No. Rabu

Elia Fajrin _ 4491200145 Date 7 April 2021

# Worksheet 4 _ Aplikasi komputer

1. Jelaskan istilah keamanan digital resiko keamanan digital dan jelaskan secara singkat jenis-jenis kejahatan dunia maya!
2. Jelaskan berbagai jenis serangan jaringan internet, dan jelaskan cara untuk melindungi dari serangan tersebut
3. Jelaskan teknik untuk mencegah akses dan penggunaan komputer secara ilegal!
4. Jelaskan cara produsen perangkat lunak (software) melindungi perangkat lunak buatan mereka dari pembajakan!
5. Jelaskan cara kerja enkripsi, tanda tangan digital dan sertifikat digital!
6. Bagaimana pengamanan data untuk mengantisipasi pencurian/ penghancurkan perangkat keras, maupun kegagalan fungsi perangkat!
7. Jelaskan hal-hal mengenai etika dalam masyarakat dan berbagai cara untuk melindungi privasi informasi di era komunikasi digital!

Jawab!

1) Keamanan digital → Suatu bentuk konsep dan upaya dalam memberikan perlindungan terhadap aset dan informasi digital yang dimiliki oleh suatu individu atau kelompok
2) Resiko keamanan digital → Setiap kejadian yang dapat menyebabkan satu kehilangan atau kerusakan terhadap hardware, software, data, informasi, dan
3) Jenis-jenis kejahatan dunia maya
   - Cybercrime → Suatu tindakan illegal yang dilakukan didalam jaringan internet
   - Hackers → Seseorang yang melakukan tindakan mengakses komputer atau jaringan tanpa izin

*White Hat Hackers → memfokuskan aksinya untuk melindungi sebuah sistem
* Black Hat Hackers → memfokuskan aksinya untuk menerobos sistem komputer (digital)
* Gray Hat Hackers → mencuri data untuk dijual ke orang lain tanpa merusak sistem komputer
- Crackers → seseorang atau sekelompok orang yang berusaha menembus suatu sistem u/ mengambil keuntungan dan melakukan kerusakan
- script kiddies → seseorang berkemampuan kurang baik dalam dunia internet yang memiliki niat buruk dengan menggunakan program lain u/ menyerang sistem komputer
- corporate spies → mata-mata perusahaan yang biasanya melakukan akses illegal untuk mengetahui rencana rival
- unethical Employees → karyawan perusahaan yang biasanya melihat data informasi yang bersifat rahasia dan tidak diperbolehkan untuk dilihat.
- cyberextortionist → orang yang mengancam suatu pihak untuk membayar dengan sejumlah uang dengan ancaman penyebaran data-data ataupun hal-hal lainnya.
- Cyberterrorist → suatu bentuk kejahatan terencana yang termotivasi secara politis yang berupa serangan terhadap informasi yang menyebabkan jatuhnya korban tidak berdosa sebab tindakan suatu kelompok / perorangan

② *Jenis serangan pada jaringan internet
a) Spoofing → teknik serangan dengan memalsukan data sehingga penyerang terlihat seperti orang rumah yg handal

* IP spoofing → teknik untuk menipu alamat IP sumber sehingga alamat IP asli tidak dapat dilacak saat pengiriman paket
* DNS spoofing → teknik untuk mengontrol server DNS sehingga alamat DNS dan IP suatu situs di transfer ke server pelaku
* Identity spoofing → teknik intrusi yang menggunakan identitas resmi untuk mengakses semua yang ada di jaringan secara ilegal

b) DDOS (Denial of service) → jenis serangan ke server di jaringan dengan metode untuk menghabiskan sumber daya yang dimiliki oleh server sampai server tidak dapat menjalankan fungsinya u/ menyediakan akses ke layanannya
- cara"nya
  - membanjiri lalu lintas dengan sejumlah besar data sehingga data dari host yang terdaftar tidak dapat masuk ke sistem
  - membanjiri traffic dengan banyak permintaan ke server sehingga server tidak dapat menangani permintaan dari host terdaftar
  - menggunakan komunikasi antar server terdaftar dan host dengan berbagai cara seperti mengubah informasi konfigurasi sistem.

c) Paket pengendus (pelacak) → teknik pencurian data dengan memantau dan menganalisis setiap paket data yang dikirim dari klien ke server.
cara" nya
- collecting → mengubah antar muka yang dulu menjadi

Node promiscus dan kemudian mengelompokan paket data yang melewati jaringan dalam bentuk biner tanpa format

- Conversion → mengubah data biner menjadi data yang mudah dibaca (dimengerti)
- Analisys → data diklasifikasikan kedalam blok protokol sesuai dengan sumber data.
- pencurian data → setelah data diklasifikasi, penyerang dapat mencuri data.

d) keracunan DNS → memberikan informasi alamat IP palsu untuk mengalihkan lalu lintas ke paket data dan tujuan yang sebenarnya.

e) kuda Trojan → jenis perangkat lunak berbahaya / malware yang dapat merusak sistem tujuannya u/ mendapatkan informasi tentang tujuan seperti kata sandi, log sistem dll

- jenis Trojan
  - pencuri kata sandi → mencuri kata sandi yang disimpan dalam sistem sehingga layar muncul seolah-olah layar login sedang menunggu host untuk memasukan kata sandi ketika masuk dan kemudian kata sandi akan dikirim ke penyerang
  - keylogger → merekam semua yang ditulis oleh tuan rumah dan mengirimnya ke penyerang
  - RAT (alat administrasi jarak jauh) → jenis Trojan yang dapat mengambil kendali penuh dari sistem dan dapat melakukan apa yang diinginkan penyerang dari jarak jauh

f) injeksi SQL → teknik serangan yang menggunakan

lubang keamanan yang mana situs web memungkinkan pengguna untuk memasukkan data tetapi tanpa filter karakter jahat sehingga penyerang dapat mengakses database aplikasi.

* Cara melindungi jaringan internet dari serangan, dapat memperhatikan:
1. keamanan fisik (physical security)
Suatu keamanan yang meliputi seluruh sistem beserta peralatan, peripheral, dan media yang digunakan
2. keamanan data dan media
Pada keamanan ini penyerang akan memanfaatkan kelemahan yang ada pada software yang digunakan untuk mengelola data.
3. keamanan dari pihak luar
memanfaatkan faktor kelemahan/kecerobohan dari orang yang berpengaruh (memilik hak akses) seing kali dilakukan oleh seorang Hacker / cracker.
4. keamanan dalam operasi
Salah satu prosedur untuk mengatur segala sesuatu yang berhubungan dengan sistem keamanan pasca serangan.

⇒ Bisa juga dengan menggunakan firewall yaitu suatu perangkat keras dan/atau perangkat lunak yang melindungi sumberdaya jaringan dari intrusi, perangkat ini juga mengatur lalu lintas jaringan, perangkat akan mengizinkan lalulintas jaringan yang dianggap aman dan mencegah lalu lintas jaringan yang tidak aman.

(3) Teknik untuk mencegah akses dan penggunaan komputer secara ilegal

- kontrol akses mendefinisikan siapa yang dapat mengakses komputer, perangkat atau jaringan serta tindakan yang harus diambil saat mengaksesnya.
- komputer, perangkat, atau jaringan harus memelihara jejak audit serta mencatatnya dalam file, baik upaya akses yang sukses dan tidak berhasil
  - nama pengguna
  - kata sandi

Teknik untuk mencegahnya dengan menggunakan:

1. Frasa sandi → kombinasi pribadi dari kata-kata sering menggunakan kapitalisasi campuran dan tanda baca terkait dengan nama pengguna yang memungkinkan akses ke sumber daya komputer tertentu.
2. PIN (Nomor Identifikasi pribadi) / kode sandi → adalah kata sandi numerik, baik yang ditetapkan oleh perusahaan atau dipilih oleh pengguna
3. perangkat biometrik mengotentikasi identitas seseorang dengan menerjemahkan karakteristik pribadi kedalam kode digital yang dibandingkan dengan komputer atau memverifikasi perangkat seluler
4. Verifikasi dua langkah menggunakan dua metode terpisah satu setelah berikutnya, u/ memverifikasi pengguna
5. Forensik digital → penemuan, pengumpulan, dan analisis bukti yang di temukan di komputer dan jaringan.

→ perangkat Biometrik meliputi

(4)

- membaca sidik jari
- Sistem pengakuan wajah
- Sistem geometri tangan
- Sistem verifikasi suara
- Sistem verifikasi tanda tangan
- Sistem pengenalan iris

④ Cara melindungi software dan pembajak
- Produsen software akan memasukkan aktivitas proses kedalam program mereka untuk memastikan perangkat lunak tidak di instal pada lebih banyak komputer dari berlisensi resmi.
- selama aktivitas produk yang dilakukan secara online atau melalui telepon, penggunna menyediakan nomor identifikasi produk perangkat lunak untuk mengaitkan perangkat lunak dengan komputer atau perangkat seluler dimana perangkat lunak diinstal.
- Produsen juga menyediakan perjanjian lisensi sebagai bukti bahwa pengguna berhak menggunakan perangkat lunak tersebut.

⑤ Cara kerja enkripsi mengubah data yang dibaca menjadi karakter yang disandikan
- public key dikenal dengan sebutan kriptografi asimetris menggunakan dua kunci berbeda yang berkaitan secara matematis. Dua kunci ini adalah kunci privat yang harus dirahasiakan dan kunci publik yang dapat dibagi ke banyak orang sekaligus. misalnya dalam mengirimkan data, si A

melakukan enkripsi dengan kunci publik pada data yang dikirimkan dan untuk membacanya, si B harus menggunakan kunci privat yang diberikan si A

- privat key di kenal dengan sebutan kunci simetris yakni penggunaan kunci yang sama untuk melakukan enkripsi dan dekripsi pada data yang dikirimkan. sebelum melakukan dekripsi, pengirim data harus terlebih dahulu membagikan kunci privatnya agar dapat didekripsi oleh penerima data. biasanya digunakan dalam operasi milik pemerintah

cara kerja tanda tangan digital

- Tanda tangan digital seperti tanda tangan tulis tangan mempunyai ciri unik dari setiap penanda tanaan. penyedia solusi tanda tangan digital, seperti Docusign, mengikuti protokol khusus yang disebut PKI. PKI mengharuskan penyedia menggunakan algoritma matematika untuk menghasilkan dua bilangan panjang yang disebut kunci satu kunci bersifat publik dan satu kunci bersifat pribadi. saat penanda tangan menandatangani dokumen secara elektronik, tanda tangan dibuat menggunakan kunci pribadi penanda tangan yang selalu disimpan dengan aman oleh penanda tangan.
- Algoritma matematika bertindak sebagai sandi, membuat data yang cocok dengan dokumen yang ditanda tangani yang disebut hash, dan mengenkripsi data itu yang akan menghasilkan tanda tangan digital. Tanda tangan tersebut juga ditandai dengan waktu penandatanganan

dokumen tersebut. jika dokumen berubah setelah penandatanganan tanda tangan menjadi tidak valid untuk melindungi integritas tanda tangan PKI mengharuskan kunci dibuat, dijalankan dan disimpan dengan cara yang aman, dan sering kali memerlukan layanan dari otoritas sertifikat (CA) yang andal penyedia tanda tangan digital seperti DocuSign memenuhi persyaratan PKI untuk penandatanganan digital yang aman.

Cara kerja sertifikat digital

- Mekanisme u/ mendapatkan sertifikat digital mirip dengan mendapatkan SIM atau ID pelajar. pertama' lakukan pendaftaran ke badan yang sesuai, menyerahkan informasi yang benar & memeriksa identitas anda dan benar - benar memiliki dokumen yang diverifikasi oleh badan tersebut. Anda harus dapat membuktikan bahwa anda adalah apa yang anda katakan. sertifikat digital memiliki cara kerja yang sama.
- Mereka berisikan informasi inti tentang individu, mesin atau perusahaan dan menautkan identitas digital ini dengan pasangan kunci, yang terbuat dari public key (kunci publik) dan private key (kunci privat).
- Sertifikat digital membuktikan kepemilikan kunci publik dan sertifikat hanya di terbitkan oleh otoritas, yang dikenal sebagai otoritas sertifikasi atau Authority certificate (CA)

- otoritas sertifikat → entitas mapan dimana pemeriksaan identitas diperlukan untuk menyerahkan sertifikat yang dipercaya. klien dan server menggunakan sertifikat yang dikeluarkan oleh CA untuk memastikan sistem mengandalkan CA terpercaya dan sertifikat digital terpercaya
- sertifikat yang dikeluarkan oleh CA mengikat kunci publik ke nama orang atau server. termudah memvalidasi: konten: dan mencegah penggunaan kunci publik palsu untuk menirukan identitas. hanya kunci publik yang benar dalam sertifikat valid yang akan berfungsi dengan kunci pribadi terkait yg dimiliki oleh orang atau perangkat yang diidentifikasi oleh sertifikat tersebut. semua ini dilakukan di latar belakang saat anda mengirim email pesan / foto melalui internet pada layanan terenkripsi.

(6) *pencurian data dan pencurian perangkat keras, Vandalism
1. Physical access control's → suatu proses untuk mengatur atau mengontrol siapa saja yang berak mengakses suatu resource - resource tertentu yang terdapat di dalam sebuah sistem. dalam proses ini akan di identifikasi siapa yang sedang melakukan request untuk mengakses suatu resource tertentu dan apakah orang tersebut memiliki hak akses untuk mengakses resource tersebut.
2. Alarm system → alarm elektronik yang dirancang untuk memperingatkan terhadap suatu bahaya

(10)

tertentu, sensornya terhubung dengan suatu unit pengendali melalui perkabelan bertenaga rendah / sinyal berfrekuensi radio sempit yang digunakan untuk berinteraksi dengan peranti respon.

3. physical security devices → menjelaskan langkah" keamanan yang dirancang u/ mendeteksi akses tidak sah ke fasilitas, peralatan dan sumber daya serta melindungi personel dan properti dari kerusakan dan bahaya, keamanan ini meliputi seluruh sistem beserta peralatan, peripheral dan media yang digunakan
4. Device - tracking app → Aplikasi yang dapat digunakan melacak mengetahui lokasi data sehingga apabila terjadi pencurian dapat dengan mudah di temukan pelakunya.

* pengamanan data dari kerusakan perangkat keras
- pelindung lonjakan arus (surge protector) → u/ melindungi jaringan anda dari sambaran petir dan lonjakan listrik
- Uninterrupt tible power supply (UPS) → perangkat yg biasanya menggunakan baterai backup sebagai catuan daya alternatif, agar dapat memberikan suplai daya yang tidak terputus untuk perangkat elektronik yang terpasang
- Duplicate components or duplicate computers → untuk membuat duplikat atau salinan satu atau lebih Objek yang terpilih saat itu juga.
- Fault - tolerant computer → (komputer yg toleran terhadap kesalahan) Feature yang

memungkinkan suatu sistem tetap berjalan normal meskipun ada komponen yang rusak pada salah satu komponennya. biasanya dipakai dalam transmisi data sehingga meskipun ada beberapa data yang gagal diterima pesan dapat diterima dengan utuh.

(7) *Hal-hal mengenai etika dalam masyarakat
Etika teknologi adalah pedoman moral yang mengatur penggunaan komputer, perangkat mobile, sistem informasi teknologi terkait
- properti intelektual merupakan pada karya unik dan asli seperti, gagasan, penemuan, seni, tulisan, proses, perusahaan dan nama produk, serta logo.
- Hak kekayaan intelektual adalah hak-hak pencipta yang berhak atas pekerjaan mereka
- Hak cipta melindungi setiap bentuk ekspresi nyata
- manajemen hak digital (DRM) → strategi yang dirancang untuk mencegah distribusi
- kode etik → pedoman tertulis yang membantu menentukan apakah suatu spesifikasi etis / tidak etis atau diperbolehkan / tidak diperbolehkan,
- komputer hijau melibatkan penggunaan listrik dan limbah lingkungan saat menggunakan komputer perangkat seluler, dan teknologi terkait.

* Cara u/ melindungi informasi privasi
1. pastikan pengguna memberikan data kepada orang yang tepat.

(12)

2. Periksa pengaturan privasi jejaring sosial
3. Tidak menggunakan penyimpanan umum u/ informasi pribadi
4. Hindari pelacakan
5. Simpan alamat email utama dan nomor ponsel anda tetap pribadi
6. menggunakan aplikasi pesan dengan Enkripsi End-to-end
7. Gunakan kata sandi yang aman
8. Tinjau izin untuk aplikasi seluler
9. amankan ponsel dan komputer dengan kata sandi
10. Nonaktifkan pemberitahuan layar kunci (lockscreen Notification)
11. Tetap menjaga privasi di jaringan Wifi