juga memerlukan kata sandi utama untuk mengakses akun. Pengguna LastPass juga memiliki tanggung jawab dalam menjaga akun mereka sendiri. Pengguna harus selalu menggunakan kata sandi utama yang rumit dan mengubah kata sandi utama secara berkala. Pengguna harus selalu waspada terhadap serangan Phishing. Contoh serangan Phishing adalah jika penyerang mengirim email palsu yang mengaku berasal dari LastPass. Email meminta pengguna untuk mengklik tautan yang disematkan dan mengubah kata sandi. Tautan dalam email mengarah ke versi situs web palsu yang digunakan untuk mencuri kata sandi utama. Pengguna tidak boleh mengklik tautan yang disematkan dalam email. Pengguna juga harus berhati-hati dengan pengingat kata sandi mereka. Pengingat kata sandi tidak boleh memberikan kata sandi Anda. Yang terpenting, pengguna harus mengaktifkan otentikasi multi-faktor bila tersedia untuk situs web mana pun yang menawarkannya. Jika pengguna dan penyedia layanan sama-sama menggunakan alat dan prosedur yang tepat untuk melindungi informasi pengguna, data pengguna masih dapat dilindungi, bahkan jika terjadi pelanggaran keamanan.

Copyright © September 2023

3. Contoh Pelanggaran Keamanan 2

Pembuat mainan berteknologi tinggi untuk anak-anak, Vtech, mengalami pelanggaran keamanan pada basis datanya pada November 2015. Pelanggaran ini dapat memengaruhi jutaan pelanggan di seluruh dunia, termasuk anak-anak. Pelanggaran data mengekspos informasi sensitif termasuk nama pelanggan, alamat email, kata sandi, gambar, dan log obrolan. Sebuah tablet mainan telah menjadi target baru bagi para peretas. Pelanggan telah berbagi foto dan menggunakan fitur obrolan melalui tablet mainan. Informasi tidak diamankan dengan benar, dan situs web perusahaan tidak mendukung komunikasi SSL yang aman. Meskipun pelanggaran tersebut tidak mengekspos informasi kartu kredit dan data identifikasi pribadi, perusahaan tersebut ditangguhkan di bursa saham karena kekhawatiran atas peretasan tersebut begitu besar. Vtech tidak melindungi informasi pelanggan dengan benar dan itu terungkap selama pelanggaran. Meskipun perusahaan memberi tahu pelanggannya bahwa kata sandi mereka telah di-hash, masih mungkin bagi para peretas untuk menguraikannya. Kata sandi dalam database diacak menggunakan fungsi hash MD5, tetapi pertanyaan keamanan dan jawaban disimpan dalam teks biasa. Sayangnya, fungsi hash MD5 memiliki kerentanan yang diketahui. Peretas dapat menentukan kata sandi asli dengan membandingkan jutaan nilai hash yang telah dihitung sebelumnya. Dengan informasi yang terungkap dalam pelanggaran data ini, penjahat dunia maya dapat menggunakannya untuk membuat akun email, mengajukan kredit, dan melakukan kejahatan sebelum anak-anak cukup umur untuk pergi ke sekolah. Untuk orang tua dari anak-anak ini, penjahat dunia maya dapat mengambil alih akun online karena banyak orang menggunakan kembali kata sandi mereka di situs web dan akun yang berbeda. Pelanggaran keamanan tidak hanya berdampak pada privasi pelanggan, tetapi juga merusak reputasi perusahaan, seperti yang ditunjukkan oleh perusahaan ketika kehadirannya di bursa ditangguhkan. Bagi orang tua, ini adalah peringatan untuk lebih waspada tentang privasi online anak-anak mereka dan menuntut

keamanan yang lebih baik untuk produk anak-anak. Untuk produsen produk yang terhubung ke jaringan, mereka harus lebih agresif dalam melindungi data dan privasi pelanggan sekarang dan di masa depan, seiring berkembangnya lanskap serangan siber.

4. Contoh Pelanggaran Keamanan 3

Equifax Inc. adalah salah satu agen pelaporan kredit konsumen nasional di Amerika Serikat. Perusahaan ini mengumpulkan informasi tentang jutaan pelanggan individu dan bisnis di seluruh dunia. Berdasarkan informasi yang dikumpulkan, skor kredit dan laporan kredit dibuat tentang pelanggan. Informasi ini dapat mempengaruhi pelanggan ketika mereka mengajukan pinjaman dan ketika mereka mencari pekerjaan. Pada bulan September 2017, Equifax secara terbuka mengumumkan peristiwa pelanggaran data. Para penyerang mengeksploitasi kerentanan dalam perangkat lunak aplikasi web Apache Struts. Perusahaan percaya bahwa jutaan data pribadi sensitif konsumen AS diakses oleh penjahat cyber antara Mei dan Juli 2017. Data pribadi termasuk nama lengkap pelanggan, nomor Jaminan Sosial, tanggal lahir, alamat dan informasi pribadi lainnya. Ada bukti bahwa pelanggaran tersebut mungkin telah mempengaruhi pelanggan di Inggris dan Kanada. Equifax mendirikan situs web khusus yang memungkinkan konsumen untuk menentukan apakah informasi mereka telah disusupi, dan mendaftar untuk pemantauan kredit dan perlindungan pencurian identitas. Menggunakan nama domain baru, alih-alih menggunakan subdomain equifax.com, ini memungkinkan pihak jahat untuk membuat situs web tidak sah dengan nama yang mirip. Situs web ini dapat digunakan sebagai bagian dari skema phishing untuk mengelabui Anda agar memberikan informasi pribadi. Selanjutnya, seorang karyawan dari Equifax memberikan tautan web yang salah di media sosial untuk pelanggan yang khawatir. Untungnya, situs web ini dihapus dalam waktu 24 jam. Itu dibuat oleh seorang individu yang menggunakannya sebagai kesempatan pendidikan untuk mengekspos kerentanan yang ada di halaman respons Equifax. Sebagai konsumen yang peduli, Anda mungkin ingin

memverifikasi dengan cepat apakah informasi Anda telah disusupi, sehingga Anda dapat meminimalkan dampaknya. Dalam masa krisis, Anda mungkin ditipu untuk menggunakan situs web yang tidak sah. Anda harus berhati-hati dalam memberikan informasi pribadi agar tidak menjadi korban lagi. Selain itu, perusahaan bertanggung jawab untuk menjaga keamanan informasi kami dari akses yang tidak sah. Perusahaan perlu secara teratur menambal dan memperbarui perangkat lunak mereka untuk mengurangi eksploitasi kerentanan yang diketahui. Karyawan mereka harus dididik dan diinformasikan tentang prosedur untuk melindungi informasi dan apa yang harus dilakukan jika terjadi pelanggaran. Sayangnya, korban sebenarnya dari pelanggaran ini adalah individu yang datanya mungkin telah disusupi. Dalam hal ini, Equifax memiliki beban untuk melindungi data konsumen yang dikumpulkan saat melakukan pemeriksaan kredit karena pelanggan tidak memilih untuk menggunakan layanan yang disediakan oleh Equifax. Konsumen harus mempercayai perusahaan untuk melindungi informasi yang dikumpulkan. Selanjutnya, penyerang dapat menggunakan data ini untuk mengasumsikan identitas Anda, dan sangat sulit untuk membuktikan sebaliknya karena penyerang dan korban mengetahui informasi yang sama. Dalam situasi ini, yang paling dapat Anda lakukan adalah waspada ketika Anda memberikan informasi identitas pribadi melalui Internet. Periksa laporan kredit Anda secara teratur (sekali per bulan atau sekali per kuartal). Segera laporkan informasi palsu.

5. LAB PRAKTIKUM – APA YANG DICURI?

Tujuan:

Cari dan baca tentang beberapa kejadian pelanggaran keamanan yang pernah terjadi pada sebuah organisasi.

Latar Belakang / Skenario:

Copyright © September 2023

Pelanggaran keamanan terjadi ketika individu atau aplikasi mencoba mendapatkan akses tidak sah ke data, aplikasi, layanan, atau perangkat. Selama pelanggaran ini, penyerang, apakah mereka orang dalam atau bukan, berusaha mendapatkan informasi yang dapat mereka gunakan untuk keuntungan finansial atau keuntungan lainnya. Di lab ini, Anda akan mempelajari beberapa pelanggaran keamanan untuk menentukan apa yang diambil, eksploitasi apa yang digunakan, dan apa yang dapat Anda lakukan untuk melindungi diri sendiri.

Sumber Daya yang Diperlukan

PC atau perangkat seluler dengan akses Internet

Penelitian Pelanggaran Keamanan

a. Cari sebuah artikel tentang sebuah Pencurian data untuk mengisi table dibawah ini sertakan link berita informasinya.

Tanggal Insiden	**Organisasi yang Terkena Dampak**	**Berapa banyak korban? Apa yang Diambil?**	**Eksploitasi apa yang digunakan?**	**Sumber Referensi**

1.3. PENYERANG DAN PROFESIONAL KEAMANA CYBER

1.3.1. Profil Penyerangan Cyber

1. Jenis Penyerang

Penyerang adalah individu atau kelompok yang mencoba mengeksploitasi kerentanan untuk keuntungan pribadi atau finansial. Penyerang tertarik pada segalanya, mulai dari kartu kredit hingga desain produk dan apa pun yang bernilai.

Amateurs – Orang-orang ini terkadang disebut Script Kiddies. Mereka biasanya penyerang dengan sedikit atau tanpa keterampilan, sering kali menggunakan alat atau instruksi yang ada di Internet untuk melancarkan serangan. Beberapa dari mereka hanya ingin tahu, sementara yang lain mencoba untuk menunjukkan keterampilan mereka dan menyebabkan kerusakan. Mereka mungkin menggunakan alat dasar, tetapi hasilnya masih bisa menghancurkan.

Hackers – Kelompok penyerang ini membobol komputer atau jaringan untuk mendapatkan akses. Bergantung pada maksud pembobolan, penyerang ini diklasifikasikan sebagai topi putih, abu-abu, atau hitam. Para penyerang topi putih membobol jaringan atau sistem komputer untuk menemukan kelemahan sehingga keamanan sistem tersebut dapat ditingkatkan. Pembobolan ini dilakukan dengan izin sebelumnya dan hasil apa pun dilaporkan kembali ke pemilik. Di sisi lain, penyerang topi hitam memanfaatkan kerentanan apa pun untuk keuntungan pribadi, finansial, atau politik yang ilegal. Penyerang topi abu-abu berada di antara penyerang topi putih dan hitam. Penyerang topi abu-abu mungkin menemukan kerentanan dalam suatu sistem. Peretas topi abu-abu dapat melaporkan kerentanan kepada pemilik sistem jika tindakan itu sesuai dengan agenda mereka

Organized Hackers – Peretas ini termasuk organisasi penjahat dunia maya, peretas, teroris, dan peretas yang disponsori negara. Penjahat dunia maya biasanya adalah kelompok penjahat

profesional yang berfokus pada kontrol, kekuasaan, dan kekayaan. Para penjahat sangat canggih dan terorganisir, dan mereka bahkan mungkin menyediakan kejahatan dunia maya sebagai layanan untuk penjahat lain. Hacktivists membuat pernyataan politik untuk menciptakan kesadaran akan isu-isu yang penting bagi mereka. Penyerang yang disponsori negara mengumpulkan intelijen atau melakukan sabotase atas nama pemerintah mereka. Penyerang ini biasanya sangat terlatih dan didanai dengan baik, dan serangan mereka difokuskan pada tujuan tertentu yang bermanfaat bagi pemerintah mereka.

2. Ancaman Internal dan Eksternal

a. Ancaman Keamanan Internal

Serangan dapat berasal dari dalam organisasi atau dari luar organisasi, seperti yang ditunjukkan pada gambar. Pengguna internal, seperti karyawan atau mitra kontrak, dapat secara tidak sengaja atau sengaja:

- Salah menangani data rahasia
- Mengancam operasi server internal atau perangkat infrastruktur jaringan
- Memfasilitasi serangan dari luar dengan menghubungkan media USB yang terinfeksi ke dalam sistem komputer perusahaan
- Secara tidak sengaja mengundang malware ke jaringan melalui email atau situs web berbahaya.

Ancaman internal juga berpotensi menimbulkan kerusakan yang lebih besar daripada ancaman eksternal, karena pengguna internal memiliki akses langsung ke gedung dan perangkat infrastrukturnya. Karyawan juga memiliki pengetahuan tentang jaringan perusahaan, sumber dayanya, dan data rahasianya, serta berbagai tingkat hak istimewa pengguna atau administratif.

b. Ancaman Keamanan Eksternal

Ancaman eksternal dari amatir atau penyerang terampil dapat mengeksploitasi kerentanan dalam jaringan atau perangkat komputasi, atau menggunakan rekayasa sosial untuk mendapatkan akses.

1.4. Cyberwarfe

1.4.1. Pengantar Cyberwarfe

1. Apa itu Cyberwarfe

Dunia maya telah menjadi dimensi penting lain dari peperangan, di mana negara dapat melakukan konflik tanpa bentrokan pasukan dan mesin tradisional. Hal ini memungkinkan negara-negara dengan kehadiran militer minimal menjadi sekuat negara lain di dunia maya. Cyberwarfare adalah konflik berbasis Internet yang melibatkan penetrasi sistem komputer dan jaringan negara lain. Penyerang ini memiliki sumber daya dan keahlian untuk meluncurkan serangan berbasis Internet besar-besaran terhadap negara lain untuk menyebabkan kerusakan atau mengganggu layanan, seperti mematikan jaringan listrik. Contoh serangan yang disponsori negara melibatkan malware Stuxnet yang dirancang untuk merusak pabrik pengayaan nuklir Iran. Malware Stuxnet tidak membajak komputer yang ditargetkan untuk mencuri informasi. Itu dirancang untuk merusak peralatan fisik yang dikendalikan oleh komputer. Itu menggunakan pengkodean modular yang diprogram untuk melakukan tugas tertentu di dalam malware. Itu menggunakan sertifikat digital curian sehingga serangan itu tampak sah bagi sistem.

2. Tujuan Cyberwarfe

Tujuan utama dari cyberwarfare adalah untuk mendapatkan keuntungan atas musuh, apakah mereka negara atau pesaing. Suatu negara dapat terus menginvasi infrastruktur negara lain, mencuri rahasia pertahanan, dan mengumpulkan informasi tentang teknologi untuk mempersempit kesenjangan dalam industri dan militernya. Selain spionase industri

Copyright © September 2023

dan militeristik, perang siber dapat menyabotase infrastruktur negara lain dan merenggut nyawa di negara yang ditargetkan. Misalnya, serangan dapat mengganggu jaringan listrik kota besar. Lalu lintas akan terganggu. Pertukaran barang dan jasa dihentikan. Pasien tidak bisa mendapatkan perawatan yang dibutuhkan dalam situasi darurat. Akses ke Internet juga dapat terganggu. Dengan mempengaruhi jaringan listrik, serangan itu dapat mempengaruhi kehidupan sehari-hari warga biasa. Selain itu, data sensitif yang disusupi dapat memberi penyerang kemampuan untuk memeras personel di dalam pemerintahan. Informasi tersebut memungkinkan penyerang untuk berpura-pura menjadi pengguna yang berwenang untuk mengakses informasi atau peralatan sensitif. Jika pemerintah tidak dapat mempertahankan diri dari serangan siber, warga dapat kehilangan kepercayaan pada kemampuan pemerintah untuk melindungi mereka. Cyberwarfare dapat mengacaukan suatu negara, mengganggu perdagangan, dan mempengaruhi kepercayaan warga negara pada pemerintah mereka tanpa pernah secara fisik menyerang negara yang ditargetkan.