WORKSPACE FOR EDUCATION PLATFORM PENDIDIKAN SISTEM KEAMANAN KOMPUTER: KONSEP DAN PRAKTIK

Hasanuddin Sirait
Mundzir
Ino Sulistiani
Marlina
Dudes Manalu
Andreas Leonardo Sumendap
Gede Erik Aktama
Sutardi
Nur Ilman
Franky Gerald Cliford Manoppo

GET PRESS INDONESIA

WORKSPACE FOR EDUCATION PLATFORM PENDIDIKAN SISTEM KEAMANAN KOMPUTER: KONSEP DAN PRAKTIK

Penulis :
Hasanuddin Sirait
Mundzir
Ino Sulistiani
Marlina
Dudes Manalu
Andreas Leonardo Sumendap
Gede Erik Aktama
Sutardi
Nur Ilman
Franky Gerald Cliford Manoppo

ISBN :

Editor : Diana Purnama Sari,. S.E M.E
Penyunting : Tri Putri Wahyuni,S.Pd
Desain Sampul dan Tata Letak : Atyka Trianisa, S.Pd

Penerbit : GET PRESS INDONESIA
Anggota IKAPI No. 033/SBA/2022

Redaksi :
Jln. Palarik Air Pacah No 26 Kel. Air Pacah
Kec. Koto Tangah Kota Padang Sumatera Barat
Website : www. getpress.co.id
Email : adm.getpress@gmail.com

Cetakan pertama, September 2023

KATA PENGANTAR

Segala Puji dan syukur atas kehadirat Allah SWT dalam segala kesempatan. Sholawat beriring salam dan doa kita sampaikan kepada Nabi Muhammad SAW. Alhamdulillah atas Rahmat dan Karunia-Nya penulis telah menyelesaikan Buku Workspace For Education Platform Pendidikan Sistem Keamanan Komputer : Konsep Dan Praktik ini.

Buku ini membahas Perinsip Keamanan Komputer, Identifikasi Ancaman Terhadap Keamanan Komputer, Konsep Dasar Keamanan Komputer, Komponen Keamanan Fisik, Pemantauan dan Audit Keamanan Komputer, Sistem Deteksi dan Pencegahan Intrusi, Antivirus dan Antimalware, Sistem Encripsi Dalam Keamanan Komputer, Tren dan Teknologi Keamanan Terbaru, Sistem Keamanan Cloud.

Proses penulisan buku ini berhasil diselesaikan atas kerjasama tim penulis. Demi kualitas yang lebih baik dan kepuasan para pembaca, saran dan masukan yang membangun dari pembaca sangat kami harapkan.

Penulis ucapkan terima kasih kepada semua pihak yang telah mendukung dalam penyelesaian buku ini. Terutama pihak yang telah membantu terbitnya buku ini dan telah mempercayakan mendorong, dan menginisiasi terbitnya buku ini. Semoga buku ini dapat bermanfaat bagi masyarakat Indonesia.

Padang, September 2023

Penulis

DAFTAR ISI

BIODATA PENULIS

DAFTAR GAMBAR

BAB 1
PERINSIP KEAMANAN KOMPUTER

Oleh Hasanuddin Sirait

1.1 Pendahuluan

Dalam era sistem digital yang semakin maju, penggunaan teknologi dalam dunia pendidikan dan lingkungan kerja yang memerlukan pelayanan cepat akurat dan terlihat nyaman. Platform pendidikan dan *workspace* digital memungkinkan para pengguna untuk mengakses informasi, berkolaborasi, dan bekerja secara efisien. Dengan kemajuan teknologi digital saat ini maka diperlukan suatu sistem keamanan data yang memadai, sehingga sistem yang ber-orientasi keamanan data merupakan tujuan dari penerapan digitalisasi data dapat terjamin.

Seiring dengan hal diatas sistem keamanan komputer penting untuk dilakukan menjadi platform pendidikan agar dapat melindungi data dengan baik, dan menangkal ancaman keamanan seperti serangan *hacking* dan *malware*. Keamanan komputer dan jaringan dalam konteks ini merupakan pengembangan sistem keamanan dengan menjelaskan beberapa aspek yang penting pertimbangkan dalam perbaikan dan penangkalannya.

1.2 Keamanan Komputer

Keamanan komputer dilakukan untuk perlindungan data dan informasi dari pencurian atau manipulasi dari data dari pengguna internet yang tidak berwenang. Dalam buku ini akan dibahas secara konsep maupun praktik dengan pembahasan: perinsip keamanan komputer dan jaringan; identifikasi ancaman terhadap keamanan komputer; konsep dasar keamanan komputer; komponen keamanan fisik; manajemen identitas dan akses

terhadap keamanan komputer; keamanan jaringan dan sistem operasi; keamanan aplikasi dan perangkat lunak; pemantauan dan audit keamanan komputer; *backup* dan *recovery data*; sistem deteksi dan pencegahan intrusi; keamanan *firewall*; antivirus dan anti malware; sistem enkripsi dalam keamanan komputer; tren dan teknologi keamanan terbaru; sistem keamanan cloud. Secara umum, pendekatan yang dilakukan antara lain:

1. Pembatasan akses fisik terhadap komputer.
2. Penjaminan informasi yang tepat.
3. Menghindari gangguan dan hilangnya data.

Beberapa langkah dilakukan meningkatkan keamanan komputer, antara lain:

1. Gunakan kombinasi karakter yang kuat menggunakan huruf kapital (ABCDEFGHIJKLMNOPQRSTU) dengan kombinasi huruf kecil (abcdefghijklmnopqrstuvwxyz) kombinasi angka (0123456789) kombinasi simbol/lambang (€£¥©®™±≠≤≥÷×∞€μαβπΩ¥∑!/#?@’ ”:&%$= dan lainnya).
2. Pastikan sistem operasi dan aplikasi yang digunakan selalu diperbarui (*update*) dengan versi terbaru, karena mengandung perbaikan keamanan yang penting.
3. *Install software* keamanan seperti *anti virus*, *anti spy ware*, dan *firewall* untuk melindungi komputer dari serangan malware dan serangan jaringan.
4. Hindari membuka *e-mail*, tautan, atau lampiran yang mencurigakan atau tidak dikenal dikenal dengan *Phishing* dan *Malware*. Jangan juga mengunduh atau meng-*install* perangkat lunak dari sumber yang tidak terpercaya.
5. Lindungi jaringan komputer dengan menggunakan kata sandi yang kuat, mengaktifkan enkripsi Wi-Fi, dan membatasi akses fisik ke *router*.

6. Lakukan cadangan data secara berkala agar jika terjadi serangan atau kehilangan data, Anda masih dapat mengembalikan informasi yang penting.
7. Aktifkan autentikasi dua faktor pada akun *online* yang mendukungnya. Ini memberikan tingkat keamanan tambahan dengan memerlukan kode verifikasi tambahan selain kata sandi.
8. Saat tidak lagi membutuhkan data sensitif, pastikan untuk menghapusnya secara permanen dengan menggunakan perangkat lunak penghapusan data yang aman.

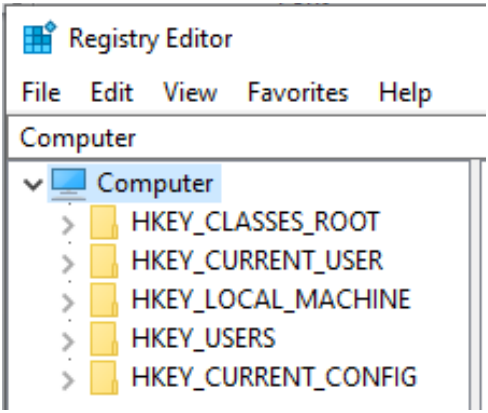
Berikut ini tabel perinsip dalam kemananan komputer yang dapat dilakukan.

Tabel 1.1. Kontrol *software* dan *hardware*

Activity	***Software/ Hardware***	***Activate***	***Security System***
Password	*Software*	*Login*	*System*
Update	*Software*	*Expire date*	*All*
Security	*Software*	*File*	*All*
Phishing/Malware	*Hardware*	*Firewall*	*System*
Policy	*Software*	*Access*	*True*
Backup data	*Hardware*	*Period*	*True*
Autentifikasi	*Software*	*Login*	*True*
Delete Data	*Software*	*Active*	*Clean*

Dari tabel terlihat bahwa pada kegiatan (*even*) yang ada dengan menggunakan *software* atau *hardware* sistem dengan mengaktifkan (*activate*) pada *security system* dengan *autentifikasi True*. Dengan Demikian seluruh aktifitas sistem harus terpantau

seluruhnya pada edit registrasi (regedit.exe) pada tampilan gambar berikut :



Gambar 1.1. Tampilan aplikasi file Regedit

Sesuai dengan gambar 1.1 diatas, maka berikut ini adalah penjelasan dari tujuan dari adanya file aplikasi yang ada pada sistem operasi windows :

1. **HKEY_CLASSES_ROOT**, tujuan dari bagian ini adalah melakukan proses komputer pada root media, sehingga aktifitas file akan dipantau melalui aplikasi HKEY_CLASSES_ROOT.
2. **HKEY_CURRENT_USER**, tujuan dari bagian ini adalah penggunaan aplikasi yang dilakukan pada komputer, sehingga pada HKEY_CURRENT_USER akan mencatat historis dari penggunaan komputer.
3. **HKEY_LOCAL_MACHINE**, tujuan dari bagian ini adalah penggunaan perangkat sumberdaya komputer dari aplikasi yang dilakukan, sehingga pada HKEY_LOCAL_MACHINE akan mencatat historis dari penggunaan sumberdaya *hardware*/komputer.
4. **HKEY_USERS**, tujuan dari bagian ini adalah hak akses dari user/penggunaan perangkat komputer melalui aplikasi,

sehingga pada HKEY_USERS akan mencatat historis akses aplikasi yang berproses.

5. **HKEY_CURRENT_CONFIG**, tujuan dari bagian ini adalah konfigurasi sistem melalui proses aplikasi dari pemberdayaan *hardware*, sehingga pada HKEY_CURRENT_CONFIG akan mencatat historis konfigurasi penggunaan sumberdaya *hardware*.

Sebagaimana tampilan diatas berikut penjelasan dari aktifitas komputer yang dapat dipantau melalui file aplikasi regedit.com. Hal ini dilakukan dengan langkah berikut :

1. Ketik regedit pada tampilan search desktop berikut dan <*enter*>

Gambar 1.2. Pengaktifan aplikasi file *regedit*.

2. Maka akan tampil sebagaimana tampilan pada gambar 1.1. Kemudian lakukan pengamanan dan pemantauan sebagaimana penjelasan diatas.

1.3 Konsep Keamanan Jaringan komputer

Konsep keamanan jaringan adalah rangkaian tindakan yang dilakukan melindungi jaringan komputer dari ancaman yang dapat mengancam kerahasiaan, integritas, dan ketersediaan data. Konsep keamanan pada jaringan melibatkan teknologi, kebijakan, dan praktik keamanan yang bertujuan untuk mengidentifikasi, mencegah, dan merespon ancaman keamanan. Beberapa konsep keamanan jaringan yang penting untuk dipertimbangkan meliputi:

1. Perindungan Fisik, Secara fisik dilindungi dikarenakan beberapa faktor dikarenakan :
   a. Kerusakan hardware;
   b. Kerusakan informasi;

c. Gangguan terhadap layanan.

2. Perlindungan *Non* Fisik, perlindungan nonfisik dilakukan karena beberapa faktor :
   a. Kerahasiaan (*Confidentially*), kerahasiaan sama dengan privasi.
   b. Perlindungan menjaga akurasi, konsistensi.
   c. Perlindungan terhadap ketersediaan.
   d. Perlindungan terhadap kebenaran informasi.
   e. Perlindungan terhadap *Access*.
   f. Pencurian Data melalui bank data.
   g. Legalitas informasi.
   h. Modifikasi secara illegal.

Keamanan jaringan menjadi faktor utama dalam sistem keamanan komputer untuk sebagai *platform* pendidikan dan *workspace*. Penggunaan *firewall* yang canggih dan pengaturan keamanan jaringan yang tepat sangat diperlukan untuk melindungi data/informasi yang ada pada jaringan komputer.

Hal lain yang terpenting yang perlu diperhatikan dalam sistem keamanan jaringan komputer adalah proses *enkripsi data*. Informasi yang dikirimkan melalui *jaringan* harus dienkripsi dan kemudian di deskripsi sehingga hanya dapat dibaca oleh pihak yang berwenang menggunaan algoritma enkripsi yang kuat, hal ini akan memberikan perlindungan tambahan terhadap data.

Selain faktor teknis, pendidikan dan kesadaran pengguna juga penting dalam menjaga keamanan komputer. Pengguna harus diberikan pelatihan dan pemahaman tentang praktik keamanan yang baik, seperti tidak mengklik tautan yang mencurigakan atau mengunduh *file* yang tidak diketahui:

1. Jenis ancaman terhadap komputer dan jaringan

   Penjelasan jenis ancaman yang dilakukan terhadap keamanan komputer dan jaringan:
   a. Melakukan akses sistem sesuai hak akses.

b. Pembuatan manajemen user.
c. Pengumpulan informasi sebagai history akses file.
d. Serangan terhadap *Denial-of-service* (DoS.
e. *Packet Snifer*.
f. *Hacking*.
g. *Malicious code* (kode berbahaya).
h. Virus trojan horse.
i. *Phishing*.
j. *Social Engineering / Exploitation of Trust*

2. Bagian utama dalam pengamanan komputer dan jaringan dipandang dari komponen informasi.
3. Manajemen keamanan jaringan berfungsi untuk menyusun sistem keamanan.

1.4 Meningkatkan sistem

Secara keseluruhan untuk meningkatkan sistem keamanan komputer adalah suatu proses yang dilakukan untuk memperbaiki dan memperkuat sistem keamanan pada perangkat komputer. Hal ini bertujuan untuk melindungi perangkat dan data dari ancaman dan serangan yang dapat membahayakan integritas, kerahasiaan, dan ketersediaan informasi.

Sesuai dengan penjelasan diatas maka langkah yang dapat diambil untuk meningkatkan keamanan komputer dn Jaringan, antara lain:

1. Keamanan perangkat lunak, lakukan peng-*Install-an* perangkat lunak keamanan seperti *antivirus*, *antispyware*, dan *firewall* untuk melindungi komputer dari serangan *malware* dan serangan jaringan.
2. *Phishing* dan *Malware*, hindari membuka email, tautan, atau lampiran yang mencurigakan atau tidak dikenal. Jangan mengunduh dan menginstal perangkat lunak dari sumber yang tidak terpercaya.

3. Mengamankan jaringan, indungi jaringan komputer dengan menggunakan kata sandi yang kuat, mengaktifkan enkripsi Wi-Fi, dan membatasi akses fisik ke router.
4. Menggunakan *autentikasi* dua faktor, dengan mengaktifkan autentikasi dua faktor pada akun *online* yang mendukungnya seperti autenfikasi *password* dan autentifikasi kode *privasi*. Hal ini dilakukan untuk memberikan tingkat keamanan tambahan sebagai pendukung *password* sebagai hak akses.

1.5 Jenis dan Sifat Virus Komputer

Virus komputer dapat dibagi menjadi beberapa jenis berdasarkan karakteristik dan cara kerjanya. Berikut adalah beberapa jenis umum dari virus komputer:

1. Jenis Virus komputer
   a. *File Infector Virus*, virus ini menempel pada file tertentu, seperti file eksekusi (exe) atau file program lainnya. Ketika file tersebut dijalankan, virus akan aktif dan mencoba untuk menginfeksi file lain di komputer.
   b. *Boot Sector Virus*, jenis virus ini menginfeksi sektor boot dari hard drive atau media penyimpanan lainnya. Saat komputer dihidupkan, virus akan aktif dan berusaha menyebar ke sektor boot perangkat lain yang terhubung.
   c. Macro Virus, virus ini menargetkan file berisi makro, seperti dokumen Microsoft Office. Virus ini aktif saat makro dijalankan dan dapat merusak atau menginfeksi dokumen lain.
   d. P*olymorphic* Virus, virus ini memiliki kemampuan untuk mengubah kode atau struktur internalnya setiap kali menginfeksi file baru. Hal ini membuatnya sulit dideteksi oleh program antivirus yang berbasis tanda tangan.

e. *Metamorphic* Virus, jenis virus ini dapat mengubah dirinya secara keseluruhan setiap kali ia menginfeksi file baru. Hal ini membuatnya bahkan lebih sulit untuk dideteksi dibandingkan dengan virus polymorphic.
f. *Resident* Virus, virus ini menempel pada memori komputer dan tetap aktif selama komputer berjalan. Virus jenis ini dapat menginfeksi file saat mereka dibuka atau diproses.
g. *Non-Resident* Virus: Virus ini tidak menempel pada memori komputer, tetapi aktif saat file yang terinfeksi dijalankan. Virus jenis ini dapat menginfeksi file lain dan kemudian keluar dari memori.
h. *Multipartite* Virus, jenis virus ini memiliki kemampuan untuk menginfeksi file dan sektor boot secara bersamaan. Ini membuatnya lebih kompleks dan sulit untuk dihapus.
i. Worm: Worm adalah program yang dapat menginfeksi komputer dan merusak atau mengambil alih sumber daya jaringan. Worm dapat menyebar melalui jaringan dan menginfeksi komputer tanpa interaksi pengguna.
j. Trojan Horse (Trojan): Meskipun bukan virus dalam arti sejati, trojan merupakan program berbahaya yang menyamar sebagai program atau file yang sah. Mereka dapat membuka akses ke komputer untuk penyerang atau menyebabkan kerusakan.
k. Ransomware: Jenis malware yang mengenkripsi data komputer dan meminta tebusan untuk mendapatkan kunci dekripsi. Ini mengakibatkan pengguna tidak dapat mengakses data mereka kecuali tebusan dibayar.
l. Spyware: Program berbahaya ini dirancang untuk mengumpulkan informasi rahasia atau data pribadi dari komputer tanpa sepengetahuan pengguna.

m. Adware: Meskipun tidak selalu merusak, adware menampilkan iklan yang tidak diinginkan pada komputer pengguna, seringkali dengan tujuan mempromosikan produk atau layanan.

2. Sifat Virus Komputer

Virus komputer adalah program perangkat lunak berbahaya yang dirancang untuk menginfeksi sistem komputer, mereplikasi diri, dan menyebar ke komputer lain. Virus komputer memiliki beberapa sifat khusus yang membedakannya dari jenis malware atau perangkat lunak berbahaya lainnya:

a. Replikasi: Virus komputer memiliki kemampuan untuk mereplikasi atau menggandakan dirinya sendiri.
b. Merusak: Virus dapat mengubah, menghapus, atau merusak file dan folder, yang dapat menyebabkan kehilangan data yang berharga atau bahkan kerusakan sistem yang serius.
c. Penyebaran: Virus dapat menyebar dengan cepat dari satu komputer ke komputer melalui jaringan, email, lampiran, perangkat penyimpanan seperti flash drive, atau bahkan melalui interaksi dengan situs web yang terinfeksi.
d. Manipulasi: Virus komputer dapat dimanipulasi untuk menjalankan tindakan tertentu pada waktu yang ditentukan atau ketika kondisi tertentu terpenuhi.
e. Penyembunyian: Beberapa virus dapat menyembunyikan diri mereka dari deteksi oleh program keamanan dengan mengenkripsi atau menyembunyikan kode berbahaya mereka di dalam file yang tampaknya aman.
f. Manipulasi Berbagai Jenis File: Virus dapat menginfeksi berbagai jenis file, termasuk dokumen,

gambar, video, dan program eksekusi. Ini berarti virus tidak terbatas pada satu jenis format file saja.

3. Cara Menghilangkan virus dari komputer
   Menghilangkan virus dari komputer memerlukan beberapa langkah hati-hati. Berikut adalah panduan langkah demi langkah untuk membersihkan virus dari komputer Anda:
   Catatan Penting Sebelum Memulai: Pastikan Anda memiliki cadangan data yang penting dan berharga sebelum melanjutkan dengan langkah-langkah ini. Menghapus virus dari komputer dapat mengakibatkan hilangnya data atau masalah lainnya, jadi penting untuk memiliki salinan data yang aman.
   a. Matikan Koneksi Internet: Jika Anda memiliki kekhawatiran bahwa virus Anda dapat mengakses internet atau mengirimkan data, matikan koneksi internet atau putuskan dari jaringan.
   b. Mode Aman (Safe Mode):
      1) Restart komputer Anda.
      2) Saat komputer mulai booting (sebelum logo Windows muncul), tekan tombol F8 berulang-ulang.
      3) Pilih opsi "Safe Mode with Networking" (atau serupa) menggunakan tombol panah pada keyboard dan tekan Enter.
      4) Masuk ke akun pengguna Anda.
   c. Perbarui dan Jalankan Antivirus:
      1) Pastikan Anda memiliki program antivirus yang mutakhir. Jika tidak, instal antivirus terbaru.
      2) Perbarui definisi virus.
      3) Jalankan pemindaian penuh (full scan) dengan antivirus Anda.
      4) Jika virus terdeteksi, biarkan antivirus menghapus atau mengkarantina file yang terinfeksi.

d. Gunakan Alat Pemindaian Tambahan:
    1) Setelah pemindaian antivirus, Anda juga dapat menggunakan alat pemindaian tambahan seperti Malwarebytes, AdwCleaner, atau HitmanPro.
    2) Unduh alat tersebut dari situs resmi, instal, dan jalankan pemindaian penuh.
e. Pemeriksaan Manual:
    1) Periksa daftar program yang terinstal di komputer Anda. Hapus program yang mencurigakan atau tidak dikenal.
    2) Periksa ekstensi browser Anda dan hapus ekstensi yang mencurigakan atau tidak diinginkan.
f. Perbarui Perangkat Lunak dan Sistem Operasi:
    1) Pastikan sistem operasi, perangkat lunak, dan driver Anda diperbarui ke versi terbaru.
    2) Perbarui browser, plugin, dan perangkat lunak lainnya yang mungkin telah dieksploitasi oleh virus.
g. Hapus File yang Tidak Dikenal:
    1) Telusuri direktori tempat virus mungkin menyembunyikan diri (misalnya, folder Temporary atau Downloads).
    2) Hapus file yang mencurigakan, tetapi pastikan Anda tahu apa yang Anda hapus.
h. Cek untuk Perubahan pada Setelan Sistem:
    1) Periksa perubahan yang mungkin dilakukan oleh virus pada pengaturan sistem atau registry.
    2) Kembalikan setelan yang mencurigakan atau tidak dikenal ke setelan default.
i. Ubah Kata Sandi, setelah virus dihilangkan, ubah kata sandi untuk akun-akun penting Anda sebagai langkah pencegahan.

j. Uji Komputer, setelah Anda merasa yakin bahwa virus telah dihapus, restart komputer Anda secara normal dan periksa apakah semua berjalan lancar. Pastikan tidak ada tanda-tanda perilaku mencurigakan atau infeksi lainnya.

1.6 Antivirus & Macam-Macam Antivirus

Antivirus adalah sebuah jenis perangkat lunak yang digunakan untuk mendeteksi dan menghapus virus komputer dari sistem komputer. Anti virus ini merupakan aplikasi disebut juga Perangkat Lunak Perlindungan dari Virus. Aplikasi ini dapat menentukan apakah sistem komputer telah terinfeksi virus atau tidak. Umumnya, perangkat lunak ini berjalan di latar belakangi (*background*) dan melakukan pemindaian terhadap semua file yang diakses (dibuka, dimodifikasi, atau ketika disimpan). Sebagian besar antivirus bekerja dengan beberapa metode seperti di bawah ini:

1. Pendeteksian dengan menggunakan basis data virus signature (*virus signature database*)
2. Pendeteksian dengan melihat cara bagaimana virus bekerja
   Tabel berikut berisi beberapa antivirus yang beredar di pasaran :

Produk	**Alamat Antivirus**
Norton Antivirus (Symantec)	https://us.norton.com/
McAfee Antivirus	https://www.mcafee.com/
Avast Antivirus	https://www.avast.com/id-id/index#pc
AVG Antivirus	https://www.avg.com/id-id/homepage#pc
Kaspersky AntivirusBitdefend	https://www.kaspersky.com/

er Antivirus	
ESET NOD32 Antivirus	https://www.eset.com/
Trend Micro Antivirus	https://www.trendmicro.com/en_id/business.html
Avira Antivirus	https://www.avira.com/en/free-antivirus-windows
Sophos Antivirus	https://home.sophos.com/en-us
Malwarebytes	https://www.malwarebytes.com/
Windows Defender (Built-in Windows Antivirus)	https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-antivirus-windows?view=o365-worldwide
Panda Antivirus	https://www.pandasecurity.com/en/homeusers/free-antivirus/
F-Secure Antivirus	https://www.f-secure.com/en/internet-security
Webroot SecureAnywhere Antivirus	https://www.webroot.com/us/en/home/products/av
Bullguard	https://www.bullguard.com/
Sophos Home	https://home.sophos.com/en-us
Comodo	https://antivirus.comodo.com/
Immunet Antivirus	https://www.immunet.com/index
dll	

Pada dasarnya, ketika semua perangkat terhubung pada sebuah jaringan maka keamanan jaringan perlu dijaga dengan baik. Sebab jaringan bisa menjadi tempat masuknya serangan kejahatan

siber, mulai dari hacking, cracking, spoofing, carding, dan lain sebagainya.

Ada 5 prinsip yang perlu ditetapkan untuk menjaga keamanan jaringan yaitu *Confidentiality*, *Integrity*, *Availability*, *Authentication*, dan *Access Control*. Tiga yang disebutkan merupakan pertama dikenal dengan CIA Triad, dimana *Confidentiality*, *Integrity*, dan *Availability* adalah unsur utama keamanan jaringan. Kemudian untuk menyempurnakannya dibutuhkan *Authentication* dan *Access Control*.

1. *Confidentiality* dalam keamanan jaringan
   Prinsip pertama dalam keamanan jaringan adalah *confidentiality* atau kerahasiaan. Dalam prinsip confidentiality, sebuah data hanya bisa diakses oleh orang yang memiliki hak, dan informasi yang ada didalamnya bersifat rahasia. Pihak yang tidak memiliki hak untuk mengakses tidak diperkenankan untuk memasuki atau membaca data yang ada didalamnya..
2. *Integrity* dalam keamanan jaringan
   Prinsip keamanan jaringan yang kedua adalah integrity atau integritas. Integritas yang dimaksud dalam keamanan jaringan adalah integritas data. Dimana data yang ada dalam sebuah sistem informasi yang terhubung dalam sebuah jaringan hanya bisa diubah oleh pihak yang memiliki wewenang legal saja. Misalkan pemilik rekening saja yang bisa memindahkan nominal isi rekeningnya. Jika isi rekening berubah tanpa sepengetahuan dirinya, maka terjadi masalah integritas data dalam sistem dan jaringan tersebut.
3. *Availability* dalam keamanan jaringan
   Prinsip ketiga dalam keamanan jaringan adalah availability. Availability masuk dalam prinsip keamanan jaringan karena sebuah data informasi yang disimpan dalam server harus dapat diakses kapan saja dan dimana saja oleh pemiliknya. Data harus selalu dapat diakses saat dibutuhkan, dan jika data tidak dapat diakses maka telah terjadi gangguan keamanan yang

mengakibatkan seorang pemilik data tidak bisa mengakses data milik mereka.

4. *Authentication* dalam keamanan jaringan
   Prinsip keempat dalam keamanan jaringan adalah autentikasi. Dengan autentikasi, sebuah sistem akan mengenali apakah pengakses data adalah orang yang memiliki hak akses atau tidak.
   Dalam sistem keamanan finansial, banyak metode autentikasi yang melibatkan metode tambahan seperti token, PIN, face detection, OTP, maupun autentikasi 2 arah. Semua itu ditujukan untuk memberikan keamanan ekstra.
5. *Access control* dalam keamanan jaringan
   Prinsip terakhir dalam keamanan jaringan adalah *access control*. Dalam sebuah sistem yang terhubung dengan jaringan, akan lebih baik jika sistem miliki role berjenjang. *Access control* akan memberikan akses kepada setiap orang yang memiliki hak, dan memiliki akses yang berbeda-beda sesuai dengan tujuan akses.

1.7 Aspek Kemanan Komputer dan Jaringan

Secara spesifik untuk menghindari dari gangguan yang ada pada komputer dan jaringan, berikut ini merupakan aspek penting dalam keamanan Komputer dan Jaringan :

1. Keamanan Jaringan (*Network Security*)
   Beberapa aspek yang termasuk dalam keamanan jaringan meliputi:
   a. *Firewall*, berfungsi untuk mengontrol lalu lintas jaringan antara jaringan internal dan eksternal. Ini membantu mencegah akses yang tidak sah ke jaringan internal.
   b. Enkripsi, melindungi informasi dari akses oleh pihak yang tidak berwenang selama transmisi.
   c. *Virtual Private Network* (VPN), memastikan koneksi jaringan yang aman melalui Internet seperti akses

jaringan internal dari lokasi eksternal dengan cara yang aman dan terenkripsi.

d. Keamanan Protokol Jaringan, memastikan bahwa protokol jaringan yang digunakan memiliki lapisan keamanan yang sesuai untuk mencegah serangan dan eksploitasi.
e. Deteksi dan Pencegahan Intrusi (IDS/IPS), digunakan untuk mendeteksi aktivitas mencurigakan di jaringan dan mengambil tindakan pencegahan untuk menghentikan serangan.
f. Segmen Jaringan, memisahkan jaringan ke dalam segmen yang berbeda untuk mengurangi dampak serangan yang menyebar di seluruh jaringan.
g. Manajemen Akses, mengelola hak akses pengguna ke sumber daya jaringan dengan tepat.
h. Pemantauan Jaringan, mengawasi lalu lintas jaringan untuk mendeteksi aktivitas yang mencurigakan atau anomali yang mungkin menandakan upaya masuk.
i. Penilaian Keamanan dan Uji Penetrasi, penilaian keamanan dan uji penetrasi secara berkala.
j. Kesadaran Pengguna, memberikan pemahaman terhadap pengguna, sehingga berupaya untuk melakukan update pengetahuan dan pengendalian penggunaan jaringan yang baik.

2. Keamanan Data (*Data Security*)

   Keamanan data dalam sistem keamanan komputer dan jaringan mengacu pada upaya untuk melindungi data dari ancaman dengan akses yang tidak sah terhadap perubahan tidak sah, dan kebocoran.. Beberapa aspek yang termasuk dalam keamanan data dalam sistem keamanan komputer dan jaringan meliputi: Enkripsi Data; Otorisasi dan Akses; Perlindungan Perimeter; Pengamanan Perangkat Lunak; Manajemen Identitas dan Akses (IAM): Pengelolaan identitas

pengguna dan hak akses mereka ke data dan sumber daya lainnya dengan tepat; Backup dan Pemulihan; Pemantauan dan Deteksi Intrusi; Penilaian Keamanan.

3. Keamanan Aplikasi (*Aplication Security*)
   Melindungi aplikasi perangkat lunak dari kerentanannya terhadap ancaman dan serangan yang dapat membahayakan integritas, kerahasiaan, dan ketersediaan data atau sistem yang dioperasikan oleh aplikasi tersebut. Aplikasi perangkat lunak adalah komponen penting dalam lingkungan teknologi informasi, dan rentan terhadap keamanan, dalam aplikasi dapat dieksploitasi oleh peretas untuk mendapatkan akses tidak sah, mencuri data, atau merusak sistem. Oleh karena itu, penting untuk memperhatikan keamanan aplikasi selama proses pengembangan, implementasi, dan pemeliharaannya.
4. Keamanan Identifikasi dan Akses (I*dentification and Access Security*).
   Keamanan identifikasi dan akses dalam sistem keamanan komputer dan jaringan adalah serangkaian langkah dan kebijakan yang diterapkan untuk melindungi informasi identitas pengguna dan memastikan bahwa hak akses ke sumber daya dan layanan dalam lingkungan IT hanya diberikan kepada pengguna yang berwenang. Tujuan utama dari keamanan identifikasi dan akses adalah untuk menjaga keutuhan data, mencegah akses tidak sah, dan mengendalikan hak pengguna dalam jaringan dan sistem.

1.8 Perinsip keamanan komputer

Prinsip keamanan komputer merupakan seperangkat pedoman dari rancangan atau usaha untuk melindungi informasi dan sistem komputer dari ancaman, serangan. Berikut adalah beberapa prinsip keamanan komputer yang penting:

1. Prinsip Pertahanan Lapisan (*Layered Defense*), menerapkan pertahanan dalam lapisan-lapisan untuk melindungi sistem.

Ini mencakup penggunaan firewall, perangkat lunak antivirus, antispyware, serta pengawasan dan pemantauan jaringan.

2. Pembaruan Teratur (*Regular Updates*), memastikan semua perangkat lunak, sistem operasi, dan aplikasi Anda diperbarui ke versi terbaru. Pembaruan ini sering kali mengatasi kerentanan keamanan yang dapat dimanfaatkan oleh penyerang.
3. Pengelolaan Sandi yang Kuat (*Strong Password Management*), menggunakan kata sandi yang kuat dan unik untuk setiap akun. Hindari kata sandi yang mudah ditebak atau terkait dengan informasi pribadi.
4. Otorisasi dan Hak Akses (*Authorization and Access Control*), mengatur tingkat akses yang tepat untuk pengguna dalam sistem. Hanya berikan akses yang diperlukan dan hindari memberikan akses administrator secara berlebihan.
5. Enkripsi Data (*Data Encryption*), menggunakan enkripsi untuk melindungi data sensitif saat disimpan atau ditransmisikan. Ini membantu mencegah akses tidak sah bahkan jika data jatuh ke tangan yang salah.
6. Pengawasan Aktivitas (*Monitoring Activities*), memantau aktivitas di dalam jaringan dan sistem untuk mendeteksi perilaku mencurigakan atau aktivitas yang tidak biasa.
7. Pengelolaan Resiko (*Risk Management*), mengidentifikasi dan mengevaluasi risiko keamanan dan mengambil tindakan untuk mengurangi risiko tersebut.
8. Pengelolaan Backup (*Backup Management*), melakukan cadangan data secara teratur untuk mengantisipasi kemungkinan kehilangan data akibat serangan atau kegagalan perangkat keras.
9. Pengetahuan dan Pelatihan Pengguna (*User Education and Training*), mengedukasi pengguna tentang ancaman

keamanan, praktik terbaik, dan cara menghindari serangan melalui pelatihan dan kesadaran keamanan.

10. Penghapusan yang Aman (*Secure Disposal*): Memastikan data sensitif dihapus secara aman dari perangkat yang tidak lagi digunakan untuk menghindari risiko penyalahgunaan data.
11. Keandalan Perangkat Keras dan Perangkat Lunak (*Hardware and Software Reliability*): Menggunakan perangkat keras dan perangkat lunak yang andal serta aman. Hindari menggunakan perangkat lunak bajakan atau tidak sah.
12. Pemantauan dan Tanggapan Insiden (*Incident Monitoring and Response*): Menyiapkan rencana untuk merespons insiden keamanan yang mungkin terjadi dan mengatasi masalah dengan cepat untuk meminimalkan dampak.

Prinsip keamanan komputer adalah suatu strategi dalam sistem keamanan yang dirancang untuk melindungi sistem komputer dan data dari ancaman, serangan, sehingga tidak terjadi risiko. Hal ini dinyatakan bebas dari virus/gangguan yang mempengaruhi proses komputer dan hilangnya data serta akuratnya informasi yang disampaikan sesuai tujuannya dan dapat di lisensikan sebagai bebas dari virus. Tujuan dari prinsip-prinsip keamanan komputer ini adalah untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi serta mengurangi risiko potensial yang dapat merugikan pengguna atau organisasi.

DAFTAR PUSTAKA

Ahyuna, A. and Aryasa, K. 2017. 'Sistem Pakar Diagnosa Dan Tatalaksana Penyakit Demam Berdarah Dengue Menggunakan Jaringan Saraf Tiruan Backpropagation', *E-JURNAL JUSITI : Jurnal Sistem Informasi dan Teknologi Informasi*, 6(1), pp. 1–11. Available at: http://ejurnal.dipanegara.ac.id/index.php/jusiti/article/view/40.

Aryasa, K. and Musu, W. 2016. 'Sistem Pakar Otomatisasi Penentuan Standar Baku Mutu Limbah Pertambangan Nikel Menggunakan Algoritma Supervised Mechine', *Konik 2016*, 1(1), pp. 82–87.

Indit Rahmawati. 2016. 'Pemanfaatan Media Pembelajaran', *El-Wasathiya: Jurnal Studi Agama*, 5(1), pp. 1–56. Available at: https://ejournal.poltektegal.ac.id/index.php/siklus/article/view/298%0Ahttp://repositorio.unan.edu.ni/2986/1/5624.pdf%0Ahttp://dx.doi.org/10.1016/j.jana.2015.10.005%0Ahttp://www.biomedcentral.com/1471-2458/12/58%0Ahttp://ovidsp.ovid.com/ovidweb.cgi?T=JS&P.

Ir. Suhanda, M.K. 2014. 'Manfaat Pembelajarankecerdasan Buatan Dan Aplikasinya Bagi Mahasiswa Informatika Dan Komputer', *Jurnal Teknik Informatika*, 4(2), pp. 23–34.

Muttaqin, K.S., Harmonvikler Dumoharis Lumban Raja, Adhi Prasetio, Harizahayu Rahmadini Darwas, Teguh Priyantoro, N. and Fergie Joanda Kaunang, Hartanto Tantriawan, Hasanuddin Sirait Zelvi Gustiana, Darsin, Andryanto. A, J.S. 2022. *BIG DATA : Informasi dalam Dunia Digital*. 1st edn, *Yayasan Kita Menulis*. 1st edn. Edited by Yayasan Kita Menulis. Medan: Yayasan Kita Menulis. Available at: https://kitamenulis.id/2022/04/28/big-data-informasi-dalam-dunia-digital/.

Usmanto, B.S. 2017. 'EXPERT JURNAL SISTEM INFORMASI', *FAKULTAS ILMU KOMPTER BANDAR LAMPUNG*, 7(2). Available at: https://doi.org/10.36448/jmsit.v7i2.963.

Wulandari, Novi Yohanes, S.A. 2018. *Sistem Pakar Untuk Mendiagnosa dan Klasifikasi Anak Berkebutuhan Khusus Dengan Backward Dan Forward Chaining Pada Slb Cahaya Pertiwi di Bekasi*. Jurnal Ilm, *Jurnal Ilmu Komputer*. Jurnal Ilm. Edited by A.Y. Siregar. BEKASI, JAW BARAT: Jurnal Ilmu Komputer-JIK.

BAB 2
IDENTIFIKASI ANCAMAN TERHADAP KEAMANAN KOMPUTER

Oleh Mundzir

2.1 Ancaman Keamanan Komputer

Ancaman terhadap keamanan komputer mengacu pada segala bentuk potensi risiko, serangan, atau gangguan yang dapat membahayakan integritas, kerahasiaan, dan ketersediaan sistem komputer, perangkat lunak, data, serta infrastruktur jaringan. Ancaman ini dapat datang dalam berbagai bentuk, seperti perangkat lunak berbahaya, tindakan penipuan, serangan siber, atau tindakan yang bertujuan mencuri, merusak, serta mengganggu operasi normal dari sistem komputer.

Menurut John D. Howard dalam bukunya "*An Analysis of security incidents on the internet*" menyatakan bahwa : "Keamanan komputer adalah tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab". (Howard, 1998)

Keamanan komputer mencakup 4 aspek yakni *privacy*, integrity, *authentication*, dan *availability* (Negara, 2014).

1. *Privacy* atau *confidentiality*
   Privacy tentang kerahasian informasi. Pada dasarnya aspek *privacy* adalah menjaga informasi agar tidak terlihat atau diakses oleh orang yang tidak berwenang. Sebagai contoh, *email* seseorang tidak boleh dibaca orang lain termasuk administrator.

2. *Integrity*
   Integrity tentang keutuhan informasi. Pada dasarnya aspek *integrity* ini yaitu menjaga informasi agar tetap aman. Informasi tidak boleh diubah, kecuali mendapat izin dari pemilik informasi. *Trojan horse*, *Virus*, atau pemakai lain yang memperbaharui informasi tanpa adanya izin dari pemiliknya merupakan contoh persoalan yang mengganggu.
3. *Authentication*
   Berkenaan dengan keabsahan pemilik informasi. Harus ada cara untuk mengetahui bahwa informasinya *valid*, lalu yang mengakses informasi tersebut adalah orang yang berwenang, yang juga diperkenankan memberikan informasi tersebut pada orang lain.
   Penerapan *access control* seperti *login* dan *password* merupakan usaha yang harus dilakukan dalam pemenuhan aspek ini. *Digital signature* dan *watermarking* juga adalah salah satu usaha untuk melindungi *intellectual property*.
4. *Avaibility*
   Hal ini berkaitan dengan ketersediaan informasi. Contoh serangan pada aspek ini adalah *Denial of Service attack* (DoS *attack*). Misalkan, *server* dikirim *request* palsu secara beruntun agar tidak bisa melayani permintaan lain.

Tujuan utama ancaman terhadap keamanan komputer adalah mengakses informasi sensitif, merusak sistem, atau memanfaatkan sumber daya komputer secara tidak sah.

Ancaman terhadap keamanan komputer sangat beragam dan terus berkembang seiring dengan perkembangan teknologi dan kebutuhan para penyerang. Berikut adalah beberapa contoh ancaman umum yang sering terjadi terhadap keamanan komputer adalah sebagai berikut :

1. *Malware*
   Termasuk virus, *worm*, trojan, *ransomware*, *spyware*, dan *adware*. *Malware* dirancang untuk merusak sistem, mencuri data, atau mengambil alih kontrol sistem.
2. Serangan DDoS (*Distributed Denial of Service*)
   Serangan ini bertujuan untuk membuat sumber daya sistem tidak tersedia bagi pengguna yang sah dengan membanjiri *server* dengan lalu lintas yang berlebihan.
3. *Phishing*
   Penipuan di mana penyerang menyamar sebagai entitas terpercaya untuk mencuri informasi pribadi, seperti kata sandi dan informasi penting dari korban.
   Contoh: Pengirim *email* palsu yang menyamar sebagai bank atau layanan lainnya dan meminta pengguna untuk memasukkan informasi pribadi atau *login* mereka di situs palsu. Adapun tujuannya adalah mencuri data pengguna.
4. Serangan *Man-in-the-Middle* (MITM)
   Penyerang mengintersepsi komunikasi antara dua pihak yang sah untuk mencuri informasi atau memanipulasi data yang dikirim.
   Penyerang yang mampu menyusup dalam komunikasi antara pengguna dan situs web yang sah. Ini memungkinkan penyerang untuk mencuri informasi seperti nama pengguna dan kata sandi.
5. Serangan *Brute Force*
   Penyerang mencoba semua kombinasi yang mungkin dari kata sandi untuk mendapatkan akses ke akun atau sistem.
   Penyerang menggunakan alat otomatis untuk mencoba semua kombinasi yang mungkin dari kata sandi hingga menemukan yang benar dan mendapatkan akses ke akun.

6. Eksploitasi Kerentanan
   Penyerang memanfaatkan kerentanan dalam perangkat lunak atau sistem operasi yang tidak diperbarui yang memungkinkan penyerang mendapatkan akses ke sistem.
7. Serangan *Zero-Day*
   Penyerang menggunakan kerentanan yang belum diketahui oleh pihak yang sah atau produsen perangkat lunak untuk menyusup ke dalam sistem atau dengan kata lain penyerang memanfaatkannya sebelum pengembang perangkat lunak mengeluarkan pembaruan .
8. *Sniffing* Jaringan
   Penyerang memantau lalu lintas jaringan untuk mencuri informasi sensitif yang dikirim dalam teks biasa.
9. *Social Engineering*
   Penyerang memanipulasi atau memanfaatkan kelicikan psikologis untuk mendapatkan akses ke sistem atau informasi sensitif.
   Contoh: Penyerang berusaha memanipulasi orang untuk membagikan informasi sensitif, seperti dengan menelepon dan berpura-pura menjadi petugas dukungan teknis yang membutuhkan informasi login.
10. Akses Tidak Sah
    Upaya masuk ke sistem atau jaringan tanpa izin atau otorisasi yang tepat.
11. Pencurian Identitas (*Identity Theft*)
    Penyerang mencuri identitas korban untuk melakukan kegiatan ilegal atau mendapatkan manfaat finansial.
12. *Keylogging*
    Penyerang menggunakan perangkat lunak untuk merekam setiap ketukan tombol pada *keyboard* korban, sehingga dapat mencuri informasi sensitif, termasuk kata sandi.

13. *Insider Threat*
    Ancaman yang berasal dari dalam organisasi, seperti karyawan yang tidak setia atau mantan karyawan yang memiliki akses ke sistem.
14. Ransomware
    Jenis *malware* yang mengenkripsi data korban dan menuntut tebusan untuk mendapatkan kunci dekripsi.
15. *Advanced Persistent Threat*
    Serangan jangka panjang yang dilakukan oleh kelompok atau entitas yang sangat terorganisir dan canggih untuk memperoleh akses ke sasaran tertentu, seperti yang dilakukan oleh kelompok mata-mata.
16. *Exploit Kit*
    Serangan berbasis web yang menggunakan kit eksploitasi untuk menyusup ke dalam sistem pengguna yang tidak disadari saat mengunjungi situs yang terinfeksi.
17. *Malvertising*
    Iklan *online* yang menyusupkan *malware* ke dalam sistem pengguna yang mengklik iklan tersebut.
18. *Botnet*
    Jaringan komputer yang dikendalikan oleh penyerang untuk melakukan serangan bersama-sama, seperti serangan DDoS.

Ini hanya beberapa contoh ancaman yang dapat membahayakan keamanan komputer. Semakin kompleks dan terhubungnya dunia digital, semakin banyak pula jenis ancaman yang muncul. Penting bagi organisasi dan pengguna untuk selalu meningkatkan kesadaran keamanan dan mengadopsi langkah-langkah perlindungan yang tepat untuk melindungi sistem dan data dari ancaman tersebut.

2.2 Identifikasi Ancaman Keamanan Komputer

Identifikasi ancaman keamanan komputer adalah proses mengenali potensi ancaman atau bahaya terhadap sistem komputer, jaringan, perangkat lunak, dan data yang disimpan di dalamnya. Tujuan dari identifikasi ancaman keamanan komputer adalah untuk memahami berbagai jenis ancaman yang mungkin terjadi dan mengidentifikasi potensi kerentanannya sehingga langkah-langkah perlindungan yang tepat dapat diambil untuk mengurangi risiko dan melindungi aset informasi.

Dengan melakukan identifikasi ancaman keamanan komputer secara efektif, organisasi dan individu dapat mengambil langkah-langkah yang diperlukan untuk melindungi data sensitif, menjaga ketersediaan dan integritas sistem, serta mencegah potensi kerugian yang ditimbulkan oleh serangan atau ancaman keamanan. Ancaman terhadap keamanan komputer berasal dari berbagai latar belakang yang melibatkan faktor teknologi, ekonomi, sosial, dan politik. Beberapa latar belakang yang mendasari terjadinya ancaman terhadap keamanan komputer antara lain :

1. Teknologi yang Berkembang
   Perkembangan teknologi informasi dan komunikasi (TIK) telah memberikan banyak manfaat bagi masyarakat, namun juga membuka celah baru untuk serangan siber. Semakin kompleksnya infrastruktur teknologi, perangkat lunak, dan jaringan membuka peluang bagi penyerang untuk menemukan dan mengeksploitasi kerentanannya.
2. Motivasi Ekonomi
   Motivasi ekonomi menjadi salah satu latar belakang utama di balik serangan siber. Penyerang dapat mencari keuntungan finansial dengan mencuri data pribadi, melakukan penipuan, memeras melalui *ransomware*, atau mencuri informasi bisnis rahasia untuk keuntungan kompetitif.

3. Perangkat Lunak dan Sistem yang Rentan
   Ketidaksempurnaan dalam perangkat lunak dan sistem operasi membuka celah bagi penyerang untuk memanfaatkan kerentanannya. Ketika perangkat lunak tidak diperbarui secara teratur, celah keamanan dapat tetap ada dan dapat dimanfaatkan oleh penyerang.
4. Kesadaran Keamanan yang Rendah
   Kurangnya kesadaran keamanan di kalangan pengguna akhir maupun di dalam organisasi menyebabkan pengguna sering kali tidak memahami risiko yang mereka hadapi dan tidak mengambil tindakan yang tepat untuk melindungi diri mereka sendiri atau perusahaan mereka.
5. Teknik Sosial
   Serangan siber seringkali melibatkan teknik sosial di mana penyerang memanipulasi korban untuk mengungkapkan informasi pribadi atau menjalankan tindakan tertentu, seperti mengklik tautan berbahaya atau membuka lampiran berbahaya.
6. Perkembangan Aplikasi dan *Internet of Things* (IoT)
   Dengan semakin banyaknya aplikasi dan perangkat yang terhubung melalui Internet of Things, potensi untuk serangan siber juga meningkat. Perangkat yang tidak aman dapat menjadi pintu masuk bagi penyerang untuk mengakses jaringan atau data sensitif.
7. Kekurangan Tenaga Ahli Keamanan
   Permintaan akan tenaga ahli keamanan siber yang berkualifikasi melebihi pasokan, yang menyebabkan celah dalam perlindungan keamanan pada banyak organisasi.
8. Politik dan Konflik Internasional
   Serangan siber juga dapat menjadi alat dalam konflik internasional dan digunakan sebagai sarana untuk spionase atau perang siber antar negara.

Semua latar belakang ini, bersamaan dengan kemajuan teknologi dan konektivitas yang terus berlanjut, mengakibatkan peningkatan jumlah dan kompleksitas ancaman terhadap keamanan komputer. Oleh karena itu, upaya untuk mengatasi ancaman ini memerlukan pendekatan yang holistik dan kolaboratif dari berbagai pihak termasuk individu, perusahaan, pemerintah, dan komunitas keamanan siber.

Identifikasi ancaman terhadap keamanan komputer sangat penting karena memiliki dampak besar dalam melindungi integritas, kerahasiaan, dan ketersediaan data dan sistem Anda. Berikut adalah beberapa alasan mengapa identifikasi ancaman perlu dilakukan :

1. Perlindungan Aktiva Berharga
   Identifikasi ancaman membantu Anda mengidentifikasi aset yang paling berharga dan rentan terhadap serangan. Ini memungkinkan Anda untuk fokus pada perlindungan aset-aset ini dengan langkah-langkah keamanan yang lebih kuat.
2. Pemahaman Tentang Ancaman
   Dengan mengidentifikasi ancaman yang mungkin, Anda dapat memahami bagaimana penyerang mungkin mencoba masuk atau merusak sistem Anda. Ini memungkinkan Anda untuk mempersiapkan pertahanan yang lebih baik.
3. Pencegahan dan Pengurangan Risiko
   Dengan mengetahui ancaman yang ada, Anda dapat mengambil langkah-langkah proaktif untuk mencegah serangan. Ini termasuk penerapan kebijakan keamanan yang lebih baik, memperbarui perangkat lunak secara teratur, dan melindungi celah yang diketahui.
4. Pemantauan dan Deteksi Dini
   Identifikasi ancaman membantu Anda dalam memilih alat pemantauan yang tepat dan mengatur deteksi dini untuk mendeteksi aktivitas yang mencurigakan atau tidak diinginkan dalam sistem.

5. Penanganan Insiden yang Lebih Baik
   Dalam hal terjadi pelanggaran keamanan atau insiden serangan, memiliki pemahaman yang baik tentang ancaman memungkinkan Anda untuk mengevaluasi kerugian yang mungkin terjadi dan merancang tanggapan yang lebih efektif.
6. Perencanaan Keamanan yang Lebih Baik
   Identifikasi ancaman membantu Anda merencanakan strategi keamanan yang lebih baik. Anda dapat mengalokasikan sumber daya dan anggaran dengan lebih efektif untuk melindungi sistem Anda.
7. Peningkatan Kesadaran Keamanan
   Dengan menyadari berbagai ancaman yang mungkin terjadi, Anda dapat meningkatkan kesadaran keamanan di kalangan pengguna dan karyawan. Ini mengurangi risiko tindakan ceroboh yang dapat menyebabkan serangan.
8. Kepatuhan Hukum dan Regulasi
   Banyak industri memiliki standar dan peraturan ketat terkait keamanan data. Dengan mengidentifikasi ancaman dan mengambil langkah-langkah untuk melindungi data, Anda dapat mematuhi persyaratan hukum dan regulasi ini.
9. Mengurangi Kerugian Bisnis
   Serangan keamanan yang berhasil dapat menyebabkan kerugian finansial dan reputasi. Identifikasi ancaman dan pencegahan yang sesuai dapat mengurangi risiko ini.
10. Perlindungan terhadap Teknologi Masa Depan
    Dengan teknologi yang terus berkembang, ancaman terhadap keamanan komputer juga akan berkembang. Identifikasi ancaman membantu Anda dalam mempersiapkan perlindungan terhadap ancaman baru yang mungkin muncul.

Secara keseluruhan, identifikasi ancaman adalah langkah penting dalam strategi keamanan komputer yang menyeluruh. Ini membantu mengurangi risiko serangan, melindungi data sensitif, dan menjaga kelancaran operasi bisnis .

Adapun proses identifikasi ancaman keamanan komputer melibatkan beberapa langkah, termasuk :

1. Pengumpulan Informasi
   Mengumpulkan informasi tentang sistem komputer, jaringan, dan perangkat lunak yang digunakan. Ini melibatkan pemahaman tentang arsitektur dan konfigurasi sistem.
2. Analisis Kerentanan
   Menganalisis sistem untuk mengidentifikasi kerentanannya. Kerentanan adalah titik lemah dalam sistem yang bisa dimanfaatkan oleh pihak yang tidak berwenang untuk merusak atau mengakses data.
3. Penilaian Ancaman
   Mengidentifikasi berbagai jenis ancaman yang mungkin dihadapi oleh sistem komputer, seperti serangan *virus*, *malware*, peretasan, serangan DDoS (*Distributed Denial of Service*), dan lain-lain.
4. Penentuan Risiko
   Mengevaluasi dampak potensial dari ancaman yang diidentifikasi terhadap sistem dan data. Ini melibatkan penilaian seberapa serius ancaman tersebut dan seberapa besar potensi kerugiannya .
5. Pemetaan Ancaman dan Kerentanan
   Menghubungkan antara ancaman yang diidentifikasi dan kerentanan yang ada dalam sistem. Ini membantu dalam memahami bagaimana ancaman dapat memanfaatkan kerentanan untuk merusak sistem.
6. Penentuan Langkah Perlindungan

Berdasarkan analisis risiko, langkah-langkah perlindungan dan mitigasi harus ditentukan. Ini bisa meliputi penerapan perangkat lunak keamanan, pembaruan sistem, konfigurasi firewall, penggunaan enkripsi, dan praktik keamanan lainnya.

7. Pemantauan dan Peningkatan
   Ancaman keamanan komputer terus berkembang, oleh karena itu identifikasi ancaman harus menjadi proses berkelanjutan. Pemantauan terus-menerus terhadap tren keamanan dan peningkatan sistem perlindungan sangat penting.

DAFTAR PUSTAKA

Amin Muftiadi. 2022. Studi kasus keamanan jaringan komputer: analisis ancaman phisingterhadap layanan online banking. *Hexatech: Jurnal Ilmiah Teknik*.

Ancaman Yang Dapat Merusak Komputer dan Internet. 2013. Diakses dari https://pemkomedan.go.id/artikel-11537-ancaman-yang-dapat-merusak-komputer-dan-internet.html

Hafiz, 2022. 2 Ancaman Keamanan Komputer Terbesar Saat Ini. Diakses dari https://aliyhafiz.com/2-ancaman-keamanan-komputer/#:~:text=Ancaman%20keamanan%20komputer%20adalah%20potensi,yang%20tidak%20berhak%20seperti%20ransomware.

Dwyer, C., & Kanguri, A. 2017. Malvertising - A Rising Threat To The Online Ecosystem. *Journal of Information Systems Applied Research*.

Herru Hardiyansah, S.Kom, 2017. Keamanan Komputer dan Jaringan. Diakses dari https://bkpsdmd.babelprov.go.id/content/keamanan-komputer-dan-jaringan#:~:text=Beberapa%20 ancaman %20keamanan%20komputer %20adalah,%2Cspam%20dan%20lain%20lain

Hasibuan, M. S. 2016. Keylogger pada Aspek Keamanan Komputer. *Teknovasi*.

Howard, J. D. 1998. An Analysis of Security Incidents on the Internet 1989-1995. In *Engineering and Public Policy*.

Kaspersky. 2021. Zero-Day Exploits & Zero-Day Attacks . In *What is a Zero-day Attack? - Definition and Explanation*.

Li, Y., & Liu, Q. 2021. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*. https://doi.org/10.1016/j.egyr.2021.08.126

Munawar, Z., Kom, M., & Putri, N. I. 2020. Keamanan Jaringan Komputer Pada Era Big Data. *Jurnal Sistem Informasi-J-SIKA*.

Negara, E. S. 2014. Implementasi Management Network Security Pada Laboratorium Cisco Universitas Bina Darma. *Jurnal Ilmiah*.

Putri Harliana, D. 2008. Sniffing dan Spoofing Pada Aspek Keamanan Komputer. *Jurnal-Keamanan-Komputer*.

PGP: Pretty good privacy. 1995. *Computers & Mathematics with Applications*. https://doi.org/10.1016/0898-1221(95)90256-2

Tatam, M., Shanmugam, B., Azam, S., & Kannoorpatti, K. 2021. A review of threat modelling approaches for APT-style attacks. In *Heliyon*. https://doi.org/10.1016/j.heliyon.2021.e05969

Venter, I. M., Blignaut, R. J., Renaud, K., & Venter, M. A. 2019. Cyber security education is as essential as "the three R's." *Heliyon*. https://doi.org/10.1016/j.heliyon.2019.e02855

BAB 3
KONSEP DASAR KEAMANAN KOMPUTER

Oleh Ino Sulistiani

3.1 Pendahuluan

Konsep dasar keamanan computer adalah sebuah metode atau konsep yang menjadi latar belakang dasar sebuah pemikiran keamanan pada sebuah sistem komputer. Sistem komputer adalah sebuah area kerja computer yang terdiri dari komponen-komponen yaitu: *hardware componen*, *software* component dan *brainware* component saling keterkaian satu dengan lainnya untuk mencapai tujuan syistem .

Pada tulisan ini penulis akan memberikan konsep dasar keamanan pada sebuah aplikasi computer yang terimplementasi pada sebuah aplikasi sistem informasi akademik. Dimana untuk membangun sebuah sistem, apapun bentuknya diperlukan aspek dasar keamanan yang merupakan pondasi awal terciptanya sebuah sistem yang *secure* walaupun tidak tertutup kemungkinan adanya *security hole* pada sistem tersebut.

Keamanan sistem dapat diketahui kapabilitas keamanannya dengan melakukan asesmen menggunakan kerangka model kualitas diantaranya ISO (Organisasi Standarisasi Internasional), *Control Objectives for Information and Related Technology* (COBIT), dengan melakukan pengukuran terhadap tata kelola keamanan informasi sebuah sistem informasi maka akan diketahui kondisi keamanan sebuah sistem. Apakah sistem tersebut benar-benar aman ataukah masih terdapat lubang-lubang yang dapat menjadi celah tidak amannya sebuah sistem.

3.2 Latar Belakang Diperlukannya Keamanan Sistem

Mengapa diperlukan keamanan sistem, merupakan pertanyaan yang mendasar yang merupakan pondasi dalam menciptakannya sebuah keamanan sistem, apapun sistemnya. Semakin tingginya penggunaan computer dan perkembangan teknologi informasi yang begitu cepat menyebabkan tingkat *computer crime* juga meningkat, ini dilihat semakin tingginya kejahatan computer pada sistem informasi ataupun sistem jaringan publik., antara lain tingginya penggunaan *mobile banking*, *electronic commerce* (*e-commerce*), *electronic government* (*e-government*) semuanya ini adalah penggunaan teknologi informasi dan jaringan computer.

Desentralisasi server adalah salah satu alasan mengapa diperlukannya keamanan. Dengan mengimplementasikan desentralisasi server maka akan memerlukan banyak waktu dan sumber daya manusia untuk mengatur server di tiap titik. Hal ini disebabkan semakin bervariasinya penggunaan suatu sistem operasi dan perangkat lunak dalam suatu sistem, akibatnya, tenaga sumber daya manusia diperlukan lebih banyak untuk melakukan monitoring terhadap isu-isu keamanan, dibandingkan dengan sistem yang dibangun oleh perangkat lunak yang homogen.

Semakin meningkatnya level kesejahteraan masyarakat pengguna computer. Sehingga pengguna level pemula sampai dengan level mahir mencoba "bermain" atau membongkar sistem yang digunakannya atau sistem milik orang lain dengan mendapatkan informasi dari buku-buku ataupun dari informasi di jaringan internet.

Kemudahan pemakai computer mendapatkan software di jaringan internet untuk menyerang computer dan jaringan computer. Banyaknya informasi dan software hacking yang disediakan oleh situs-situs di jaringan internet yang memberikan

dukungan dari yang berkemampuan sederhana sampai dengan berkemampuan dahsyat.

Selain itu keterlambatan terlirisnya *Security Patch*. Seringnya *patching* sekuriti terlambat dilakukan oleh administrator. *Security patch* adalah program perbaikan yang berkaitan dengan keamanan suatu sistem. Contohnya computer dan server yang banyak harus ditangani oleh sebab itu vendor perangkat lunak atau sistem operasi seperti Microsoft selalu mendalukan dukungan teknis dan bantuan *hot-line* terhadap permasalahan costumer.

Diperlukannya komitmen bersama antara praktisi IT, aparat, dan pihak berwenang untuk melaksanakan dan menegakkan *cyberlaw*.

3.3 *Information Based Security*

Information Based Security atau keamanan informasi adalah sebuah kebutuhan mutlak bagi semua pengguna dan pengelola informasi. Keamanan informasi adalah perlindungan terhadap sumberdaya informasi pada semua pihak yang tidak bertanggung jawab yang dapat menyalahgunakannya.

Information Based Security atau keamanan informasi menurut G. J. Simons adalah bagaimana usaha untuk dapat mencegah penipuan (*cheating*) atau bisa mendeteksi adanya penipuan pada sistem yang berbasis informasi, di mana informasinya sendiri tidak memiliki arti fisik.

Ada empat kebenaran utama yang sering dikaitkan dengan sistem informasi, yang dikenal dengan istilah "Four Information System Truths." Keempat kebenaran ini adalah:

1. Data is the foundation: Informasi yang dihasilkan oleh sistem informasi bersumber dari data. Data adalah kumpulan fakta-fakta mentah yang tidak memiliki makna atau konteks. Data ini perlu diolah dan dikonversi menjadi informasi yang bermakna.

2. Processes create information: Proses atau aktivitas yang dilakukan menghasilkan data yang kemudian diubah menjadi informasi. Proses-proses ini bisa berupa pengolahan transaksi, analisis, komunikasi, dan lain sebagainya.
3. Information is distributed: Informasi yang dihasilkan oleh sistem informasi perlu didistribusikan kepada orang yang membutuhkannya dalam organisasi. Distribusi informasi ini harus efisien dan tepat waktu, sehingga orang yang tepat mendapatkan informasi yang diperlukan untuk mengambil keputusan.
4. Information is a corporate resource: Informasi dianggap sebagai sumber daya yang penting, sejajar dengan sumber daya lain seperti tenaga kerja, modal, dan material. Pengelolaan informasi yang baik dapat memberikan keuntungan kompetitif bagi organisasi.

Dengan terimplementasinya keempat kebenaran maka keamanan informasi akan tercipta pada sebuah sistem.

Selain itu sebuah sistem juga harus memiliki parameter-parameter yang menjadi acuan akan terciptanya sebuah keamanan pada sistemnya. Paramenetr-parameter tersebut penulis menyebutnya sebagai elemen utama keamanan informasi yaitu :

1. Kerahasiaan (*Confidentiality*): Ini berarti memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang. Cara-cara untuk mencapai kerahasiaan meliputi enkripsi data, pengaturan izin akses, dan penggunaan autentikasi yang kuat seperti kata sandi yang kompleks.
2. Integritas (*Integrity*): Integritas berarti melindungi informasi dari perubahan yang tidak sah atau tidak diinginkan. Ini melibatkan penggunaan kontrol integritas

yang memungkinkan untuk mendeteksi perubahan data yang tidak sah dan memastikan bahwa data tetap utuh.

3. Ketersediaan (*Availability*): Informasi harus tersedia untuk orang-orang yang berwenang ketika mereka membutuhkannya. Ini melibatkan manajemen risiko terhadap gangguan atau kegagalan sistem yang dapat menghambat ketersediaan informasi.
4. Otentikasi (*Authentication*): Ini adalah proses memverifikasi identitas seseorang atau entitas yang mencoba mengakses sistem atau data. Contohnya termasuk autentikasi berbasis kata sandi, kartu akses, sidik jari, atau pengenalan wajah.
5. Otorisasi (*Authorization*): Setelah otentikasi, otorisasi menentukan apa yang diperbolehkan oleh pengguna yang telah diverifikasi. Ini melibatkan pengaturan izin dan hak akses yang sesuai untuk setiap pengguna atau peran dalam sistem.
6. Pemantauan (*Monitoring*): Ini adalah proses pemantauan aktivitas sistem dan jaringan untuk mendeteksi dan merespons ancaman atau insiden keamanan. Alat pemantauan dan inspeksi intrusi digunakan untuk mengidentifikasi aktivitas mencurigakan.
7. Pengelolaan Risiko (*Risk Management*): Organisasi perlu mengidentifikasi, mengevaluasi, dan mengelola risiko keamanan informasi. Ini melibatkan tindakan seperti analisis risiko, penilaian kerentanan, dan penerapan kontrol keamanan yang sesuai.
8. *Pelatihan dan Kesadaran (Training* and Awareness): Mengedukasi pengguna dan staf tentang praktik keamanan informasi yang baik sangat penting. Ini membantu mencegah insiden yang disebabkan oleh kesalahan manusia dan membuat pengguna lebih sadar tentang ancaman keamanan.

9. Pengelolaan Kejadian Keamanan (*Security Incident Management*): Organisasi perlu memiliki prosedur dan rencana untuk mengatasi insiden keamanan jika terjadi. Ini termasuk pelaporan, investigasi, dan respons yang cepat terhadap insiden.
10. Kontinuitas Bisnis (*Business Continuity*): Organisasi perlu merencanakan bagaimana mereka akan menjalankan operasi mereka dalam situasi darurat atau setelah insiden besar. Ini melibatkan perencanaan pemulihan bencana dan backup data yang baik.
11. Kepatuhan (*Compliance*): Organisasi mungkin harus mematuhi regulasi dan standar keamanan tertentu yang berlaku, seperti GDPR, HIPAA, atau ISO 27001. Kepatuhan ini sering melibatkan audit dan pelaporan rutin.

Sedangkan algoritma kriptografi dibedakan menjadi beberapa jenis yaitu:

1. Kriptografi Simetris (*Symmetric Cryptography*):
    a. Dalam kriptografi simetris, kunci yang sama digunakan untuk enkripsi dan dekripsi data.
    b. Contoh algoritma simetris termasuk AES (Advanced Encryption Standard), DES (Data Encryption Standard), dan 3DES (Triple DES).
2. Kriptografi Asimetris (*Asymmetric Cryptography*):
    a. Dalam kriptografi asimetris, ada sepasang kunci: kunci publik untuk enkripsi dan kunci pribadi untuk dekripsi.
    b. Contoh algoritma asimetris termasuk RSA (Rivest-Shamir-Adleman), DSA (*Digital Signature Algorithm*), dan ECC (*Elliptic Curve Cryptography*).
3. *Hash Functi*ons (Fungsi Hash):
    a. Fungsi hash mengambil data dan menghasilkan nilai hash (*checksum*) tetap panjang.

   b. Tidak seperti enkripsi, fungsi hash tidak dapat didekripsi; mereka digunakan untuk memeriksa integritas data.
   c. Contoh fungsi hash termasuk SHA-256 (*Secure Hash Algorithm 256-bit*) dan MD5 (*Message Digest Algorithm 5*).
4. Kriptografi Hibrida (*Hybrid Cryptography*):
   a. Adalah kombinasi dari kriptografi simetris dan asimetris.
   b. Kunci simetris digunakan untuk mengenkripsi data, dan kunci asimetris digunakan untuk mengamankan kunci simetris yang digunakan.
   c. Metode ini menggabungkan efisiensi enkripsi simetris dengan manfaat keamanan kunci asimetris.
5. Kriptografi Kunci Umum (*Homomorphic Cryptography*):
   a. Adalah jenis kriptografi yang memungkinkan komputasi dilakukan pada data terenkripsi tanpa harus mendekripsi data tersebut.
   b. Kriptografi Kunci Umum penting dalam komputasi terdistribusi dan privasi data.
6. Kriptografi Kuantum (*Quantum Cryptography*):
   a. Ini adalah jenis kriptografi yang dirancang untuk mengamankan komunikasi dalam lingkungan kuantum.
   b. Dengan memanfaatkan prinsip-prinsip mekanika kuantum, ini dapat menawarkan tingkat keamanan yang sangat tinggi.
7. Kriptografi Multi-pihak (*Multi-party Computation*):
   a. Adalah jenis kriptografi yang memungkinkan berbagai pihak untuk berbagi dan mengolah data tanpa mengungkapkan informasi rahasia mereka kepada yang lain.

b. Kriptografi Multi-pihak berguna dalam skenario di mana beberapa pihak perlu bekerja bersama namun ingin menjaga kerahasiaan data mereka.

3.4 Cyber security Crime

3.4.1 Definisi Cyber Security

Cyber security crime adalah upaya yang dilakukan untuk melindungi sistem komputer dari berbagai ancaman atau akses ilegal. *Cybersecurity* adalah disiplin yang mencakup berbagai tindakan, teknologi, kebijakan, dan praktik yang dirancang untuk:

1. Melindungi Data dan Informasi Sensitif: Ini melibatkan mencegah akses yang tidak sah atau pencurian data rahasia, seperti informasi pribadi, data perusahaan, atau rahasia industri.
2. Mencegah Serangan Terhadap Sistem: Ini termasuk melindungi perangkat keras dan perangkat lunak komputer dari serangan yang dapat mengganggu operasi normal atau merusak sistem.
3. Mengamankan Jaringan Komputer: Ini melibatkan perlindungan terhadap serangan jaringan, termasuk serangan DoS (*Denial of Service*), serangan phishing, malware, dan banyak lagi.
4. Menjaga Integritas Data: Mencegah perubahan atau manipulasi data yang tidak sah selama penyimpanan atau transmisi.
5. Menjaga Ketersediaan Sistem: Memastikan bahwa sistem dan layanan yang penting tetap tersedia untuk pengguna yang sah dan tidak terpengaruh oleh serangan atau gangguan.
6. Mengelola Identitas dan Akses: Mengelola dan memverifikasi identitas pengguna yang mengakses sistem, serta memberikan hak akses yang sesuai.

7. Deteksi dan Respons Terhadap Serangan: Mendeteksi serangan yang terjadi dan meresponsnya dengan cepat untuk membatasi kerusakan yang mungkin terjadi.
8. Pemulihan Data: Memiliki rencana pemulihan bencana untuk mengembalikan sistem dan data ke kondisi normal setelah insiden keamanan.

3.4.2 Jenis Keamanan Siber

Keamanan siber melibatkan berbagai jenis perlindungan, tindakan, dan teknik yang dirancang untuk melindungi sistem, jaringan, data, dan pengguna dari berbagai ancaman siber. Berikut adalah beberapa jenis keamanan siber yang umum:

1. Keamanan Jaringan (*Network Security*):
   a. Melibatkan perlindungan terhadap jaringan komputer dari serangan, gangguan, atau akses yang tidak sah.
   b. Teknik meliputi firewall, IDS (*Intrusion Detection System*), IPS (*Intrusion Prevention System),* dan isolasi jaringan.
2. Keamanan Perangkat Lunak (*Software Security*):
   a. Melibatkan perlindungan perangkat lunak dari kerentanannya terhadap serangan siber.
   b. Termasuk pembaruan perangkat lunak, patching kerentanan, dan pemindaian keamanan perangkat lunak.
3. Keamanan Sistem Operasi (*Operating System Security*):
   a. Berfokus pada perlindungan sistem operasi dari ancaman seperti malware, rootkit, dan serangan jaringan.
   b. Administrasi hak akses dan kebijakan keamanan adalah bagian penting dari ini.

4. Keamanan Aplikasi Web (*Web Application Security*):
   a. Melibatkan perlindungan aplikasi web dari serangan seperti SQL *injection*, *Cross-Site Scripting* (XSS), dan *Cross-Site Request Forgery* (CSRF).
   b. Pengembangan aman dan pengujian keamanan aplikasi web merupakan aspek penting.
5. Keamanan End-User (*End-User Security*):
   a. Fokus pada kesadaran dan perilaku pengguna akhir dalam upaya mencegah serangan phishing, social engineering, dan serangan yang mengandalkan kesalahan pengguna.
6. Keamanan Email (*Email Security*):
   a. Berfokus pada perlindungan email dari spam, phishing, malware, dan ancaman lainnya yang dapat dikirim melalui email.
   b. Pemfilteran email dan pelatihan pengguna adalah komponen penting.
7. Keamanan Cloud (*Cloud Security*):
   a. Melibatkan perlindungan data dan aplikasi yang disimpan di lingkungan komputasi awan.
   b. Ini melibatkan pengaturan kebijakan, kontrol akses, enkripsi data, dan pemantauan dalam lingkungan awan.
8. Keamanan Mobile (*Mobile Security*):
   a. Fokus pada perlindungan perangkat mobile, aplikasi, dan data dari serangan siber.
   b. Ini mencakup penggunaan kata sandi yang kuat, enkripsi, dan pemantauan perangkat mobile.
9. Keamanan Jaringan Nirkabel (*Wireless Network Security*).
   a. Melibatkan perlindungan jaringan nirkabel (Wi-Fi) dari akses yang tidak sah dan serangan terhadap protokol jaringan nirkabel.
   b. Penggunaan enkripsi WPA/WPA2 adalah salah satu teknik umum.

10. Keamanan Internet of Things (*IoT Security*):
    a. Berfokus pada perlindungan perangkat IoT yang terhubung ke internet dari serangan dan penyalahgunaan.
    b. Penggunaan kata sandi yang kuat, pembaruan perangkat lunak, dan kontrol akses adalah komponen penting.
11. Keamanan Kriptografi (*Cryptography Security*):
    a. Melibatkan penggunaan teknik kriptografi untuk melindungi data saat berpindah antara pihak yang terlibat dalam komunikasi.
    b. Ini termasuk enkripsi data dan manajemen kunci.
12. Keamanan Fisik (*Physical Security*):
    a. Melibatkan perlindungan fisik perangkat keras, perangkat komputer, dan data dari akses yang tidak sah atau pencurian.
13. Keamanan Manajemen Identitas (*Identity Management*):
    a. Fokus pada pengelolaan identitas pengguna dan hak akses mereka ke dalam sistem dan aplikasi.

Beberapa cara yang dapat memastikan bahwa proses keamanan bekerja dengan baik pada sebuah aplikasi yaitu dengan membuat prosedur autentikasi, otorisasi, enkripsi, logging, dan uji keamanan aplikasi.

3.4.3 Jenis Ancaman *Security Crime*

Kejahatan siber (*cybersecurity crime*) mencakup berbagai jenis ancaman yang dirancang untuk merusak, mengakses, atau mengendalikan sistem komputer, jaringan, data, atau informasi pribadi secara ilegal atau tidak sah. Berikut adalah beberapa jenis ancaman keamanan siber yang umum:

1. Malware (*Malicious Software*):
    a. *Virus*: Program yang dapat menggandakan diri dan menyisipkan diri ke dalam program atau file lain.

b. *Worm*: Program yang dapat menyebar ke komputer lain melalui jaringan tanpa bantuan manusia.
c. *Trojan* (*Trojan Horse*): Program yang tampaknya bermanfaat atau sah tetapi sebenarnya mengandung kode berbahaya.
d. *Ransomware*: Malware yang mengenkripsi data korban dan meminta tebusan untuk mendapatkan kunci dekripsi.
e. *Spyware*: Perangkat lunak yang dirancang untuk memantau dan mencuri informasi pribadi pengguna tanpa izin mereka.
f. Adware: Perangkat lunak yang menampilkan iklan yang tidak diinginkan kepada pengguna.

2. Phishing:
   Teknik manipulasi sosial di mana penyerang mencoba untuk memperoleh informasi sensitif, seperti kata sandi dan informasi keuangan, dengan menyamar sebagai entitas tepercaya melalui email, pesan teks, atau situs web palsu.
3. Serangan DDoS (*Distributed Denial of Service*):
   Serangan yang bertujuan membuat sumber daya komputer atau situs web tidak tersedia dengan cara mengalirkan lalu lintas internet yang sangat besar ke target, sehingga menghambat akses pengguna yang sah.
4. Serangan *Man-in-the-Middle* (MITM):
   Penyerang mencoba memasuki komunikasi antara dua pihak yang sah dan memata-matai atau mengubah data yang sedang ditransmisikan tanpa sepengeta*huan mereka.*
5. *Serangan Brute Force*:
   Penyerang mencoba untuk menebak kata sandi atau kunci enkripsi dengan mencoba semua kombinasi yang mungkin secara berurutan.

6. Serangan *Zero-Day*:
   Serangan yang mengeksploitasi kerentanan perangkat lunak yang belum diketahui oleh pembuat perangkat l*unak atau pihak berwenang.*
7. *Serangan RCE (*Remote Code Execution):
   Penyerang memanfaatkan kerentanan dalam aplikasi atau sistem untuk menjalankan kode jahat dari jarak jauh.
8. Serangan *Ransomware-as-a-Service* (RaaS):
   Penyerang menggunakan perangkat lunak ransomware yang dapat disewa atau dibeli untuk melakukan serangan.
9. Serangan Insider:
   Ancaman yang berasal dari dalam organisasi, seperti karyawan yang memanfaatkan akses mereka untuk tujuan jahat.
10. Serangan *Internet of Things (IoT*):
    Penyerang menargetkan perangkat IoT yang lemah keamanannya, seperti kamera keamanan atau alat rumah pintar, untuk mengakses jaringan atau data sensitif.
11. Serangan *Supply Chain*:
    Ancaman yang terkait dengan rantai pasokan, di mana penyerang mencoba menyusupkan perangkat lunak berbahaya atau perangkat keras yang telah dimodifikasi ke dalam produk atau layanan yang digunakan oleh target mereka.
12. Serangan Pencurian Identitas (*Identity Theft*):
    Penyerang mencuri informasi identitas individu dengan tujuan penggunaan ilegal atau penipuan.
13. Serangan Rongrongan (Spoofing):
    Penyerang memalsukan identitas, alamat IP, atau informasi lainnya untuk mengecoh korban atau sistem keamanan.
14. Serangan Web Application:
    Penyerang mengeksploitasi kerentanan dalam aplikasi web untuk meretas atau merusak data.

15. Serangan Cryptojacking:
    Penyerang menggunakan perangkat komputer atau server korban untuk menambang mata uang kripto tanpa izin.

Setiap jenis ancaman keamanan siber ini memiliki karakteristik, tujuan, dan metode yang berbeda. Upaya keamanan siber yang efektif melibatkan deteksi dini, pencegahan, dan respons terhadap berbagai jenis ancaman ini.

3.5 *Security Hole* (Lubang Keamanan)

Security Hole atau lubang keamanan adalah celah keamanan yang terjadi akibat beberapa faktor yang membuat sistem menjadi lemah yang memungkinkan untuk terjadi kerusakan, teretas dan lain sebagainya. Security hole juga merupakan kesalahan pada analisis awal dalam sebuah perancangan sistem jaringan yang bisa saja terjadi dari beberapa kesalahan yaitu salah desain, salah implementasi, salah konfigurasi, dan salah penggunaan.

3.5.1 Salah Desain

Salah desain adalah kesalahan yang sangat sulit untuk diperbaiki, disebabkan kesalahan desain adalah faktor kelemahan walaupun sistem telah diimplementasikan dengan baik tetap terdapat kesalahan yang merupakan kelemahan dari sistem disebabkan kesalahan pendesainan. Contohnya saat membangun dan mendesain jaringan, salah membuat dan membagi subnet jaringan yang akan secara tidak langsung akan mempengaruhi kinerja dan membuka lubang-lubang keamanan. Contoh lainnya adalah implementasi yang salah dalam penggunaan alamat IP Private sehingga terlihat penempatan perangkat yang salah yaitu tidak menggunakan firewall pada mesin server, konfigurasi paket data yang salah dimana paket data dapat langsung menuju ke mesin server.

3.5.2 Salah Konfigurasi

Kesalahan konfigurasi adalah kesalahan yang dilakukan mengakibatkan celah keamanan sebuah sistem. Contohnya ada sebuah sistem seharusnya berkas pada sistem tersebut tidak dapat diubah kecuali oleh pemilik sah. Dengan kondisi seperti itu maka ada celah user lain dapat mengganti informasi tersebut.

3.5.3 Implementasi Kurang Baik

Implementasi kurang baik, artinya biasanya terjadi disebabkan masalah waktu sehingga membuatkan kesalahan proses pengkodean akibatnya tidak dilakukan proses testing karena mengganggap sistem sudah sempurna tanpa ada celah. Selain tidak dilakukan testing juga pada software yang dibeli dari pihak ketiga.

Konstruksi jaringan yang kurang baik, misalnya menempatkan hardware pada tempat-tempat yang bisa diakses oleh orang lain secara mudah, menenpatkan mesin server pada komputer client lainnya, menempatkan hub atau switch tanpa adanya keamanan sedikitpun misalnya dibawah meja, atau sistem kabel yang berserakan dan tidak ditutup dengan pipa khusus ke dinding akan memudahkan orang lain yang tidak berhak mengakses layanan secara fisik

3.5.4 Salah Menggunakan Program atau Sistem

Lubang keamanan bisa juga diakibatkan oleh salah menggunakan program atau sistem. Biasanya kesalahan dalam memilih software misalnya antivirus atau program firewall, walaupun sudah menggunakannya tetap saja kebobolan dari serangan virus-virus disebabkan adanya kesalahan konfigurasi yaitu dengan menonaktifkan firewall sedangkan antivirus bekerja sendirian menghadapi serangan virus. Akibatnya, sistem tetap terkontaminasi virus dan tidak aman. Hal inilah yang

menyebabkan adanya celah keamanan yang bisa berdampak negatif terhadap sistem.

3.6 Instrumen Keamanan *Privacy, Confidentiality, Integrity, Authentication, Availability, dan Control Access* sebagai Aspek Dasar Keamanan Sebuah Sistem Informasi.

Definisi sistem informasi adalah kombinasi dari teknologi informasi dan aktivitas orang yang menggunakannya untuk mendukung operasi dan manajemen. Sistem informasi juga bisa di definisikan sebagai gabungan yang terorganisasi dari manusia, perangkat lunak, perangkat keras, jaringan komunikasi dan sumber data dalam mengumpulkan, mengubah dan menyebarkan informasi dalam organisasi. Tujuan dari sistem informasi adalah menghasilkan informasi. Sistem informasi selalu melibatkan data-data penting dimana data yang diolah menjadi bentuk yang berguna bagi para pemakainya.

Komponen sistem informasi terdiri dari komputer, instruksi, fakta yang tersimpan, manusia dan prosedur sehingga dapat dikategorikan dalam empat bagian yaitu sistem informasi manajemen, sistem pendukung keputusan, sistem informasi eksekutif, dan sistem pemprosesan transaksi.

Tulisan ini berfokus pada sistem informasi manajemen, khususnya sistem informasi akademik. Sistem Informasi Akademik adalah sistem atau aplikasi yang diimplementasikan pada sebuah perguruan tinggi atau sekolah dimana dalam proses penciptaannya dilakukan proses analisis dan desain, dimana sistem ini bertujuan melakukan pengelolaan data terkait informasi pendidikan. Untuk melindungi data-data pada sebuah sistem informasi manajemen khususnya sistem informasi akademik diperlukan 6 (enam) aspek dasar keamanan penulis menyebutnya sebagai instrumen kualitas dimana instrumen kualitas ini menunjang keamanan sebuah

sistem informasi manajemen yaitu *privacy, confidentiality, integrity, authentication, availability*, dan *control access.*

3.6.1 Privacy

Dideskripsikan sebagai usaha menjaga informasi dari orang yang tidak berhak mengakses dan sifat data privat.

Inti utama aspek privacy atau confidentiality adalah usaha untuk menjaga informasi informasi dari orang yang tidak berhak mengakses. Privacy lebih kearah data-data yang bersifat privat, sedangkan confidentiality biasanya berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu tersebut.

Privacy mempunyai 2 (dua) faktor kualitas yang penting untuk diimplementasikan pada sebuah sistem informasi akademik agar sistem tersebut *secure* yaitu kontrol terhadap orang yang tidak berhak mengakses yaitu usaha yang dilakukan untuk menjaga informasi dari orang yang tidak berhak mengakses. dan klasifikasi data bersifat privat yaitu mengklasifikasikan kearah data-data yang sifatnya privat. Kedua faktor kualitas inilah yang wajib ada pada semua sistem informasi khususnya sistem informasi akademik.

3.6.2 *Confidentiality*

Dideskripsikan sebagai usaha untuk menjaga informasi dengan memberikan data-data sistem informasi akademik kepada pihak lain untuk keperluan tertentu dan hanya diperbolehkan untuk keperluan tertentu tersebut.

Confidentiality mempunyai 11 (sebelas) faktor kualitas yang harus terimplementasi pada sebuah sistem informasi akademik bertujuan membuat sistem menjadi *secure* yaitu (1)kontrolabilitas akses adalah akses kontrol sistem informasi akademik yang berada dibawah kontrol pengguna, (2) kontrol akses terhadap source code adalah kontrol membatasi pengguna untuk mengakses informasi menggunakan source code pada sistem informasi akademik, (3) perlindungan informasi log adalah melindungi

informasi terhadap akses yang tidak sah dari penyerang, (4) perlindungan data uji adalah usaha melindungi hasil uji sistem informasi akademik, (5) kontrol terhadap kode jahat adalah membatasi kode-kode yang tidak diketahui fungsi dan manfaatnya yang sewaktu-waktu dapat aktif dan beraksi membahayakan sistem, (6) manajemen *removeable* media adalah proses pengaturan terhadap *removeable* media yaitu media penyimpanan komputer yang dirancang untuk dimasukkan dan dilepas dari sistem informasi akademik, (7) time out sesi adalah waktu yang digunakan pengguna login tetapi tanpa aktvitas sama sekali, akibatnya pengguna dilogout secara otomatis, (8) Kekuatan algoritma kriptografik, (9) kekuatan algoritma kriptografik adalah fungsi algoritma kriptografi yang berfungsi menyembunyikan informasi dari orang-orang yang tidak berhak atas informasi tersebut, (10) ketepatan enkripsi data adalah pengaman data yang dikirimkan agar terjaga kerahasiannya, dimana plaintext (pesan asli) diubah menjadi kode-kode yang tidak dimengerti, dan (11) manajemen kunci kriptografik adalah proses pengaturan pengamanan data oleh private key dan public key saat melakukan enkripsi dan dekripsi.

3.6.3 *Integrity*

Dideskripsikan sebagai sifat informasi yang tidak boleh diubah tanpa seizin pemilik informasi. Integrity memiliki faktor kualitas yang harus dimiliki sebuah sistem informasi khususnya sistem informasi akademik agar menciptakan sebuah sistem yang *secure* yaitu (1) kesesuaian integritas data adalah informasi atau data yang diterima harus sesuai dan sama persis seperti saat informasi atau data dikirimkan, (2) pencegahan korupsi data internal adalah tindakan yang mencegah terjadinya kerusakan atau hilangnya data, (3) inventaris asset adalah pengelolaan data dan informasi agar tidak terjadi kerusakan atau kehilangan yang disebabkan oleh virus, trojanhorse, atau pemakai lain yang

mengubah informasi tanpa izin, (4) back up informasi adalah proses membuat data cadangan dengan cara menyalin atau membuat arsip data computer sehingga data tersebut dapat digunakan kembali apabila terjadi kerusakan atau kehilangan, (5) prosedur pengoperasian terdokumentasi adalah prosedur pengoperasian sistem informasi akademik dibuat, didokumentasikan, diterapkan dan dipelihara, (6) logging keliru adalah laporan atau pencatatan keliru yang terjadi di sebuah sistem informasi akademik disebabkan virus, trojan horse dan *hacker*, dan (7) dokumentasi keamanan adalah proses pengumpulan, pemilihan, pengolahan, dan penyimpanan informasi dan data sistem informasi akademik sebagai sebagai prosedur keamanan.

3.6.4 *Authentication*

Authentication dideskripsikan sebagai cara untuk menyatakan bahwa informasi, orang, ataupun server adalah betul-betul asli. Adapun faktor-faktor kualitas yang wajib dimiliki agar sebuah sistem menjadi *secure* adalah (1) kesesuaian protocol otentikasi adalah proses konfirmasi identitas sebagai prosedur persetujuan mengakses atau memberikan informasi kepada yang berhak, (2) registrasi pengguna adalah pendaftaran pengguna sebelum menggunakan sistem, (3) manajemen sandi pengguna adalah mengatur kata sandi, (4) manajemen hak akses adalah proses pengaturan hak terkoneksi dengan server dan mendapat layanan sistem, dan (5) pembatasan akses informasi adalah prosedur akses control terhadap yang berhak mengakses informasi.

3.6.5 *Availability*

Availability dideskripsikan *sebagai* ketersediaan data dan informasi saat dibutuhkan dan dimanfaatkan oleh orang yang berhak. Adapun faktor-faktor kualitas yang diimplementasikan pada sistem informasi akademik agar sistem tersebut menjadi

secure adalah sebagai berikut (1) ketersedian layanan adalah kondisi dimana layanan sistem informasi akademik siap dimanfaatkan saat dibutuhkan, (2) ketersedian informasi yang dibutuhkan kondisi dimana informasi siap dimanfaatkan saat dibutuhkan dan (3) pemanfaatan informasi oleh orang yang berhak adalah kondisi dimana informasi hanya siap digunakan dan dimanfaatkan oleh orang berhak

3.6.6 *Control Access*

Control access dideskripsikan sebagai cara pengaturan akses informasi. Ada beberapa faktor kualitas yang menjadi membuat sistem menjadi *secure* yaitu pengaturan akses informasi adalah metode yang dilakukan untuk membatasi akses informasi sesuai kebutuhan, (2) klasifikasi data adalah pengaturan data dari yang berhak mengakses, dan (3) klasifikasi user adalah pengaturan user berdasarkan tingkat kebutuhannya.

DAFTAR PUSTAKA

Deris Stiawan. 2005. *Sistem Keamanan Komputer* Jakarta PT Elex Media Komputindo Kelompok Gramedia, Jakarta

Faisal Halim. 2022. Pelayanan Perubahan Data pada Sistem Informasi Akademik di Perguruan Tinggi. Bening Media Publishing

Febria Sri Handayani, Meidyan Permata Putri, D Tri Octafian. 2021. Rekayasa Kualitas Perangkat Lunak (Teori dan Praktek)

Ino Sulistiani. 2023. Disertasi Analisis Desain Implementasi Aspek DasarKeamanan dan Usabilitas pada Layanan Aplikasi Sistem Informasi Akademik Quality Model Berbasis User Experience. Program Studi S3 Teknik Elektro Fakultas Teknik Universitas Hasanuddin

Nurrofiq, Nurjaya, Ahmad. 2021. *Steganografi* dalam Keamanan. Komputer (Teori dan Praktik). Penerbit Pascal Books

BAB 4
KOMPONEN KEAMANAN FISIK

Oleh Marlina

4.1 Pendahuluan

Komponen Keamanan fisik adalah salah satu komponen keamanan komputer yang paling penting untuk diperhatikan. Alasannya sederhana saja, percuma merancang aplikasi terbaik yang bebas *bug, server* terbaik, sistem keamanan logis yang baik, *firewall* terbaik, jika peretas dapat mengakses komputer secara fisik. Dengan mendapatkan akses secara fisik, maka perusakan data bisa langsung dilakukan dengan merusak *server* secara fisik, sehingga sistem sama sekali tidak dapat digunakan.

Gambar 4.1. Ilustrasi peretas yang mendapatkan akses fisik. (Sumber: https://media.istockphoto.com)

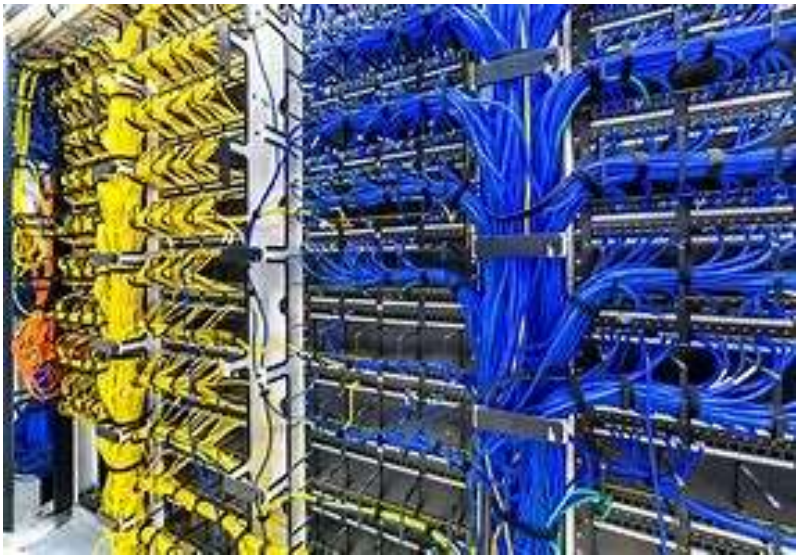
Secara umum, dapat diterapkan sepuluh lapis keamanan untuk melindungi server dari ancaman peretas secara fisik, yaitu:

1. Penempatan *server*.
2. Penempatan media *backup*.
3. Perimeter keamanan.
4. Pos jaga perimeter.
5. Pintu masuk gedung.
6. Akses pribadi ke zona aman.
7. Kontrol akses lift.
8. Koridor keamanan ruang data.
9. Keamanan ruangan data center.
10. Akses tingkat rak.

Tentu saja tidak harus menerapkan keseluruhan aspek diatas. Hanya saja, semakin banyak aspek yang diterapkan, maka semakin aman layanan dan data dari para peretas.

4.2 Penempatan *server*.

Penempatan *server* seharusnya ditempatkan pada rak *server* yang sulit di akses secara fisik, bebas dari banjir dan kebakaran. Oleh sebab itu, sebaiknya *server* tidak ditempatkan pada lantai dasar apalagi basement, melainkan pada lantai atas gedung yang bebas dari banjir serta memungkinkan untuk menerapkan beberapa lapis keamanan yang akan dijelaskan berikutnya.



Gambar 4.2. Ilustrasi penempatan *server* pada rak.
(Sumber: https://www.align.com)

4.3 Penempatan media *backup*.

Penempatan media *backup* adalah hal yang penting untuk diperhatikan. Beberapa *admin* secara ceroboh meletakkan media backup pada gedung yang sama dengan *production server*. Akibatnya, jika terjadi kebakaran, gempa bumi, huru hara atau kerusakan lainnya, maka media *backup* menjadi tidak berguna. Media *backup* harus disimpan pada lokasi yang berbeda secara geografis, minimal berada pada Gedung yang berbeda dengan *production server* nya.

Gambar 4.3. Lokasi *server* google yang terpisah secara geografis. (Sumber : https://qwords.com)

4.4 Perimeter keamanan.

Dalam Bahasa mudahnya, perimeter keamanan bisa berupa tembok pagar sekeliling gedung yang tidak mudah ditembus oleh *user* yang tidak berhak. Tembok pagar merupakan aspek pertama yang harus ada untuk mengamankan server dari *user* yang tidak berhak. Dengan pemisahan gedung dari wilayah umum menggunakan pagar tembok, maka petugas keamanan akan lebih mudah melaksanakan tugasnya untuk melakukan pencegahan awal dari akses yang tidak berkepentingan.

Gambar 4.4. Ilustrasi tembok pagar gedung data center.
(Sumber : https://arkonsuperpanel.co.id)

4.5 Pos jaga perimeter

Pos jaga harus ditempatkan pada pintu masuk halaman gedung, dan dijaga oleh petugas keamanan yang professional. Dengan penjagaan yang baik, maka setiap orang yang masuk dalam halaman gedung dapat diperiksa dengan teliti oleh petugas keamanan, termasuk dan tidak terbatas pada:

1. Memastikan yang datang adalah orang yang berhak, misalnya karyawan atau admin server.
2. Jika yang datang adalah pengunjung, maka petugas harus memastikan pada karyawan atau admin server yang akan datang.
3. Memeriksa kendaraan pengunjung, untuk memastikan keamanannya.

Gambar 4.5. Ilustrasi pos jaga Gedung data center.
(Sumber : https://www.minimalist.id)

4.6 Pintu masuk gedung.

Setelah pengunjung memarkirkan kendaraannya pada tempat yang ditentukan, maka pengunjung akan memasuki gedung. Pada pintu masuk gedung, pengunjung akan sekali lagi diperiksa oleh petugas gedung, untuk memastikan tujuan dari pengunjung, dan karyawan atau admin server yang akan menerima mereka. Pengunjung harus diberikan penanda, misalnya papan nama yang sesuai dengan tujuan pengunjung, serta menitipkan kartu identitas.

Gambar 4.6. Ilustrasi pintu masuk Gedung data center.
(Sumber : https://www.hospitalityinside.com)

4.7 Akses pribadi ke zona aman.

Data center yang baik seharusnya mempunyai ruang tamu yang aman, sehingga karyawan dapat menerima tamu pada zona yang aman, dan menjauhkan tamu dari akses yang tidak diinginkan pada server.

4.8 Kontrol akses lift.

Seperti yang sudah dijelaskan sebelumnya, server sebaiknya tidak ditempatkan pada lantai dasar, melainkan pada lantai atas, untuk menghindari bahaya banjir. Oleh sebab itu, akses ke ruang *server* biasanya akan menggunakan *lift*. Jika menggunakan *lift*, maka dapat menerapkan sistem keamanan berikutnya pada *lift*, sehingga pengunjung dan karyawan hanya dapat mencapai lantai yang diperbolehkan saja, dan tidak dapat mencapai lantai yang

bukan peruntukannya. Untungnya, hampir semua *lift* jaman sekarang mendukung penggunaan access *control card,* yang membatasi lantai yang dapat dicapai.

Gambar 4.7. Ilustrasi access control lift
(Sumber : https://www.fourwallssecurity.com.au)

4.9 Koridor keamanan ruang data.

Aspek keamanan berikutnya diterapkan sebelum memasuki ruang data. Pada koridor ruang data, sebaiknya ditempatkan karyawan, misalnya petugas keamanan atau receptionist untuk sekali lagi memastikan bahwa hanya user yang berhak yang dapat memasuki ruang data, misalnya hanya admin *server* yang ditempatkan pada ruangan tersebut.

Gambar 4.8. Ilustrasi penerima tamu Gedung data center (Sumber : https://thereceptionist.com)

4.10 Keamanan ruangan data center.

Ruang data center merupakan wilayah terpenting yang harus diamankan. Ruangan data server wajib mempunyai CCTV berkualitas tinggi yang selama 24 jam sehari nonstop merekam siapa pun yang ada didalam ruang server.

Gambar 4.9. Ilustrasi ruang server yang dilindungi CCTV
(Sumber : https://cild.eu)

4.11 Akses tingkat rak.

Pertahanan terakhir dan yang terpenting dari akses fisik adalah pengamanan rak server. Hanya teknisi yang berhak saja yang boleh membuka rak server dan mengakses semua peralatan didalamnya. Jadi, rak server harus dilindungi dengan pengaman sidik jari, atau yang lebih baik.

Gambar 4.10. Ilustrasi rak server yang dilindungi sidik jari
(Sumber : https://ipvm.com/)

4.12 Penutup

Setelah membaca bab ini, diharapkan agar pembaca dapat mengerti dan menerapkan komponen keamanan fisik pada servernya. Mengingat pentingnya keamana fisik ini karena walau sistem keamanan *software* sudah dibuat secanggih mungkin, namun jika ada celah keamanan pada akses fisik, maka semua itu menjadi tidak berguna. Jika peretas dapat mengakses secara fisik, maka cukup dengan membanting server atau memotong kabel jaringan, maka layanan akan terdisrupsi seketika itu juga.

DAFTAR PUSTAKA

Jauhary, Hilaluddin & Eldisa, Geta & Salim, Ariq & Fitroh, Fitroh. 2022*. Penerapan ISO27001 dalam Menjaga dan Meminimalisir Risiko Keamanan Informasi*: Literatur Review. Media Jurnal Informatika. 14. 43. 10.35194/mji.v14i1.1581.

Salman Nuzuli, Avon Budiyono, Ahmad Almaarif. 2020. *Analisis Dan Perancangan Keamanan Fisik Data Center Berdasarkan Standar Tia-942 Menggunakan Ppdioo Life-cycle Approach Di Pemerintahan Kabupaten Bandung Barat*. eProceedings of Engineering. ISSN: 2355-9365.

Setiawan, Erwin & Ijmania, Laras. 2020. *Perancangan Infrastruktur Teknologi Informasi Pada Sistem Pengelolaan Jaringan*: *Studi Kasus PT AJN*. Computer Science and Information Systems. 4. 90-101. 10.24912/computatio.v4i2.8958.

BAB 5
PEMANTAUAN DAN AUDIT KOMPUTER

Oleh Dudes Manalu

5.1 Pendahuluan

Pemantauan dan audit komputer adalah dua komponen penting dalam menjaga keamanan dan integritas sistem informasi. Dalam era digital yang semakin maju, organisasi mengandalkan sistem komputer dan jaringan untuk menyimpan, memproses, dan mengelola data penting mereka. Namun, dengan berkembangnya teknologi, juga ada peningkatan ancaman terhadap keamanan sistem-sistem ini.

Pemantauan komputer melibatkan pengamatan terus-menerus terhadap sistem komputer dan jaringan untuk mendeteksi aktivitas yang mencurigakan atau tidak sah. Tujuannya adalah untuk mengidentifikasi dan merespons serangan keamanan secara cepat, serta mencegah kerugian yang lebih besar.

Di sisi lain, audit komputer merupakan proses peninjauan dan evaluasi independen terhadap keamanan sistem komputer dan praktik pengelolaannya. Audit ini bertujuan untuk memastikan kepatuhan terhadap kebijakan keamanan yang ditetapkan, mengidentifikasi celah keamanan, dan memberikan rekomendasi perbaikan.

Pemantauan dan audit komputer bekerja secara sinergis untuk memberikan perlindungan yang kuat terhadap sistem informasi organisasi. Pemantauan berperan dalam mendeteksi serangan dan ancaman potensial secara real-time, sementara

audit memberikan gambaran menyeluruh tentang keadaan keamanan sistem dan memberikan langkah-langkah perbaikan yang diperlukan.

Dalam Bab ini, kita akan menjelajahi berbagai aspek penting yang terkait dengan pemantauan dan audit komputer. Kami akan membahas metode, teknik, dan praktik terbaik yang dapat digunakan untuk meningkatkan keamanan sistem informasi. Selain itu, kami juga akan membahas peran auditor komputer, etika dalam audit komputer, serta tantangan dan tren terbaru dalam bidang pemantauan dan audit komputer.

Dengan memahami pentingnya pemantauan dan audit komputer, serta menerapkan praktik yang tepat, organisasi dapat melindungi data sensitif mereka, mencegah kerugian finansial, dan menjaga kepercayaan pengguna dan mitra bisnis mereka.

5.2 Pengantar ke Pemantauan dan Audit Komputer

Pemantauan dan audit komputer adalah dua komponen penting dalam menjaga keamanan dan integritas sistem informasi suatu organisasi. Dalam era digital yang semakin maju, organisasi bergantung pada sistem komputer dan jaringan untuk menyimpan, memproses, dan mengelola data mereka. Namun, dengan perkembangan teknologi, juga ada peningkatan risiko keamanan yang harus ditangani dengan serius.

Pemantauan komputer melibatkan pengamatan terus-menerus terhadap sistem komputer dan jaringan untuk mendeteksi aktivitas yang mencurigakan atau tidak sah. Tujuannya adalah untuk mengidentifikasi dan merespons serangan keamanan secara cepat, serta mencegah kerugian yang lebih besar. Dengan pemantauan yang efektif, organisasi

dapat mengidentifikasi serangan, melacak jejak serangan, dan mengambil tindakan yang tepat untuk meminimalkan kerugian.

Audit komputer, di sisi lain, adalah proses peninjauan independen terhadap keamanan sistem komputer dan praktik pengelolaannya. Audit ini melibatkan evaluasi menyeluruh terhadap kebijakan keamanan yang ada, proses pengendalian, serta pemantauan dan perlindungan data sensitif. Tujuannya adalah untuk menilai keefektifan sistem keamanan, mengidentifikasi celah dan kelemahan, memberikan rekomendasi perbaikan, dan memastikan kepatuhan terhadap kebijakan dan standar yang ditetapkan.

Pemantauan dan audit komputer saling melengkapi dalam menjaga keamanan sistem informasi. Pemantauan berperan dalam mendeteksi serangan dan ancaman keamanan secara real-time, sementara audit memberikan tinjauan menyeluruh tentang keadaan keamanan sistem dan memberikan rekomendasi perbaikan yang diperlukan. Kombinasi keduanya membantu organisasi untuk memitigasi risiko keamanan, melindungi aset informasi, dan menjaga integritas sistem mereka.

5.2.1 Definisi dan Tujuan Pemantauan dan Audit Komputer

Pemantauan komputer adalah proses pengamatan dan pengawasan terus-menerus terhadap sistem komputer dan jaringan untuk mendeteksi aktivitas yang mencurigakan atau tidak sah. Pemantauan ini dilakukan dengan menggunakan alat dan teknik khusus untuk mengumpulkan dan menganalisis data yang relevan dengan tujuan mengidentifikasi ancaman keamanan, kerentanan sistem, atau pelanggaran kebijakan. Pemantauan komputer dapat melibatkan pengawasan lalu lintas jaringan, aktivitas pengguna, log sistem, dan penggunaan sumber daya komputer.

A. Tujuan Pemantauan Komputer

1. Mendeteksi serangan keamanan
   Pemantauan komputer membantu dalam mendeteksi serangan dan aktivitas mencurigakan, seperti upaya tidak sah untuk mendapatkan akses, percobaan penyerangan, malware, atau intrusi jaringan.
2. Tanggap terhadap insiden
   Dengan memantau sistem secara aktif, tim keamanan dapat merespons insiden keamanan dengan cepat dan mengambil langkah-langkah untuk membatasi kerusakan yang mungkin terjadi.
3. Pencegahan kerugian lebih lanjut
   Pemantauan komputer memungkinkan identifikasi awal dari ancaman dan celah keamanan, sehingga tindakan perbaikan dapat diambil untuk mencegah kerugian lebih lanjut dan melindungi aset informasi.
4. Pengumpulan bukti
   Pemantauan komputer juga dapat membantu dalam pengumpulan bukti terkait kegiatan yang mencurigakan atau melanggar hukum, yang dapat digunakan dalam proses penyelidikan atau litigasi.
5. Audit Komputer
   Audit komputer adalah proses peninjauan independen terhadap keamanan sistem komputer dan praktik pengelolaannya. Audit ini melibatkan evaluasi menyeluruh terhadap kebijakan keamanan yang ada, proses pengendalian, serta pemantauan dan perlindungan data sensitif. Tujuan audit komputer adalah untuk menilai keefektifan sistem keamanan, mengidentifikasi celah dan kelemahan, memberikan rekomendasi perbaikan, dan memastikan kepatuhan terhadap kebijakan dan standar yang ditetapkan.

B. Tujuan Audit Komputer:

1. Mengidentifikasi kelemahan keamanan:
   Audit komputer membantu dalam mengidentifikasi celah keamanan dalam sistem komputer, termasuk konfigurasi yang tidak aman, kelemahan perangkat lunak, atau kebijakan yang tidak memadai.
2. Memastikan kepatuhan
   Audit komputer memverifikasi apakah organisasi telah mematuhi kebijakan keamanan yang ditetapkan dan standar keamanan yang berlaku, baik dari perspektif internal maupun eksternal (misalnya, kepatuhan terhadap undang-undang dan peraturan yang berlaku).
3. Memberikan rekomendasi perbaikan
   Auditor komputer memberikan rekomendasi perbaikan yang spesifik dan praktis untuk memperbaiki kelemahan yang ditemukan dalam sistem keamanan.
4. Meningkatkan kesadaran keamanan
   Audit komputer membantu dalam meningkatkan kesadaran tentang kebutuhan akan keamanan sistem komputer di antara pemangku kepentingan organisasi.
5. Menjamin integritas dan kepercayaan
   Melalui audit komputer, organisasi dapat memastikan integritas dan kepercayaan terhadap sistem dan data mereka, baik untuk pengguna internal maupun eksternal.

Dengan melakukan pemantauan dan audit komputer secara teratur, organisasi dapat meningkatkan keamanan sistem informasi mereka, mencegah kerugian finansial, menjaga reputasi, dan memenuhi kepatuhan hukum dan regulasi yang berlaku.

5.2.2 Pentingnya pemantauan dan audit komputer dalam konteks keamanan sistem informasi.

Pemantauan dan audit komputer memainkan peran yang sangat penting dalam menjaga keamanan sistem informasi. Berikut ini adalah beberapa alasan mengapa pemantauan dan audit komputer sangat penting dalam konteks keamanan sistem informasi:

1. Mendeteksi Ancaman Keamanan
   Pemantauan komputer yang efektif memungkinkan organisasi untuk mendeteksi serangan keamanan secara real-time. Dengan memonitor aktivitas sistem, jaringan, dan pengguna, organisasi dapat mengidentifikasi tanda-tanda serangan seperti upaya tidak sah untuk mendapatkan akses, percobaan penyerangan, atau aktivitas mencurigakan lainnya. Dengan mendeteksi ancaman dengan cepat, langkah-langkah yang sesuai dapat diambil untuk merespons dan meminimalkan dampak serangan.
2. Mencegah Kerugian Lebih Lanjut
   Pemantauan komputer yang teratur membantu dalam mengidentifikasi celah keamanan dan kerentanan sistem yang dapat dieksploitasi oleh penyerang. Dengan mendeteksi dan mengatasi masalah keamanan sejak dini, organisasi dapat mencegah terjadinya kerugian finansial atau kerugian reputasi yang lebih besar akibat serangan yang berhasil.
3. Mengumpulkan Bukti dan Penyelidikan Keamanan
   Pemantauan komputer juga berperan penting dalam pengumpulan bukti terkait aktivitas mencurigakan atau pelanggaran keamanan. Data yang dikumpulkan melalui pemantauan dapat digunakan dalam proses penyelidikan keamanan atau litigasi. Bukti yang diperoleh dari pemantauan komputer dapat mendukung proses hukum

dan memfasilitasi penegakan hukum terhadap pelaku serangan.

4. Evaluasi Kepatuhan Terhadap Kebijakan dan Standar Keamanan
   Audit komputer membantu dalam mengevaluasi kepatuhan organisasi terhadap kebijakan keamanan yang ditetapkan dan standar keamanan yang berlaku. Dengan melakukan audit secara teratur, organisasi dapat memastikan bahwa sistem mereka mematuhi standar keamanan yang diterima dan bahwa kebijakan keamanan diikuti dengan tepat. Audit juga membantu mengidentifikasi area yang perlu perbaikan untuk memperkuat keamanan sistem.
5. Meningkatkan Kesadaran Keamanan
   Pemantauan dan audit komputer membantu dalam meningkatkan kesadaran tentang kebutuhan akan keamanan sistem informasi di antara pemangku kepentingan organisasi. Dengan menunjukkan hasil pemantauan dan audit, organisasi dapat membuktikan komitmen mereka terhadap keamanan informasi kepada karyawan, mitra bisnis, dan pelanggan mereka. Kesadaran yang lebih tinggi tentang keamanan dapat mendorong praktik yang lebih baik dan memperkuat budaya keamanan dalam organisasi.

Dengan memadukan pemantauan komputer yang efektif dan audit yang teratur, organisasi dapat mengurangi risiko serangan keamanan, melindungi data sensitif, dan menjaga integritas sistem informasi mereka. Pemantauan dan audit komputer memberikan kepercayaan dan jaminan bahwa langkah-langkah yang tepat diambil untuk melindungi sistem informasi dari serangan dan ancaman keamanan yang terus berkembang.

5.2.3 Perbedaan Antara Pemantauan Dan Audit Komputer.

Meskipun pemantauan dan audit komputer memiliki tujuan yang serupa dalam menjaga keamanan sistem informasi, ada perbedaan mendasar antara keduanya. Berikut ini adalah perbedaan antara pemantauan dan audit komputer:

A. Definisi

1. Pemantauan Komputer
   Pemantauan komputer melibatkan pengamatan terus-menerus terhadap sistem komputer dan jaringan untuk mendeteksi aktivitas yang mencurigakan atau tidak sah. Tujuannya adalah untuk mengidentifikasi dan merespons serangan keamanan secara cepat, serta mencegah kerugian yang lebih besar.
2. Audit Komputer
   Audit komputer adalah proses peninjauan independen terhadap keamanan sistem komputer dan praktik pengelolaannya. Audit ini melibatkan evaluasi menyeluruh terhadap kebijakan keamanan yang ada, proses pengendalian, serta pemantauan dan perlindungan data sensitif. Tujuannya adalah untuk menilai keefektifan sistem keamanan, mengidentifikasi celah dan kelemahan, memberikan rekomendasi perbaikan, dan memastikan kepatuhan terhadap kebijakan dan standar yang ditetapkan.

B. Fokus Utama:

1. Pemantauan Komputer
   Fokus utama dari pemantauan komputer adalah untuk mendeteksi dan merespons serangan keamanan secara real-time. Ini melibatkan pengamatan aktif terhadap aktivitas sistem, jaringan, dan pengguna, serta analisis data untuk mengidentifikasi ancaman keamanan dan aktivitas yang mencurigakan.
2. Audit Komputer

Fokus utama dari audit komputer adalah untuk mengevaluasi keamanan sistem komputer secara menyeluruh. Ini melibatkan peninjauan independen terhadap kebijakan keamanan, proses pengendalian, perlindungan data, dan kepatuhan terhadap standar keamanan yang berlaku. Audit komputer bertujuan untuk mengidentifikasi celah keamanan, memberikan rekomendasi perbaikan, dan memastikan kepatuhan terhadap kebijakan dan standar yang ditetapkan.

C. Waktu Pelaksanaan:

1. Pemantauan Komputer
   Pemantauan komputer dilakukan secara terus-menerus atau dalam interval waktu tertentu. Ini berfokus pada deteksi real-time dan respons segera terhadap serangan keamanan.
2. Audit Komputer
   Audit komputer dilakukan secara periodik atau sesuai jadwal yang ditentukan. Ini melibatkan evaluasi menyeluruh terhadap keamanan sistem komputer dengan menggunakan metodologi audit yang terstruktur.

D. Sumber Daya yang Digunakan

1. Pemantauan Komputer
   Pemantauan komputer melibatkan penggunaan alat pemantauan dan teknik khusus untuk mengumpulkan dan menganalisis data terkait dengan aktivitas sistem, jaringan, dan pengguna.
2. Audit Komputer
   Audit komputer melibatkan penggunaan metodologi audit yang terstruktur dan standar keamanan yang berlaku untuk mengevaluasi sistem keamanan, melakukan peninjauan dokumen, melakukan wawancara dengan personel terkait, dan menganalisis

kepatuhan terhadap kebijakan dan standar yang ditetapkan.

Pemantauan komputer dan audit komputer merupakan dua pendekatan yang saling melengkapi dalam menjaga keamanan sistem informasi. Pemantauan berfokus pada deteksi real-time dan respons segera terhadap serangan keamanan, sementara audit melibatkan evaluasi menyeluruh dan penilaian kepatuhan terhadap kebijakan dan standar keamanan. Kombinasi dari keduanya membantu organisasi untuk memitigasi risiko keamanan, mengidentifikasi celah keamanan, dan meningkatkan kepatuhan terhadap praktik keamanan yang baik.

5.3 Konsep Dasar Keamanan Sistem Informasi

Keamanan sistem informasi adalah upaya untuk melindungi integritas, kerahasiaan, dan ketersediaan data serta sistem komputer secara keseluruhan. Ada beberapa konsep dasar yang harus dipahami dalam konteks keamanan sistem informasi:

1. Kerahasiaan (*Confidentiality*)
   Konsep kerahasiaan berkaitan dengan perlindungan data dari akses yang tidak sah. Ini berarti hanya orang yang berwenang yang memiliki hak akses untuk melihat atau menggunakan data tersebut. Alat dan praktik keamanan seperti enkripsi, kebijakan akses yang ketat, dan autentikasi digunakan untuk menjaga kerahasiaan data.
2. Integritas (*Integrity*)
   Integritas berarti memastikan bahwa data tidak diubah atau dimanipulasi oleh pihak yang tidak berwenang. Keutuhan data dapat dilindungi dengan menggunakan kontrol akses yang kuat, tanda tangan digital, checksum, dan metode verifikasi lainnya. Dalam konteks sistem informasi, integritas juga mencakup menjaga keutuhan

sistem secara keseluruhan, termasuk perangkat keras, perangkat lunak, dan konfigurasi sistem.

3. Ketersediaan (*Availability*)
   Ketersediaan berarti memastikan bahwa sistem dan data tetap dapat diakses oleh pengguna yang berwenang saat dibutuhkan. Serangan atau kegagalan sistem dapat mengakibatkan gangguan layanan yang dapat berdampak negatif pada operasional organisasi. Upaya keamanan seperti pemantauan, pemulihan bencana, dan backup rutin dilakukan untuk menjaga ketersediaan sistem.
4. Autentikasi (*Authentication*)
   Autentikasi adalah proses untuk memverifikasi identitas pengguna atau sistem sebelum memberikan akses ke data atau sumber daya yang terkait. Ini melibatkan penggunaan kombinasi kredensial seperti username dan password, kunci enkripsi, kartu pintar, atau biometrik untuk memastikan bahwa entitas yang meminta akses adalah yang sebenarnya.
5. Otorisasi (*Authorization*)
   Otorisasi berkaitan dengan pemberian hak akses yang sesuai kepada pengguna yang telah terotentikasi. Setelah pengguna terotentikasi, sistem harus memastikan bahwa pengguna hanya memiliki hak akses yang sesuai dengan peran dan tanggung jawab mereka. Otorisasi dilakukan melalui penentuan hak akses berbasis peran atau hak akses yang ditentukan secara individu.
6. Enkripsi (*Encryption*)
   Enkripsi adalah proses mengubah data menjadi bentuk yang tidak dapat dibaca oleh pihak yang tidak berwenang. Enkripsi melibatkan penggunaan kunci enkripsi untuk mengamankan data saat ditransmisikan atau disimpan. Dalam hal ini, enkripsi dapat melindungi kerahasiaan data

jika data tersebut jatuh ke tangan pihak yang tidak berwenang.

7. Audit dan Pemantauan (*Audit and Monitoring*)
   Audit dan pemantauan adalah praktik penting dalam keamanan sistem informasi. Audit melibatkan peninjauan independen terhadap kebijakan, proses, dan sistem untuk memastikan kepatuhan dan identifikasi celah keamanan. Pemantauan, di sisi lain, melibatkan pengawasan terus-menerus terhadap aktivitas sistem untuk mendeteksi ancaman keamanan atau aktivitas yang mencurigakan secara real-time.

Konsep dasar keamanan sistem informasi ini membentuk dasar untuk merancang, mengimplementasikan, dan menjalankan keamanan sistem informasi yang efektif. Dengan memahami dan menerapkan konsep-konsep ini, organisasi dapat menjaga integritas, kerahasiaan, dan ketersediaan data mereka, serta melindungi sistem informasi dari ancaman keamanan yang ada.

5.3.1 Ancaman Dan Serangan Terhadap Sistem Informasi.

Ancaman dan serangan terhadap sistem informasi merupakan masalah yang serius dan terus berkembang dalam lingkungan teknologi informasi. Pemahaman mengenai jenis-jenis ancaman dan serangan yang mungkin dihadapi oleh sistem informasi penting agar organisasi dapat mengambil langkah-langkah pencegahan yang tepat. Berikut ini beberapa contoh ancaman dan serangan yang umum terhadap sistem informasi:

1. Malware
   Malware (*malicious software*) adalah perangkat lunak yang dirancang untuk merusak, mengganggu, atau mencuri informasi dari sistem. Contoh malware termasuk virus, worm, trojan, ransomware, spyware, dan adware. Malware dapat menyebabkan kerusakan pada sistem, mencuri data sensitif, atau membatasi akses pengguna ke sistem.

2. Serangan DDoS (*Distributed Denial of Service*)
   Serangan DDoS adalah upaya untuk mengganggu ketersediaan layanan sistem dengan membanjiri server dengan lalu lintas jaringan yang tidak normal. Serangan ini dilakukan dengan menggunakan banyak komputer yang terinfeksi (botnet) untuk mengirimkan jumlah lalu lintas yang sangat besar ke server target, sehingga menyebabkan penurunan kinerja atau bahkan kegagalan sistem.
3. Serangan Phishing
   Serangan phishing melibatkan upaya untuk mendapatkan informasi sensitif, seperti kata sandi atau data keuangan, dengan menyamar sebagai entitas tepercaya melalui email, pesan instan, atau situs web palsu. Phishing seringkali memanfaatkan manipulasi psikologis atau teknik sosial untuk memancing korban memberikan informasi pribadi yang berharga.
4. Serangan *Man-in-the-Middle* (MITM)
   Serangan MITM terjadi ketika penyerang memposisikan dirinya di antara komunikasi antara dua pihak yang sah. Penyerang dapat memantau atau mengubah data yang ditransmisikan antara kedua pihak, sehingga memungkinkannya untuk mencuri informasi sensitif atau memanipulasi komunikasi tersebut.
5. Serangan *Zero-day*
   Serangan *Zero-day* merujuk pada eksploitasi celah keamanan yang belum diketahui atau belum diperbaiki oleh vendor perangkat lunak. Serangan ini dimungkinkan karena penyerang menemukan kelemahan yang tidak diketahui oleh pihak yang bertanggung jawab atas perangkat lunak tersebut, sehingga memberikan mereka akses tidak sah ke sistem.

6. Serangan Penolakan Layanan (DoS - *Denial of Service*)
   Serangan DoS bertujuan untuk mengganggu ketersediaan sistem dengan membanjiri sumber daya sistem, seperti bandwidth jaringan, daya komputasi, atau memori, sehingga membuat sistem tidak responsif atau bahkan mengalami kegagalan. Serangan ini dapat dilakukan dengan mengirimkan lalu lintas yang berlebihan ke server target atau dengan memanfaatkan kerentanan tertentu dalam perangkat lunak atau protokol jaringan.
7. Serangan Melalui Jaringan Nirkabel
   Serangan melalui jaringan nirkabel, seperti Wi-Fi, melibatkan penyerang yang memanfaatkan kelemahan dalam protokol atau pengaturan jaringan nirkabel untuk memperoleh akses ke sistem atau mencuri data. Contoh serangan ini termasuk serangan "man-in-the-middle" pada jaringan Wi-Fi publik atau serangan "eavesdropping" untuk memantau dan mencuri data yang dikirimkan melalui jaringan nirkabel.
8. Serangan Insider
   Serangan insider melibatkan ancaman dari dalam organisasi, yaitu dari seseorang yang memiliki akses yang sah ke sistem. Ancaman ini dapat berasal dari karyawan yang tidak puas, mantan karyawan, atau orang dalam yang disengaja mencuri data sensitif, merusak sistem, atau membocorkan informasi rahasia.

Penting untuk memahami bahwa ancaman dan serangan terhadap sistem informasi terus berkembang seiring dengan kemajuan teknologi. Oleh karena itu, organisasi harus terus memperbarui kebijakan keamanan, menerapkan kontrol yang memadai, dan meningkatkan kesadaran pengguna tentang ancaman keamanan yang ada untuk melindungi sistem informasi mereka dari serangan yang berpotensi merugikan.

5.3.2 Prinsip Dasar Keamanan Yang Harus Diterapkan Dalam Pemantauan Dan Audit Komputer.

Dalam pemantauan dan audit komputer, ada beberapa prinsip dasar keamanan yang harus diterapkan untuk memastikan integritas, kerahasiaan, dan ketersediaan sistem informasi. Berikut ini adalah prinsip dasar keamanan yang penting dalam konteks pemantauan dan audit komputer:

1. Prinsip Kebutuhan untuk Tahu (*Need to Know*)
   Prinsip ini mengacu pada praktek memberikan hak akses hanya kepada individu yang membutuhkan akses tersebut untuk menjalankan tugas dan tanggung jawab mereka. Dalam pemantauan dan audit komputer, hanya personel yang berwenang yang harus memiliki akses ke sistem dan data terkait untuk melaksanakan tugas mereka. Ini membantu mencegah akses yang tidak sah dan melindungi kerahasiaan informasi yang sensitif.
2. Prinsip Pembagian Tugas (*Separation of Duties*)
   Prinsip ini melibatkan pemisahan tugas dan tanggung jawab di antara beberapa individu atau entitas yang berbeda. Dalam konteks pemantauan dan audit komputer, prinsip ini berarti memisahkan tugas pemantauan dan audit antara individu atau tim yang berbeda. Ini membantu mencegah penyalahgunaan akses atau manipulasi data yang tidak terdeteksi.
3. Prinsip Kebutuhan Minimum (*Least Privilege*)
   Prinsip ini mengacu pada memberikan hak akses minimal yang diperlukan bagi individu atau entitas untuk melaksanakan tugas mereka. Dalam pemantauan dan audit komputer, ini berarti memberikan hak akses hanya pada tingkat yang diperlukan untuk melaksanakan tugas pemantauan atau audit yang relevan. Ini membantu membatasi potensi penyalahgunaan akses dan melindungi data dari akses yang tidak sah.

4. Prinsip Keberlanjutan (*Continuity*)
   Prinsip ini melibatkan upaya untuk menjaga ketersediaan dan kontinuitas operasional sistem. Dalam pemantauan dan audit komputer, prinsip ini berarti memastikan bahwa pemantauan dan audit dilakukan secara berkelanjutan untuk mendeteksi ancaman atau celah keamanan yang muncul seiring waktu. Selain itu, prinsip ini juga mencakup penyediaan rencana pemulihan bencana dan tindakan mitigasi untuk memastikan operasional sistem tetap berjalan bahkan dalam situasi darurat.
5. Prinsip Keamanan Berlapis (*Defense in Depth*)
   Prinsip ini melibatkan penerapan lapisan perlindungan yang berbeda untuk mengurangi risiko serangan dan kerentanan sistem. Dalam pemantauan dan audit komputer, prinsip ini berarti menggunakan berbagai kontrol keamanan seperti firewall, enkripsi, pemantauan jaringan, dan validasi keamanan kode untuk memastikan keamanan yang komprehensif.
6. Prinsip Kebijakan Keamanan yang Kuat (*Strong Security Policies*)
   Prinsip ini melibatkan penerapan kebijakan keamanan yang jelas, ketat, dan terkini. Dalam pemantauan dan audit komputer, prinsip ini berarti memiliki kebijakan keamanan yang mengatur penggunaan sistem, akses, retensi data, penggunaan sandi yang kuat, dan tindakan lainnya. Kebijakan keamanan yang kuat membantu memberikan panduan dan kerangka kerja yang jelas untuk pemantauan dan audit yang efektif.

Menerapkan prinsip dasar keamanan ini dalam pemantauan dan audit komputer membantu memastikan bahwa sistem informasi dilindungi dengan baik dan risiko serangan diminimalkan. Prinsip-prinsip ini memberikan dasar untuk

merancang dan menjalankan pemantauan dan audit komputer yang efektif dalam rangka menjaga keamanan sistem informasi.

5.4 Persiapan Audit Komputer

5.4.1 Langkah-Langkah Yang Harus Diambil Sebelum Melakukan Audit Komputer.

Sebelum melakukan audit komputer, ada beberapa langkah yang perlu diambil untuk memastikan audit dilakukan dengan efektif dan efisien. Berikut ini adalah langkah-langkah yang harus diambil sebelum melakukan audit komputer:

A. Perencanaan Audit:

1. Tentukan tujuan dan ruang lingkup audit
   Tetapkan tujuan audit komputer dan ruang lingkup audit yang akan dilakukan. Identifikasi sistem yang akan diaudit, data yang akan dievaluasi, dan aspek keamanan yang akan diperiksa.
2. Rencanakan jadwal audit
   Tentukan jadwal audit yang sesuai dengan kebutuhan organisasi. Pastikan bahwa waktu yang cukup dialokasikan untuk melaksanakan audit dengan cermat.
3. Bentuk tim audit
   Tentukan tim audit yang terdiri dari auditor yang berpengalaman dan memiliki pengetahuan yang relevan tentang keamanan sistem komputer.
4. Siapkan dokumen dan sumber daya
5. Kumpulkan dokumen yang relevan seperti kebijakan keamanan, prosedur, log aktivitas, dan konfigurasi sistem. Pastikan bahwa sumber daya yang diperlukan, seperti perangkat lunak audit dan alat pemantauan, tersedia.

B. Evaluasi Risiko
   1. Identifikasi aset penting
      Identifikasi aset informasi penting yang perlu dilindungi, termasuk data sensitif, infrastruktur kritis, atau sistem kunci lainnya.
   2. Tinjau kebijakan keamanan
      Tinjau kebijakan keamanan yang ada untuk memastikan bahwa mereka sesuai dengan standar keamanan yang berlaku dan mencakup aspek yang relevan untuk audit.
   3. Identifikasi ancaman dan kerentanan
      Identifikasi ancaman keamanan yang mungkin dihadapi dan kerentanan yang ada dalam sistem. Tinjau catatan keamanan, kejadian sebelumnya, atau laporan keamanan untuk mendapatkan wawasan yang diperlukan.
   4. Evaluasi kontrol keamanan: Tinjau kontrol keamanan yang ada dan identifikasi kelemahan atau kekurangan yang mungkin ada. Identifikasi daerah yang memerlukan perbaikan atau peningkatan.

C. Persiapan Audit
   1. Komunikasi dengan pihak yang berkepentingan
      Komunikasikan rencana audit kepada pihak yang berkepentingan, termasuk manajemen senior dan pemegang kepentingan lainnya. Pastikan bahwa mereka memahami tujuan dan manfaat dari audit yang akan dilakukan.
   2. Pemberitahuan kepada tim terkait
      Beri tahu tim operasional terkait tentang audit yang akan dilakukan, agar mereka dapat mempersiapkan dokumen dan data yang diperlukan.
   3. Jalin hubungan dengan personel kunci

4. Identifikasi dan jalin hubungan dengan personel kunci yang terkait dengan sistem yang akan diaudit. Hal ini akan membantu dalam memperoleh pemahaman yang lebih baik tentang lingkungan operasional dan menjalin kerjasama yang diperlukan selama audit.

D. Penetapan Lingkungan Audit
   1. Peroleh akses yang diperlukan
      Dapatkan hak akses yang diperlukan ke sistem yang akan diaudit. Pastikan bahwa auditor memiliki izin dan kredensial yang diperlukan untuk mengakses sistem dan data yang relevan.
   2. Tinjau lingkungan operasional
      Tinjau konfigurasi dan struktur sistem yang akan diaudit. Pastikan bahwa auditor memiliki pemahaman yang memadai tentang lingkungan operasional, termasuk infrastruktur, jaringan, dan aplikasi yang terlibat.
   3. Periksa alat dan perangkat keras audit
      Pastikan bahwa alat dan perangkat keras audit yang diperlukan tersedia dan berfungsi dengan baik. Uji alat dan pastikan mereka dapat mengumpulkan dan menganalisis data dengan benar.

Dengan mengikuti langkah-langkah di atas sebelum melakukan audit komputer, Anda dapat mempersiapkan audit dengan baik, memahami risiko keamanan yang ada, dan memastikan bahwa Anda memiliki sumber daya dan persiapan yang diperlukan untuk melakukan audit dengan efektif.

5.4.2 Penentuan Lingkup Audit Dan Identifikasi Sumber Daya Yang Akan Di Audit.

Dalam melakukan audit komputer, penentuan lingkup audit dan identifikasi sumber daya yang akan diaudit adalah langkah

penting untuk memastikan bahwa audit dilakukan dengan fokus dan efisien. Berikut ini adalah langkah-langkah yang dapat diambil dalam penentuan lingkup audit dan identifikasi sumber daya yang akan diaudit:

1. Tinjau Tujuan Audit
   Pertama, tinjau tujuan audit secara keseluruhan. Apa yang ingin dicapai melalui audit ini? Misalnya, apakah tujuannya adalah mengevaluasi keamanan sistem komputer secara umum atau fokus pada aspek tertentu seperti kebijakan keamanan, manajemen akses, atau kepatuhan terhadap standar tertentu.
2. Identifikasi Sumber Daya yang akan Diaudit: Tentukan sumber daya yang akan menjadi fokus audit. Sumber daya ini bisa berupa:
   a. Sistem Operasi
      Identifikasi sistem operasi yang akan diaudit, seperti Windows, Linux, atau macOS. Tinjau konfigurasi keamanan, pembaruan sistem, pengaturan akun pengguna, dan kebijakan keamanan yang terkait.
   b. Aplikasi
      Identifikasi aplikasi yang penting dan sensitif untuk organisasi. Tinjau konfigurasi, kebijakan akses, pengaturan keamanan, dan kepatuhan terhadap praktik keamanan terbaik dalam penggunaan aplikasi tersebut.
   c. Jaringan
      Identifikasi komponen jaringan yang relevan seperti firewall, router, switch, atau perangkat jaringan lainnya. Tinjau kebijakan keamanan, konfigurasi jaringan, tata letak, dan perlindungan terhadap serangan jaringan.

d. Database
   Identifikasi database yang kritis dan penting. Tinjau kebijakan akses, pengaturan keamanan, pembaruan, dan perlindungan data sensitif dalam database.

3. Tinjau Keberlanjutan dan Interaksi Sumber Daya
   Pertimbangkan bagaimana sumber daya yang akan diaudit berinteraksi satu sama lain. Apakah ada ketergantungan antara sumber daya tersebut? Misalnya, sistem operasi dapat berinteraksi dengan aplikasi dan database. Memahami hubungan ini membantu dalam mengidentifikasi risiko dan dampak potensial pada keamanan sistem secara keseluruhan.
4. Identifikasi Ancaman dan Kerentanan
   Identifikasi ancaman dan kerentanan yang mungkin terkait dengan sumber daya yang akan diaudit. Tinjau catatan keamanan, laporan kejadian sebelumnya, dan temuan audit sebelumnya untuk memahami ancaman yang relevan dan kerentanan yang perlu diperiksa.
5. Tinjau Persyaratan Regulasi dan Kepatuhan
   Jika organisasi tunduk pada persyaratan kepatuhan tertentu, tinjau persyaratan tersebut dan pastikan audit mencakup aspek-aspek yang relevan. Misalnya, jika organisasi harus mematuhi standar keamanan tertentu seperti ISO 27001 atau HIPAA, pastikan audit mencakup pemeriksaan kepatuhan terhadap standar tersebut.
6. Batasi Lingkup Sesuai dengan Ketersediaan Sumber Daya
   Pertimbangkan ketersediaan sumber daya (waktu, tim, perangkat, dll.) yang tersedia untuk melaksanakan audit. Pastikan bahwa lingkup audit dapat dilakukan dengan efisien dan realistis dengan sumber daya yang ada.
7. Tetapkan Batasan dan Pengecualian
   Setelah mengidentifikasi sumber daya yang akan diaudit, tetapkan juga batasan dan pengecualian yang perlu

diperhatikan. Misalnya, mungkin ada sumber daya atau area yang dikecualikan dari audit karena alasan khusus seperti keterbatasan akses atau kebijakan organisasi.

5.4.3 Penetapan Standar Keamanan Yang Harus Dipatuhi.

Penetapan standar keamanan yang harus dipatuhi merupakan langkah penting dalam menjaga keamanan sistem informasi. Standar keamanan memberikan kerangka kerja dan pedoman yang jelas untuk menerapkan kontrol keamanan yang efektif. Berikut ini adalah beberapa contoh standar keamanan yang umumnya digunakan dan harus dipatuhi oleh organisasi:

1. ISO/IEC 27001
   Standar ini adalah standar internasional yang mengatur sistem manajemen keamanan informasi (*Information Security Management System*/ISMS). ISO/IEC 27001 memberikan panduan dan persyaratan untuk mendesain, menerapkan, memantau, dan meningkatkan keamanan informasi dalam sebuah organisasi.
2. NIST *Cybersecurity Framework*
   Framework ini dikembangkan oleh *National Institute of Standards and Technology* (NIST) di Amerika Serikat. NIST Cybersecurity Framework memberikan kerangka kerja yang komprehensif untuk mengidentifikasi, melindungi, mendeteksi, merespon, dan memulihkan sistem dari serangan keamanan.
3. PCI DSS: *Payment Card Industry Data Security Standard* (PCI DSS) adalah standar keamanan yang diterapkan oleh industri kartu pembayaran. Standar ini mengatur keamanan sistem yang memproses data kartu pembayaran, dengan fokus pada perlindungan data kartu kredit dan debit serta pencegahan penyalahgunaan.

4. CIS Controls
   Center for Internet Security (CIS) *Controls* adalah rangkaian kontrol keamanan yang dikembangkan oleh CIS. Rangkaian ini mencakup 20 kontrol keamanan yang sangat penting untuk melindungi sistem dan data dari serangan keamanan yang umum.
5. COBIT (*Control Objectives for Information and Related Technologies*)
   Control Objectives for Information and Related Technologies (COBIT) adalah kerangka kerja yang digunakan untuk mengelola dan mengendalikan teknologi informasi dalam organisasi. COBIT menyediakan panduan tentang pengelolaan risiko, pengendalian keamanan, dan pengelolaan aset teknologi informasi.

Pilihan standar keamanan yang harus dipatuhi akan bergantung pada jenis industri, wilayah hukum, dan persyaratan khusus yang relevan untuk organisasi. Penting bagi organisasi untuk memahami dan mematuhi standar keamanan yang berlaku untuk menjaga kepatuhan, mengurangi risiko, dan melindungi sistem informasi mereka secara efektif.

5.5 Pelaporan Dan Tindak Lanjut

Pelaporan dan tindak lanjut adalah bagian penting dari proses pemantauan dan audit sistem komputer. Setelah melaksanakan pemantauan dan audit, langkah-langkah berikut dapat diambil untuk melakukan pelaporan dan tindak lanjut yang efektif:

1. Analisis Temuan
   Analisis temuan dari pemantauan dan audit sistem komputer adalah langkah pertama. Tinjau temuan dan hasil audit dengan cermat untuk memahami implikasi dan dampaknya terhadap keamanan dan kinerja sistem.

2. Penyusunan Laporan
   Setelah melakukan analisis temuan, buat laporan yang merangkum hasil pemantauan dan audit. Laporan ini harus mencakup temuan yang relevan, kesimpulan, rekomendasi perbaikan, serta ringkasan tindakan yang harus diambil.
3. Identifikasi Prioritas
   Berdasarkan temuan dan rekomendasi dalam laporan, identifikasi prioritas tindakan yang perlu diambil. Prioritaskan tindakan berdasarkan tingkat kepentingan, urgensi, dan dampak terhadap keamanan dan kinerja sistem.
4. Penetapan Tanggung Jawab
   Tetapkan tanggung jawab kepada individu atau tim yang bertanggung jawab untuk melaksanakan tindakan yang diperlukan. Pastikan bahwa tanggung jawab ditetapkan dengan jelas, termasuk batas waktu yang ditentukan untuk setiap tindakan.
5. Implementasi Tindakan Perbaikan
   Melaksanakan tindakan perbaikan yang diperlukan sesuai dengan prioritas dan tanggung jawab yang ditetapkan. Tindakan ini dapat meliputi perbaikan kelemahan keamanan, perubahan konfigurasi sistem, pelatihan pengguna, atau penerapan kontrol keamanan tambahan.
6. Pemantauan Implementasi
   Setelah melakukan tindakan perbaikan, lakukan pemantauan untuk memastikan bahwa tindakan tersebut diimplementasikan dengan benar dan efektif. Tinjau kembali sistem untuk memastikan bahwa temuan dan masalah yang diidentifikasi telah diperbaiki.
7. Evaluasi Keefektifan
   Evaluasi keefektifan tindakan yang diambil untuk memperbaiki kelemahan atau masalah yang ditemukan. Tinjau kembali sistem untuk memverifikasi bahwa

tindakan perbaikan telah mengurangi risiko dan meningkatkan keamanan dan kinerja sistem.

8. Pemantauan Berkelanjutan
   Teruskan pemantauan sistem komputer secara berkelanjutan untuk mendeteksi ancaman baru, perubahan konfigurasi, atau kejadian yang dapat mempengaruhi keamanan dan kinerja sistem. Pemantauan yang berkelanjutan membantu dalam mendeteksi dan merespons perubahan yang mungkin terjadi seiring waktu.
9. Pelaporan Lanjutan
   Buat laporan lanjutan yang mencatat tindakan yang telah diambil, hasil evaluasi, dan langkah-langkah yang direkomendasikan untuk pemantauan dan audit berikutnya. Laporan ini menjadi bagian penting dalam siklus pemantauan dan audit yang berkesinambungan.

Pelaporan dan tindak lanjut yang efektif memainkan peran penting dalam menjaga keamanan dan kinerja sistem komputer. Melalui analisis temuan, identifikasi prioritas, dan implementasi tindakan perbaikan, organisasi dapat meningkatkan keamanan sistem dan merespons dengan cepat terhadap temuan atau ancaman yang teridentifikasi.

5.5.1 Penyusunan Laporan Audit Komputer Yang Efektif.

Penyusunan laporan audit komputer yang efektif memerlukan struktur yang jelas, ringkasan yang mudah dipahami, dan rekomendasi yang relevan. Berikut ini adalah langkah-langkah yang dapat diikuti dalam menyusun laporan audit komputer yang efektif:

1. Pendahuluan
   a. Deskripsikan tujuan dan ruang lingkup audit komputer.
   b. Jelaskan metode yang digunakan dalam melakukan audit.

c. Berikan ikhtisar singkat tentang sistem atau infrastruktur yang diaudit.

2. Ringkasan Eksekutif:
   a. Sajikan ringkasan temuan dan rekomendasi secara jelas dan ringkas.
   b. Berikan gambaran singkat tentang hasil audit dan implikasinya.
   c. Tinjau dampak keamanan dan kinerja yang signifikan.
3. Temuan Audit:
   a. Identifikasi temuan audit secara terperinci.
   b. Jelaskan setiap temuan dengan jelas, termasuk contoh konkret jika memungkinkan.
   c. Gunakan istilah teknis yang relevan dengan pemahaman yang dapat dipahami oleh pembaca non-teknis.
4. Analisis dan Evaluasi:
   a. Berikan analisis mendalam tentang temuan audit.
   b. Tinjau dampak temuan terhadap keamanan, kinerja, dan kepatuhan.
   c. Evaluasi keefektifan kontrol yang ada dan identifikasi kelemahan atau kekurangan yang mungkin perlu diperbaiki.
5. Rekomendasi:
   a. Berikan rekomendasi yang jelas dan terperinci untuk memperbaiki temuan audit.
   b. Prioritaskan rekomendasi berdasarkan urgensi dan dampak.
   c. Sertakan langkah-langkah spesifik yang harus diambil untuk mengimplementasikan rekomendasi.
6. Tindak Lanjut:
   a. Tentukan tindakan lanjut yang harus diambil oleh manajemen atau tim yang bertanggung jawab.

b. Tetapkan tanggung jawab dan batas waktu untuk setiap tindakan yang direkomendasikan.
c. Pastikan bahwa tindakan lanjut memiliki jadwal yang realistis dan dapat diukur.

7. Kesimpulan:
   a. Berikan kesimpulan singkat yang merangkum hasil audit.
   b. Tinjau kembali tujuan audit dan tingkat kepatuhan terhadap kebijakan keamanan.
8. Lampiran:
   a. Lampirkan dokumentasi dan data pendukung yang relevan, seperti log audit, hasil pengujian, atau bukti temuan.
   b. Lampirkan daftar kontrol atau kerangka kerja yang digunakan selama audit.

Pastikan laporan audit komputer disusun dengan bahasa yang jelas, tidak ambigu, dan dapat dipahami oleh pembaca yang mungkin tidak memiliki latar belakang teknis yang mendalam. Gunakan grafik, tabel, dan diagram jika diperlukan untuk memperjelas informasi. Selain itu, pastikan laporan audit dikomunikasikan dengan jelas kepada pihak yang berkepentingan yang relevan, seperti manajemen senior, tim IT, atau entitas lain yang terkait.

5.5.2 Identifikasi Dan Penanganan Temuan Audit.

Identifikasi dan penanganan temuan audit adalah langkah penting dalam memastikan bahwa masalah keamanan dan kelemahan yang ditemukan selama audit komputer diperbaiki dengan tepat. Berikut adalah langkah-langkah yang dapat diambil untuk mengidentifikasi dan menangani temuan audit secara efektif:

1. Identifikasi Temuan Audit:
    a. Tinjau hasil audit secara menyeluruh dan identifikasi temuan yang telah diungkapkan.
    b. Klasifikasikan temuan berdasarkan tingkat kepentingan, dampak, dan urgensi.
2. Evaluasi Dampak:
    a. Evaluasi dampak temuan audit terhadap keamanan, kinerja, dan kepatuhan sistem.
    b. Tinjau potensi risiko yang mungkin timbul dari temuan tersebut.
3. Prioritaskan Tindakan:
    a. Prioritaskan temuan berdasarkan tingkat kepentingan dan urgensi.
    b. Fokus pada temuan yang memiliki dampak yang signifikan terhadap keamanan atau kinerja sistem.
4. Tentukan Penanggung Jawab:
    a. Tentukan individu atau tim yang bertanggung jawab untuk menangani setiap temuan.
    b. Pastikan tanggung jawab ditetapkan dengan jelas dan komunikasikan kepada pihak terkait.
5. Rencanakan Tindakan Perbaikan:
    a. Rencanakan tindakan perbaikan yang harus diambil untuk mengatasi temuan.
    b. Tentukan langkah-langkah spesifik yang harus diambil untuk memperbaiki kelemahan atau masalah yang ditemukan.
6. Tetapkan Batas Waktu:
    a. Tetapkan batas waktu yang realistis untuk menyelesaikan tindakan perbaikan.
    b. Pastikan batas waktu yang ditetapkan memungkinkan cukup waktu untuk menangani temuan dengan baik.

7. Implementasikan Tindakan Perbaikan:
    a. Lakukan tindakan perbaikan sesuai dengan rencana yang telah ditetapkan.
    b. Pastikan tindakan perbaikan diimplementasikan dengan benar dan efektif.
8. Verifikasi Tindakan Perbaikan:
    a. Lakukan verifikasi untuk memastikan bahwa tindakan perbaikan yang diimplementasikan telah berhasil mengatasi temuan.
    b. Pastikan bahwa tindakan perbaikan telah mengurangi risiko dan meningkatkan keamanan atau kinerja sistem.
9. Dokumentasikan Tindakan:
    a. Dokumentasikan semua tindakan perbaikan yang telah diambil.
    b. Buat catatan yang mencakup langkah-langkah yang telah dilakukan, tanggung jawab, dan batas waktu yang telah diselesaikan.
10. Pelaporan dan Komunikasi:
    a. Laporkan kemajuan penanganan temuan kepada pihak yang berkepentingan yang relevan, termasuk manajemen senior dan tim IT.
    b. Komunikasikan hasil tindakan perbaikan yang telah diambil dan sampaikan laporan akhir yang mencerminkan status penanganan temuan.
11. Pemantauan Berkelanjutan:
    a. Lanjutkan pemantauan sistem secara berkelanjutan untuk memastikan bahwa temuan yang telah ditangani tetap diperbaiki dan tidak muncul kembali.
    b. Tinjau secara berkala efektivitas langkah-langkah perbaikan yang telah diimplementasikan.

Dalam menangani temuan audit, penting untuk menjaga transparansi, mengoordinasikan upaya dengan tim yang relevan, dan memastikan bahwa tindakan perbaikan yang diambil sesuai dengan rekomendasi yang diberikan. Selain itu, penting juga untuk belajar dari temuan audit dan menggunakannya sebagai pelajaran untuk meningkatkan keamanan dan kinerja sistem secara keseluruhan.

5.5.3 Tindak lanjut terhadap rekomendasi audit.

Tindak lanjut terhadap rekomendasi audit komputer merupakan langkah penting dalam memastikan bahwa masalah keamanan dan kelemahan yang teridentifikasi selama audit diperbaiki dengan efektif. Berikut ini adalah beberapa langkah yang dapat diambil dalam tindak lanjut terhadap rekomendasi audit komputer:

1. Evaluasi Rekomendasi:
    a. Tinjau rekomendasi audit dengan cermat dan pahami implikasi dan manfaatnya.
    b. Evaluasi kepentingan dan urgensi dari setiap rekomendasi.
2. Tetapkan Prioritas:
    a. Prioritaskan rekomendasi berdasarkan tingkat kepentingan, dampak, dan risiko yang terkait.
    b. Fokus pada rekomendasi yang memiliki dampak signifikan terhadap keamanan dan kepatuhan sistem.
3. Tentukan Penanggung Jawab:
    a. Tentukan individu atau tim yang bertanggung jawab untuk melaksanakan setiap rekomendasi.
    b. Pastikan tanggung jawab ditetapkan dengan jelas dan komunikasikan kepada pihak yang terlibat.
4. Rencanakan Implementasi:
    a. Rencanakan langkah-langkah konkret yang harus diambil untuk mengimplementasikan rekomendasi.

b. Tetapkan target waktu yang realistis untuk menyelesaikan implementasi.

5. Alokasikan Sumber Daya:
   a. Pastikan sumber daya yang diperlukan, seperti personel, anggaran, dan peralatan, tersedia untuk melaksanakan rekomendasi dengan efektif.
   b. Koordinasikan dengan tim terkait untuk memastikan ketersediaan sumber daya yang diperlukan.

Implementasikan Rekomendasi:

1. Lakukan implementasi rekomendasi sesuai dengan rencana yang telah ditetapkan.
2. Pastikan langkah-langkah yang diperlukan dilakukan dengan benar dan tepat waktu.

Verifikasi dan Uji Coba:

1. Verifikasi bahwa implementasi rekomendasi telah berhasil mengatasi masalah atau kelemahan yang teridentifikasi.
2. Lakukan pengujian dan pengawasan untuk memastikan efektivitas rekomendasi yang diimplementasikan.

Dokumentasikan Tindakan:

1. Dokumentasikan semua tindakan yang telah diambil dalam melaksanakan rekomendasi audit.
2. Buat catatan yang mencakup langkah-langkah yang telah dilakukan, tanggung jawab, dan tanggal penyelesaian.

Evaluasi Keefektifan:

1. Tinjau kembali hasil implementasi rekomendasi dan evaluasi keefektifannya.
2. Identifikasi dan perbaiki masalah yang mungkin muncul selama atau setelah implementasi.

Pelaporan dan Komunikasi:

1. Laporkan kemajuan implementasi rekomendasi kepada pihak yang berkepentingan yang relevan.
2. Komunikasikan hasil tindak lanjut kepada manajemen senior dan tim terkait.

Pemantauan Berkelanjutan:

1. Lanjutkan pemantauan sistem secara berkelanjutan untuk memastikan keberlanjutan dan efektivitas tindakan yang telah diambil.
2. Tinjau secara berkala efektivitas implementasi dan identifikasi kebutuhan perbaikan atau perubahan tambahan.
3. Tindak lanjut terhadap rekomendasi audit komputer harus dilakukan secara sistematis dan terdokumentasi. Pastikan bahwa semua langkah yang diambil untuk melaksanakan rekomendasi terdokumentasi dengan baik agar dapat dipantau, dievaluasi, dan diaudit di masa mendatang. Tindak lanjut yang efektif akan membantu meningkatkan keamanan dan kepatuhan sistem informasi organisasi.

5.6 Peran dan Tanggung Jawab Auditor Komputer

Peran dan tanggung jawab auditor komputer adalah sebagai berikut:

1. Mengevaluasi Keamanan Sistem: Auditor komputer bertanggung jawab untuk mengevaluasi keamanan sistem komputer dengan tujuan mengidentifikasi kelemahan, celah keamanan, dan risiko yang ada. Mereka melakukan audit terhadap infrastruktur IT, kebijakan keamanan, kontrol akses, serta prosedur yang terkait dengan keamanan sistem.
2. Melakukan Pemeriksaan dan Analisis: Auditor komputer melakukan pemeriksaan mendalam terhadap sistem

komputer dan melakukan analisis terhadap temuan yang ditemukan. Mereka menggunakan teknik dan alat audit untuk mengumpulkan data dan informasi yang relevan untuk evaluasi keamanan.

3. Menyusun Laporan Audit: Auditor komputer menyusun laporan audit yang berisi hasil temuan, rekomendasi, dan langkah-langkah perbaikan yang harus diambil. Laporan audit harus disusun secara jelas dan objektif, serta dapat dipahami oleh pihak yang berkepentingan.
4. Memberikan Rekomendasi Perbaikan: Auditor komputer memberikan rekomendasi kepada manajemen dan pemangku kepentingan terkait tindakan perbaikan yang harus diambil untuk mengatasi temuan audit. Rekomendasi ini dapat berupa perubahan kebijakan, peningkatan kontrol keamanan, atau perbaikan sistem yang ditemukan.
5. Memastikan Kepatuhan: Auditor komputer memastikan kepatuhan terhadap kebijakan keamanan dan standar yang berlaku. Mereka memeriksa apakah sistem dan prosedur telah mematuhi persyaratan keamanan yang ditetapkan, serta apakah kontrol keamanan yang diterapkan sudah memadai.
6. Memberikan Konsultasi dan Edukasi: Auditor komputer dapat memberikan konsultasi kepada organisasi terkait praktik terbaik dalam keamanan sistem komputer. Mereka juga dapat memberikan edukasi kepada personel tentang ancaman keamanan, kebijakan keamanan, dan langkah-langkah yang dapat diambil untuk meningkatkan keamanan.

Keterampilan dan Pengetahuan yang Diperlukan oleh Auditor Komputer:

1. Keahlian dalam Teknologi Informasi: Auditor komputer harus memiliki pemahaman yang baik tentang teknologi

informasi, infrastruktur jaringan, arsitektur sistem, serta aplikasi yang digunakan dalam organisasi.

2. Pengetahuan Keamanan Komputer: Auditor komputer harus menguasai prinsip-prinsip keamanan komputer, standar keamanan yang berlaku, dan metode serangan yang umum dilakukan oleh penyerang.
3. Pemahaman tentang Audit dan Pemeriksaan: Auditor komputer harus memahami prinsip-prinsip audit dan pemeriksaan, termasuk metodologi audit, teknik pemeriksaan, serta proses dan kerangka kerja audit.
4. Analisis dan Pemecahan Masalah: Auditor komputer harus memiliki kemampuan analisis yang kuat untuk mengidentifikasi kelemahan keamanan, memecahkan masalah, dan memberikan rekomendasi perbaikan yang efektif.
5. Komunikasi yang Efektif: Auditor komputer harus memiliki kemampuan komunikasi yang baik untuk berinteraksi dengan personel teknis maupun non-teknis. Mereka harus dapat menjelaskan temuan secara jelas dan memberikan rekomendasi dengan mudah dipahami oleh pihak yang berkepentingan.

Etika dalam Audit Komputer:

1. Integritas: Auditor komputer harus bertindak dengan integritas tinggi, menjaga objektivitas dan kejujuran dalam melakukan audit, serta tidak terlibat dalam tindakan yang melanggar etika profesional.
2. Kerahasiaan: Auditor komputer harus menjaga kerahasiaan data dan informasi yang diperoleh selama audit. Mereka harus mematuhi kebijakan privasi dan menjaga kerahasiaan informasi yang sensitif.
3. Profesionalisme: Auditor komputer harus menjalankan tugas mereka dengan tingkat profesionalisme yang tinggi.

Mereka harus memiliki kompetensi yang memadai, menjaga standar profesional yang berlaku, serta memberikan pelayanan yang berkualitas.

4. Independensi: Auditor komputer harus bersikap independen dalam melakukan audit. Mereka tidak boleh terpengaruh oleh kepentingan pribadi atau organisasi lain yang dapat mengorbankan objektivitas dan kejujuran dalam penilaian mereka.
5. Tanggung Jawab kepada Pihak yang Berkepentingan: Auditor komputer harus menjalankan tanggung jawab mereka dengan mempertimbangkan kepentingan pihak yang terlibat, seperti manajemen, pemilik bisnis, dan pemangku kepentingan lainnya.

Etika yang kuat dalam audit komputer sangat penting untuk mempertahankan integritas dan kepercayaan dalam proses audit. Auditor komputer harus mengikuti kode etik profesional yang berlaku dan menjunjung tinggi prinsip-prinsip etika dalam setiap aspek pekerjaan mereka.

5.7 Tantangan dan Trend dalam Pemantauan dan Audit Komputer

Tantangan yang dihadapi dalam pemantauan dan audit komputer:

1. Kompleksitas Infrastruktur IT
   Infrastruktur IT yang kompleks, seperti lingkungan multi-cloud, teknologi berbasis kontainer, dan sistem yang terdistribusi, dapat menyulitkan pemantauan dan audit. Mengelola dan memantau lingkungan yang kompleks membutuhkan pemahaman yang mendalam tentang berbagai teknologi dan interaksi antara mereka.

2. Volume Data yang Tinggi
   Pemantauan dan audit komputer menghasilkan jumlah data yang besar. Menyaring, menganalisis, dan mengelola data dalam skala besar dapat menjadi tantangan. Dibutuhkan alat dan teknik analisis yang canggih untuk mengidentifikasi pola, ancaman, atau perilaku mencurigakan dari data yang melimpah.
3. Kebutuhan Kecepatan dan Respons yang Tinggi
   Perubahan dan serangan terjadi dengan cepat dalam lingkungan teknologi saat ini. Pemantauan dan audit harus dilakukan secara real-time dan responsif untuk mendeteksi dan merespons ancaman secepat mungkin. Memastikan bahwa sistem pemantauan dan audit mampu menangani kecepatan yang tinggi adalah tantangan tersendiri.
4. Kekurangan Sumber Daya
   Pemantauan dan audit yang efektif membutuhkan sumber daya manusia, waktu, dan anggaran yang cukup. Namun, sering kali organisasi menghadapi kekurangan dalam hal sumber daya ini. Hal ini dapat menghambat kemampuan untuk melakukan pemantauan dan audit secara menyeluruh dan menyediakan waktu yang cukup untuk menganalisis data dan mengambil tindakan.

Trend Terbaru dalam Pemantauan dan Audit Komputer:

1. Pemantauan Berbasis AI dan Analitik Lanjutan
   Penggunaan kecerdasan buatan (AI) dan analitik lanjutan semakin berkembang dalam pemantauan dan audit komputer. Teknik ini memungkinkan deteksi otomatis dan respons yang cepat terhadap ancaman dan perilaku mencurigakan berdasarkan pola dan analisis data yang kompleks.

2. Pemantauan dan Audit Cloud
   Dalam era komputasi awan, pemantauan dan audit komputer semakin terfokus pada lingkungan cloud. Organisasi perlu memantau dan mengaudit infrastruktur dan layanan cloud mereka untuk memastikan keamanan, ketersediaan, dan kepatuhan.
3. Konvergensi Pemantauan dan Keamanan
   Pemantauan sistem komputer semakin terintegrasi dengan solusi keamanan. Solusi pemantauan dapat memasukkan deteksi ancaman dan respons keamanan secara real-time, sehingga menggabungkan pemantauan dan respons dalam satu platform.

Perkembangan Teknologi yang Berdampak pada Pemantauan dan Audit Komputer:

1. Komputasi Awan
   Penerapan teknologi cloud computing telah mengubah cara pemantauan dan audit dilakukan. Penggunaan infrastruktur cloud membutuhkan pendekatan baru dalam memantau dan mengaudit sumber daya yang ada di dalamnya.
2. Internet of Things (IoT)
   Pertumbuhan IoT menghasilkan jumlah perangkat yang terhubung dalam jaringan. Pemantauan dan audit harus dapat mengakomodasi perangkat IoT dan mampu mengidentifikasi dan mengamankan perangkat tersebut dalam lingkungan yang terus berkembang.
3. Kecerdasan Buatan (AI) dan Analitik Lanjutan
   Penggunaan AI dan analitik lanjutan telah membantu dalam mengatasi kompleksitas pemantauan dan audit komputer. Teknologi ini memungkinkan analisis data yang lebih efisien, identifikasi pola tersembunyi, serta deteksi dan respons yang lebih cepat terhadap ancaman.

4. Keamanan Berbasis Perilaku (Behavior-based Security)
   Perkembangan teknologi telah mendorong pergeseran dari pendekatan keamanan tradisional berbasis tanda tangan ke keamanan berbasis perilaku. Pemantauan dan audit komputer harus dapat mengidentifikasi perilaku aneh atau mencurigakan dalam sistem untuk mendeteksi ancaman yang baru atau tidak dikenal.

Perkembangan teknologi terus berlanjut dan mempengaruhi pemantauan dan audit komputer. Organisasi harus tetap up-to-date dengan tren terbaru dan memanfaatkannya untuk meningkatkan kemampuan pemantauan dan audit mereka guna melindungi sistem dan data mereka dari ancaman keamanan yang terus berkembang.

5.8 Kesimpulan

Bab ini memberikan panduan komprehensif dan praktis untuk pemantauan dan audit komputer dalam konteks keamanan sistem informasi. Dengan memahami konsep dasar, metodologi, dan praktik terbaik, pembaca akan dapat meningkatkan keamanan sistem informasi organisasi mereka dan melindungi aset informasi yang berharga. Bab ini juga memberikan wawasan tentang tren terbaru dan tantangan yang dihadapi dalam bidang pemantauan dan audit komputer.

DAFTAR PUSTAKA

Hall, J.A. 2010. Information Technology Auditing and Assurance. Cengage Learning.

Peltier, T.R. 2013. Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. Auerbach Publications.

Beasley, M.S., Branson, J.L., & Hancock, B. 2014. Principles of Auditing: An Introduction to International Standards on Auditing. Pearson.

Pfleeger, C.P., Pfleeger, S.L., & Margulies, J. 2014. Security in Computing. Prentice Hall.

Reynolds, J. 2016. Computer and Information Security Handbook. Morgan Kaufmann.

Nigrini, M. J., & Mittermaier, L. J. 2017. Data Analytics for Auditing: Techniques, Tools, and Applications. John Wiley & Sons.

Bishop, M. 2018. Computer Security: Art and Science. Addison-Wesley Professional.

Vallabhaneni, S.R. 2020. ISACA's Cybersecurity Audit Certificate Program. ISACA.

CISA Review Manual, 27th Edition. 2021. ISACA.

NIST SP 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations. 2020. National Institute of Standards and Technology.

ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. (2013). International Organization for Standardization.

BAB 6
DETEKSI DAN PENCEGAHAN INTRUSI

Oleh Andreas L. Sumendap

6.1 Pendahuluan

Jaringan Komputer memberikan kemampuan antar komputer untuk dapat berkomunikasi dan saling terhubung membentuk grid data yang besar. Jaringan Komputer yang ada sekarang itu telah di temukan sejak bertahun-tahun yang lalu, dan saat jaringan komputer ini di gunakan secara luas kemungkinan intrusi terhadap jaringan tersebut menjadi nyata. Langkah logis berikutnya setelah menemukan teknologi dan kerentanan terkait yang tak terelakkan adalah mengidentifikasi parameter keamanan. Salah satu cara untuk membantu menentukan parameter keamanan ini adalah dengan membuat formula untuk mewakili ide keamanan (Holland, 2021).

Deteksi intrusi adalah proses pemantauan peristiwa yang terjadi dalam sistem komputer atau jaringan dan menganalisisnya untuk tanda-tanda kemungkinan insiden, yang merupakan pelanggaran atau ancaman pelanggaran kebijakan keamanan komputer, kebijakan penggunaan yang dapat diterima, atau praktik keamanan standar(Rehman, 2003). Pencegahan intrusi adalah proses melakukan deteksi intrusi dan berusaha menghentikan kemungkinan insiden yang terdeteksi. Sistem deteksi dan pencegahan intrusi (IDPS) terutama difokuskan pada identifikasi kemungkinan insiden, logging informasi tentang mereka, berusaha menghentikan mereka, dan melaporkannya ke administrator keamanan. Selain itu, organisasi menggunakan IDPS untuk tujuan

lain, seperti mengidentifikasi masalah dengan kebijakan keamanan, mendokumentasikan ancaman yang ada, dan mencegah individu melanggar kebijakan keamanan. IDPS telah menjadi tambahan yang diperlukan untuk infrastruktur keamanan di hampir setiap organisasi.

IDPS biasanya merekam informasi terkait dengan peristiwa atau kejadian yang diamati, memberi notifikasi kepada administrator keamanan tentang peristiwa penting yang diamati, dan membuat laporan('Intrusion Detection Systems: A Modern Investigation', 2004). Banyak IDPS juga dapat merespons ancaman yang terdeteksi dengan mencoba mencegahnya agar tidak berhasil. Mereka menggunakan beberapa teknik respons, yang melibatkan IDPS menghentikan serangan itu sendiri, mengubah lingkungan keamanan (misalnya, mengkonfigurasi ulang firewall), atau mengubah konten serangan.

Ada empat jenis umum sistem deteksi dan pencegahan intrusi, yaitu *network-based*, *wireless*, *network behaviour analysis*, dan *host-based*(Sturmer, 2023). IDPS berbasis jaringan menganalisis berbagai protokol jaringan dan umumnya digunakan pada server akses jarak jauh, server dan router jaringan pribadi virtual. IDPS nirkabel mengawasi aktivitas mencurigakan di jaringan nirkabel dan juga mencari jaringan nirkabel yang tidak sah di suatu area. Analisis perilaku jaringan mencari ancaman yang dapat mematikan jaringan atau menyebarkan malware dan biasanya digunakan dengan jaringan pribadi yang tersambung ke Internet. IDPS berbasis host bekerja pada satu sistem dan mencari proses aplikasi yang aneh, lalu lintas jaringan yang tidak biasa ke host, modifikasi sistem file, dan perubahan konfigurasi.

6.2 Sistem Deteksi dan Pencegahan Intrusi

Deteksi intrusi adalah proses pemantauan peristiwa yang terjadi dalam sistem komputer atau jaringan dan menganalisisnya untuk tanda-tanda kemungkinan masalah, yaitu pelanggaran atau

ancaman yang akan datang. melanggar kebijakan keamanan komputer, kebijakan penggunaan yang diterima, atau praktik keamanan standar(Cahyanto, 2018). Masalah memiliki banyak penyebab, seperti malware (mis. worm, virus), penyerang mendapatkan akses tidak sah ke sistem dari Internet, dan sistem yang kasar memberi hak istimewa kepada pengguna atau mencoba mendapatkan hak istimewa tambahan yang tidak diizinkan. Sementara banyak insiden bersifat jahat, banyak lainnya tidak; misalnya, seseorang mungkin memasukkan alamat komputer yang salah dan secara tidak sengaja mencoba menyambung ke sistem lain tanpa izin.

Deteksi intrusi adalah proses pemantauan peristiwa yang terjadi dalam sistem komputer atau jaringan dan menganalisisnya untuk tanda-tanda kemungkinan masalah, yaitu pelanggaran atau ancaman yang akan datang. untuk pelanggaran kebijakan keamanan komputer, kebijakan penggunaan yang diterima, atau praktik keamanan standar. (IDS) adalah perangkat lunak yang mengotomatiskan proses deteksi intrusi. (IPS) adalah perangkat lunak yang memiliki semua kemampuan sistem deteksi intrusi dan juga dapat mencoba mencegah kemungkinan masalah. Teknologi IDS dan IPS menyediakan banyak fitur yang sama, dan administrator seringkali dapat menonaktifkan fitur pemblokiran di produk IPS, menjadikannya bertindak sebagai IDS. Oleh karena itu, untuk singkatnya, istilah sistem deteksi dan pencegahan intrusi (IDPS) digunakan sepanjang sisa bab ini untuk merujuk pada teknologi IDS an IPS.

IDPS berfokus pada identifikasi kemungkinan insiden. Misalnya, IDPS dapat mendeteksi ketika penyerang berhasil menyusupi sistem dengan mengeksploitasi kerentanan dalam sistem. IDPS akan mencatat informasi tentang aktivitas dan melaporkan kejadian tersebut ke administrator keamanan sehingga mereka dapat melakukan tindakan tanggap kejadian untuk meminimalkan kerusakan. Banyak IDPS juga dapat

dikonfigurasi untuk mengenali pelanggaran kebijakan penggunaan yang dapat diterima dan kebijakan keamanan lainnya contohnya termasuk penggunaan aplikasi berbagi file peer-to-peer yang dilarang dan transfer file database besar ke media yang dapat dipindahkan atau perangkat seluler. Selain itu, banyak IDPS dapat mengidentifikasi aktivitas pengintaian, yang mungkin menunjukkan bahwa serangan akan segera terjadi atau bahwa sistem atau karakteristik sistem tertentu menjadi perhatian khusus penyerang. Kegunaan lain dari IDPS adalah untuk mendapatkan pemahaman yang lebih baik tentang ancaman yang mereka deteksi, khususnya frekuensi dan karakteristik serangan, sehingga langkah-langkah keamanan yang tepat dapat diidentifikasi. Beberapa IDPS juga dapat mengubah profil keamanannya ketika ancaman baru terdeteksi. Misalnya, IDPS mungkin mengumpulkan informasi yang lebih mendetail untuk sesi tertentu setelah aktivitas jahat terdeteksi dalam sesi tersebut.

Ada Dua tipe Intrusi yang umumnya di alami oleh jaringan Komputer yaitu:

1. Internal, yang merupakan intrusi yang datangnya dari dalam sesama pengguna jaringan
2. Eksternal yang umumnya Intrusi ini lewat jaringan Internet dari luar

Alasan mengapa serangan dari dalam lebih menyakitkan adalah karena orang dalam (penyerang) akan memanfaatkan kepercayaan dan akses fisik karena sumber daya di jaringan area lokal perusahaan dianggap tepercaya. Praktisnya, kami tidak secara tegas membatasi aktivitas mereka karena upaya untuk mengontrol pengguna tepercaya ini terlalu dekat akan menghambat arus bebas bisnis. Dengan meningkatnya jumlah intrusi internal di industri dan persyaratan peraturan dan kepatuhan yang lebih ketat, organisasi menghadapi tantangan berat untuk melindungi data

sensitif mereka dari ancaman internal dan memenuhi persyaratan peraturan dan kepatuhan.

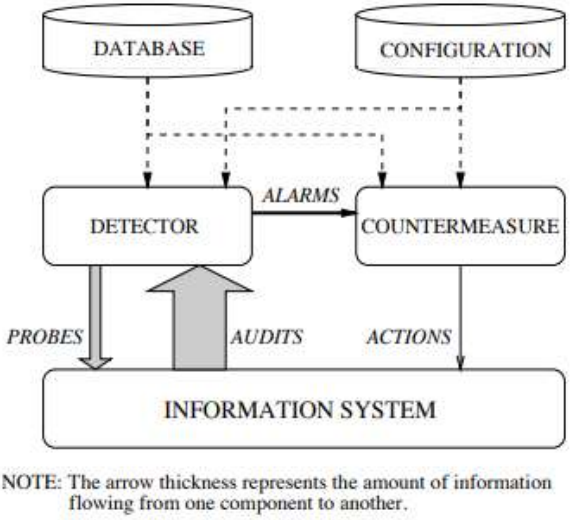
Berdasarkan Statistik oleh (Magalhaes, 2003):

1. Hampir 90% jaringan interkoneksi yang menggunakan Intrusion Detection System mendeteksi pelanggaran keamanan komputer dalam 12 bulan terakhir meskipun telah dipasang beberapa firewall.
2. Institut Keamanan Komputer, 4/7/02 melaporkan bahwa 80% melaporkan kerugian finansial lebih dari $455 juta disebabkan oleh penyusupan dan tindakan jahat sesudahnya.
3. Jutaan pekerjaan telah terpengaruh karena intrusi.
4. Hanya 0,1% perusahaan yang membelanjakan anggaran yang sesuai untuk Sistem Deteksi Intrusi.
5. Sistem Deteksi Intrusi kebanyakan dikira sebagai firewall atau penggantinya.
6. Dengan menggunakan Intrusion Detection System akan berperan sebagai barrier tambahan di atas sebuah antivirus. Sebagian besar organisasi yang menggunakan perangkat lunak antivirus tidak menggunakan IDS.

Sifat umum dari semua teknologi IDPS adalah bahwa mereka tidak dapat memberikan deteksi yang sepenuhnya akurat. Salah mengidentifikasi aktivitas tidak berbahaya sebagai aktivitas berbahaya disebut sebagai *false positive*; di sisi lain, kegagalan untuk mengidentifikasi aktivitas jahat, adalah *false negative*. Tidak mungkin menghilangkan semua positif dan negatif palsu; Dalam kebanyakan kasus, mengurangi terjadinya salah satu akan meningkatkan terjadinya yang lain. Banyak organisasi memilih untuk mengurangi jumlah negatif palsu dengan mengorbankan peningkatan jumlah positif palsu, yang berarti lebih banyak peristiwa berbahaya yang terdeteksi, tetapi lebih banyak sumber

daya analitik diperlukan untuk membedakan positif palsu dari yang berbahaya lainnya. peristiwa berbahaya yang nyata.

Sebagian besar teknologi IDPS juga lemah terhadap penggunaan teknik penghindaran umum. Penghindaran memodifikasi format atau waktu aktivitas jahat sehingga tampilannya berubah tetapi efeknya adalah sama. Penyerang menggunakan teknik penghindaran untuk mencoba mencegah teknologi IDPS mendeteksi serangan. Misalnya, penyerang dapat menyandikan karakter teks dengan cara tertentu yang akan dipahami target, berharap IDPS yang memantau aktivitas tidak akan melakukannya. Sebagian besar teknologi IDPS dapat mengatasi teknik penghindaran dengan menduplikasi pemrosesan khusus yang dilakukan oleh target.



Gambar 6.1. Deteksi Intrusi paling sederhana
Sumber (Debar, 2000)

6.2.1 Metode Deteksi IDPS

Teknologi IDPS menggunakan banyak metodologi untuk mendeteksi serangan. Kelas utama dari metodologi deteksi adalah analisis protokol *signature-based*, *anomali-based*, dan *stateful*.

Sebagian besar teknologi IDPS menggunakan beberapa metodologi, baik secara terpisah maupun terintegrasi, untuk memberikan deteksi yang lebih luas dan akurat. Metodologi ini dijelaskan secara lebih rinci di bawah ini.

1. Deteksi *Signature-Based*

   Signature atau tanda khusus adalah pola serangan atau jenis serangan yang diketahui. Deteksi berbasis *signature* adalah proses membandingkan tanda tertentu dengan peristiwa yang diamati untuk mengidentifikasi kemungkinan serangan. Contoh tanda tangan adalah:

   a. Upaya telnet dengan nama pengguna "root", yang merupakan pelanggaran terhadap kebijakan keamanan organisasi
   b. Email dengan subjek "Gambar gratis!" dan nama file lampiran "freepics.exe", yang merupakan karakteristik dari bentuk malware yang dikenal
   c. Entri log sistem operasi dengan nilai kode status 645, yang menunjukkan bahwa audit host telah dinonaktifkan.

   Deteksi berbasis tanda tangan sangat efektif dalam mendeteksi serangan yang sudah di ketahui tandanya tetapi tidak efektif dalam mendeteksi serangan yang sebelumnya tidak diketahui, serangan yang disamarkan dengan penggunaan teknik penghindaran, dan banyak varian serangan yang dikenal. Misalnya, jika penyerang memodifikasi malware di contoh sebelumnya untuk menggunakan nama file "freepics2.exe", *signature* yang mencari "freepics.exe" tidak akan cocok dengannya.

Deteksi berbasis *signature* adalah metode deteksi paling sederhana karena hanya membandingkan unit aktivitas saat ini, seperti paket atau entri log, ke daftar *signature* menggunakan operasi perbandingan string. Teknologi deteksi yang semata-mata berbasis *signature* memiliki sedikit pemahaman tentang banyak jaringan atau protokol aplikasi dan tidak dapat melacak dan memahami keadaan komunikasi—misalnya, mereka tidak dapat memasangkan permintaan dengan respons yang sesuai, atau dapatkah mereka mengingat permintaan sebelumnya saat memproses permintaan saat ini. Ini mencegah metode berbasis tanda tangan untuk mendeteksi serangan yang terdiri dari beberapa peristiwa jika tidak ada satu peristiwa pun yang mengandung indikasi serangan yang jelas.

2. Deteksi *Anomaly-Based*

Deteksi berbasis anomali adalah proses membandingkan definisi aktivitas apa yang dianggap normal dengan peristiwa yang diamati untuk mengidentifikasi penyimpangan yang signifikan. IDPS yang menggunakan deteksi berbasis anomali memiliki profil yang mewakili perilaku normal hal-hal seperti pengguna, host, koneksi jaringan, atau aplikasi. Profil dikembangkan dengan memantau karakteristik aktivitas tipikal selama periode waktu tertentu. Misalnya, profil untuk jaringan mungkin menunjukkan bahwa aktivitas Web terdiri dari rata-rata 13% bandwidth jaringan di perbatasan Internet selama jam kerja biasa. IDPS kemudian menggunakan metode statistik untuk membandingkan karakteristik aktivitas saat ini dengan ambang yang terkait dengan profil, seperti mendeteksi ketika aktivitas Web terdiri dari bandwidth yang jauh lebih besar dari yang diharapkan dan

memperingatkan administrator tentang anomali tersebut. Profil dapat dikembangkan untuk banyak atribut perilaku, seperti jumlah email yang dikirim oleh pengguna, jumlah upaya login yang gagal untuk sebuah host, dan tingkat penggunaan prosesor untuk sebuah host dalam jangka waktu tertentu.

Manfaat utama dari metode deteksi berbasis anomali adalah metode ini bisa sangat efektif dalam mendeteksi serangan yang sebelumnya tidak diketahui. Misalnya, komputer terinfeksi malware jenis baru. Malware dapat menghabiskan sumber daya pemrosesan komputer, mengirim banyak email, memulai koneksi jaringan dalam jumlah besar, dan melakukan perilaku lain yang akan sangat berbeda dari profil yang dibuat untuk komputer.

Profil awal dihasilkan selama periode waktu yang terkadang disebut periode pelatihan. Profil dapat berupa statis atau dinamis. Setelah dibuat, profil statis tidak berubah kecuali IDPS secara khusus diarahkan untuk membuat profil baru. Profil dinamis disesuaikan terus-menerus saat peristiwa tambahan diamati. Karena sistem dan jaringan berubah dari waktu ke waktu, ukuran perilaku normal yang sesuai juga berubah; profil statis akhirnya akan menjadi tidak akurat, sehingga perlu dibuat ulang secara berkala. Profil dinamis tidak memiliki masalah ini, tetapi rentan terhadap upaya penghindaran dari penyerang. Misalnya, penyerang dapat sesekali melakukan aktivitas jahat dalam jumlah kecil, kemudian secara bertahap meningkatkan frekuensi dan kuantitas aktivitas. Jika laju perubahan cukup lambat, IDPS mungkin menganggap aktivitas berbahaya tersebut sebagai perilaku normal dan memasukkannya ke dalam profilnya.

Masalah lain dengan membangun profil adalah dalam beberapa kasus bisa sangat menantang untuk membuatnya akurat karena aktivitas komputasi sangat kompleks. Misalnya, jika aktivitas pemeliharaan tertentu yang melakukan transfer file besar hanya terjadi sebulan sekali, mungkin tidak diamati selama periode pelatihan; ketika pemeliharaan terjadi, kemungkinan akan dianggap sebagai penyimpangan yang signifikan dari profil. Produk IDPS berbasis anomali sering menghasilkan banyak positif palsu karena aktivitas jinak yang menyimpang secara signifikan dari profil, terutama di lingkungan yang lebih beragam atau dinamis. Masalah penting lainnya dengan penggunaan teknik deteksi berbasis anomali adalah seringkali sulit bagi analis untuk menentukan apa yang memicu peringatan tertentu.

3. Analisa Protokol *Stateful*

Analisis protokol stateful adalah proses membandingkan profil yang telah ditentukan sebelumnya dari definisi aktivitas protokol jinak yang diterima secara umum untuk setiap status protokol terhadap peristiwa yang diamati untuk mengidentifikasi penyimpangan. Tidak seperti deteksi berbasis anomali, yang menggunakan profil khusus host atau jaringan, analisis protokol stateful bergantung pada profil universal yang dikembangkan vendor yang menentukan bagaimana protokol tertentu harus dan tidak boleh digunakan. “Stateful” dalam analisis protokol stateful berarti bahwa IDPS mampu memahami dan melacak status protokol jaringan, transportasi, dan aplikasi yang memiliki pengertian status. Misalnya, saat pengguna memulai sesi File Transfer Protocol (FTP), sesi awalnya dalam keadaan tidak diautentikasi. Pengguna yang tidak diautentikasi hanya boleh melakukan beberapa

perintah dalam keadaan ini, seperti melihat informasi bantuan atau memberikan nama pengguna dan kata sandi. Bagian penting dari memahami status adalah memasangkan permintaan dengan tanggapan, jadi ketika upaya otentikasi FTP terjadi, IDPS dapat menentukan apakah itu benar, berhasil dengan memeriksa kode status dalam respons yang sesuai. Setelah pengguna berhasil mengautentikasi, sesi berada dalam status terotentikasi, dan pengguna diharapkan untuk melakukan salah satu dari beberapa lusin perintah. Melakukan sebagian besar perintah ini saat dalam keadaan tidak diautentikasi akan dianggap mencurigakan, tetapi dalam keadaan diautentikasi melakukan sebagian besar darinya dianggap tidak berbahaya.

Analisis protokol stateful dapat mengidentifikasi urutan perintah yang tidak terduga, seperti mengeluarkan perintah yang sama berulang kali atau mengeluarkan perintah tanpa terlebih dahulu mengeluarkan perintah lain yang menjadi ketergantungannya. Fitur pelacakan status lainnya dari analisis protokol stateful adalah bahwa IDPS dapat melacak autentikator yang digunakan untuk setiap sesi, dan mencatat autentikator yang digunakan untuk aktivitas mencurigakan. Beberapa IDPS juga dapat menggunakan informasi autentikator untuk menentukan aktivitas yang dapat diterima secara berbeda untuk beberapa kelas pengguna atau pengguna tertentu.

"Analisis protokol" yang dilakukan oleh metode analisis protokol stateful biasanya mencakup pemeriksaan kewajaran untuk masing-masing perintah, seperti panjang minimum dan maksimum untuk argumen. Jika suatu perintah biasanya memiliki argumen nama pengguna, dan nama pengguna memiliki maksimum panjang 20 karakter, maka argumen dengan panjang 1000 karakter

mencurigakan. Jika argumen besar berisi data biner, maka itu akan lebih mencurigakan.

Metode analisis protokol stateful menggunakan model protokol, yang biasanya didasarkan terutama pada standar dari vendor perangkat lunak dan badan standar (misalnya, *Internet Engineering Task Force* [IETF] *Request for Comments* [RFC]). Model protokol biasanya juga mempertimbangkan variasi akun dalam setiap implementasi protokol. Banyak standar yang tidak lengkap, dan vendor mungkin melanggar standar atau menambahkan fitur hak milik; semua situasi ini dapat menyebabkan variasi di antara implementasi. Untuk protokol berpemilik, detail lengkap tentang protokol seringkali tidak tersedia, sehingga menyulitkan teknologi IDPS untuk melakukan analisis yang komprehensif dan akurat. Selain itu, karena protokol direvisi dan vendor mengubah implementasi protokolnya, model protokol IDPS perlu diperbarui untuk mencerminkan perubahan tersebut.

Kelemahan utama metode analisis protokol stateful adalah bahwa mereka sangat intensif sumber daya karena kompleksitas analisis dan biaya tambahan yang terlibat dalam melakukan pelacakan status untuk banyak sesi simultan. Masalah lainnya adalah metode analisis protokol stateful tidak dapat mendeteksi serangan yang tidak melanggar karakteristik perilaku protokol yang dapat diterima secara umum, seperti melakukan banyak tindakan jinak dalam waktu singkat yang menyebabkan penolakan layanan. Namun masalah lain adalah bahwa model protokol yang digunakan oleh IDPS mungkin bertentangan dengan cara protokol diimplementasikan dalam versi tertentu dari aplikasi dan sistem operasi tertentu, atau bagaimana implementasi klien dan server yang berbeda dari protokol berinteraksi.

6.2.2 Komponen IDPS

Komponen umum dalam IDPS adalah:

1. Sensor atau Agen. Sensor dan agen memantau dan menganalisis aktivitas. Istilah "sensor" biasanya digunakan untuk IDPS yang memantau jaringan, dan istilah "agen" untuk teknologi IDPS yang hanya memantau satu host.
2. Manajemen Server. Server manajemen adalah perangkat yang menerima informasi dari sensor atau agen dan mengelolanya. Beberapa server manajemen melakukan analisis pada informasi yang diterima dan dapat mengidentifikasi insiden yang tidak dapat dilakukan oleh sensor atau agen individual. Mencocokkan informasi kejadian dari berbagai sensor atau agen, seperti menemukan kejadian yang dipicu oleh alamat IP yang sama, dikenal sebagai korelasi. Beberapa penerapan IDPS kecil tidak menggunakan server manajemen apa pun. Dalam penerapan IDPS yang lebih besar, seringkali terdapat beberapa server manajemen, terkadang dalam tingkatan.
3. Server Basis Data. Server basis data adalah gudang untuk informasi acara yang direkam oleh sensor, agen, dan server manajemen. Banyak IDPS mendukung penggunaan server database.
4. Konsol. Konsol adalah program yang menyediakan antarmuka untuk pengguna dan administrator IDPS. Perangkat lunak konsol biasanya diinstal ke komputer desktop atau laptop standar. Beberapa konsol hanya digunakan untuk administrasi IDPS, seperti mengonfigurasi sensor atau agen dan menerapkan pembaruan perangkat lunak, sementara konsol lainnya hanya digunakan untuk pemantauan dan analisis. Beberapa konsol IDPS menyediakan kemampuan administrasi dan pemantauan.

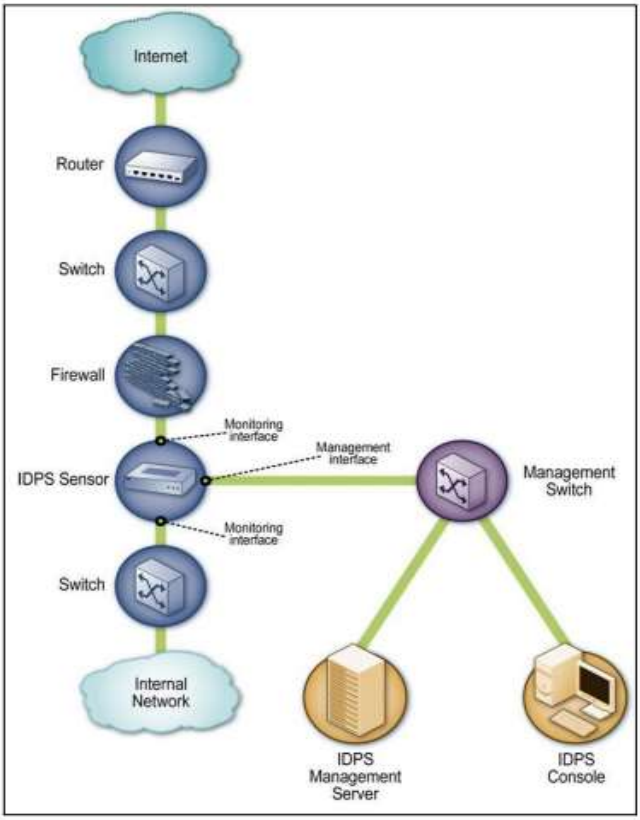
Komponen IDPS dapat dihubungkan satu sama lain melalui jaringan biasa atau jaringan terpisah yang dirancang untuk manajemen perangkat lunak keamanan yang dikenal sebagai jaringan manajemen. Jika jaringan manajemen digunakan, setiap host sensor atau agen memiliki antarmuka jaringan tambahan yang dikenal sebagai antarmuka manajemen yang terhubung ke jaringan manajemen, dan host dikonfigurasikan sehingga mereka tidak dapat melewatkan lalu lintas apa pun antara antarmuka manajemen dan antarmuka jaringan lainnya. Server manajemen, server basis data, dan konsol hanya terpasang ke jaringan manajemen. Arsitektur ini secara efektif mengisolasi jaringan manajemen dari jaringan produksi, menyembunyikan IDPS dari penyerang dan memastikan bahwa IDPS memiliki bandwidth yang memadai untuk berfungsi dalam kondisi buruk. Jika IDPS digunakan tanpa jaringan manajemen terpisah, cara untuk meningkatkan keamanan IDPS adalah dengan membuat jaringan manajemen virtual menggunakan jaringan area lokal virtual (VLAN) dalam jaringan standar. Menggunakan VLAN memberikan perlindungan untuk komunikasi IDPS, tetapi tidak sebanyak perlindungan jaringan manajemen terpisah.

6.3 Network-Based IDPS

Network-Based IDPS memantau dan menganalisis lalu lintas jaringan untuk segmen atau perangkat jaringan tertentu untuk mengidentifikasi aktivitas yang mencurigakan. IDPS berbasis jaringan paling sering digunakan di divisi antar jaringan. *Network Interface Card (NIC)* IDPS yang akan melakukan pemantauan ditempatkan dalam mode promiscuous sehingga mereka menerima semua paket yang mereka lihat, terlepas dari tujuan yang dituju. IDPS berbasis jaringan biasanya melakukan sebagian besar analisisnya pada lapisan aplikasi (misalnya, *Hypertext Transfer Protocol* [HTTP], *Simple Mail Transfer Protocol* [SMTP], *Domain Name System* [DNS]). Mereka juga menganalisis aktivitas

pada lapisan transport (misalnya, TCP, UDP) dan jaringan (misalnya, IPv4) untuk mengidentifikasi serangan pada lapisan tersebut dan memfasilitasi analisis lapisan aplikasi. Beberapa IDPS berbasis jaringan juga melakukan analisis terbatas pada lapisan perangkat keras (misalnya, *Address Resolution Protocol* [ARP]).

Sensor IDPS berbasis jaringan dapat digunakan dalam salah satu dari dua mode: inline atau pasif. Sensor inline dikerahkan sehingga lalu lintas yang dipantau melewatinya. Beberapa sensor inline adalah perangkat *hybrid firewall*/IDPS. Motivasi utama penerapan sensor inline adalah untuk menghentikan serangan dengan memblokir lalu lintas. Sensor pasif dikerahkan sehingga memonitor salinan lalu lintas yang sebenarnya; tidak ada lalu lintas yang melewati sensor. Sensor pasif dapat memantau lalu lintas melalui berbagai metode, termasuk port rentang sakelar, yang dapat melihat semua lalu lintas melalui sakelar; tap jaringan, yang merupakan koneksi langsung antara sensor dan media jaringan fisik itu sendiri, seperti kabel serat optik; dan penyeimbang beban IDS, yang merupakan perangkat yang menggabungkan dan mengarahkan lalu lintas ke sistem pemantauan. Sebagian besar teknik untuk memiliki sensor mencegah intrusi mengharuskan sensor dipasang dalam mode inline. Teknik pasif biasanya tidak memberikan cara yang dapat diandalkan untuk sensor memblokir lalu lintas. Dalam beberapa kasus, sensor pasif dapat menempatkan paket ke jaringan untuk mencoba mengganggu koneksi, tetapi metode tersebut umumnya kurang efektif dibandingkan metode inline.



Gambar 6.2. Inline Network IDPS
Sumber :(Scarfone and Mell, 2012)

IDPS berbasis jaringan biasanya menawarkan kemampuan deteksi yang ekstensif dan luas. Sebagian besar menggunakan kombinasi teknik deteksi analisis protokol berbasis *signature*, berbasis anomali, dan stateful. Teknik-teknik ini biasanya terjalin erat; misalnya, mesin analisis protokol stateful mengurai aktivitas menjadi permintaan dan tanggapan, yang masing-masing diperiksa untuk anomali dan dibandingkan dengan *signature* aktivitas buruk yang diketahui.

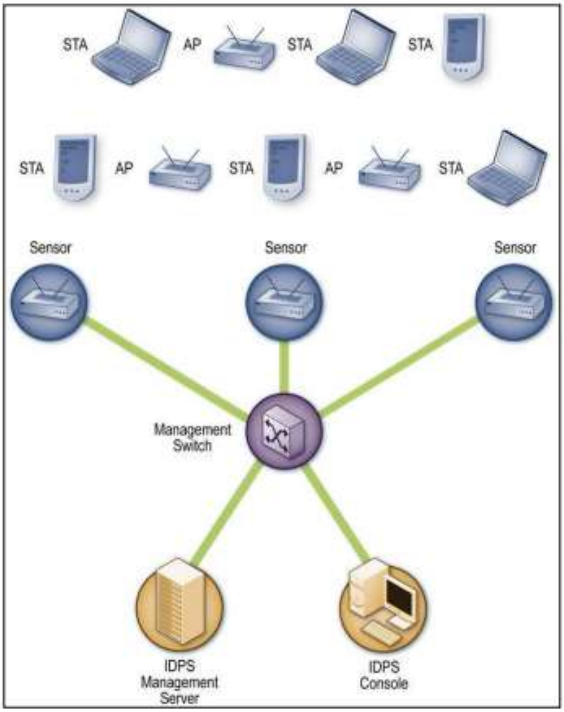
Meskipun IDPS berbasis jaringan menawarkan kemampuan deteksi yang ekstensif, mereka memiliki beberapa keterbatasan yang signifikan. IDPS berbasis jaringan tidak dapat mendeteksi serangan dalam lalu lintas terenkripsi, termasuk koneksi jaringan pribadi virtual (VPN), HTTP melalui SSL (HTTPS), dan sesi SSH. Untuk memastikan bahwa analisis yang memadai dilakukan pada muatan dalam lalu lintas terenkripsi, IDPS dapat diterapkan untuk menganalisis muatan sebelum dienkripsi atau setelah didekripsi. Contohnya termasuk menempatkan sensor IDPS berbasis jaringan untuk memantau lalu lintas yang didekripsi dan menggunakan perangkat lunak IDPS berbasis host untuk memantau aktivitas di dalam host sumber atau tujuan.

6.4 Wireless IDPS

Wireless IDPS memantau lalu lintas jaringan nirkabel dan menganalisis protokol jaringan nirkabelnya untuk mengidentifikasi aktivitas mencurigakan yang melibatkan protokol tersebut. IDPS nirkabel paling sering digunakan untuk memantau jaringan area lokal nirkabel (WLAN). WLAN biasanya digunakan oleh perangkat dalam jangkauan yang cukup terbatas, seperti gedung perkantoran atau kampus perusahaan, dan diimplementasikan sebagai ekstensi ke jaringan area lokal (LAN) kabel yang ada untuk menyediakan mobilitas pengguna yang ditingkatkan.

Sebagian besar WLAN menggunakan keluarga standar WLAN *Institute of Electrical and Electronics Engineers* (IEEE) 802.11. IEEE 802.11 WLAN memiliki dua komponen arsitektur dasar: sebuah stasiun (STA), yang merupakan perangkat titik akhir nirkabel (misalnya, komputer laptop, asisten digital pribadi [PDA]), dan titik akses (AP), yang secara logis menghubungkan STA dengan jaringan organisasi. infrastruktur jaringan kabel atau jaringan lainnya. Beberapa WLAN juga menggunakan sakelar nirkabel, yang

bertindak sebagai perantara antara Titik Akses dan jaringan berkabel. Jaringan berdasarkan STA dan AP dikonfigurasi dalam mode infrastruktur; jaringan yang tidak menggunakan AP, di mana STA terhubung langsung satu sama lain, dikonfigurasi dalam mode ad hoc. Hampir semua WLAN organisasi menggunakan mode infrastruktur. Setiap AP dalam WLAN memiliki nama yang ditetapkan untuknya yang disebut *service set identifier* (SSID). SSID memungkinkan STA untuk membedakan satu WLAN dari yang lain.



Gambar 6.3. Infrastruktur *wireless* IDPS
Sumber :(Scarfone and Mell, 2012)

IDPS nirkabel dapat mendeteksi serangan, kesalahan konfigurasi, dan pelanggaran kebijakan di tingkat protokol WLAN, terutama memeriksa komunikasi protokol IEEE 802.11. IDPS nirkabel tidak memeriksa komunikasi pada tingkat yang lebih tinggi (misalnya, alamat IP, muatan aplikasi). Beberapa produk hanya melakukan deteksi berbasis tanda tangan sederhana, sementara yang lain menggunakan kombinasi teknik deteksi analisis protokol berbasis tanda tangan, berbasis anomali, dan stateful. Jenis peristiwa yang paling sering terdeteksi oleh sensor IDPS nirkabel termasuk WLAN dan perangkat WLAN yang tidak sah dan perangkat WLAN yang tidak diamankan dengan baik (mis., pengaturan WLAN yang salah konfigurasi). IDPS nirkabel juga dapat mendeteksi pola penggunaan WLAN yang tidak biasa, yang dapat mengindikasikan adanya penyusupan perangkat atau penggunaan WLAN yang tidak sah, dan penggunaan pemindai jaringan nirkabel. Penolakan kondisi layanan, termasuk serangan logis (misalnya, membebani AP dengan sejumlah besar pesan) dan serangan fisik (misalnya, memancarkan energi elektromagnetik pada frekuensi WLAN agar WLAN tidak dapat digunakan), juga dapat dideteksi oleh IDPS nirkabel. Beberapa IDPS nirkabel juga dapat mendeteksi perangkat WLAN yang mencoba memalsukan identitas perangkat lain.

Meskipun IDPS nirkabel menawarkan kemampuan deteksi yang kuat, mereka memiliki beberapa keterbatasan yang signifikan. Satu masalah dengan beberapa sensor IDPS nirkabel adalah penggunaan teknik penghindaran, khususnya terhadap skema pemindaian saluran sensor. Salah satu contohnya adalah melakukan serangan dalam semburan yang sangat singkat pada saluran yang saat ini tidak dipantau. Penyerang juga dapat meluncurkan serangan pada dua saluran pada saat yang bersamaan. Jika sensor mendeteksi serangan pertama, ia tidak dapat mendeteksi serangan kedua kecuali ia memindai jauh dari saluran serangan pertama. Sensor IDPS nirkabel juga rentan

terhadap serangan. Serangan penolakan layanan yang sama (baik logis maupun fisik) yang mencoba mengganggu WLAN juga dapat mengganggu fungsi sensor. Sensor juga seringkali sangat rentan terhadap serangan fisik karena biasanya terletak di lorong, ruang konferensi, dan area terbuka lainnya. Beberapa sensor memiliki fitur anti-tamper, seperti dirancang agar terlihat seperti alarm kebakaran atau AP biasa, yang dapat mengurangi kemungkinan diserang. Semua sensor rentan terhadap serangan fisik seperti jamming yang mengganggu RF; tidak ada pertahanan terhadap serangan semacam itu selain membangun perimeter fisik di sekitar fasilitas sehingga penyerang tidak bisa cukup dekat dengan WLAN untuk menghentikannya.

DAFTAR PUSTAKA

Cahyanto, T.A. 2018. *Intrusion Detection System*.

Debar, H. 2000. *An Introduction to Intrusion-Detection Systems*.

Holland, T. 2021. *Understanding IPS and IDS: Using IPS and IDS together for Defense in Depth*.

'Intrusion Detection Systems: A Modern Investigation' (2004). Available at: https://doi.org/10.5121/ijnsa.

Magalhaes, R.M. 2003. 'Host-Based IDS vs Network-Based IDS (Part 1)', *http://www.windowsecurity.com/articlestutorials/intrusion_detection/Hids_vs_Nids_Part1.html* [Preprint].

Rehman, R.U. 2003. *Intrusion Detection Systems with Snort Advanced IDS Techniques Using Snort, Apache, MySQL, PHP, and ACID*. New Jersey. Available at: www.phptr.com.

Scarfone, K. and Mell, P. 2012. *Guide to Intrusion Detection and Prevention Systems (IDPS) (Draft) Recommendations of the National Institute of Standards and Technology*.

Sturmer, G. 2023. 'What Is an Intrusion Prevention System?', *https://www.easytechjunkie.com/what-is-an-intrusion-prevention-system.htm* [Preprint].

BAB 7
ANTIVIRUS DAN ANTI MALWARE

Oleh Gede Erik Aktama

7.1 Pengenalan Keamanan Cyber

Diera digital yang penuh dengan inovasi teknologi, acaman terhadap keamanan komputer semakin tinggi. Serangan siber yang semakin canggih dan beragam, mengintai setiap aspek kehidupan online dan offline dari perangkat individu hingga jaringan korporat. Keamanan siber atau cyber security adalah serangkaian langkah dan tindakan yang dilakukan untuk melindungi sistem komputer, jaringan, dan data dari serangan atau akses ilegal. Penting untuk selalu menerapkan praktik keamanan siber mengingat segalanya kini mulai terhubung secara digital. Dari memesan makanan, membayar di toko, sampai moda transportasi, Anda hampir selalu terlibat dengan ruang siber. Tanpa langkah-langkah keamanan yang tepat, data sensitif Anda dapat dicuri, sistem dapat disusupi, dan operasi bisnis dapat terganggu. Bahkan ketika hanya mengobrol atau online di media sosial, bahaya ancaman cyber akan tetap mengintai. Terlebih lagi kalau memiliki website atau toko online, Anda tidak boleh lengah sedikit pun. Sebab, transaksi di website atau toko online biasanya memerlukan informasi pribadi seperti detail kartu kredit pelanggan. Jika data mereka terancam oleh penjahat siber, bisnis Anda dapat kehilangan kepercayaan pelanggan dan reputasi akan memburuk. Jadi, bisa dibilang bahwa cyber security adalah checklist utama bagi Anda yang aktif di internet. Pastikan selalu menggunakan protokol keamanan yang kuat, seperti enkripsi data , sertifikat SSL dan menggunakan Antivirus dan antimalware yang tepat (Aura Nisrina Hesanty, 2023).

7.2 Virus dan Malware

Virus dan malware adalah dua jenis perangkat lunak berbahaya yang dapat merusak sistem komputer dan mengambil alih data pribadi. Virus dan malware adalah ancaman serius bagi keamanan komputer. Virus adalah program komputer yang dapat menggandakan dirinya sendiri dan menyebar dari satu komputer kekomputer lain baik melalui flashdisk ataupun dari internet. Malware adalah intilah yang lebih luas yang mencakup semua jenis perangkat lunak berbahaya seperti virus, trojan, worm, dan perangkat lunak yang berbahaya lainnya yang dapat merusak sistem komputer.

Berikut ini dijelaskan secara rinci jenis-jenis malware:

7.2.1 Virus

Virus komputer adalah program perangkat lunak yang dirancang untuk merusak atau mengambil alih sistem komputer (Dwi Ananto, 2018). Virus komputer dapat menyebar melalui email, situs web, atau bahkan melalui perangkat USB. Virus komputer dapat menyebabkan kerusakan pada sistem komputer seperti menghapus file penting, mengubah pengaturan sistem, dan bahkan mencuri data pribadi.

7.2.2 Worm

Worm adalah malware yang dapat menyebar melalui jaringan atau perangkat yang terhubung tanpa memerlukan interaksi pengguna. Worm dapat menggandakan diri dan mengirim salinan dirinya melalui jaringan, sering kali dengan tujuan merusak jaringan atau merusak data. Worm tidak seperti virus komputer biasa, yang menggandakan dirinya dengan cara menyisipkan program dirinya pada program yang ada dalam komputer tersebut, Worm sering kali menggunakan celah keamanan dalam perangkat untuk menyebar dengan cepat. worm dapat mengakibatkan overloading jaringan dan merusak infrastruktur

digital. Beberapa worm juga menghabiskan bandwidth yang tersedia.

7.2.3 Trojan

Trojan merupakan program yang bersembunyi di dalam atau tampak seperti program sah atau legal. malware ini biasa menyembunyikan dirinya di dalam perangkat lunak yang seolah-olah bermanfaat atau sah. Ketika pengguna menjalankan perangkat lunak tersebut, trojan dapat membuka pintu belakang yang memungkinkan penyerang untuk mengambil alih perangkat atau mencuri informasi. (Rastri Prathivi and Vensy Vydia, 2017)

7.2.4 Ransomware

Ransomware adalah Malware yang mengunci file dan data pengguna, dengan ancaman akan menghapusnya kecuali pemilik data membayar tebusan. Ini dapat mengakibatkan kehilangan data yang signifikan jika Anda tidak membayar tebusan. (Aura Nisrina Hesanty, 2023)

7.2.5 Adware

Adware adalah semacam perangkat lunak berbahaya yang berusaha menawarkan sesuatu kepada pengguna yang akibatnya muncul sebagai jendela pop-up bahkan jika pengguna buka biasanya adware masuk ke sistem dalam bentuk perjudian, iklan, atau jendela pop-up lainnya. (Nugraha, Budiono and Almaarif, 2019) Adware yang sering kali dianggap sebatas iklan, tetapi sebenarnya memiliki aspek yang jauh lebih dalam. Adware singkatan dari "advertising-supported software," adalah jenis perangkat lunak yang biasanya disertai dengan iklan-iklan yang muncul saat kita menggunakan program atau menjelajahi internet.

7.2.6 Spyware

Spyware adalah jenis malware yang dirancang untuk mengumpulkan informasi rahasia tentang aktivitas pengguna tanpa izin. Spyware dapat mencatat keystroke, memantau aktivitas browsing, dan bahkan mengambil screenshot tanpa sepengetahuan pengguna. Spyware secara diam-diam mengumpulkan informasi tentang Anda tanpa sepengetahuan Anda. Informasi yang dikumpulkan dapat digunakan untuk tujuan periklanan atau bahkan kegiatan kriminal.

7.2.7 Backdoor

Backdoor adalah suatu metode atau fitur yang disisipkan dalam perangkat lunak, sistem, atau jaringan untuk memberikan akses yang tidak sah atau tidak terotorisasi ke sistem.

7.2.8 Rootkits

Rootkits adalah sebuah koleksi software yang dirancang khusus untuk memperbolehkan malware untuk mengumpulkan informasi. Jenis malware ini bekerja dibalik layar sehingga pengguna komputer tidak akan curiga. (Nugraha, Budiono and Almaarif, 2019)

7.2.9 Keyloggers

Keyloggers adalah jenis perangkat lunak atau perangkat keras yang digunakan untuk merekam setiap tombol yang ditekan pada papan ketik suatu perangkat. Tujuan utama dari keyloggers adalah untuk merekam aktivitas pengguna dengan cara mencatat setiap karakter, angka, atau tanda baca yang ditekan oleh pengguna pada papan ketik. Informasi yang direkam ini dapat mencakup kata sandi, pesan teks, informasi kartu kredit, dan data sensitif lainnya.

7.2.10 Browser Hijacker

Browser hijacker adalah jenis perangkat lunak berbahaya yang dirancang untuk mengambil alih pengaturan browser internet pada suatu perangkat. Tujuannya adalah untuk mengubah berbagai pengaturan browser tanpa izin pengguna dan mengarahkan pengguna ke halaman-halaman web yang tidak diinginkan. Browser Hijacker seringkali mengganti halaman beranda, mesin pencari default, dan halaman tab baru pada browser dengan situs yang dikendalikan oleh penyerang.

Cara umum yang digunakan oleh Browser Hijacker untuk menginfeksi perangkat meliputi:

1. Bundling: Perangkat lunak ini bisa tersembunyi dalam perangkat lunak lain yang sah dan diunduh oleh pengguna. Saat pengguna menginstal perangkat lunak tersebut, Browser Hijacker juga akan diinstal tanpa sepengetahuan pengguna.
2. Tautan yang Menyesatkan: Pengguna dapat diarahkan ke tautan yang menyesatkan atau mengunduh berkas yang tampak sah, tetapi sebenarnya adalah Browser Hijacker.
3. Ekstensi atau Add-on Palsu: Browser Hijacker dapat menyamar sebagai ekstensi atau add-on yang berguna untuk browser. Setelah diinstal, mereka mengubah pengaturan browser.
4. Pembaruan Palsu: Pengguna mungkin diberitahu bahwa mereka perlu mengunduh pembaruan penting untuk browser mereka, tetapi pembaruan tersebut sebenarnya adalah Browser Hijacker.

7.2.11 Rogue Security Software

Rogue Security Software, atau yang dikenal juga sebagai perangkat lunak keamanan palsu, adalah jenis perangkat lunak yang meniru perangkat lunak keamanan yang sah, tetapi sebenarnya tidak memiliki kemampuan untuk melindungi atau

membersihkan sistem dari ancaman keamanan. Tujuan utama dari *Rogue Security Software* adalah untuk menipu pengguna dengan membuat mereka percaya bahwa sistem mereka terinfeksi oleh malware atau virus yang serius, dan kemudian memaksa mereka untuk membeli versi lengkap dari perangkat lunak palsu tersebut.

Caranya adalah dengan menampilkan pemberitahuan palsu tentang adanya ancaman yang serius di dalam sistem, kadang-kadang dalam bentuk pop-up atau pesan yang tampak mengintimidasi. Pesan ini sering kali menunjukkan hasil pemindaian palsu dan mengajak pengguna untuk mengunduh atau membeli perangkat lunak palsu tersebut agar dapat membersihkan masalah yang sebenarnya tidak ada.

Rogue Security Software biasanya diinstal melalui tautan yang menyesatkan, iklan palsu, atau metode lain yang mengelabui pengguna. Pengguna yang tidak waspada dapat dengan mudah tertipu oleh taktik ini.

7.3 Antivirus Dan Anti Malware

Antivirus dan anti-malware adalah perangkat lunak yang dirancang untuk melindungi komputer dari virus dan malware. Antivirus bekerja dengan memindai file dan program untuk mencari tanda-tanda virus. Jika antivirus menemukan virus, maka akan menghapusnya dari komputer. Anti-malware bekerja dengan cara yang sama, tetapi juga dapat melindungi komputer dari malware yang lebih canggih. Antivirus adalah program yang dirancang untuk mendeteksi, mencegah, dan menghapus virus komputer. Sedangkan Antimalware adalah jenis perangkat lunak yang lebih luas dalam cakupannya daripada antivirus. Antimalware adalah perangkat lunak yang dirancang untuk mendeteksi dan menghapus malware lainnya, seperti spyware, adware, dan ransomware. Selain melawan virus, antimalware juga berfokus pada mendeteksi dan menghapus berbagai jenis malware, seperti spyware (yang mengumpulkan informasi tanpa izin), adware (yang

menampilkan iklan berlebihan), trojan (yang menyembunyikan diri dalam program yang tampak sah), dan masih banyak lagi. Antimalware cenderung lebih canggih dalam mendeteksi ancaman yang lebih kompleks.

Secara umum, antivirus dan antimalware bekerja sama untuk melindungi komputer Anda dari malware. Antivirus akan mendeteksi virus, dan antimalware akan mendeteksi malware lainnya. Namun, ada beberapa situasi di mana Anda mungkin ingin menggunakan antivirus dan antimalware secara terpisah. Misalnya, jika Anda baru saja mengunduh file dari internet, Anda mungkin ingin menjalankan antivirus terlebih dahulu untuk memeriksa apakah file tersebut mengandung virus. Jika file tersebut tidak mengandung virus, Anda kemudian dapat menjalankan antimalware untuk memeriksa apakah file tersebut mengandung malware lainnya. Beberapa antivirus juga dilengkapi dengan fitur antimalware sehingga tidak perlu menggunakan antimalware yang terpisah.

Ada banyak manfaat menggunakan antivirus dan antimalware, termasuk:

1. Melindungi komputer dari virus dan malware lainnya.
2. Menjaga keamanan data pribadi.
3. Memblokir akses ke situs web dan file berbahaya.
4. Mempercepat kinerja komputer.
5. Mencegah kerusakan pada file dan program.
6. Melindungi komputer dari serangan hacker.

7.3.1 Antivirus

Antivirus adalah sebuah jenis perangkat lunak yang digunakan untuk mengamankan, mendeteksi, dan menghapus virus komputer dari sistem komputer. Umumnya, perangkat lunak ini berjalan di latar belakang (*background*) dan melakukan pemindaian terhadap semua berkas yang diakses (dibuka, dimodifikasi, atau ketika disimpan). (Kurniawati and Ardiansyah,

2020) Cara kerja antivirus melibatkan serangkaian langkah yang kompleks untuk mengidentifikasi dan mengatasi ancaman siber. Berikut adalah langkah-langkah umum yang dilakukan oleh antivirus dalam menjalankan tugasnya:

1. Pendeteksian: Antivirus pertama-tama melakukan pemindaian (scanning) pada berbagai file, program, dan area dalam sistem yang mungkin terinfeksi. Pemindaian ini dapat dilakukan secara on-demand (pemindaian manual oleh pengguna) atau real-time (pemindaian otomatis saat berkas diakses).
2. Database Definisi: Antivirus menggunakan database definisi malware yang diperbarui secara teratur. Database ini berisi tanda-tanda karakteristik unik dari virus dan malware lainnya. Ketika antivirus melakukan pemindaian, ia membandingkan berkas yang diperiksa dengan tanda-tanda dalam database ini.
3. Pembandingan Tanda-Tanda: Antivirus membandingkan tanda-tanda karakteristik dalam database dengan berkas yang diperiksa. Jika ada kesamaan yang signifikan, antivirus akan mengidentifikasi berkas tersebut sebagai ancaman potensial.
4. Tindakan Lanjutan: Setelah mengidentifikasi berkas yang mencurigakan, antivirus akan mengambil tindakan sesuai dengan jenis infeksi yang terdeteksi:
    a. Pembersihan: Antivirus akan berusaha membersihkan berkas yang terinfeksi dengan menghapus atau mengisolasi kode berbahaya.
    b. Karantina: Jika tidak mungkin membersihkan berkas, antivirus akan memindahkan berkas tersebut ke karantina, tempat berkas diisolasi dari sistem utama untuk mencegah penyebaran lebih lanjut.

c. Penghapusan: Jika berkas terinfeksi tidak dapat dibersihkan atau dikarantina, antivirus dapat menghapus berkas tersebut sepenuhnya.

5. Analisis Heuristik: Beberapa antivirus menggunakan analisis heuristik, yaitu teknik yang memeriksa perilaku berkas atau program untuk mendeteksi pola yang mencurigakan. Ini memungkinkan antivirus mengenali ancaman yang belum terdaftar dalam database definisi.
6. Pembaruan Rutin: Perangkat lunak antivirus harus diperbarui secara berkala untuk menjaga database definisi dan metode deteksi yang diperbarui. Ini penting karena ancaman siber terus berkembang, dan pembaruan membantu antivirus mengenali ancaman baru.
7. Laporan dan Notifikasi: Antivirus biasanya memberikan laporan hasil pemindaian kepada pengguna, menunjukkan berkas yang ditemukan dan tindakan yang diambil. Jika ada ancaman serius, antivirus akan memberikan notifikasi segera kepada pengguna.

7.3.2 Antimalware

Antimalware adalah perangkat lunak yang dirancang untuk melindungi sistem komputer dari berbagai jenis ancaman siber, termasuk virus, spyware, trojan, worm, adware, dan lain-lain. Sedangkan menurut (Kramer and Bradfield, 2010) Malware mengacu pada perangkat lunak berbahaya yang dapat merusak, mencuri informasi, atau mengganggu operasi normal dari sistem komputer atau perangkat elektronik lainnya. Antimalware bekerja dengan cara mendeteksi, mencegah, dan menghapus malware yang mungkin ada dalam sistem. Malware diciptakan dengan maksud tertentu yaitu melakukan aktifitas berbahaya yang berdampak sangat merugikan bagi para korbannya, antara lain seperti penyadapan serta pencurian informasi pribadi, hingga kasus perusakan sistem yang dilakukan oleh penyusup (Intruder)

terhadap perangkat korban dengan berbagai alasan. (Cahyanto, Wahanggara and Ramadana, 2017).

Ada beberapa jenis antimalware yang tersedia, termasuk:

1. Antivirus: Ini adalah jenis antimalware yang fokus pada mendeteksi dan menghapus virus yang dapat merusak atau menginfeksi file sistem. Antivirus sering diperbarui secara berkala untuk mengenali virus-virus baru.
2. Antispyware: Jenis antimalware ini berfokus pada mendeteksi dan menghapus perangkat lunak mata-mata (spyware) yang dapat mencuri informasi pribadi atau data sensitif.
3. Anti-adware: Antimalware ini berusaha untuk mengenali dan menghapus perangkat lunak iklan yang mungkin mengganggu pengalaman pengguna dan mengumpulkan data tentang perilaku browsing.
4. Anti-rootkit: Perangkat lunak ini berusaha mendeteksi dan menghapus rootkit, yaitu program yang digunakan oleh penyerang untuk menyembunyikan aktivitas jahat mereka di dalam sistem.
5. Firewall: Firewall adalah bagian dari solusi keamanan yang memantau lalu lintas jaringan dan mengatur izin akses untuk mencegah ancaman dari luar masuk ke sistem.

Antimalware menggunakan pendekatan yang lebih holistik dan kompleks dalam mendeteksi serta melawan ancaman. Berikut adalah cara kerja umum antimalware:

1. Pemindaian Berbasis Tanda-Tanda:
   Antimalware memulai proses dengan melakukan pemindaian berkas dan program dalam sistem. Seperti antivirus, antimalware juga menggunakan database definisi yang diperbarui secara berkala. Database ini berisi tanda-tanda karakteristik yang terkait dengan berbagai jenis malware.

2. Analisis Heuristik:
   Antimalware menggunakan analisis heuristik yang canggih untuk mengidentifikasi perilaku yang mencurigakan. Ini mencakup mengamati aktivitas berkas atau program yang tidak biasa, seperti mencoba mengakses area sensitif atau melakukan tindakan yang tidak sesuai dengan jenisnya.
3. Pembelajaran Mesin:
   Beberapa antimalware menggunakan teknik pembelajaran mesin (*machine learning*) untuk mengenali pola-pola yang berkaitan dengan malware. Dengan mempelajari pola-pola ini dari berbagai jenis ancaman, antimalware dapat mengenali ancaman baru yang belum terdaftar dalam database definisi.
4. Analisis Perilaku:
   Antimalware memantau perilaku program dan berkas dalam sistem. Jika suatu program tiba-tiba mulai melakukan aktivitas mencurigakan, seperti mengumpulkan informasi pribadi atau mengubah berkas sistem, antimalware dapat mengambil tindakan untuk mencegah aktivitas tersebut.
5. Deteksi dan Penanganan Ancaman Lainnya:
   Selain virus, antimalware juga melindungi sistem dari berbagai jenis ancaman seperti spyware (mencuri informasi), trojan (program berbahaya yang menyamar sebagai program sah), worm (menyebar melalui jaringan), dan adware (menampilkan iklan yang tidak diinginkan). Antimalware berusaha untuk mengidentifikasi dan menghapus ancaman-ancaman ini.
6. Pembaruan Rutin:
   Seperti antivirus, antimalware juga memerlukan pembaruan rutin untuk menjaga keefektifan dalam mengenali ancaman-ancaman baru. Pembaruan ini termasuk penambahan definisi baru, pembaruan algoritma analisis, dan peningkatan kemampuan deteksi.

7. Notifikasi dan Tindakan:
   Antimalware memberikan laporan hasil pemindaian kepada pengguna dan memberikan notifikasi segera jika ada ancaman serius. Pengguna dapat memilih tindakan yang akan diambil terhadap ancaman tersebut, seperti membersihkan, mengkarantina, atau menghapus berkas yang terinfeksi.

7.3.3 Kelebihan Dan Kekurangan Antivirus Dan Antimalware

Setiap antivirus atau antimalware memiliki kelebihan dan kekurangan masing masing. Berikut ini kelebihan dan kekuarangan antivirus dan antimalware.

Kelebihan Antivirus:

1. Spesifik: Dirancang khusus untuk melawan virus.
2. Efektif: Biasanya efektif dalam mengidentifikasi dan menghapus virus yang sudah dikenali.
3. Cepat: Pendeteksian virus sering kali cepat dan dilakukan secara real-time saat berkas diakses.

Kekurangan Antivirus:

1. Terbatas: Tidak efektif dalam mendeteksi jenis malware lain, seperti spyware atau trojan.
2. Tidak bisa menghadapi ancaman baru: Bergantung pada database definisi virus yang diperbarui, sehingga tidak efektif melawan ancaman yang belum dikenali.

Kelebihan Antimalware:

1. Fleksibel: Dapat mendeteksi berbagai jenis malware, termasuk ancaman yang belum dikenali.
2. Heuristik canggih: Menggunakan analisis heuristik dan pembelajaran mesin untuk mendeteksi pola perilaku yang mencurigakan.
3. Perlindungan yang lebih luas: Melawan berbagai ancaman siber, termasuk virus, spyware, trojan, worm, dan lainnya.

Kekurangan Antimalware: Lebih kompleks: Kadang-kadang dapat menghasilkan lebih banyak positif palsu, yaitu kesalahan mendeteksi sesuatu sebagai ancaman saat sebenarnya tidak.

7.3.4 Memilih Antivirus dan Antimalware yang Tepat

Ada banyak antivirus dan antimalware yang tersedia di pasaran. Berikut adalah beberapa tips untuk memilih antivirus dan antimalware yang tepat untuk Anda:

1. Pertimbangkan kebutuhan keamanan Anda. Jika Anda hanya menggunakan komputer untuk browsing web dan email, maka Anda mungkin tidak memerlukan antivirus dan antimalware yang paling mahal. Namun, jika Anda menggunakan komputer untuk pekerjaan atau menyimpan data penting, maka Anda perlu memilih antivirus dan antimalware yang lebih canggih.
2. Perhatikan fitur-fitur yang ditawarkan. Pastikan antivirus dan antimalware yang Anda pilih menawarkan fitur-fitur yang Anda butuhkan, seperti perlindungan terhadap virus, malware, ransomware, dan phishing.
3. Baca ulasan. Sebelum membeli antivirus dan antimalware, bacalah ulasan dari pengguna lain. Ini akan membantu Anda mendapatkan gambaran tentang perangkat lunak mana yang terbaik untuk Anda.
4. Pertimbangkan harga. Antivirus dan antimalware bisa mahal. Namun, ada juga banyak perangkat lunak gratis yang tersedia. Pastikan Anda memilih perangkat lunak yang sesuai dengan anggaran Anda.

7.3.5 Berbagai Gejala Infeksi Malware

Ada banyak gejala yang dapat menunjukkan bahwa komputer Anda mungkin terinfeksi malware. Berikut adalah beberapa gejala umum infeksi malware:

1. Kinerja komputer yang lambat atau tidak stabil

2. Perangkat tiba-tiba melakukan sesuatu yang tidak Anda harapkan, seperti membuka situs web yang tidak dikenal atau mengunduh file yang tidak diminta.
3. Terdapat Iklan yang tidak diharapkan.
4. Email atau pesan teks yang tidak diinginkan
5. Perangkat menjadi panas atau mengeluarkan suara yang tidak biasa.
6. File yang hilang atau rusak
7. Tidak dapat masuk ke akun Anda.
8. Program yang berjalan di latar belakang yang tidak Anda kenal.
9. Terdapat pesan kesalahan yang tidak biasa.
10. Komputer crash atau reboot secara tidak sengaja.
11. Perangkat mengalami masalah lain yang tidak dapat jelaskan.

Jika mengalami salah satu gejala ini, kemungkinan perangkat Anda telah terinfeksi malware. Penting untuk memindai perangkat dengan program antivirus untuk menghapus malware dan memperbaiki kerusakan yang disebabkan. Berikut adalah beberapa tips untuk mencegah infeksi malware:

1. Gunakan program antivirus yang diperbarui secara berkala.
2. Hindari membuka email atau file dari sumber yang tidak dikenal.
3. Jangan mengunduh file dari situs web yang tidak aman.
4. Perbarui perangkat lunak secara berkala.
5. Gunakan kata sandi yang kuat dan unik untuk setiap akun.
6. Berhati-hati saat menggunakan Wi-Fi publik.
7. Matikan komputer saat tidak digunakan.

Langkah Langkah Mengamankan Perangkat dari malware :

1. Perbaharui Sistem dan Perangkat Lunak: Pastikan sistem operasi dan semua perangkat lunak selalu diperbarui

dengan versi terbaru. Pembaruan ini sering mengatasi kerentanan keamanan yang ditemukan.

2. Aktifkan Firewall: Pastikan firewall diaktifkan di perangkat Anda. Firewall membantu mengontrol lalu lintas data yang masuk dan keluar dari perangkat Anda, melindungi Anda dari serangan jaringan.
3. Gunakan Sandboxing: Jika perangkat mendukung, gunakan lingkungan terisolasi atau "sandbox" untuk menjalankan aplikasi yang mencurigakan atau tidak dikenal. Ini membantu mencegah penyebaran malware.
4. Enkripsi Data: Gunakan enkripsi pada data sensitif di perangkat Anda. Enkripsi memastikan bahwa data hanya dapat dibuka oleh pihak yang memiliki kunci enkripsi yang sesuai.
5. Kata Sandi Kuat: Gunakan kata sandi yang kuat dan berbeda untuk setiap akun dan perangkat. Gunakan kombinasi huruf besar-kecil, angka, dan simbol untuk meningkatkan keamanan kata sandi.
6. Autentikasi Dua Faktor (2FA): Aktifkan autentikasi dua faktor (2FA) di akun Anda yang mendukungnya. Ini menambahkan lapisan keamanan ekstra dengan memerlukan verifikasi tambahan selain kata sandi.
7. Hapus Aplikasi Tidak Digunakan: Hapus atau nonaktifkan aplikasi yang tidak digunakan lagi. Aplikasi yang tidak diperbarui dapat menjadi titik masuk bagi penyerang.
8. Hindari WiFi Umum: Hindari mengakses informasi sensitif melalui jaringan WiFi publik atau tidak aman. Gunakan jaringan pribadi atau gunakan VPN untuk mengamankan koneksi Anda.
9. Lindungi Dari Malware: Instal perangkat lunak antivirus yang terpercaya dan perbarui secara berkala. Hindari mengunduh atau mengklik tautan dari sumber yang tidak dikenal.

10. Pengaturan Privasi: Periksa pengaturan privasi di perangkat Anda dan atur sesuai dengan preferensi Anda. Matikan berbagi lokasi jika tidak diperlukan dan batasi izin aplikasi.
11. Pemantauan Aktivitas: Selalu pantau aktivitas yang mencurigakan di perangkat Anda. Perhatikan perubahan yang tidak diinginkan dalam performa atau perilaku perangkat.
12. Pemulihan dan Cadangan: Buat cadangan data penting secara teratur. Siapkan rencana pemulihan jika perangkat Anda terkena serangan atau kerusakan.
13. Edukasi Pengguna: Berikan pelatihan kepada diri sendiri dan pengguna lain tentang praktik keamanan yang baik, seperti menghindari tautan atau lampiran yang mencurigakan.

7.3.6 Jenis-Jenis Antivirus

Antivirus adalah program yang dirancang untuk mencegah, mendeteksi, dan menghapus malware dari komputer atau perangkat lain. Setiap antivirus memiliki kelebihan dan kekurangan masing-masing. Berikut adalah beberapa jenis antivirus yang dapat digunakan :

1. Norton
2. Bitdefender
3. McAfee
4. TotalAV
5. Kaspersky
6. AVG
7. Avira
8. Avast

DAFTAR PUSTAKA

Aura Nisrina Hesanty. 2023. *Cyber Security: Arti, Konsep, dan Cara Menerapkannya*, *niagahoster*. Available at: https://www.niagahoster.co.id/blog/cyber-security-adalah/ (Accessed: 13 August 2023).

Cahyanto, T.A., Wahanggara, V. and Ramadana, D. 2017. 'Analisis dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis dan Malware Analisis Statis', *JUSTINDO, Jurnal Sistem & Teknologi Informasi Indonesia*, 2(1). Available at: https://core.ac.uk/download/pdf/289799715.pdf (Accessed: 13 August 2023).

Dwi Ananto, P.P. 2018. 'Analisis Cara Kerja Sistem Infeksi Virus Komputer', *Bina Insani Ict Journal* [Preprint]. Available at: http://ejournal-binainsani.ac.id/index.php/BIICT/article/view/773 (Accessed: 13 August 2023).

Kramer, S. and Bradfield, J.C. 2010. 'A general definition of malware', *Journal in Computer Virology*, 6(2), pp. 105–114. Available at: https://doi.org/10.1007/s11416-009-0137-1.

Kurniawati, A. and Ardiansyah. 2020. 'ANALISIS PERFORMA PERANGKAT LUNAK ANTIVIRUS DENGAN MENGGUNAKAN METODOLOGI PENGUKURAN PERFORMANCE (Studi Kasus: Perusahaan Perlindungan Tenaga Kerja)', *Jurnal Ilmiah MATRIK*, 22(1). Available at: https://journal.binadarma.ac.id/index.php/jurnalmatrik/article/download/838/476/ (Accessed: 13 August 2023).

Nugraha, J.D., Budiono, A. and Almaarif, A. 2019. 'Analisis Malware Berdasarkan API Call Memory Dengan Metode Deteksi Signature-Based', *Jurnal Rekayasa Sistem & Industri (JRSI)*, 6(02), p. 77. Available at: https://doi.org/10.25124/jrsi.v6i02.351.

Rastri Prathivi and Vensy Vydia. 2017. 'ANALISA PENDETEKSIAN WORM dan TROJAN PADA JARINGAN INTERNET UNIVERSITAS SEMARANG MENGGUNAKAN METODE KALSIFIKASI PADA DATA MINING C45 dan BAYESIAN NETWORK', *JURNAL TRANSFORMATIKA*, 14. Available at: https://journals.usm.ac.id/index.php/transformatika/article/download/440/275 (Accessed: 13 August 2023).

BAB 8
SISTEM ENKRIPSI DALAM KEAMANAN KOMPUTER

Oleh Sutardi

8.1 Pendahuluan

Kemajuan teknologi informasi membuat peluang besar dalam pengembangan aplikasi-aplikasi komputer, akan tetapi mempermudah setiap orang untuk melakukan kejahatan yang merugikan orang lain. Setiap data dan informasi yang melintas pada jaringan publik *(internet)* sudah pasti akan dengan mudahnya untuk diakses oleh banyak orang termasuk kalangan yang tidak berkepentingan dengan maksud mengambil atau merubah informasi tersebut. Berbagai cara yang bisa dilakukan untuk menutupi dan memproteksi informasi terhadap akses, penukaran bahkan pembajakan data atau informasi yang dilakukan oleh orang-orang yang tidak berhak, karena itu dibutuhkan sebuah teknik atau algoritma tersendiri untuk melindungi data atau informasi tersebut. (Rifki Sadikin, 2012).

Sistem keamanan komputer menjabarkan dua kategori keamanan yang berbeda, yaitu keamanan jaringan dan keamanan komputer, perbedaan yang paling mendasar dari dua buah keamanan tersebut, (Stalling, 2006). Untuk keamanan komputer itu sendiri merupakan sekumpulan perangkat yang dirancang untuk melindungi data komputer dengan aman, sedangkan keamanan jaringan merupakan sekumpulan perangkat yang dirancang untuk melindungi data atau informasi yang dikirim lewat jalur transmisi baik berupa transmisi *guided (twisted pair, serat optik*) ataupun transmisi *unguided* (udara, air, ruang hampa).

Seiring kemajuan teknologi, mengharuskan semua kegiatan komunikasi dan transaksi elektronik dilakukan melalui jalur publik (*internet*) sehingga kekhawatiran adanya data yang hilang atau data yang diubah semakin marak. Data elektronik merupakan data yang sangat urgen, sehingga dalam proses pengambilan sebuah keputusan dibutuhkan keakuratan dan ketepatan data.

Dalam menggunakan data digital bukan saja untuk kepentingan individu, akan tetapi juga kepada sektor-sektor lainnya yang dianggap penting seperti perusahaan, industri serta lembaga-lembaga kemasyarakatan dan pemerintahan lainnya.

Akibat pentingnya nilai dari sebuah data, menyebabkan harus tersedianya keamanan data itu sendiri seperti kerahasiaan data, autentikasi data, kredibilitas data dan integritas data sehingga data jatuh ke tangan pihak-pihak yang bertanggung jawab secara tepat dan akurat.

8.2 Kryptografi dan Steganografi

Layanan keamanan data atau informasi diwujudkan dengan menggunakan mekanisme keamanan data atau informasi itu sendiri. Implementasi dari keamanan data, tentunya dengan melakukan teknik penyandian dengan metode kriptografi dan steganografi.

8.2.1 Kryptografi

Istilah kriptografi (*cryptography*) mulai ada dari kata Yunani, terdiri dari dua kata *krypt'os* artinya **tersembunyi** dan *I'ogos* artinya **kata**. Sehingga kriptografi berarti **kata yang tersembunyi**. (Janner Simarmata, Sriadhi, 2019).

Kriptografi bermula dari konsep yang mempelajari teknik penyamaran pesan, namun dengan perkembangan teknologi modern kriptografi bukan hanya bertumpu kepada penyamaran

pesan namun lebih kepada sekumpulan metode pemecahan matematika dalam urusan perlindungan data dan informasi.

Terdapat banyak teknik *kriptografi* yang bisa diterapkan dalam pengamanan data seperti DES, Blowfish, RC4, RSA dan lain sebagainya. Pemilihan algoritma yang cocok untuk melindungi data-data aplikasi atau sistem informasi dapat dilihat dari suatu parameter yang dapat menentukan apakah algoritma yang digunakan baik dan aman. Parameter tersebut seperti ukuran kunci yang digunakan, waktu komputasi yang cepat, mode operasi yang digunakan, dan nilai *Avalanche Effect* (seberapa besar perubahan bit ketika karakter plaintext diubah).

Enkripsi adalah sistem keamanan dengan proses pengkodean yang rumit menggunakan rumus yang telah didefinisikan menggunakan algoritma tertentu untuk mengubah nilai data agar tidak bisa dibaca oleh pengguna yang tidak sah, sehingga memungkinkan data-data pengguna terlindungi dengan baik. Enkripsi adalah suatu proses dalam menjalankan perubahan sebuah kode atau *chiper* yang dapat dibaca menjadi kode atau *chiper* yang tidak bisa dibaca, dengan kata lain setelah informasi atau data di *enkripsi* maka harus membutuhkan sebuah kode kunci untuk membukanya atau membacanya.

Dalam ilmu *kriptografi* terdapat teks *enkripsi* yang disebut dengan *ciphertext*. *Ciphertext* yaitu teks terenkripsi yang dirubah dari *plaintext* menggunakan algoritma *enkripsi* untuk pengamanan data atau informasi pengguna, *Ciphertext* ini tidak bisa dibaca sebelum diubah kembali menjadi *plaintext* melalui sebuah proses *enkripsi* dengan menggunakan sebuah kunci yang disebut *cipher*. *Cipher* merupakan suatu algoritma kunci dalam ilmu *kriptografi* yang diimplementasikan pada *plaintext* atau informasi tertentu untuk merubahnya menjadi *ciphertext*. Metode seperti ini sering dipakai untuk keamanan komputer dan keamanan jaringan.

Enkripsi terbentuk berdasarkan algoritma tertentu untuk mengacaukan dan menyamarkan suatu informasi yang bisa

dipahami menjadi informasi yang tidak bisa dipahami bahkan tidak bisa dilihat. Sedangkan d*ekripsi* adalah sebuah proses dengan algoritma yang sama untuk memulihkan informasi yang tidak bisa dipahami atau teracak ke bentuk semula.

Algoritma *kriptografi* sering disebut dengan *ciper* yang merupakan fungsi/rumus dalam ilmu matematika yang sering dipakai untuk melakukan proses enkripsi dan dekripsi. Pada kriptografi modern sebuah kunci *(key)* dipakai untuk memecahkan permasalahan, sebuah kunci bisa mempunyai satu nilai *(keyspace)* atau lebih. (Algoritma kunci *simetris* dan algoritma *asimetris*).

Cryptographer adalah orang yang terlibat melakukan transformasi teks yang bisa dibaca menjadi teks yang tidak bisa dibaca/teracak dengan suatu algoritma dan kunci tertentu.

Kriptanalisis *(cryptanalysis)* adalah orang yang mendalami ilmu dan seni untuk memecahkan teks yang tidak bisa dibaca/teracak *(chipertext)* menjadi teks yang bisa dibaca *(plainteks)* tanpa harus memiliki kunci yang digunakan terlebih dahulu.

Arti lain dari Kriptografi adalah ilmu atau seni untuk menjaga kerahasiaan/keamanan data.

Kriptografi memiliki 5 bagian utama yaitu:

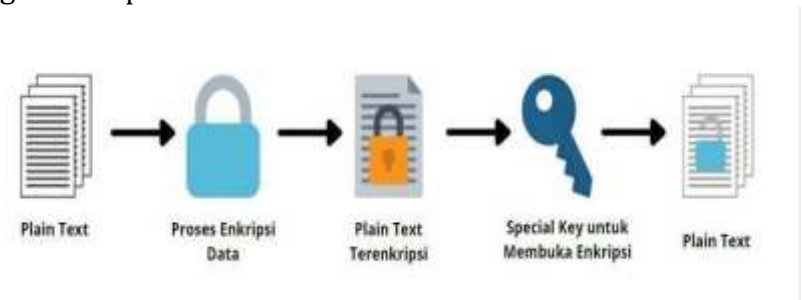
1. *Plaintext*, yaitu data asli yang belum mengalami perubahan sehingga dapat dibaca dan dipahami maknanya juga merupakan masukan bagi algoritma enkripsi.
2. *Ciphertext*, yaitu hasil keluaran dari algoritma enkripsi berupa data acak yang sudah mengalami perubahan sehingga tidak bisa dibaca
3. *Secret Key*, yaitu kunci rahasia yang terbentuk dari parameter teks asli dan merupakan masukan untuk menentukan hasil output bagi algoritma enkripsi.
4. Enkripsi, adalah perubahan informasi bit karakter dalam melakukan transformasi untuk mendapatkan teks sandi.

5. dari teks yang dapat dipahami *(plaintext)* menjadi teks yang tidak dapat dipahami *(ciphertext).*
6. Dekripsi, Pengubahan bit karakter yang tidak dapat dipahami *(ciphertext)* menjadi bit karakter yang dapat *dipahami (plaintext)* berupa dua masukan yaitu teks asli dan kunci rahasia, kunci rahasia yang digunakan sama dengan kunci rahasia pada algoritma enkripsi semula.

Enkripsi dan Dekripsi

Algoritma Enkripsi adalah metode pengacakan data dengan pengkodean yang rumit, sehingga membuat data dan informasi tidak dapat dibaca dan terlindungi dengan baik. Dengan enkripsi semua data dan pengolahan data yang diakses oleh pengguna terjamin keamanannya tanpa bantuan pengetahuan atau alat khusus. (Arius, 2008)

Enkripsi memiliki peran penting terkait masalah privasi dan perlindungan data, tentunya dengan metode pengacakan bit karakter, dari bit karakter yang bisa dibaca menjadi bit karakter yang tidak bisa dibaca. Pengertian lain dari enkripsi adalah *cipher*. C*ipher* memakai suatu algoritma yang dapat menyandikan semua aliran data (*stream*) bit/karakter dari data menjadi *cryptogram* yang tidak dapat dibaca.



Gambar 8.1. Proses terjadinya enkripsi
(Sumber : https://www.dewaweb.com)

Melihat banyaknya kasus kebocoran data yang dilakukan oleh peretas, maka metode enkripsi juga selalu mengalami pembaharuan contoh pada sistem operasi modern, seperti sistem operasi iOS, Android, dan Windows sudah menggunakan metode enkripsi tingkat tinggi. Penggunaan metode enkripsi dalam perlindungan dan keamanan data kian bertambah luas dan semakin diminati, sudah banyak digunakan oleh banyak penyedia layanan media sosial seperti *Facebook* dan *Whatsapp*. Kedua layanan media sosial ini mudah diakses menggunakan lebih dari satu perangkat dan keamanannya terjaga karena hanya bisa diakses jika pengguna tersebut yang memberikannya.

Dengan metode enkripsi, maka data yang acak hanya bisa diterima dan dibaca oleh orang tertentu saja, yaitu si pengirim dan penerima.

Sedangkan dekripsi adalah sebuah algoritma yang bisa membaca kembali data atau informasi yang telah disamarkan dalam enkripsi. (Arius, 2008)

Gambar 8.2. Enkripsi End-to-End Whatsapp
(Sumber : https://www.nesabamedia.com)

Cara Kerja Keamanan Enkripsi

Meskipun terlihat mudah dan sederhana, dalam prakteknya Enkripsi memiliki kinerja yang kompleks dan rumit. sistem keamanan enkripsi mirip seperti tembok penghalang besar. Dalam enkripsi ada yang disebut dengan istilah *Cipher*, menggunakan variabel, hingga *Asymmetric Cipher*.

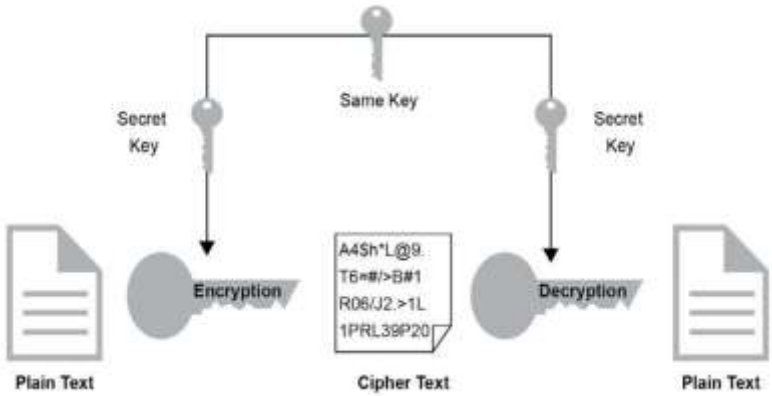
Cipher bekerja untuk menyembunyikan kata sandi dengan menggunakan algoritma tertentu, sehingga kata sandi yang dibangun tidak akan diketahui oleh orang lain. Sistem enkripsi akan membuat sebuah variabel yang digunakan sebagai kunci masuk ke akun. Jika yang digunakan Enkripsi dengan satu kunci, umumnya disebut dengan *Symmetric Cipher*. Sedangkan jika menggunakan dua kunci yang terhubung, maka disebut dengan *Asymmetric Cipher*.

Teknik: Kriptografi sebagai berikut.

1. **Kryptografi Kunci Simetris (*Symmetric Cipher*)**

   Kriptografi kunci simetris sering disebut juga dengan kunci rahasia (*Secret Key Encryption),* kadang disebut algoritma konvensional, yaitu algoritma yang memakai kunci enkripsi dari hasil kalkulasi kunci dekripsi dan sebaliknya. Dengan kata lain, pengirim dan penerima informasi hanya memakai sebuah kunci tunggal untuk melakukan enkripsi dan dekripsi data. (Janner Simarmata, Sriadhi, 2019) contoh beberapa algoritma yang termasuk kunci simetris seperti *DES, IDEA, RC4* yang Keamanannya telah terkenal dan bahkan digunakan di bidang pemerintahan. Pendekatan yang dilakukan oleh kriptografi kunci simetris dianggap lebih efisien dan sering digunakan oleh layanan VPN serta beberapa platform. Algoritma pada kriptografi simetris terbagi dua bagian, yaitu algoritma aliran (*Stream Cipher*) dan algoritma blok (*Block Cipher*). Pada algoritma *block cipher*, teknik enkripsi dan dekripsi melakukan pembagian *plainteks* menjadi bagian-bagian kecil, sehingga

masing-masing bagian dilakukan enkripsi menggunakan kunci yang sama. Beberapa algoritma *block cipher* berikut: *blowfish, DES, IDEA* dan lain sebagainnya. Sedangkan pada algoritma *stream cipher*, *plainteks* tidak melakukan pembagian, tetapi enkripsi dikerjakan secara terarah menggunakan kunci yang terarah pula. Adapun contoh algoritma kriptografi stream cipher yang banyak digunakan yaitu RC4.

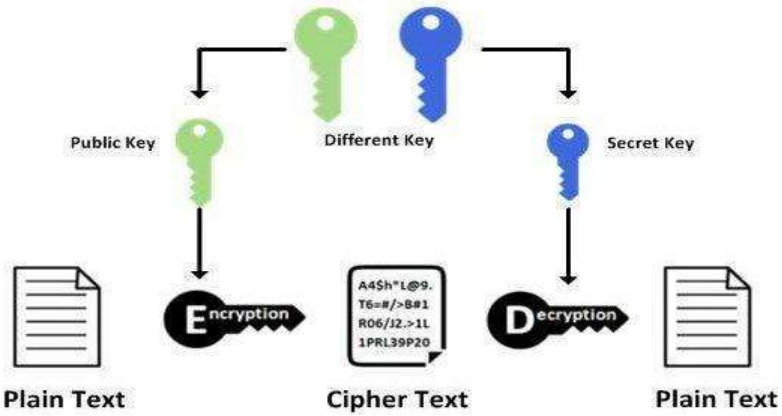


Gambar 8.3. Kriptografi Kunci Simetris
(Sumber : https://www.nesabamedia.com)

2. Kryptografi Kunci Asymmetric (*Asymmetric Cipher*)

Kriptografi kunci asimetris adalah metode yang menggunakan dua kunci yang saling berkaitan dan sering disebut dengan kunci publik (*Public Key Encryption*) yang dibagi kepada semua pengguna, sedangkan kunci private dirahasiakan dan hanya diketahui oleh seorang pengguna saja. (Janner Simarmata, Sriadhi, 2019) pada umumnya algoritma ini digunakan untuk melindungi data pribadi yang sangat penting dengan keamanan yang sangat tinggi dan sering digunakan dalam bidang pemerintahan dengan tujuan mengenkripsi data, kunci privatenya untuk mendekripsi data. Algoritma asimetris dianggap sangat aman dibanding dengan kriptografi kunci

simetris. Beberapa metode yang menggunakan kriptografi ini: algoritma RSA, dan beberapa metode lain DSA, PKC,teknik kurva elips dll.



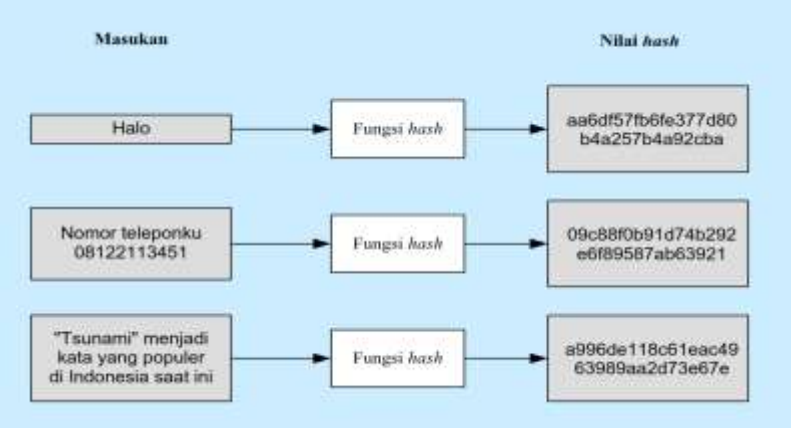
Gambar 8.4. Kriptografi Kunci Asimetris
(Sumber : https://www.nesabamedia.com)

3. Fungsi *Hash*.

Fungsi hash satu arah (*One Way Function*), merupakan fungsi matematika yang sering digunakan untuk memproses pesan sehingga menghasilkan teks khusus yang disebut dengan *message digest* dengan integritas yang sangat tinggi dengan menghasilkan teks yang berbeda. Algoritma ini mengacak data menjadi angka dan karakter menjadi informasi terenkripsi tanpa harus mengubah ukuran filenya.

Fungsi hash adalah fungsi matematika yang mendapat nilai masukan dari karakter dengan panjang karakter bebas untuk menghasilkan karakter lain yang panjangnya tetap seberapa panjang pun karakter masukannya.

Fungsi Hash ini berguna untuk memverifikasi tanda tangan digital, pembuatan sidik jari, *message authentication code* serta meregenerasi *bi*t acak.(Putra, 2009). Gambar 13.5 merupakan proses terjadinya fungsi hash pada sebuah pesan.



Gambar 8.5. Fungsi hash
(Sumber : https://informatika.stei.itb.ac.id)

Salah satu contoh implementasi algoritma kriptografi kunci simetris (*Symmetric Cipher*) Pada Gambar 8.6 menunjukan arsitektur sistem enkripsi dekripsi kriptografi kunci simetris,
Penginputan data pada aplikasi untuk mencari sumber koneksi database server, sehingga database server menampilkan isi dari database pada form aplikasi, sehingga user dapat melakukan proses enkripsi dan dekripsi pada sebuah tabel dalam database dengan menggunakan sebuah kunci simetris *(Symmetric Cipher)* yang diberikan oleh admin.
Algoritma enkripsi dan dekripsi dilakukan ketika pengguna melakukan klik proses pada tombol enkripsi dan dekripsi sehingga sistem akan mengambil data pada database.

Gambar 8.6. Penggunaan kunci simetris pada file database.

Tujuan Kriptografi

Metode kerja dari kriptografi adalah menyediakan keamanan data selama pemrosesan dan penyimpanan informasi.

Algoritma kriptografi dikembangkan semakin komplek dengan tujuan untuk memastikan kerahasiaan, integritas, autentikasi, serta ketidaktahuan dari orang yang tidak bertanggung jawab.(Munir, Rinaldi, 2006)

1. Kerahasiaan data *(data confidentiality)*
   Adalah layanan yang melindungi pesan atau informasi tetap terjaga kerahasiaanya dari orang yang tidak berwenang. dengan merealisasikan penyandian pesan menjadi cipherteks
2. Keutuhan data *(data integrity)*
   Memastikan bahwa sebuah data atau informasi yang diperoleh penerima adalah valid dan tidak mengalami perubahan dan dipastikan data tersebut betul-betul sama dengan informasi yang dikirimkan oleh pengirim.
3. Tidak ada penyangkalan *(Non-repudiation)*
   Layanan ini dapat memberikan bukti bahwa pesan atau informasi terkirim oleh pengirim yang benar, layanan ini

menghindari adanya penolakan dari pengirim/penerima informasi.

4. *Authentication*
   Layanan ini mengidentifikasi keaslian sumber pesan dan memberikan jaminan keotentikannya, memungkinkan pihak pengirim dan penerima pesan saling berkomunikasi dan saling mengautentikasi kebenaran sumber pesan.

Elemen Kriptografi

Beberapa Elemen-elemen Kryptografi :

1. *Plaintext* dan *Ciphertext.*
   *Plaintex*t atau teks asli yang dapat dibaca, merupakan media input untuk algoritma enkripsi, *cipherteks* adalah output dari algoritma enkripsi, merupakan pesan teks yang disandikan kedalam bentuk lain sehingga tidak bisa dipahami artinya oleh orang lain.
2. Pengirim dan Penerima
   Pengirim pesan adalah objek yang mengirim pesan kepada penerima pesan (objek lain). Penerima pesan adalah objek yang menerima pesan. objek bisa berupa orang, mesin (komputer), dan sebagainya.
3. Enkripsi dan dekripsi
   Enkripsi merupakan metode penyamaran atau pengacakan teks asli (*plainteks*) menjadi teks acak (*cipherteks*). Sedangkan metode mengembalikan *ciphertext* menjadi *plaintext* merupakan hasil pengolahan dekripsi.
4. *Cipher*
   Kriptografi sering disebut *cipher* yaitu aturan dengan Konsep matematis yang mendasarinya dan merupakan dua buah elemen himpunan *plainteks* dan *cipherteks*. Enkripsi dan dekripsi adalah suatu fungsi matematis yang menjabarkan kedua elemen himpunan tersebut.

5. Penyadap

   Penyadap adalah orang yang memposisikan dirinya (berprofesi) melakukan menangkap dan pembacaan data yang ditransmisikan lewat jaringan lokal atau internet dengan tujuan memperoleh informasi sebanyak mungkin dengan tujuan tertentu.

8.2.2 Steganografi

Kata *steganografi* berasal dari kata bangsa Yunani *steganos*, yang artinya "tidak dapat tampak", dan *graphein*, "menulis", artinya tulisan yang tidak bisa di tembus/tampak (Janner Simarmata, Sriadhi, 2019)

Keamanan data atau informasi merupakan kebutuhan yang paling penting bagi setiap orang, apalagi data atau informasi tersebut terkait dengan privasi seseorang atau perusahaan . dengan perkembangan teknologi yang begitu pesat dan mudah digunakan mengakibatkan pencurian informasi semakin gencar, Maraknya penyalahgunaan teknologi menyebabkan informasi wajib diproteksi dari penyadapan orang yang tidak bertanggung jawab. Suatu cara yang dapat digunakan dalam penyalahgunaan teknologi dan pencurian data tersebut adalah dengan melakukan metode enkripsi informasi-informasi yang dianggap sangat penting.

Steganografi merupakan ilmu atau seni menyembunyikan teks dengan cara *hiding message* pada objek lain dengan teknik tertentu sehingga teks yang disembunyikan menyatu dengan objek lainnya (media teks, gambar, video, dan suara) dengan tidak merusak data itu sendiri dan tidak menimbulkan kecurigaan orang lain yang tidak berhak, sehingga tidak seorangpun yang mengetahui dan mendeteksi keberadaan bahwa pesan itu mengandung sebuah rahasia selain pembawa dan penerima pesan tersebut.

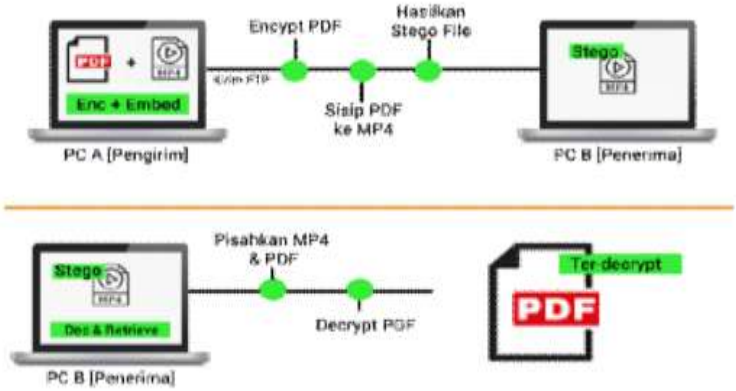
Cara Kerja Steganografi

Ada dua unsur menyisipkan data yang ingin disembunyikan. Pertama ialah media penampung yang akan disisipi teks atau informasi yang tidak mencurigakan untuk disisipkan informasi rahasia berupa: gambar, suara, video dan lainnya Unsur kedua adalah pesan atau informasi yang akan disisipkan yaitu sarana penampung citra yang disebut *cover-object* dan gambar yang telah disisipi pesan disebut *stego-object*.

Dua proses dalam steganografi yaitu proses penyematan (*embedding),* proses penambahan objek ke objek lain untuk menyembunyikan pesan kedalam *cover-object* dan *decoding,* proses penerimaan kode-kode untuk mengartikan pesan terenkripsi, ekstraksi pesan dari *stego-object*. Kedua proses ini membutuhkan kunci rahasia (*stego-key)* sehingga orang yang mempunyai otoritas saja yang berhak melakukan penyisipan dan ekstraksi pesan.

Pada Gambar 13.7, pengujian dilakukan menggunakan dua set perangkat komputer, dimana komputer pengirim bertugas sebagai client (komputer-A) dan komputer Penerima bertugas sebagai server (komputer-B). Komputer penerima akan mencari sebuah file pdf untuk di sisipkan ke file video MP4 dan mencantumkan kunci rahasia dan mensetting IP address, port, nama pemakai sistem beserta password pada komputer penerima (komputer-B). Selanjutnya file pdf tersebut di enkripsi menggunakan algoritma kriptografi untuk disisipkan pada file video MP4 dengan teknik steganografi EoF. Pada komputer penerima(komputer-B) dan komputer pengirim (komputer-A) menggunakan kunci rahasia yang serupa dengan yang digunakan untuk melakukan enkripsi.

Selanjutnya file video MP4 tersebut akan diolah dengan steganografi EoF untuk memisahkan file video MP4 dan file pdf, proses dekripsi menggunakan kunci rahasia yang sama (Laliha,, 2019).



Gambar 8.7. Proses steganografi citra digital
(Sumber : http://ojs.uho.ac.id/index.php/semantik/article)

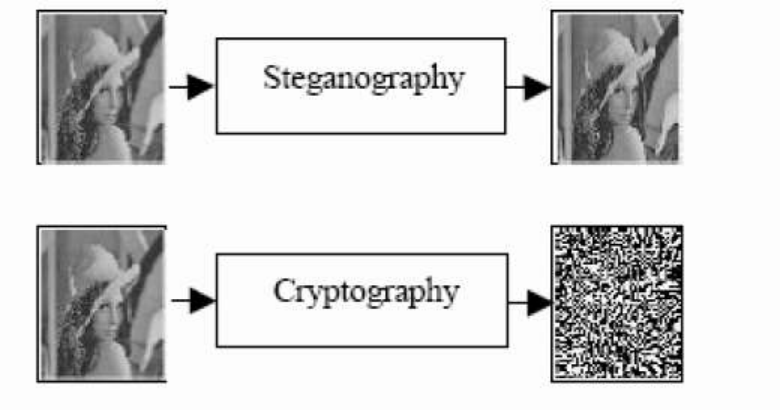
Tujuan utama dari steganografi adalah merahasiakan keberadaan pesan atau informasi penting dalam media lain berupa media teks, gambar, video, dan suara . Kebanyakan pesan yang disisipkan ke media lain membuat perubahan yang sangat halus sehingga isinya tidak akan menarik minat dari pihak lain (penyerang), contohnya sebuah gambar atau video yang terlihat tidak berbahaya ternyata menyimpan sebuah pesan atau informasi yang sangat penting.

Bentuk Format Steganografi

Beberapa format steganografi yang sering :

1. Format text file, html, pdf, dll.
   Metode penyamaran pesan dalam karakter teks merupakan metode klasik dan sudah jarang pakai sebab file teks memiliki jumlah redundansi data yang terbatas, dalam teknik steganografi ini bekerja dengan cara menyisipkan pesan teks rahasia di setiap huruf ke-n dari setiap kalimat dalam pesan teks yang digunakan sebagai objek penampung.

2. Format gambar: bitmap (bmp), gif, pcx, jpeg, dll.
   Penggunaan media gambar pada teknik steganografi sangat diminati dan paling populer pada zaman sekarang ini, sebab format gambar/citra mempunyai redundansi yang cukup besar dan sudah umum dan paling sering dipertukarkan di dunia maya.
3. Format suara: wav, voc, mp3, mp4, dll.
   Penggunaan file audio dalam menyembunyikan informasi sangat potensial, hampir sama dengan teknik yang digunakan dalam penyembunyian pesan pada media gambar. Steganografi ini kurang populer dan tidak praktis, karena harus menggunakan memori komputer yang cukup besar.
4. Protocol
   Protocol steganografi merupakan teknik menyisipkan pesan atau informasi lewat transmisi menggunakan protokol kontrol jaringan. Perbedaan mendasar antara steganografi dengan kriptografi adalah Pada steganografi pesan atau informasi yang disisipkan tidak menimbulkan kecurigaan serta tidak menarik minat, sedangkan pada kriptografi pesan atau informasi yang disisipkan melalui proses pengacakan tidak bisa dipecahkan dan dibaca, tetap akan menimbulkan kecurigaan. Kedua metode steganografi dan kriptografi sering dipakai bersamaan dengan tujuan menjamin pesan atau informasi yang dirahasiakan.



Gambar 8.8. Perbedaan Kriptografi dan Steganografi
(Sumber : https://www.kangruli.net.eu.org)

Pada teknik kriptografi hasil ekstraksi antara media yang sudah disisipkan pesan dengan media sebelum disisipkan pesan rahasia terlihat sangat berbeda dan mencurigakan pihak lain. walaupun pihak lain tidak memahami maksud dan tujuan dari pesan tersebut.

Pada teknik steganografi, media yang sudah disisipkan pesan rahasia akan tampak sama dengan media sebelum disisipkan pesan rahasia, pesan rahasia yang disisipkan tersembunyi dalam *cover text* sehingga orang lain tidak mengetahui bahwa dibalik *cover text* tersembunyi sebuah pesan rahasia didalamnya.

Metode Steganografi

Ada empat jenis metode Steganografi, yaitu:

1. *Least Significant Bit Insertion* (LSB)
   Least Significant Bit (LSB) memakai cara memasukkan bit rendah atau bit yang paling kanan pada pixel gambar, Metode ini umum digunakan untuk menyisipkan informasi dalam media

citra karena tidak terlalu rumit dan kompleks pesan yang disembunyikan terjamin keamanannya (Munir, Rinaldi, 2006).

2. *Algorithms and Transformation*
   Algoritma compression merupakan fungsi matematika yang bekerja dengan cara menyamarkan data dalam algoritma steganografi. Fungsi matematika tersebut adalah *Discrete Cosine Transformation* (DCT) dan *Wavelet Transformation* (WT) dengan cara mentransformasikan data dari satu bidang ke bidang yang lain.
3. *Redundant Pattern Encoding*
   Redundant Pattern Encoding adalah algoritma penyisipan pesan menggunakan media gambar sebagai wadahnya dari pesan yang akan disisipkan. Keamanan dari metode ini rentan diretas oleh orang lain, akibat dari perubahan ukuran media yang digunakan, sehingga data yang akan diamankan dapat diketahui dan diambil dengan mudah oleh orang lain.
4. *Spread Spectrum method*
   Spread Spectrum steganografi terpencar-pencar berupa pesan yang terenkripsi melalui media image, Pada algoritma ini membaca pesan terenkripsi, penerima membutuhkan algoritma tertentu yaitu *crypto-key* dan *stego-key*. Keamanan dari metode ini rentan diretas dan di hancurkan oleh orang lain.

DAFTAR PUSTAKA

Ariyus, D. 2008. *Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi, I.* Yogyakarta: Yogyakarta: C.V Andi Offset (Penerbit Andi), 2008.

Ayun Qolbu, N.M. *et al.* (no date) *APLIKASI KEAMANAN EMAIL MENGGUNAKAN ALGORITMA AES (ADVANCED ENCRYPTION STANDARD) BERBASIS ANDROID*.

Janner Simarmata, Sriadhi, R.R. 2019. *KRIPTOGRAFI Teknik Keamanan Data dan Informasi*. Edited by 2019. Yogyakarta: C.V Andi Offset (Penerbit Andi).

Karima, A. and Diyatan, M.N. 2016. 'Algoritma Kriptografi Gost Dengan Implementasi MD5 Untuk Meningkatkan Nilai Avalanche Effect', *Jurnal Techno.COM*, 15(4), pp. 292–302.

Laliha, M., Sutardi and Ransi, N. 2019. 'Aplikasi Pengamanan File Bertipe *.PDF Pada VIDEO *.MP4 Menggunakan Kriptografi Vernam Cipher dan Steganografi End of File', 5(1), pp. 1–5. Available at: http://ojs.uho.ac.id/index.php/semantik.

Munir, Rinaldi, 2006. 2006. 'Pendahuluan', pp. 1–18. Available at: https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2017-2018/Fungsi-Hash-(2018).pdf.

Putra, A.E. 2009. 'Fungsi Hash pada Kriptografi', *Jurnal Informatika Institut Teknologi Bandung*, 1(1), pp. 1–6.

Rifki Sadikin. 2012. *Kriptografi Untuk Keamanan Jaringan:Implementasi*. Yogyakarta: C.V Andi Offset (Penerbit Andi), 2012.

BAB 9
TREND SECURITY

Oleh Nur Ilman

9.1 Pendahuluan

Kejahatan teknologi intenet berkembang dari model tradisional seperti pemerasan dan pencurian data dengan mode otomatis para Penjahat cyber dapat melakukan automatisasi serangan mereka,serangan mereka tidak lagi terbatas pada Bank atau perusahaan besar akan tetapi mengarah pada jutaan pengguna online (Philip O'Kane;Sakir Sezer & Domhnall Carlin, 2018).Pertumbuhan Serangan sistem Komputer sangat cepat ibarat mahluk hidup dan sering berubah sehingga pekerjaan tim keamanan akan tidak pernah selesai, serangan kepada beberapa Puluh juta Pemilik IP Publik sangat beresiko dengan bisnis pengguna**.**Dengan bermunculnya teknologi baru akan muncul juga metode serangan yang baru,dengan semakin banyaknya pengguna digital akan semakin banyak pula serangan kepada sistem komputer dan semakin bervariasi,pelaku ancaman terus memperluas dan mengembangkan metode serangan mereka dengan menggunakan Teknik yang baru dan mengeksploitasi celah-celah yang rentan diserang (lee, 2023),Sistem cangih pada kendaran yang dikemas dalam perangkat lunak otomatis akan menghasilkan konektivitas antara pengemudi dalam memudahkan untuk menyalakan mesin mengunci pintu yang sebahagian besar menggunakan Bluetooth dan WiFi dalam berkomunikasi,virus dan malware cendeung menyerang pada perangkat seluler serta pada browser internet (Duggal, 2023),serangan dengan ransomware akan semakin meningkat secara pesat serangan ransomware juga tlah menyerng sistem cloud target paling besar adalah server email

berbasis cloud metode yang popular untuk serngan ini adalah piggybacking singkronisasi file (Anupama A & Amrita Saravanam, 2023)

9.2 Perangkat-perangkat yang Trend diserang di masa akan datang

9.2.1 Perangkat Otomotif

Mobil modern terhubung ke internet melalui Bluetooth dan Wi-Fi . Kendaraan ini yang dilengkapi dengan perangkat lunak otomatis yang menyediakan konektivitas lancar bagi pengemudi di berbagai bidang seperti cruise control, pengaturan waktu mesin, penguncian pintu, kantung udara, dan sistem bantuan pengemudi canggih, membuat mereka rentan terhadap kelemahan keamanan dan risiko peretasan (Narang, 2023),serangan terhadap kendaran sangat berpengaruh pada keselamatan penumpang kendaraan itu, tren industr kendaraan itu mengarah pada aoutomatisasi berkendara setiap kendaraan akan terpasang alat komunikasi, sensor, aktuator dan unit control.kebutuhan akan keamanan system pada kendaraan sangat penting dikarenakan semakin banyak permukaan serangan untuk diseramg oleh penjahat cyber, jalu serangan diambil dari permukaan serangan melalui titik masuk ke sistem melalui jaringan internal hingga ke komponen target.komponen komponen target itu antara lain lampu indicator , Penutup Jendela, Deteksi pencitraan cahaya dan Kamera hingga manipulasi pengenalan rambu lalu lintas (Florian Sommer; Jürgen Dürrwang;& Reiner Kriesten, 2019).

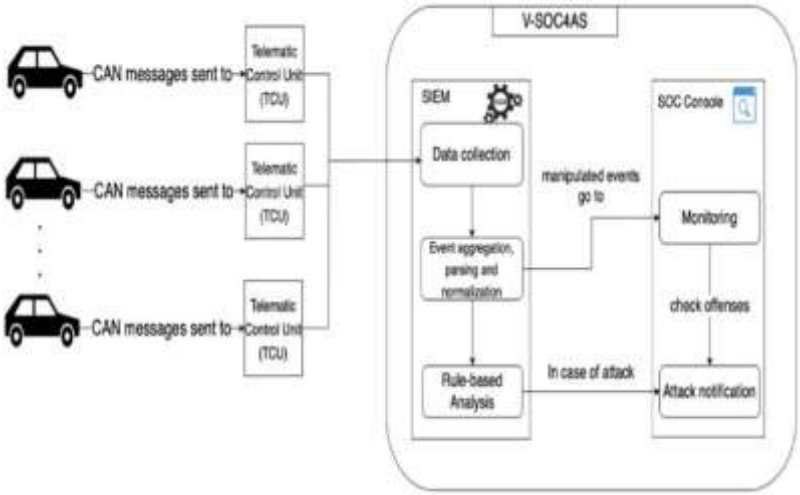
Aplikasi perangkat lunak memainkan peran penting dalam inovasi kendaraan, yang bertujuan untuk meningkatkan keselamatan, efisiensi, dan kenyamanan, serta menciptakan area baru sistem transportasi cerdas kooperatif dan kendaraan otonom. Untuk mengakomodasi aplikasi modern, kendaraan menjadi semakin terkomputerisasi dan terhubung. Terlepas dari manfaat penerapan aplikasi ini bagi sektor otomotif dan konsumen, aplikasi

otomotif bersama dengan inovasi teknologi yang memungkinkan membuka tantangan besar terhadap keamanan dan privasi. Aplikasi otomotif yang ada mencakup tiga kategori utama: sistem kontrol yang mengelola fungsi fisik kendaraan termasuk fungsi mesin, sasis, bodi, dan keselamatan pasif; sistem telematika yang menyediakan informasi dan mendukung hiburan serta transaksi keuangan; dan sistem bantuan pengemudi lanjutan yang kompleks (ADAS) yang bertujuan mengubah kendaraan menjadi sistem cerdas, meningkatkan keselamatan, dan meningkatkan pengalaman berkendara (Sommer, F, Dürrwang, J, & Kriesten, R . Hartog, J den, & Zannone, N , 2018)

Peralatan ECU (*Electronic Computer Unit*) adalah peralan yang terpasang secara fisik pada setiap kendaraan dimana sangat dominan untuk melakukan berbagai aktifitas pada kndaraan seperti aktifitas untuk mengetahui kondisi mesin , kondisi Air Conditioner dan perangkat ini terhubung secara daring melalui jaringan Bluetooth maupn wifi control otomatis pada ECU ini memungkikan para penjahat cyber dapat melakukan segala aktifitas kejahatan pada sistem otomotif. Ratusan dari ECU ini berkomunikasi menggunakan berbagai macam protocol komunikasi harus melalui serangkaian rancangan yang sangat baik agar terhidari dari berbagai macam serangan baik serangan local maupn serangan jarak jauh, beberapa protocol- protocol tersebut seperti *Control Area Network* (CAN), *Local Interkoneksi Network* (LIN) dam FlexRay serta Ethernet otonom.

Protokol CAN memiliki keunggulan dibandingkan yang lain berkaitan dengan Efisiensi biaya dan flexibilitas, protokol ini bersifat plug and play karena ECU-ECU tersebut dapat dihubungkan dengan mudah ke jaringan kendaraan tanpa perlu melakukan modifiksi jaringan pada kendaraan tersebut namun titik lemah pada protokol CAN yang popular diterapkan pada kendaraan adalah rentan teradap serangan karena protocol CAN tidak menerapkan Teknik ekripsi apapun sehingga sering

mendapat serangan oleh penjahat cyber apalagi serangan dengan Teknik sniffing paling sering dilakukan. Untuk mengatasi masalah tersebut penerapan peningkatan keamanan pada kendaran di terapkan dengan *vehicle-security operation center for improving automotive security* (V-SOCAAS), (Barletta, V.S.; Caivano, D.; &M D Viccentile, 20023)



Gambar 9.1. Arsitektur V-SOCAAS
(Sumber : www.mdpi.com/1999-4893/16/2/112)

Security Information System Even Managenement (SIEM) berguna untuk memantau dan mendeteksi serangan penjahat dalam komunikasi intra kendaraan dan antar kendaraan pesan tersebut dikirim melalui ECU – ECU kendaraan, kemudian mengumpulkan dan menganalisis data berbagai jenis kendaraan termasuk upaya-upaya login yang gagal dan penolakan berkali-kali oleh firewall.jika serangan terdeteksi dan telah diidentifikasi oleh SIEM maka dapat diketahui apakah serangan itu adalah betul-betul terjadi atau hanya bersifat palsu saja, komunikasi antara kendaraan dengan SIEM, Ketika ECU menghasilkan frame CAN, ECU

mengirimkan frame CAN ke *Telematic Control Unit* (TCU). TCU mengubah pesan menjadi format JSON dan mengirimkannya ke SIEM. Saat SIEM menerima kejadian ini, SIEM mengumpulkan dan menampilkannya di konsol SOC. Secara bersamaan, SIEM, dengan mekanisme berbasis aturan, memeriksa apakah peristiwa ini dapat dianggap sebagai serangan atau tidak. yang dianggap sebagai serangan akan ditampilkan di konsol SOC.Keuntungan dari penerapan V-SOCAAS adalah mengeahui kendaraan mana yang diserang dan perangkat ECU mana yang rentan untuk diserang sehingga dapat memperbaiki celah-celah yang mudah diserang dan memperbaharui ECU trsebut dengan model yang sama dan membantu mencegah serangan yang sama pada kendaraan ang lain selain itu Aristektur V-SOCAAS melalui konsol SOC untuk IP setip kendaraan menghasilkan respon yang tepat sehingga bukan hanya untuk mengidentifikasi dan mendeteksi serangan juga dapat menganalisis keseluruhan kendaran bukan dengan satu protocol yaitu CAN tetapi dapat digunakan untuk protocol yang lain. (Barletta, V.S.; Caivano, D.; &M D Viccentile, 20023)

Perangkat Cloud

Komputasi awan menyediakan layanan sesuai permintaan melalui Internet dengan bantuan sejumlah besar penyimpanan virtual. Fitur utama komputasi awan adalah pengguna tidak perlu menyiapkan infrastruktur komputasi yang mahal dan biaya layanannya lebih murah. Dalam beberapa tahun terakhir, komputasi awan terintegrasi dengan industri dan banyak bidang lainnya semakin banyak pengguna individu dan organisasi mentransfer data mereka ke Server Cloud bukan lagi di computer local, penyedia layanan web banyak menggunakan internet dan layanan web sehingga akan menimbulkan persoalan keamanan, Cloud menggunakan lingkungan virtual ,mesin virtual tersebut memiliki kerentanan keamanan yang hadi pada Aplication Program Interface (API) browser dan saluran jaringan sumber

daya cloud dibagikan dengan banyak pengguna (Multi User) sehingga menjadi penghalang dalam membangun arsitektur keamanan, dan menyebabkan pengguna cloud kehilangan kendali atas data dimana konsumen cloud tidak mengetahui kebijakan keamanan, kerentanan an informasi malware, penyerang dapat mencapai serangan pada tingkat fisik sehingga dapat membaca data yang tersimpan pada cloud (Singh, A, & Chatterjee, K , 2017)

Terdapat 4 model layanan berbeda terhadap sistem cloud:

1. *Software as a Services* (SaaS)
   Dimana layanan awan ini perangkat lunak beradapada tingkat penyedia, pengguna dapat mengakses perangkat lunak menggunakan browser web atau API tanpa perlu merasa khawatir dalam perawatan dan peningkatan perangkat lunak contoh yang paling popuer adalah office 365 dan salesforce
2. *Platform as a Service* (PaaS)
   Dimana layanan awan ini konsumen mengembangkan aplikasinya sendiri beserta datanya sehingga lebih cepat dalam hal pengembangan, pengujian dan penyebaran aplikasi,aplikasi yang dibuat oleh konsumen diperuntukkan bagi pengguna akhir.
3. *Infrastruktur as a Service* (IaaS)
   Layanan ini menyediakan Sistem Operasi besera aplikasinya, konsumen membayar sesuai dengan konsumsinya, kebtuhan infrastruktur berdasarkan kebutuhan pemrosesan dan penyimpanan, konsumen memiliki kendali ats
4. *Anything as a Service* (XaaS)
   Layanan ini menawarkan berbagai layanan mulai dari layanan pribadi hingga sumber daya yang besar melalui internet.

Saat ini layanan cloud juga melayani pada layanan Kesehatan dengan berbagai keunggulan yaitu

1. Peningkatan layanan kepada pasien dengan interaksi yang berkelanjutan data pasien tersedi kapan saja dan dimana saja untuk dianalisis oleh dokter serta untuk kepentingan perawatan yang berbeda.
2. Penghematan biaya tanpa perlu membeli peralatan perangkat keras dan perangkat lunak seta biaya pemeliharaan.
3. Tidak perlu menyimpan server pada local server sehingga dapat menghemat energi tanpa ada lagi ruang yang membutuhkan pendingin yang mahal.
4. Mengatasi kelangkaan sumber daya dokter khususnya pada daerah terpencil dapat menggunakan telemedicine
5. Ketersediaan data yang dapat digunakan oleh Dokter, perawat, Klinik,Rumah Sakit hingga perusahaan Asuransi.

Kelemahan Layanan Cloud

1. Sangat membutuhan jaringan internet jika jaringan mengalami kendala sperti putus,tidak aktif atau lambat akan sangat berpengaruh pada pengguna akhir
2. Keamana dan Privasi rentan mengalami serangan hingga dilakukan pencurian data atau kehilangan data
3. Memerlukan paying hukum dan kerangka kerja etis

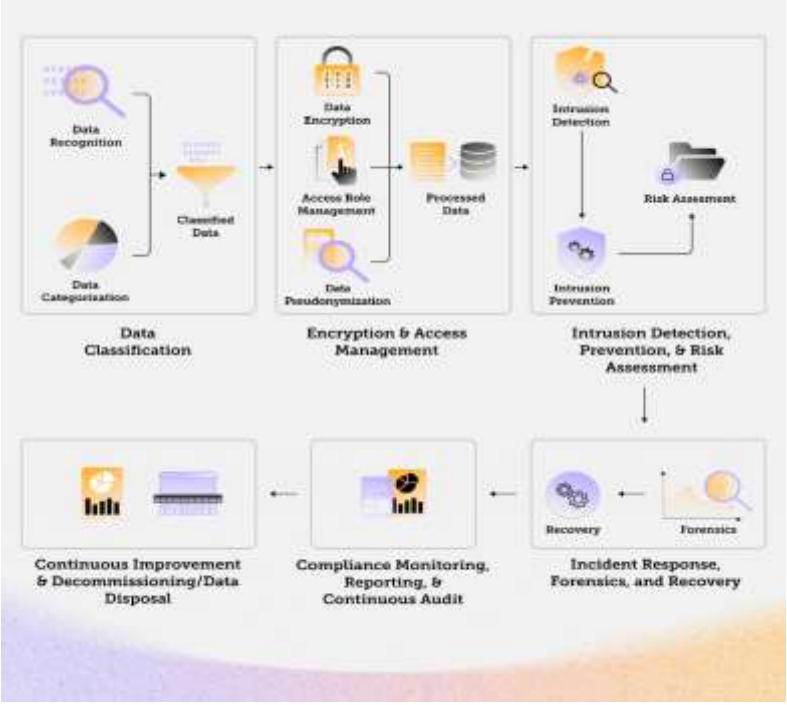
Keamanan Data Cloud

Cloud Data Security adalah bagian dari model perlindungan data tradisional, pengaman data cloud bergantung pada proses dinamis dan memitigasi perkembangan ancaman, tidak hanya melindungi data akan tetapi kepatuhan akan standar peraturan yang menerapkan panduan ketat bagaimana data tersebut harus disimpan, diproses dan ditransfer. Berbeda dengan model komputaasi tradisional lingkungan cloud menghadirkan berbagai

tantangan unik seperti type data yang beragam model tanggung jawab Bersama aristektur multi-tenant data yang tersebar dari berbagai server.

Ada beberapa asumsi yang kurang tepat berkaitan dengan layanan keamana di Cloud bahwa masalah keamanan adalah tanggung jawab penyedia layanan cloud, disini harus ada pembagian tanggung jawab , dibagian mana menjadi tanggung jawab penyedia cloud (CSP) dan dibagian mana menjadi tanggung jawab Penyewa Cloud. Mereka harus bekerja sama utuk melindungi Proses Data dan juga bisnis pelanggan.

Gambar dibawah ini adalah siklus hidup keamanan Data Cloud (Sentra.io, 2023)



Gambar 9.2. Siklus Hidup Cloud Data Security
(Sumber : https://www.sentra.io/cloud-data-security)

1. Klasifikasi & Penemuan Data: Kenali dan kategorikan data Anda sesuai dengan sensitivitasnya. Mengetahui sifat data merupakan bagian integral untuk mengelola kontrol keamanan yang tepat.
2. Manajemen Enkripsi & Akses: Menerapkan tindakan perlindungan seperti enkripsi dan nama samaran. Pasangkan ini dengan manajemen akses untuk memastikan hanya personel yang berwenang yang dapat mengakses data sensitif.
3. Deteksi Intrusi, Pencegahan, dan Penilaian Risiko: Memanfaatkan intelijen ancaman canggih dan alat keamanan untuk deteksi ancaman yang cepat dan pencegahan proaktif. Selain itu, lakukan penilaian risiko secara rutin untuk memperkirakan dan mencegah potensi ancaman secara efektif.
4. Tanggapan Insiden, Forensik, dan Pemulihan: Persiapkan skenario pelanggaran, tidak hanya secara teoritis, tetapi secara praktis. Menerapkan rencana tanggap cepat, melakukan analisis forensik pasca-insiden, dan memastikan layanan cepat dan pemulihan data untuk menjaga kelangsungan bisnis.
5. Pemantauan Kepatuhan, Pelaporan, dan Audit Berkelanjutan: Tinjauan dan audit rutin memastikan kepatuhan terhadap peraturan dan mengidentifikasi area potensial untuk peningkatan. Pantau kepatuhan secara teratur dan laporkan temuan untuk menjaga transparansi.
6. Berkesinambungan dan Penonaktifan/Pembuangan Data: Langkah iteratif untuk terus meningkatkan postur keamanan Anda. Ini juga memastikan praktik penonaktifan dan pembuangan data yang aman saat data atau sistem tidak lagi diperlukan

Adapun persyaratan keamanan terhadap layanan cloud adalah

1. Rahasia

   Kerahasiaan data adalah properti yang konten data tidak tersedia atau diungkapkan kepada pengguna ilegal. Data yang dialihdayakan disimpan di awan dan di luar kendali langsung pemilik. Hanya pengguna yang berwenang yang dapat mengakses data sensitif sementara yang lain, termasuk CSP, tidak boleh mendapatkan informasi apa pun dari data tersebut. Sementara itu, pemilik data berharap untuk sepenuhnya menggunakan layanan data cloud, misalnya, penelusuran data, penghitungan data, dan pembagian data, tanpa kebocoran konten data ke CSP atau lawan lainnya.

2. Integritas

   Integritas data menuntut pemeliharaan dan menjamin keakuratan dan kelengkapan data. Seorang pemilik data selalu mengharapkan bahwa datanya di cloud dapat disimpan dengan benar dan dapat dipercaya. Ini berarti bahwa data tidak boleh dirusak secara ilegal, dimodifikasi secara tidak tepat, sengaja dihapus, atau dibuat secara jahat. Jika ada operasi yang tidak diinginkan merusak atau menghapus data, pemilik harus dapat mendeteksi korupsi atau kehilangan. Lebih lanjut, ketika sebagian dari data yang di-outsource rusak atau hilang, itu masih dapat diambil oleh pengguna data.

3. Pengendalian Access

   Access controllability berarti bahwa pemilik data dapat melakukan pembatasan selektif akses ke dirinya atau datanya dialihdayakan ke cloud. Pengguna legal dapat diotorisasi oleh pemiliknya untuk mengakses data, sementara yang lain tidak dapat mengaksesnya tanpa izin. Lebih lanjut, diinginkan untuk memberlakukan kontrol akses halus ke data yang dialihdayakan, yaitu, pengguna

yang berbeda harus diberikan hak akses yang berbeda terkait dengan potongan data yang berbeda. Otorisasi akses harus dikontrol hanya oleh pemilik dalam lingkungan cloud yang tidak dipercaya.

Dalam upaya memitigasi resiko layanan keamanan cloud beberapa praktik yang dapat dikerjakan (Kumaraswamy, 2011)

1. *Architect for security-as-a-service*

   Penerapan pengurangan ancaman akibat kesalahan manusia dapat dilakukan dengan menerapkan Aoutomatisasi keamanan termasuk pula automatisasi kebijakan keamanan laynan untuk automatisasi DNS, QoS jaringan termasuk pula kebijakan firewall, konfigurasi sistem mesin virtual Penyediaan Sertificate Secure Layer (SSL), konfigurasi Log dan Penyediaan Akun Istimewa

2. *Access Management Identify*

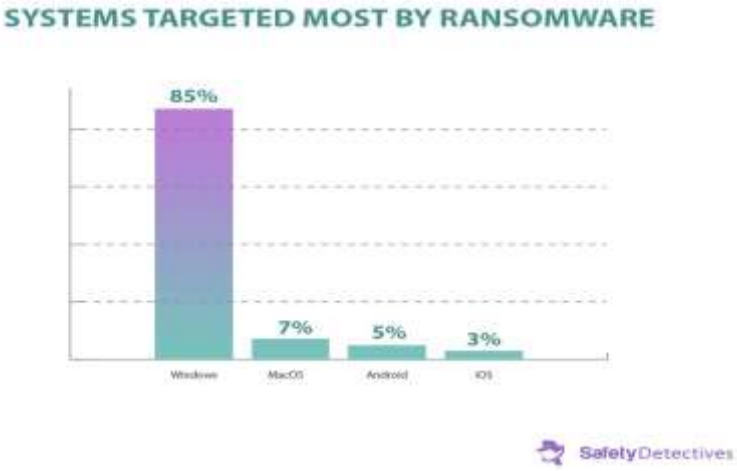
   Arsitektur kontrol akses cloud harus menangani semua aspek pengguna dan siklus hidup manajemen akses untuk pengguna akhir dan pengguna istimewa – penyediaan & deprovisi pengguna, autentikasi, federasi, otorisasi, dan audit. Arsitektur yang baik akan memungkinkan penggunaan kembali layanan identitas dan akses untuk semua kasus penggunaan dalam model cloud publik, privat, dan hybrid. Ini adalah praktik yang baik untuk menggunakan layanan, Pemanfaatan API untuk mengaoutomatisasi perlindungan termasuk aoutomatisasi Firewall, dan control akses selain itu pencatatan alamat IP pengunjung sebagai bagian dari integrasi tambahan dalam identifikasi pengunjung.

9.2.2 Trend Teknik Penyerangan Ransomware

Merupakan perangkat perusak yang dirancang untuk melakukan pemerasan, serangan ransomware telah meningkat dalam beberapa tahun terakhir dan pada tahun akan datang serangan *ransomware as a service* (RaaS) akan lebih dikenal. Penggunaan trojan dalam Serangan Ransomware biasanya dilakukan dengan menipu pengguna untuk mengunduh atau membukanya ketika tiba sebagai lampiran email, menurut hasil perhitungan statistic sekitar 623 juta serangan ransomware pada tahun 2021 dan 493 juta serangan pada tahun 2022 dan juga pada tahun 2022 sekitar 70% serangan ransomware menelan korban untuk perusahaan-perusahaan (Petrosyan, 2022).

Serangan ransomware juga telah merambah pada sistem operasi mobile yang sebahagian besar target mereka adalah platform android, sitem distribusi menggunakan file apk melalui pengguna yang polos tidak menaruh curiga dan juga serangan melalui ransomware pada kamera digital dengan sistem DSLR dimana cara menginfeksi melalui *Picture Transer Protocol* (PTP).Banyak pengguna pribadi maupun perusahaan yang mengalami kerugian besar akibat serangan ransomware bukan hanya perusahaan kecil perusahaan-perusahaan besar juga mengalami kendala yang sama mendapatkan serangan ransomware. Dan bisa menghancurkan sebuah perusahaan, negara-negara yang lebih canggih dalam sistem keamanan ini serta kesadaran yang lebih tinggi terhadap ancaman dunia maya dalam hal ini mengalami hal yang sama perusahaan-perusahaan Amerika serikat banyak mendapatkan juga serangan, tahun 2021 tiga negara teratas yang mengalami serangan dari ransomware ini yaitu Arab Saudi, Turki dan China. Pembayaran tebusan dari serangan ransomware cenderung meningkat pertumbuhannya setiap tahun hingga mencapai puluhan milyar dollar Amerika setiap tahun. Sistem Operasi Windows paling besar mengalam

serangan dikarenakan sistem operasi ini sangat banyak penggunanya dan juga dari pengguna tersebut kurang melakukan pembaruan sistem operasi sehingga menjadi sasaran yang empuk untuk dilakukan serangan selain itu layanan cloud untuk Software as a Servisyang popuer juga menjadi sasaran yang paling banyak dilakukan penyerangan seperti Dropbox,Office365, dan Sales Force serta Box (Eric, 2023).

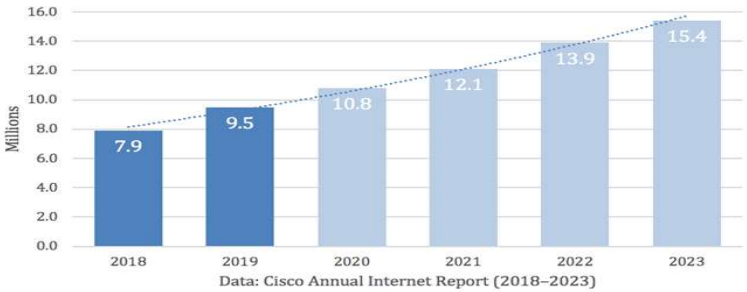


Gambar 9.3. Persentase Target Serangan Terhadap Sistem Operasi Oleh Ransomware
(Sumber : https://id.safetydetectives.com/blog/ransomware-statistics-id)

Ransomware masih menjadi ancaman yang serius dimasa akan datang efek ekonomi yang ditimbulkan masih sangat besar dalam pasar dan dapat menjadi sebuah epidemi dalam dunia komputasi

Distributed Denial Of Service (DDoS)

Salah satu tie serangan yang sangat banyak saat ini adalah dengan metode DDoS seiring dengn adanya perang fisik di Ukraina dan Rusia hamper semua layanan-layanan berbasis web baik itu Email, Web Hosting dan situs web sehingga dapat menganca inforastruktur jaringan,serangan DDoS dapat pula sebagai pengalihan serangan aktifitas krimilan cyber lainnya seperti Sniffing dan Penyebaran Ransomware.



Gambar 9.4. Analisa sejarah Dan Prediksi Serangan DDos Oleh Cisco. (Sumber: https://www.a10networks.com/blog/5-most-famous-ddos-attacks)

Ada beberapa serangan menggunakan DDoS yang paing popular saat ini:

1. Serangan Google, 2020

   Pada 16 Oktober 2020, Grup Analisis Ancaman (TAG) Google memposting pembaruan blog tentang bagaimana ancaman dan aktor ancaman mengubah taktik mereka karena pemilu AS 2020. Dipasang dari tiga ISP Cina, serangan terhadap ribuan alamat IP Google berlangsung selama enam bulan dan memuncak pada 2,5Tbps.Damian Menscher, Insinyur Keandalan Keamanan di Google, menuliskan bahwa Penyerang menggunakan beberapa jaringan untuk memalsukan 167 Mpps (jutaan paket per

detik) ke 180.000 server CLDAP, DNS, dan SMTP yang terbuka, yang kemudian akan mengirimkan respons besar kepada kami. Hal ini menunjukkan volume yang dapat dicapai oleh penyerang dengan sumber daya yang baik Ini empat kali lebih besar dari serangan pemecah rekor 623 Gbps dari botnet Mirai setahun sebelumnya.

2. Serangan DDoS AWS pada tahun 2020

   Amazon Web Services terkena serangan DDoS raksasa pada Februari 2020. Ini adalah serangan DDoS paling ekstrem yang pernah ada dan menargetkan pelanggan AWS yang tidak dikenal menggunakan Teknik refleksi yang disebut *Connectionless Lightweight Directory Access Protocol* (CLDAP). Teknik ini mengandalkan server CLDAP pihak ketiga yang rentan dan memperkuat jumlah data yang dikirim ke alamat IP korban sebanyak 56 hingga 70 kali lipat. Serangan itu berlangsung selama tiga hari dan mencapai puncaknya dengan kecepatan 2,3 terabyte per detik.Sehingga pelanggan hosting AWS banyak kehilangan pendapatannya

3. Serangan Mirai Krebs dan OVH DDoS di tahun 2016

   Pada tanggal 20 September 2016, blog pakar keamanan siber Brian Krebs diserang oleh serangan DDoS dengan kecepatan lebih dari 620 Gbps. Situs Krebs pernah diserang sebelumnya. Krebs telah mencatat 269 serangan DDoS sejak Juli 2012, tetapi serangan ini hampir tiga kali lebih besar dari apa pun yang pernah dilihat situs atau internetnya sebelumnya.Sumber serangan itu adalah botnet Mirai, yang pada puncaknya akhir tahun itu, terdiri dari lebih dari 600.000 perangkat IoT yang disusupi seperti kamera IP, router rumah, dan pemutar video. Botnet Mirai telah ditemukan pada bulan Agustus di tahun yang sama, tetapi serangan terhadap blog Krebs adalah serangan besar pertamanya.

Serangan botnet Mirai berikutnya pada 19 September menargetkan salah satu penyedia hosting terbesar di Eropa, OVH, yang menampung sekitar 18 juta aplikasi untuk lebih dari satu juta klien. Serangan ini terjadi pada satu pelanggan OVH yang dirahasiakan dan didorong oleh sekitar 145.000 bot, menghasilkan beban lalu lintas hingga 1,1 terabit per detik. Itu berlangsung sekitar tujuh hari. Namun OVH tidak menjadi korban botnet Mirai terakhir di tahun 2016. (Nicholson, 2022)

DAFTAR PUSTAKA

Anupama A & Amrita Saravanan. 2023, 2023 31. 7 cyber security trends to watch in 2023 Data Security. monthly, p. 4.

;Barletta, V.S.; Caivano, D.; &M D Viccentile. 2023.V-SOCAAS; A Vehicle-SOC for Improving Automotive Security. *Algorithms*, 1-19.

Duggal, N. 2023, August 1. top -cybersecurity-trends-article. *Top 20 Cyber Security Trends to Watch out for in 2023*, pp. 1-3.

Eric, C. 2023, August 17. *Fakta, Tren & Statistik Ransomware di Tahun 2023*. Retrieved from Safety Detectives: https://id.safetydetectives.com/blog/ransomware-statistics-id/

Florian Sommer; Jürgen Dürrwang;& Reiner Kriesten. 2019. Survey and Classification of Automotive Security Attacks. *EEM* 3.

Kumaraswamy, S. (2011, December 07). *www.infoq.com/articles/cloud-security-architecture-intro*. Retrieved from https://www.infoq.com: https://www.infoq.com/articles/cloud-security-architecture-intro/

lee, j. 2023, 2023. 4--key-security-trends-fr-2023. *month*, p. 1.

Narang, M. 2023, july 26. 10 Biggest Cybersecurity Trends in 2023. *Top 10 Cybersecurity Trends to Watch Out For in 2023*, p. 3.

Nicholson, P. 2022, January 21. *Five Most Famous DDoS Attacks and Then Some*. Retrieved from A10: Five Most Famous DDoS Attacks and Then Some

Petrosyan, A. 2022, 06 23. *The Annual number of ransomware attacks worldwide from 2017 to 2022*. Retrieved from Statista: https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/

Philip O'Kane;Sakir Sezer & Domhnall Carlin. 2018. Evolution Of Ransomware. *IET Network*, 8-14.

Sentra.io. 2023, August 14. *cloud-data-security*. Retrieved from www.Sentra.io: https://www.sentra.io/cloud-data-security

Singh, A, & Chatterjee, K . 2017. Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications, Elsevier*, 88-115.

Sommer, F, Dürrwang, J, & Kriesten, R . Hartog, J den, & Zannone, N. 2018. Security and privacy for innovative automotive applications: A survey. *Computer Communications, Elsevier*, 17-41.

BAB 10
SISTEM KEAMANAN CLOUD

Oleh Franky G. C. Manoppo

10.1 Pendahuluan

Cloud computing saat ini telah menjadi tren utama dalam dunia teknologi informasi. Banyak organisasi beralih dari *data center* tradisional ke cloud karena keuntungan skalabilitas, aksesibilitas, dan penghematan biaya yang ditawarkan. Diperkirakan lebih dari 90% beban kerja Perusahaan akan berjalan di cloud pada 2025. (Weins, 2020) .Namun di balik keuntungan tersebut, adopsi cloud juga membawa tantangan baru terkait dengan risiko keamanan data dan aplikasi.

Sistem keamanan cloud adalah sekumpulan kebijakan, teknologi, dan kontrol yang diterapkan untuk melindungi data, aplikasi, dan infrastruktur cloud dari ancaman keamanan siber.

Gambar 10.1. *Cloud Computing*
(Sumber : https://id.wikipedia.org)

Data dan aplikasi di cloud disimpan di *data center* milik penyedia layanan cloud, bukan di lokasi pengguna. Ini membuat rentan terhadap serangan siber, kebocoran data, dan penyalahgunaan akses.

Ancaman terhadap layanan cloud mencakup:

1. Serangan phishing untuk mencuri kredensial login.
2. Serangan brute force untuk menebak kata sandi.
3. Eksploitasi kerentanan sistem atau aplikasi.
4. Insider threats dari karyawan penyedia cloud.

Keamanan cloud sangat penting untuk melindungi data sensitif /bersifat rahasia dari perusahaan dan privasi pelanggan dari akses yang tidak sah. Insiden keamanan dapat mengakibatkan downtime, kehilangan data, dan rusaknya reputasi organisasi.

Membangun sistem keamanan cloud yang komprehensif adalah kunci untuk meminimalkan risiko dan memastikan kelangsungan sebuah bisnis.

Cloud computing telah menjadi trend utama dalam teknologi informasi dewasa ini. Sebagian besar organisasi telah mengadopsi cloud dalam skala tertentu. Penggunaan cloud yang pesat ini didorong oleh keuntungan signifikan yang ditawarkan cloud computing, seperti skalabilitas, aksesibilitas, colocation, dan model harga berbasis penggunaan (*pay as you use*). Namun, bersamaan dengan keuntungan tersebut, penggunaan cloud juga meningkatkan paparan organisasi terhadap ancaman keamanan siber. Oleh karena itu, sistem keamanan cloud menjadi sabgat penting untuk melindungi kerahasiaan, integritas, dan ketersediaan data serta aplikasi di lingkungan cloud.

Sistem keamanan cloud merujuk pada kebijakan, teknologi, dan kontrol yang diterapkan untuk melindungi data, aplikasi, dan infrastruktur cloud dari akses yang tidak sah serta serangan siber (Singh & Chatterjee, 2017). Teknologi seperti firewall, enkripsi, otentikasi multifaktor, sistem deteksi/pencegahan intrusi, dan

manajemen identitas digunakan untuk mencegah, mendeteksi, dan merespons ancaman terhadap aset digital di cloud. Selain teknologi, kebijakan seperti kontrol akses berbasis peran dan audit log juga penting untuk memastikan bahwa hanya pengguna yang berwenang saja yang dapat mengakses sumber daya cloud. Dengan menerapkan sistem keamanan cloud yang komprehensif, risiko keamanan dapat diminimalkan sehingga organisasi dapat memanfaatkan *cloud computing* dengan tenang.

Terdapat beberapa alasan mengapa sistem keamanan cloud sangat penting. Pertama, cloud menyimpan data dan aplikasi milik organisasi di lokasi yang tidak dikelola sendiri, yaitu infrastruktur milik penyedia layanan cloud. Ini membuat pengguna cloud kehilangan visibilitas dan kontrol penuh atas aset digital mereka(Singh & Chatterjee, 2017). Kedua, cloud bersifat accessible dari mana saja, sehingga memperluas area serangan yang harus diproteksi. Ketiga, sifat multi-tenant cloud memungkinkan beberapa data/aplikasi pengguna disimpan di sistem fisik yang sama, sehingga insiden keamanan di satu tempat dapat memengaruhi banyak pengguna cloud lainnya. Keempat, ancaman cloud terus berkembang seiring makin canggihnya teknik dari serangan siber.

Berdasarkan alasan di atas, sistem keamanan cloud harus dibangun dengan matang agar organisasi dapat memanfaatkan *cloud computing* dengan aman. Insiden keamanan cloud dapat berdampak signifikan pada reputasi, keuangan, bahkan kelangsungan bisnis organisasi. Oleh karena itu, keamanan cloud merupakan fondasi penting yang memungkinkan transformasi digital berbasis cloud dilakukan dengan risiko yang terkendali.

10.2 Jenis-Jenis Ancaman Cloud

Penggunaan *cloud computing* membawa risiko keamanan baru bagi organisasi. Data dan aplikasi yang berada di cloud berpotensi menghadapi beragam jenis serangan dan ancaman.

Adopsi *cloud computing* yang pesat dalam beberapa tahun terakhir telah mengubah cara organisasi mengelola infrastruktur dan aplikasi TI mereka. Diperkirakan lebih dari 90% organisasi telah menggunakan setidaknya satu layanan cloud pada tahun 2021 (Weins, 2020). Cloud computing memberikan keuntungan fleksibilitas, skalabilitas, dan penghematan biaya bagi organisasi. Namun di sisi lain, cloud juga memperkenalkan tantangan baru terkait risiko keamanan data dan aplikasi.

Menurut (ENISA, 2016), ancaman utama keamanan cloud mencakup:

10.2.1 Ancaman Eksternal

Ancaman eksternal berasal dari luar lingkungan cloud organisasi. Jenis ancaman eksternal utama antara lain:

1. Serangan peretasan (*hacking*) dan kelompok kriminal terus meningkatkan kecanggihan serangan mereka untuk memanfaatkan kerentanan sistem cloud.. Teknik serangan yang digunakan mencakup phishing, exploitasi kerentanan, brute force attack, dan lainnya.
2. Serangan DoS/DDoS dilakukan untuk membanjiri jaringan dan sistem cloud dengan trafik berlebihan sehingga mengganggu ketersediaan layanan. Serangan DDoS pada server cloud dapat menghambat layanan bisnis organisasi.
3. Malware seperti virus, worm, dan trojan horse yang menginfeksi sistem cloud. Malware dapat disebarkan melalui email, situs web berbahaya, atau aplikasi cloud yang terinfeksi.
4. Penyusupan jaringan (*network intrusion*) untuk mencuri data sensitif organisasi.
5. Akses ilegal ke interface manajemen cloud. Penyerang mencuri kredensial admin untuk memperoleh akses tingkat tinggi pada lingkungan cloud korban.

10.2.2 Ancaman Internal

Ancaman internal berasal dari dalam lingkungan cloud organisasi. Beberapa contohnya (Fernandes *et al.,* 2014):

1. Insider Threats. Karyawan jahat dengan akses sistem cloud dapat menyalahgunakan hak istimewa mereka untuk kepentingan pribadi, seperti mencuri data sensitif perusahaan.
2. Kesalahan Konfigurasi. Kesalahan human error dalam mengonfigurasi pengaturan keamanan cloud dapat menurunkan tingkat proteksi sistem cloud organisasi.
3. Bug & Kerentanan Perangkat Lunak. Exploitasi bug dan celah keamanan pada aplikasi atau platform cloud oleh penyerang dapat mengakibatkan pelanggaran data.

10.2.3 Pelanggaran Data

Pelanggaran data (data *breach*) terjadi ketika informasi sensitif organisasi diakses tanpa otorisasi/izin. Hal ini dapat terjadi karena serangan siber atau kesalahan manusia. Dampaknya meliputi kebocoran data pelanggan, rahasia dagang, dan lainnya.

10.2.4 Kehilangan Data

Kegagalan sistem, bencana alam, atau kesalahan manusia dapat menyebabkan kehilangannya data organisasi di cloud. Hal ini mengganggu ketersediaan layanan bisnis sebuah organisasi.

10.3 Langkah-Langkah Keamanan Dasar Cloud

10.3.1 Enkripsi Data

Enkripsi merupakan mekanisme penting untuk melindungi kerahasiaan data sensitif organisasi baik selama transit di jaringan cloud maupun selama penyimpanan (data at rest) di *cloud storage*. Enkripsi mencegah pihak yang tidak berwenang mengakses konten data jika berhasil mendapatkannya. Beberapa rekomendasi enkripsi data cloud:

1. Gunakan algoritma enkripsi kuat seperti AES-256 untuk enkripsi data cloud.
2. Kelola kunci enkripsi secara terpusat dan terintegrasi dengan manajemen identitas cloud.
3. Kewajiban enkripsi pada data sensitif seperti informasi keuangan, data pribadi, dsb.
4. Selalu gunakan enkripsi saat data cloud ditransmisikan melalui jaringan.
5. Lakukan enkripsi pada semua layer: IaaS, PaaS, SaaS, dan kontainer/serverless.

10.3.2 Otentikasi Multifaktor

Otentikasi multifaktor menambahkan lapisan keamanan ekstra dengan meminta lebih dari satu bukti identitas saat login ke sistem cloud. Hal ini mencegah penggunaan credential yang dicuri untuk akses cloud tanpa otorisasi. Beberapa opsi otentikasi multifaktor (Fernandes et al., 2014):

1. Password ditambah kode token dari aplikasi authenticator.
2. Password ditambah kode OTP (*one-time password*) dikirim via SMS.
3. Password ditambah autentikasi sidik jari atau facial recognition.
4. Smartcard ditambah PIN untuk akses on-premise ke cloud.

Semua administrator dan pengguna dengan akses sensitif harus diwajibkan menggunakan multifaktor authentication

10.3.3 Backup Dan Pemulihan Data

Backup dan replikasi data cloud secara reguler sangat penting untuk memastikan ketersediaan layanan bisnis saat terjadi insiden seperti bencana alam, kegagalan sistem, kesalahan manusia, maupun serangan siber. Backup yang disimpan secara offsite memungkinkan pemulihan cepat setelah bencana.

10.3.4 Manajemen Akses Berbasis Peran

Hak akses ke sumber daya cloud perlu diberikan berdasarkan peran dan fungsi pengguna dengan model least privilege. Hal ini mencegah penyalahgunaan akses cloud serta meminimalkan dampak dari ancaman dari orang dalam.

10.3.5 Pemantauan Aktivitas

Pemantaian rutin terhadap aktivitas pengguna dan sistem cloud diperlukan untuk perilaku tidak biasa yang dapat mengindikasikan aktivitas berbahaya atau ilegal. Log dari berbagai sumber seperti IaaS, SaaS, DNS, firewall, dan titik akhir harus dikumpulkan dan dianalisis untuk investigasi dan pembuktian aktivitas mencurigakan. Tools seperti SIEM dan user behavior analytics dapat membantu mengotomatisasi pemantauan cloud.

10.4 Arsitektur Keamanan Cloud

Migrasi ke cloud computing membawa banyak keuntungan sekaligus tantangan baru terkait risiko keamanan data dan aplikasi. Diperlukan arsitektur keamanan cloud yang matang agar organisasi dapat mengadopsi cloud dengan aman dan manajemen risiko yang memadai.

Berikut adalah beberapa komponen inti yang harus dipertimbangkan saat merancang arsitektur keamanan *cloud/cloud security architecture* (CSA). (Samani *et al*., 2015):

10.4.1 Keamanan Jaringan Cloud

Jaringan merupakan landasan konektivitas bagi seluruh layanan cloud. Oleh karena itu, keamanan jaringan cloud harus menjadi prioritas utama. Beberapa kontrol keamanan jaringan cloud yang direkomendasikan:

1. Firewall - Aturan firewall harus dikonfigurasi dengan tepat untuk memfilter lalu lintas jaringan agar hanya koneksi yang valid dan diotorisasi yang diizinkan. Firewall juga mencegah akses ilegal ke sumber daya cloud.

2. *Intrusion Prevention System* (IPS) - IPS memantau lalu lintas jaringan secara deep packet inspection untuk mendeteksi aktivitas mencurigakan dan exploitation attempt. IPS kemudian memblokir serangan secara real-time.
3. *Intrusion Detection System* (IDS) - IDS berfungsi mengidentifikasi dan melaporkan upaya serangan jaringan dan aktivitas anomali. Output dari IDS dianalisis lebih lanjut untuk investigasi dan perbaikan keamanan.
4. Enkripsi - Enkripsi menjaga kerahasiaan dan integritas data saat melewati jaringan cloud. Protokol enkripsi seperti SSL/TLS harus digunakan untuk semua sesi komunikasi cloud.
5. Microsegmentation - Membagi jaringan cloud ke dalam zona keamanan terisolasi berdasarkan fungsi dan sensitivitas datanya dapat memperlambat pergerakan penyerang di lingkungan cloud.

10.4.2 Keamanan Server Virtual dan Hypervisor

Lingkungan virtualisasi seperti mesin virtual (virtual machine) adalah komponen kunci dalam arsitektur cloud. Keamanan hypervisor dan server virtual sangat penting agar penyerang tidak dapat melakukan eksploitasi yang berdampak lintas mesin virtual. Beberapa rekomendasi untuk keamanan hypervisor dan virtualisasi server :

1. *Hardening hypervisor* - Menerapkan benchmark keamanan seperti CIS dan NIST pada hypervisor untuk meminimalkan kerentanan yang dapat dieksploitasi.
2. *Patching* dan upgrade rutin - Memastikan hypervisor selalu di-patch ke versi terbaru untuk menutup celah keamanan yang ditemukan.

3. Enkripsi - Mengamankan data VM yang di-rest pada storage dengan enkripsi agar tidak dapat diakses secara ilegal.
4. Isolated management network - Memisahkan jaringan manajemen hypervisor dari jaringan produksi untuk mencegah serangan.
5. *Access control* - Membatasi dan mengaudit akses privilege ke interface manajemen hypervisor.

10.4.3 Keamanan Kontainer

Virtualisasi berbasis kontainer (*container*) seperti Docker sangat populer digunakan untuk mengemas dan menjalankan aplikasi cloud karena portabilitas dan skalabilitasnya. Namun, lingkungan kontainer juga perlu dilindungi dari eksploitasi melalui langkah-langkah berikut :

1. *Resource isolation* antar kontainer - Memastikan tiap kontainer hanya memiliki akses terbatas ke resource seperti CPU, memori, dan storage.
2. Enkripsi - Mengamankan sensitive data dalam kontainer menggunakan enkripsi saat di-rest.
3. *Vulnerability scanning* - Melakukan vulnerability assessment pada image kontainer sebelum digunakan untuk mendeteksi konfigurasi dan kode berbahaya.
4. *Access control* - Memberikan akses yang minimal untuk setiap kontainer berdasarkan prinsip least privilege.
5. *Continuous monitoring* - Memantau dan mengaudit aktivitas serta log kontainer secara terus menerus.

10.4.4 Enkripsi Data

Enkripsi harus diterapkan untuk melindungi kerahasiaan data sensitif organisasi baik saat transit di jaringan cloud maupun saat penyimpanan (*at rest*) di *cloud storage*.

10.4.5 Identity and Access Management

Akses ke sumber daya dan layanan cloud harus dikontrol dan diaudit dengan ketat berdasarkan prinsip least privilege. Identity and access management (IAM) yang matang sangat diperlukan untuk menegakkan access control di lingkungan cloud. Beberapa komponen inti IAM :

1. Otentikasi multifaktor - Menambah lapis keamanan dengan meminta lebih dari satu bukti identitas pengguna cloud.
2. Single sign-on - Pengguna hanya perlu login sekali untuk mengakses seluruh aplikasi dan layanan cloud.
3. *Access policy* berbasis peran - Hak akses diberikan sesuai peran pengguna di organisasi.
4. Audit log - Mencatat dan memantau aktivitas pengguna cloud untuk deteksi penyalahgunaan.

10.4.6 Pemantauan dan Audit Keamanan

Aktivitas pada sistem cloud perlu dipantau secara intensif untuk mendeteksi serangan siber dan aktivitas berisiko. Beberapa kapabilitas pemantauan dan audit keamanan cloud :

1. SIEM - Mengumpulkan dan menganalisis log dari berbagai sumber untuk korelasi dan deteksi ancaman.
2. IDS/IPS - Memantau lalu lintas jaringan dan sistem untuk detection dan prevention serangan.
3. Scan kerentanan - Melakukan *vulnerability assessment* secara berkala pada sistem dan aplikasi cloud.
4. Uji penetrasi - Simulasi serangan siber untuk mengidentifikasi celah keamanan sebelum dieksploitasi.
5. User activity monitoring - Memantau perilaku pengguna cloud untuk deteksi aktivitas berisiko dan insider threat.

Dengan memantau infrastruktur dan aktivitas cloud secara intensif, insiden keamanan dapat direspons dengan cepat sebelum menyebabkan kerusakan signifikan.

10.5 Masa Depan Keamanan Cloud

Seiring adopsi cloud yang makin meluas, ancaman dan tantangan baru terus bermunculan dalam bidang keamanan cloud. Oleh karena itu, penting bagi organisasi untuk memahami bagaimana keamanan cloud dapat berevolusi di masa mendatang agar dapat menyiapkan strategi dan investasi yang tepat sasaran.

10.5.1 Kecerdasan Buatan untuk Keamanan Cloud

Salah satu prediksi mengenai masa depan keamanan cloud adalah pemanfaatan kecerdasan buatan (*Artificial Intelligence*/AI) dan *machine learning* (ML) untuk meningkatkan otomatisasi deteksi dan respon ancaman cloud (Mohurle & Patil, 2017). Kemampuan teknologi AI dan ML diharapkan dapat:

1. Mengenali pola-pola serangan canggih dan mutakhir yang mungkin terlewatkan manusia. AI dapat menemukan korelasi yang tidak terlihat dari jutaan data log keamanan.
2. Melakukan analisis risiko, memberikan rekomendasi mitigasi, hingga mengambil tindakan keamanan secara otomatis dan real-time saat mendeteksi indikasi awal serangan.
3. Memperbaiki siklus respon insiden keamanan cloud melalui otomatisasi dan orkestrasi proses yang saat ini masih manual.
4. Menghasilkan dan menguji secara kontinu hipotesis ancaman baru untuk menutup celah deteksi yang ada.

Pemanfaatan AI dan ML untuk keamanan cloud diperkirakan akan terus meningkat seiring makin besar dan kompleksnya data serta ancaman yang harus ditangani.

10.5.2 Enkripsi Kuat sebagai Fondasi Keamanan Cloud

Kekuatan enkripsi akan terus ditingkatkan untuk menjaga kerahasiaan data sensitif di cloud. Enkripsi dengan panjang kunci yang lebih panjang seperti AES-256 dan RSA-4096 diproyeksikan

akan menjadi standar untuk lingkungan cloud. Selain itu, algoritma enkripsi post-quantum yang tahan serangan kuantum komputer juga akan dibutuhkan.
Penerapan enkripsi yang konsisten pada data saat transit, proses, dan penyimpanan akan menjadi fondasi keamanan cloud masa depan. Teknologi blockchain juga dapat diterapkan untuk manajemen kunci enkripsi data di cloud agar lebih terdesentralisasi dan fleksibel. Dengan enkripsi data yang kuat, kerahasiaan informasi penting organisasi di cloud dapat terjamin bahkan jika terjadi kebocoran akses.

10.5.3 Adopsi Model Zero Trust

Model keamanan *Zero Trust*, yang tidak secara default mempercayai entitas mana pun di dalam maupun di luar jaringan, akan semakin dominan diterapkan pada arsitektur cloud di masa mendatang. Zero Trust mensyaratkan otentikasi dan otorisasi yang kuat berdasarkan konteks untuk setiap akses ke sumber daya cloud, meskipun dari entitas yang sudah diverifikasi sebelumnya .
Dengan Zero Trust, risiko keamanan cloud dapat diminimalkan karena semua akses harus diverifikasi dan divalidasi berdasarkan kebutuhan bisnis sebelum diizinkan. Model ini diharapkan akan menjadi standar keamanan cloud di masa depan untuk mengatasi ancaman internal maupun eksternal yang terus berkembang.

10.5.4 Pelatihan dan Sertifikasi SDM Keamanan Cloud

Sumber daya manusia (SDM) merupakan unsur penting dalam keamanan cloud. Pelatihan dan sertifikasi keahlian keamanan cloud diperkirakan akan terus ditingkatkan di masa mendatang. Beberapa skenario di masa depan:

1. Sertifikasi keamanan cloud menjadi syarat wajib untuk engineer cloud.
2. Pelatihan simulasi insiden cloud menjadi wajib bagi tim keamanan TI organisasi.

3. Perguruan tinggi menyediakan program studi khusus keamanan cloud.
4. Sertifikasi kepatuhan standar cloud security bagi penyedia layanan cloud.

Dengan SDM yang tersertifikasi dan terlatih, kematangan keamanan cloud organisasi dapat meningkat secara sistematis.

10.5.5 Regulasi Keamanan Cloud yang Lebih Ketat

Regulasi dan standar kepatuhan terkait keamanan cloud diperkirakan akan semakin diperkuat, khususnya untuk sektor kritikal seperti kesehatan dan keuangan. Beberapa contoh potensi regulasi di masa depan (Weins, 2020):

1. Mandatory pelaporan insiden keamanan cloud setelah ambang tertentu terlampaui.
2. Wajib sertifikasi framework keamanan cloud bagi penyedia layanan cloud.
3. Pembatasan lokasi data sensitif disimpan dan diolah.
4. Denda finansial bagi organisasi yang lalai dalam keamanan cloud.

DAFTAR PUSTAKA

ENISA. 2016. ENISA strategy 2016-2020. *European Union Agency for Network and Information Security*.

Fernandes, D. A. B., Soares, L. F. B., Gomes, J. V., Freire, M. M., & Inácio, P. R. M. 2014. Security issues in cloud environments: A survey. *International Journal of Information Security*, *13*(2), 113–170. https://doi.org/10.1007/s10207-013-0208-7

Mohurle, S., & Patil, M. 2017. A brief study of Wannacry Threat: Ransomware Attack 2017. *International Journal of Advanced Research in Computer Science*, *8*(5). www.ijarcs.info

Samani, R., Reavis, J., & Honan, B. 2015. *CSA Guide to Cloud Computing: Implementing Cloud Privacy and Security*. http://ppdi.stmik-banjarbaru.ac.id/data.bc/4.%20Cloud%20Computing/2015%20CSA%20Guide%20to%20Cloud%20Computing%20Implementing%20Cloud%20Privacy%20and%20Security.pdf

Singh, A., & Chatterjee, K. 2017. Cloud security issues and challenges: A survey. In *Journal of Network and Computer Applications* (Vol. 79, pp. 88–115). Academic Press. https://doi.org/10.1016/j.jnca.2016.11.027

Weins, K. 2020. *Cloud Computing Trends: 2020 State of the Cloud Report*. Flexera.

BIODATA PENULIS

Ir. Hasanuddin Sirait., MT
Dosen program studi Teknik Informatika

Penulis lahir di Rawang Baru-Panca Arga -- Asahan – Sumatera Utara. Saat ini menekuni profesi sebagai dosen program studi Teknik Informatika. Penulis menyelesaikan pendidikan S1 pada STMIK YPTK Padang dan melanjutkan S2 pada di Universitas Hasanuddin Ujung Pandang - Sulawesi Selatan. Penulis telah banyak membangun aplikasi sistem dan proyek teknologi informatika pada perusahaan swasta dan pemerintah. Penulis telah menerbitkan beberapa buku teks dan buku modul praktik bidang Teknologi informatika dan Telekomunikasi yang ber ISBN dan HaKI. Penulis juga telah banyak artikel ilmiah hasil penelitian terkait bidang ilmu komputer sebagai perwujudan Tridharma Perguruan Tinggi. Penulis juga aktif dalam organisasi perguruan tinggi dan profesi dibidang komputer sejak tahun 2005. e-Mail : hsirait2020@gmail.com. Phone : 0812-444-6335

BIODATA PENULIS

Mundzir, S.Kom., M.T
Dosen Program Studi Sistem Informasi
Fakultas Ilmu Komputer Universitas Mulia

Penulis lahir di Makassar tanggal 08 Agustus 1975. Penulis adalah dosen tetap pada Program Studi Sistem Informasi Fakultas Ilmu Komputer, Universitas Mulia. Menyelesaikan pendidikan S1 pada Jurusan Teknik Informatika dan melanjutkan S2 pada Jurusan Teknik Elektro. Penulis menekuni bidang ilmu komputer.

BIODATA PENULIS

Dr. Ino Sulistiani, ST, MT
Dosen di IAIN Palopo

Dr. Ino Sulistiani, ST., MT lahir di Ujung Pandang Tanggal Lahir: 25 September 1977. Saat ini menjadi dosen di IAIN Palopo. Telah mempublikasi beberapa artikel pada Jurnal Ilmian Nasional dan Internasional antara lain: (1) Quality Model Engineering for Evaluation for Academic Information Instrument. Pada Jurnal: IEEE Publishing. Pada Tahun 2020; (2) IS Quality Model on Academic Information System Software : A Proposed Model. Pada Jurnal: Journal of Theoretical and Applied Information Technology. Tahun 2021.; (3) Security-Focused IS Quality Instrument a Proposed Quality Instrument on Academic Information System. Pada Journal of Theoretical and Applied Information Technology. Tahun 2021.; (4) Implementasi Asesmen Instrumen Kualitas Menggunakan Model Kualitas ISO/IEC 25010 dan ISO/IEC 9126 Pada Sistem Informasi Akademik SIPAKATAU. Berbasis Pengalaman Pengguna. Pada Jurnal INSPIRATION tahun 2022.; (5) Instrumen Kualitas Keamanan Sistem Informasi Akademik Berbasis Model Kualitas.. Pada Jurnal Sains dan Informatika. Tahun 2023.; (6) Quality Instrument is Focused Reusability for Academic Information System Software. Pada Jurnal INSPIRATION. Tahun 2023.

Buku yang sudah diterbitkan dengan Judul: (1) Sistem Komputer. Tahun 2015. Penerbit Aksara Timur.; (2) Desain Web. Tahun 2018. Lembaga Penerbit Kampus IAIN Palopo.
e-Mail: inosulistiani@iainpalopo.ac.id

BIODATA PENULIS

Marlina, S.T., M.T.
Dosen Program Studi Sistem Informasi
STMIK Karisma Makassar.

Penulis menyelesaikan studi S1 pada Fakultas Teknik Universitas Hasannuddin, dan menjadi dosen pada STMIK KHARISMA Makassar sejak didirikan tahun 2000. Penulis mengambil S2 pada Fakultas Teknik Universitas Hasannuddin dan tamat tahun 2010. Penulis mengikuti suami pindah ke Kupang dan menjadi dosen di STIKOM Uyelindo Kupang dari tahun 2010 sampai 2015. Karena mengikuti suami kembali ke Makassar, maka penulis kembali mengabdi jadi dosen pada STMIK KHARISMA Makassar sampai saat ini. Semoga *book chapter* ini dapat memberikan kontribusi positif bagi pembaca. Akhir kata penulis berharap agar bisa menulis lebih banyak lagi dan dapat memberi kontribusi kepada dunia pendidikan.

BIODATA PENULIS

Dudes Manalu, S.Kom., M.Kom
Dosen Program Studi Ilmu Komputer
Fakultas MIPA (Matematika dan Ilmu Pengetahuan Alam)
Universitas HKBP Nommensen Pematangsiantar

Penulis lahir di Porsea tanggal 22 Desember 1977. Penulis adalah dosen tetap pada Program Studi Ilmu Komputer Fakultas MIPA, Universitas HKBP Nommensen Pematangsiantar. Menyelesaikan pendidikan S1 pada Jurusan Teknik Informatika dan melanjutkan S2 pada Teknologi Informasi. Penulis menekuni bidang Menulis dan Praktisi di Bidang Jaringan Komputer.

Penulis Juga Tenaga Ahli IT Bidang *Networks And Security* dan membangun Data Center serta Jaringan Fiber Optik Pada Dinas Komunikasi dan Informatika pada salah satu Kabupaten di Sumatera Utara. Email : manalu.dudes@gmail.com

BIODATA PENULIS

Andreas Leonardo Sumendap S.T., M.T.
Dosen Program Studi Sistem Komputer
Universitas Parna Raya Manado

Penulis lahir di Manado tanggal 8 Juli 1988. Penulis adalah dosen tetap pada Program Studi Sistem Komputer Universitas Parna Raya Manado. Menyelesaikan pendidikan S1 pada Fakultas Teknik Elektro Universitas Sam Ratulangi pada tahun 2011 S2 pada Fakultas Teknologi Industri Jurusan Jaringan Cerdas Multimedia Institut Teknologi Sepuluh Nopember Surabaya.

Penulis menekuni bidang Computer Vision dan Computer Networking. Selain sebagai dosen penulis juga sebagai praktisi di saah satu Perusahaan swasta di Kota Manado

BIODATA PENULIS

Gede Erik Aktama, S.Pd., M.Pd.
Dosen Program Studi Sistem Komputer
Universitas Parna Raya

Penulis lahir di Padang Bulia tanggal 02 Oktober 1992. Penulis adalah dosen tetap pada Program Studi Sistem Komputer Universitas Parna Raya. Menyelesaikan pendidikan S1 pada Jurusan Pendidikan Teknologi Informasi dan Komunikasi di Universitas Negeri Manado dan melanjutkan S2 pada Jurusan Pendidikan Teknologi dan Kejuruan di Universitas Negeri Manado.

Selain sebagai dosen IT di Universitas Parna Raya penulis Saat ini penulis sebagai anggota Computer Security Insident Response Team (CSIRT).

BIODATA PENULIS

Sutardi, S.Kom., M.T.
Dosen Program Studi Teknik Informatika
Fakultas Teknik Universitas Halu Oleo

Penulis lahir di Wakatobi tanggal 22 Februari 1976. Penulis adalah dosen tetap pada Program Studi Teknik Informatika Fakultas Teknik Universitas Halu Oleo Kendari. Menyelesaikan pendidikan S1 pada Sekolah Tinggi Manajemen Informatika Komputer (STMIK Handayani) Makassar Jurusan Teknik Informatika dan melanjutkan S2 pada Jurusan Teknik Elektro Konsentrasi Teknik Informatika Pada Universitas Hasanuddin Makassar (UNHAS). Penulis menekuni bidang Menulis.

BIODATA PENULIS

Nur Ilman, ST,MT
Dosen Program Studi Manajemen Informatika
AMIK Ibnu Khaldun Palopo

Penulis lahir di Ujung Pandang sekarang Makassar tanggal 26 Juli 1975 . Penulis adalah dosen tetap pada Program Studi Manajemen Informatika sejak tahun 2005 menyelesaikan Pendidikan Strata satu pad Sekolah Tinggi Teknlogi Telkom sekarang Univ,Telkom tahun 2001 dan S 2 di Universitas Hasanuddin tahun 2010 program studi Teknik Elektro beberapa tulisan telah diterbitkan.

BIODATA PENULIS

Franky G. C. Manoppo, ST., M.Kom.
Dosen Program Studi Teknik Informatika
Universitas Parna Raya

Penulis lahir di Manado tanggal 7 November 1976. Penulis adalah dosen tetap pada Program Studi Teknik Informatika, Universitas Parna Raya. Menyelesaikan pendidikan S1 pada Jurusan Teknik Elektro Universitas Sam Ratulangi dan melanjutkan S2 pada Jurusan Teknik Informatika Universitas AMIKOM Yogyakarta.