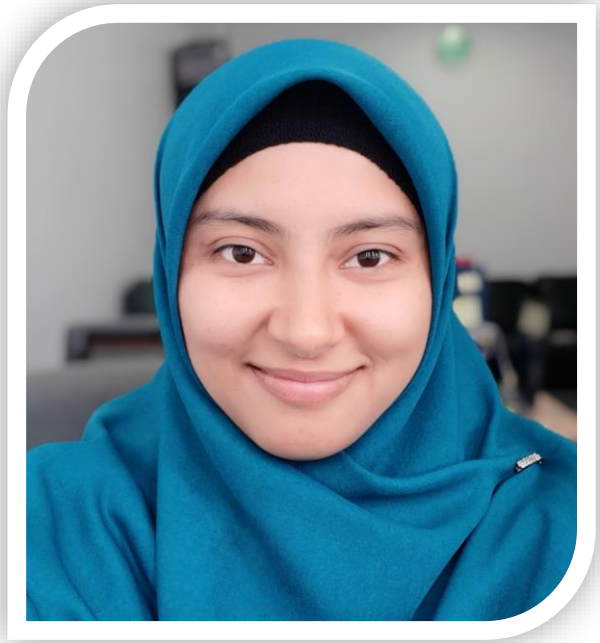
Profil Instruktur



KATRINA PERMASSARI, S.Pd

katr001@kominfo.go.id

- S1 Psikologi Pendidikan UNJ
- Instruktur dan Asesor BPPTIK Kominfo
- Certified: Junior Office Operator, Junior Mobile Programmer
- Pengalaman Mengajar: 2011 - Sekarang

“No System is Safe”

-Who am I (2015)-

Keamanan Informasi Pengguna

Disusun oleh:

- Tim BPPTIK

Ringkasan Mata Pelatihan

Unit Kompetensi Acuan	Mengidentifikasi Aspek Keamanan Informasi Pengguna
Kode Unit Kompetensi Acuan	J.63OPR00.016.2
Deskripsi singkat	Mata Pelatihan ini berkaitan dengan pengetahuan, keterampilan dan sikap kerja dalam mengidentifikasi aspek keamanan informasi pengguna.
Tujuan Pembelajaran	
Hasil Belajar	Setelah mengikuti seluruh rangkaian pembelajaran pada mata pelatihan ini, peserta kompeten mengidentifikasi aspek keamanan informasi pengguna.
Indikator Hasil Belajar	Setelah mengikuti pembelajaran ini, peserta kompeten: 1. Mengidentifikasi ancaman keamanan informasi pengguna. 2. Mengidentifikasi aspek *confidentiality*. 3. Mengidentifikasi aspek *integrity* 4. Mengidentifikasi aspek *availability*

Agenda

1. Ancaman keamanan informasi pengguna
2. Aspek *confidentiality, integrity, availability*

Ancaman Keamanan Informasi Pengguna

Pendahuluan

- **Sumber ancaman** keamanan informasi adalah acaman keamanan informasi bisa berasal dari **orang, organisasi, mekanisme, atau peristiwa** yang memiliki potensi membahayakan sumber daya informasi perusahaan (lingkungan pengguna).
- **Target ancaman** keamanan informasi adalah kejahatan/ kriminilitas di dunia maya (cyber crime) berupa **pencurian data terhadap** berbagai **situs** baik milik **pemerintah**, maupun situs-situs **komersial** dan **perbankan**, kebocoran informasi pribadi atau rahasia perusahaan yang digunakan untuk menyerang server, penipuan dengan satu kali **klik gambar atau video dapat menyebabkan penagihan**, **serangan terhadap surat elektronik (email) dengan lampiran yang terinfeksi virus, password yang dicuri atau terinfeksi virus**, dll.

Malwares

Malwares

Merupakan kode atau software yang didesain secara khusus untuk mengganggu, merusak, mencuri atau memberikan dampak negatif lain terhadap data atau jaringan pada komputer user.

Tipe *malwares* diantaranya:

1. virus,
2. trojan,
3. worm,
4. bots,
5. ransomware, dll

Virus

- Virus adalah tipe malware yang **dapat menggandakan dirinya** dengan memasukkan copy dari dirinya menjadi bagian dari program lain. Dapat menyebar dari satu komputer ke komputer lain, meninggalkan jejaknya yang berbahaya. **Penyebaran** dari virus ini biasanya **menggunakan jaringan**, **file sharing**, **e-mail atau usb**.
- Hampir semua **virus dijalankan bersamaan dengan file *executable***, yang berarti virus tidak dapat aktif jika user tidak menjalankan atau membuka file atau program yang berbahaya tersebut.

Worm

Worm serupa dengan virus, dimana mereka **menggandakan dirinya** dan menyebar melalui jaringan secara otomatis. Perbedaannya adalah jika dalam penyebarannya virus bergantung atas file atau program berbahaya tempatnya berada, worm tidak. Worm adalah sebuah software yang **berdiri sendiri** dan **tidak bergantung ke program atau file lain**.

Trojan

- **Trojan** adalah tipe lain dari malware yang namanya mengikuti nama kude kayu Yunani pada saat mereka memasuki Troy. Merupakan potongan **software berbahaya yang terlihat** legal atau **tidak membahayakan**, hal inilah yang menipu user untuk menjalankannya. Sesudah dijalankan, ia dapat menyebabkan beberapa serangan seperti, menyebabkan rasa jengkel (**membuka window baru secara terus menerus**) atau merusak komputer (**menghapus file, mencuri data atau mengaktifkan malware lain**).
- Biasanya **tujuan** utama Trojan adalah **memberikan jalan ke user lain untuk mengakses sistem**. Tidak seperti virus dan worm, Trojan **tidak dapat menggandakan dirinya**, mereka hanya **menyebar melalui interaksi user seperti e-mail atau file di Internet**.

BOT

Didapatkan dari kata "robot" yang dimana merupakan sebuah proses otomatis yang berinteraksi dengan layanan jaringan lain. Bot dapat digunakan untuk tujuan yang baik atau jahat. **Jika digunakan untuk tujuan yang jahat**, **Bot dapat bekerja seperti Worm** dimana ia menggandakan dirinya dan menginfeksi komputer, **bedanya adalah ia menunggu perintah dari si pembuat bot dalam melakukan pekerjaannya**. Seperti **mendapatkan informasi finansial**, **serangan DoS**, **Spam** dan sebagainya.

Ransomware

- Ransomware adalah **program jahat komputer yang menyandera dokumen korban dengan algoritma enkripsi khusus**. Setiap dokumen yang terkunci oleh peranti lunak ini hanya bisa diakses dengan cara memasukkan kode unik yang hanya dimiliki si penyebarnya. Untuk membuka akses dari dokumen yang terkunci, si penyebar ransomware biasanya meminta uang tebusan kepada korbannya dalam bentuk Bitcoin. Jika korban tidak membayar, maka penjahat siber ini mengancam akan menghapus dokumennya.
- Tapi, ransomware sendiri **tidak terbatas hanya pada mengunci dokumen saja, ada varian lain yang mengunci komputer sepenuhnya**. Saat komputer dinyalakan, ransomware akan menampilkan pesan agar korban membayar tebusan untuk bisa mengoperasikan komputer. Selain itu, **ada juga varian ransomware yang memunculkan pesan pop-up yang sulit untuk ditutup** dan membuat komputer sulit untuk digunakan.

TOP 10 Surefire Ways to Lose Your Data in 2013

10 Plug in the USB drive you just found and use it

You wouldn't want to waste free storage, would you? USB storage devices are commonly used to spread malware. Even plugging a phone into your USB slot to charge it can spread malware.

9 Advertise your absence

Out of office notifications seem innocent but can give cybercriminals valuable reconnaissance to launch attacks (who to contact, how long or why you're out) – targeted attacks against SMBs doubled to 36% in the past year. Limit the info in your auto-reply so cybercriminals have less to work with.

8 Accept friend requests from people you don't know

You can never have too many friends, right? Cybercriminals use social networks to spread viruses, perpetrate fraud, and distribute spam and phishing messages – 70% of SMBs do not have policies for social media use. Keep your guard up – a "friend" or "follower" isn't necessarily who they say they are.

7 Skip using screen lock on your phone or tablet, it's a pain

When a business-connected mobile device is lost, there's more than an 80% chance an attempt will be made to breach corporate data and/or networks. Use the screen lock feature with a strong password or "draw to unlock" pattern.

6 Download mobile apps willy nilly

Mobile malware has increased by an average 55% every month. Only use app marketplaces from legitimate vendors and always read the fine print to avoid apps requiring excessive permissions, like uploading all of your contacts.

5 Send financial reports to your boss via free Wi-Fi at the airport

Mobile devices and free Wi-Fi mean you can be productive anytime, anywhere, but who else is lurking there? 67% of people use unsecured Wi-Fi. If it's an unknown network, use https connection or opt for a Wi-Fi privacy application.

4 Take confidential data home with you; you're just doing your job

Employees copy confidential data to unencrypted USBs, send to personal email accounts or upload to file sharing sites – 54% admit to removing information without permission. If it's confidential, encrypt it before it leaves the office.

3 Click here to confirm your flight or claim your obscure lottery winnings

Attackers hide malware in random email or text messages. These fake messages can be very convincing. If you didn't book the flight or it just seems phishy, don't click – 1 in 267 emails sent to SMBs are malicious.

2 Wait to back up your files/server until tomorrow, or the next day

Backups take time, but putting them off can devastate a small business – 52% lost productivity and 29% lost revenue in a typical outage. Identify critical resources, use backup solutions and test frequently that recovery is working.

1 Use “Fluffy” (your pet’s name) for your password on multiple sites

Passwords can be easy to crack – 82% of users re-use passwords and 40% write them down. Use unique passwords with 8 characters or more, and letters, numbers & symbols (e.g., # $ % ! ?), but don’t keep them on a sticky note.


Avoid a Weak Password...
DONT REUSE PASSWORDS
for at least a year.
DONT
use a duplicated good password example—create your own.
BEEP
DONT USE THE SAME PASSWORDS
for multiple accounts.
Don't use a password with
PERSONAL INFORMATION
(name, birth date, etc.)
Don't use
DICTIONARY WORDS
Don't use keyboard patterns
QWERTY
or sequential numbers
12345
Don't make your password all numbers, uppercase letters or lowercase letters—
MIX IT UP
Don't use repeating characters
22TT

Seven Cybersecurity Myths Busted

Myth: Viruses and other malicious software ("malware") only affect computers and laptops.

Reality: Mobile malware families, which affect smartphones, tablets and other mobile devices, increased by **58 percent** last year.

This malware can steal information such as phone numbers and email addresses (**32 percent** of the time), or use the phone's GPS to track the user (**19 percent** of the time).

Myth: I can't get a virus or be attacked on popular social networking sites.

Reality: Many well-known social networks, including several of the newest ones, are prime targets for scammers, with **56 percent** of social media attacks involving fake gift cards and survey scams.

Myth: Apple products aren't susceptible to viruses and online attacks.

Reality: While hackers still primarily target PCs, more than **600,000 Mac computers** were infected by one attack last April; just one example that no operating system is safe from online threats.

Myth: Free antivirus software on my computer is good enough to protect my information

Reality: "Ransomware" (where cybercriminals lock you out of your computer unless you pay their "ransom") is one example of the trend toward increasingly vicious malware, which is known for being harder to undo, more aggressive and more professional than other malware.* This malware requires protection beyond what basic, free antivirus software can offer.

Myth: It's easy to tell if a site is fake -- typos or foreign characters are key indications.

Reality: Many spoofed sites today look exactly like the websites of legitimate brands, down to the smallest details. Adding to that, the number of fake sites that imitated legitimate social networks more than doubled in 2012.*

Myth: My computer won't get infected since I don't visit risky sites.

Reality: **Sixty-one percent** of malicious sites are actually legitimate websites that have been compromised and infected with malicious code. Business, technology and shopping websites were among the top five types of sites hosting infections.*

Myth: I'll know right away if my computer is infected.

Reality: Cybercriminals today rely on stealth – the longer they're on your machine undetected, the more damage they can do. Your computer could even be part of a "botnet" – a network of remotely-controlled computers that send spam emails or participate in widespread attacks – and you might not even know it.

Social engineering

- Social engineering adalah **manipulasi psikologis** seseorang dengan tujuan **untuk mendapatkan informasi tertentu** atau melakukan hal tertentu **dengan cara menipu** secara halus **dan tidak disadari**.
- Manipulasi psikologis dilakukan dengan berbagai **media** yang tujuannya untuk mempengaruhi pikiran korban, misalnya menggunakan **suara** (berbicara untuk menyakinkan korban), **gambar** (memasang gambar yang erotis agar di klik), **tulisan** (menulis artikel yang persuasif dan menyakinkan misal menulis tutorial cara hack akun facebook, tapi palsu).

Aspek *Confidentiality, Integrity, Availability*

Aspek *Confidentiality*

- **Tingkat keterbukaan informasi** adalah tingkat kesiapan pengamanan informasi penyelenggara layanan public dan pengamanan unit data strategis dengan teknik keamanan, sistem manajemen keamanan informasi dengan standarisasi SNI ISO/IEC 27001 teknologi informasi.
- **Kebutuhan personal organisasi** adalah kebutuhan untuk mengamankan sumber daya informasi organisasi, melindungi baik peralatan komputer atau non komputer, fasilitas, data dan informasi dari penyalahgunaan pihak-pihak yang tidak berwewenang.
- **Proses autentifikasi** password dipilih sesuai dengan kebijakan password pada organisasi (kompleksitas, panjang proses), password digunakan secara aman sesuai dengan panduan pada organisasi tersebut.
- **Teknologi enkripsi** adalah salah satu solusi/cara yang paling efektif untuk mengamankan data, melindungi dari penjahat siber, dengan metode: enkripsi file, enkripsi folder, enkripsi full disk, shredder, atau enkripsi e-mail.

Aspek *Integrity*

- **Akses kontrol** adalah akses pembatasan selektif ke suatu tempat atau sumber daya lainnya, pembatasan pintu masuk ke suatu property, bangunan, atau ruangan yang menyimpan informasi hanya untuk orang yang berwenang.
- **Metadata** adalah informasi terstruktur yang mendeskripsikan, menjelaskan, menemukan, atau setidaknya menjadikan suatu informasi mudah untuk ditemukan kembali, digunakan, atau dikelola.

Aspek *Availability*

- **Tingkat kekritisan** adalah aksi yang terjadi baik dari dalam sistem atau dari luar sistem yang dapat mengganggu keseimbangan sistem informasi (ancaman) seperti: ancaman alam (banjir, gempa, tsunami, longsor), ancaman manusia (hacking, cracking, DDoS, 65 backdoor, social engineering), ancaman lingkungan (kebocoran A/C, atap bocor, penurunan/kenaikan tegangan listrik), cacat atau kelemahan dari suatu sistem yang mungkin timbul saat mendesain, menetapkan prosedur, mengimplementasikan maupun kelemahan atas sistem kontrol yang ada, dan setting firewall.
- **Prosedur backup** adalah Siapkan media penyimpanan hasil backup (harddisk, flashdisk, atau dvd), hidupkan komputer, masuk desktop atau start klik kanan this PC, pilih Manage, klik disk management, klik kanan partisi sistem operasi pilih properties, memulai proses backup, masuk control panel, klik file history, klik system image backup, pemilihan media penyimpanan backup lalu klik next, pemilihan partisi yang akan di-backup lalu pilih next, konfirmasi konfigurasi backup yang telah diset lalu klik start backup, proses pembuatan image backup dimulai, cek hasilnya pada file eksplorer bila sudah selesai proses backup.
- **Prosedur restorasi** adalah siapkan dvd bootable sistem operasi, masukan dvd tersebut ke dvd ROM, lalu restart computer, pilih booting dari dvd ROM, tekan sembarang tombol untuk masuk menu instalasi, proses setup dimulai lalu klik next, pilih repair your computer.

Aspek-aspek dalam Keamanan Komputer

- *Privacy / **Confidentiality***
- ***Integrity***
- *Authentication*
- ***Availability***
- *Access Control*
- *Non-Repudiation*

Aspek-aspek dalam Keamanan Komputer

Perbedaan	Privacy/Confidentiality	Integrity	Authentication	Availability	Acces control	Non repudiation
Definisi	**Menjaga informasi dari orang yang tidak berhak mengakses**	**Informasi tidak boleh diubah tanpa seizin pemilik informasi**	Menyatakan bahwa informasi benar"nasli, org yg mengakses benar" org yg dimaksud	**Upaya pencegahan ditahannya informasi**	Sistem yang di rancang utk memungkinkan wewenang membatasi pnguna utk mengakses	Aspek menjaga agar seorang tidak dapat menyangkal telah melakukan sebuah transaksi
Bentuk serangan	**Usaha penyadapan**	**Adanya virus trojan, pemakai lain yang mengubah informasi tanpa izin**	Data dapat dimanupulasi	**Pemakai diirimi permintaan yg bertubi2**	Masuk kedalam suatu sistem tanpa diketahui admin,	Usaha penipuan Carding
Contoh	**Data data yang sifatnya pribadi harus dapat di proteksi dlm penggunaan dan penyebarannya**	**Email di intercept di tengah jalan, di ubah isinya kemudian diteruskan ke alamat yang di tuju**	Data dikonfirmasi ulang dgn captcha (kode)	**Tidak dapat membuka email atau kesulitan mengakses emailnya**	Pembatasan orang yang dapat mengakses informasi dan user harus menggunakan password	Seorang mengirimkan email untuk memesan barang tidak dapat menyangkal bahwa dia telah mengirim email tersebut padahal dia tidak memesan barang apapun
Usaha	**Dengan menggunakan Teknologi Kriptografi, jangan memberikan data akun kepada orang lain**	**Menginstall anti virus, jangan menyebarkan informasi kita ke orang lain**	1. Adanya tools yg membuktikan keaslian dokumen. 2. Akses control	**Kinerja sistem harus selalu memadai tanpa menghiraukan jumlah user atau proses yg harus dijalankan**	Memberikan hak akses kepada orang orang terpercaya dengan id	Jangan asal menyuruh orang lain untuk menfoto copy kartu kredit atau identitas

Aspek-aspek dalam Keamanan Komputer

Perbedaan	Privacy/Confidentiality	iIntegrity	Authentication	Availability	Acces control	Non repudiation
Definisi	**Pencegahan agar suatu informasi tidah dapat diakses oleh orang yang tidak berhak**	**Informasi tidak boleh diubah tanpa seizin pemilik informasi**	Metode untuk menyatakan bahwa informasi asli, atau orang yang mengakses	**Upaya pencegahan diitahannya informasi yang berlebihan oleh yg tidak berhak**	Mengacu pada sistem yang dapat mengkontrol, memantau dan membatasi pergerakan	Merupakan hal yang bersangkutan dengan si pengirim, agar sesorg tdk menyangkal telah melakukan transaksi
Bentuk serangan	**Usaha pembajakan, penyadapan, pencurian informasi**	**Adanya virus, trojan horse, atau user lain yang mengubah tanpa izin**	Pencurian informasi	**DOS (Denial Of Service) & Mailbomb**	Masuk kedalam suatu sistem tanpa diketahui admin, tanpa hak izin akses	Adanya akun palsu/ email yang sengaja memesan barang
Contoh	**Mengubah status/identitas diri pada suatu akun data pribadi, pencurian pada kartu kredit**	**Email di intercept di tengah jalan, diubah isinya, kemudian di teruskan ke alamat yang di tuju**	Terjadi pada saat login	**Membanjiri email korban dengan data / kiriman email yg banyak**	Login website Database	Seseorg yang mengirim email untuk memesan tdk dpt menyangkal bahwa sudah mengirim
Usaha	**Menggunakan teknologi enkskripsi untuk meningkatkan privacy**	**Pemasangan antivirus, mengenkripsi data & digital signature.**	Watermarking (teknik penyembunyian data atau informasipada suatu media	**Email firewall & Tarpitting (mencegah spam)**	-Menambahkan alat keamanan, seperti RFID, Voice -- kombinasi angka dan huruf sebagai password -- firewall	Melakukan mengkornfirmasi agar menggunakan identitas Asli/KTP

Kesimpulan

Kesimpulan

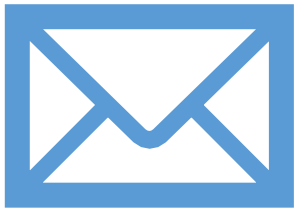
Pengetahuan akan keamanan informasi sangat penting agar dapat menjaga komputer dari gangguan dan segala ancaman yang membahayakan. Keamanannya melingkupi keamanan data atau informasinya ataupun pelaku sistem (*user*).

Referensi / Bacaan Lebih Lanjut

Referensi / Bacaan Lebih Lanjut

- **SKKNI Nomor 56 Tahun 2018**
- Purwandari, Nuraini . ***Sistem Keamanan Teknik Informasi.***
- Donny B.U. 2014. ***Information Security: Fundamental***

Terima Kasih



Kantor:
Balai Pelatihan dan Pengembangan
Teknologi Informasi dan Komunikasi
Kementerian Kominfo
Website: https://bpptik.kominfo.go.id
Email: bpptik@kominfo.go.id
Twitter: @bpptik
Facebook: @bpptik
Instagram: @bpptik
Google Plus: +bpptikkemkominfo