CABARAN KESELAMATAN SIBER BAGI KESEJAHTERAAN UMMAH

Dr. WIDA SUSANTY HAJI SUHAILI
SCHOOL OF COMPUTING & INFORMATICS,
UNIVERSITI TEKNOLOGI BRUNEI

Agenda

1. Cabaran dan isu keselamatan siber
2. Langkah-langkah keselamatan
3. Cara mengatasi dan menangani jenayah siber

Kemudahan dari kepesatan teknologi

- Perhubungan
  - Skype
  - Whatsapp
  - IoT (Internet of Things)
- Pendidikan
  - Mendeley
  - Google Scholar
- Perniagaan dan Pergaulan
  - Facebook
  - Instagram

Cabaran & Isu Keselamatan

1. Kesahihan maklumat
2. Pencerobohan

- Mengugat ketentraman, kestabilan dan kesejahteraan negara, bangsa dan ugama

Kesahihan Maklumat

- Cabaran
  - Maklumat sahih dan tepat
  - Maklumat tidak menyesatkan dan memesong
  - Kesilapan dalam melayari link yang ada dalam search result
- Pendidikan
  - Google
- Perhubungan, Perniagaan & Pergaulan
  - Facebook, Instagram, Whatsapp

Kesahihan Maklumat

- Trolling
  - Membangkitkan kemarahan
  - Menyebarkan propaganda jahat
- Arab Springs ”(Howard, et al, 2011, Knott, 2014)
  - Syria, Libya, Mesir, Lebanon, Oman dan yang lain
- Siber Terrorism
  - Malaysia, Indonesia, Philippines and Singapore

Pencerobohan

- Disebabkan:
  1. Kelalaian manusia,
  2. proses yang tidak efektif dan kurang efisen dan
  3. teknologi yang tidak sesuai
- Website defacement
  - 2011 – 160 laman web yang dihack: no security patch
  - 2012 dan 2013 Meningkat, Sebab 3rd party website no security control
- Menyebabkan kesukaran pengaksesn informasi dan menghalang operasi harian
- Paling recent affecting MORA

Pencerobohan

- DoS (Denial of service)
- – menyekat urusan
- Bahaya if focal point diserang –memutuskan perhubungan institusi berkenaan
- Rugi beribu malahan juta

Pencerobohan

- IoT , Remote access
  - CCTV
  - *Hijacking or sniffing wireless communication*
- Atau bila kita lupa menutup camera computer atau membenarkan komputer dicerobohi
  - Atau istilah ‘Big Brother”
  - Sebahagian dari serangan *botnet/zombie army*.
- menjejak penyenayah siber seperti ini sangat mencabar

Pencerobohan

- Location Detection – Pokemon Go

- FBI: connected devices risiko ancaman including lights and any wearable (Hammond, 2015, Higginbotham, 2015)

- The Inductrial Control System CERT – mengkategori penjenayah siber kepada 3 kumpulan

  (Edward, 2015, ICT - CERT)

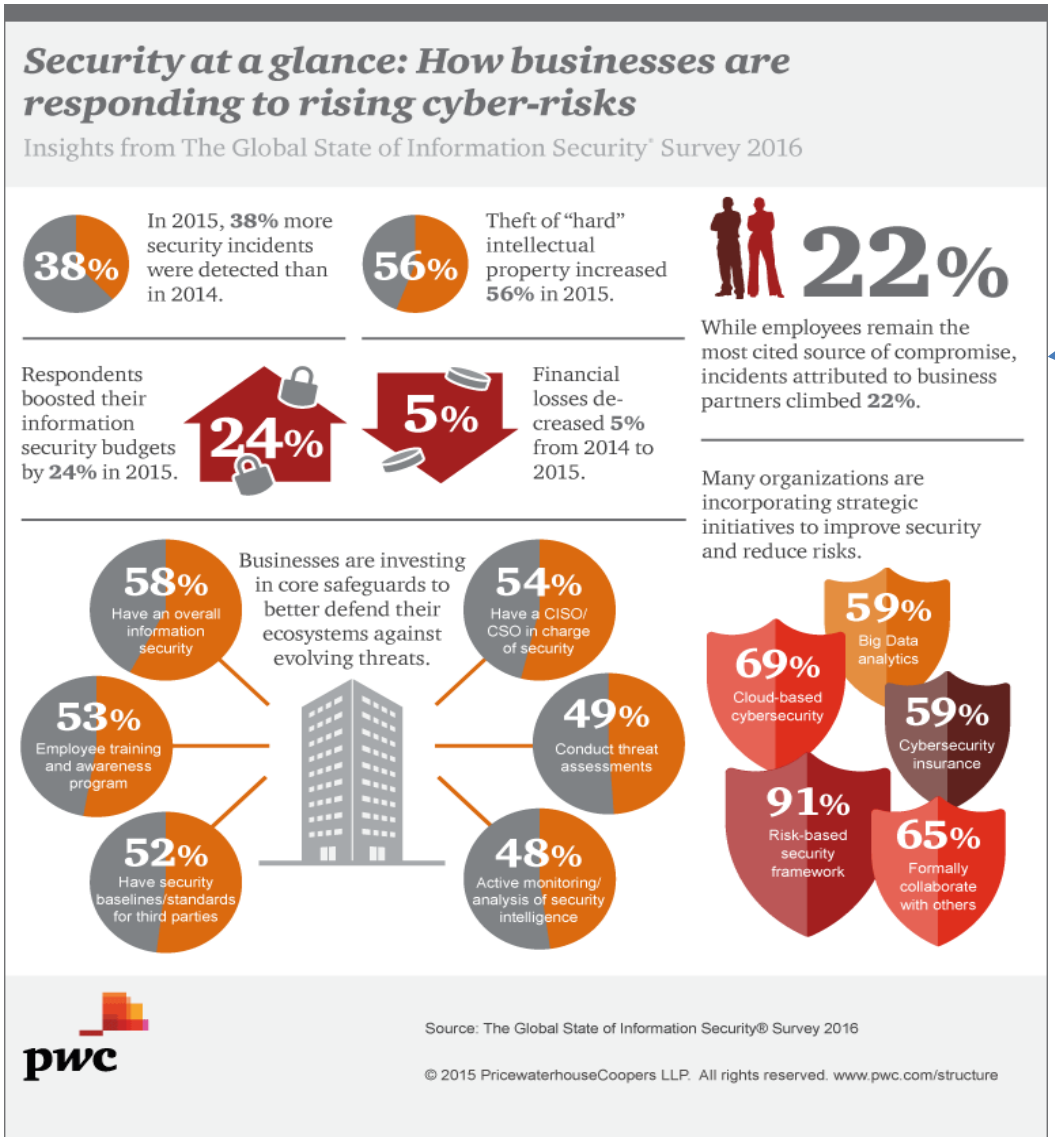
Langkah-langkah Keselamatan - Manusia

- Jangan jadi mangsa
- Jangan mudah mempercayai maklumat
- Jangan mengongsi maklumat peribadi kepada orang yang baru dikenali
- Berfikir sebelum mengongsikan maklumat walaupun pasangan kekasih
- Bahaya berkawan orang di atas talian
- Jangan dilayan Cyber bullying
- Jangan dilayan Cyber trolls

Langkah keselamatan Kesahihan - Pastikan

- Jangan melayari laman web yang diragui
- ‘http’ diganti dengan ‘https’
- Pastikan adanya simbol mangga kecil di status bar
- Two-factor authentication (Online Banking)

Pencerobohan – berpunca kelalaian Manusia



Langkah-langkah Keselamatan – Kata laluan

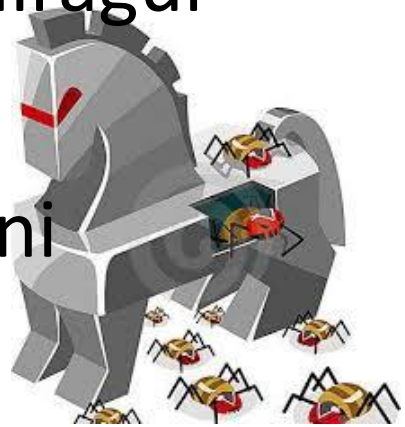
- Jangan pendek, mengandungi maklumat peribadi seperti tarikh lahir, plate lesen, numbur telipon, nama
- Jangan menggunakan perkataan yang dapat diperoleh dalam kamus
- Perlu terdiri dari
  - A-Z, a-z, 0-9, simbols, characters
- Kekuatan: Senang di ingati tapi susah diteka
  - Hello123 – lemah
  - Combination @(H31iL0)@ - kuat

Password Cracking

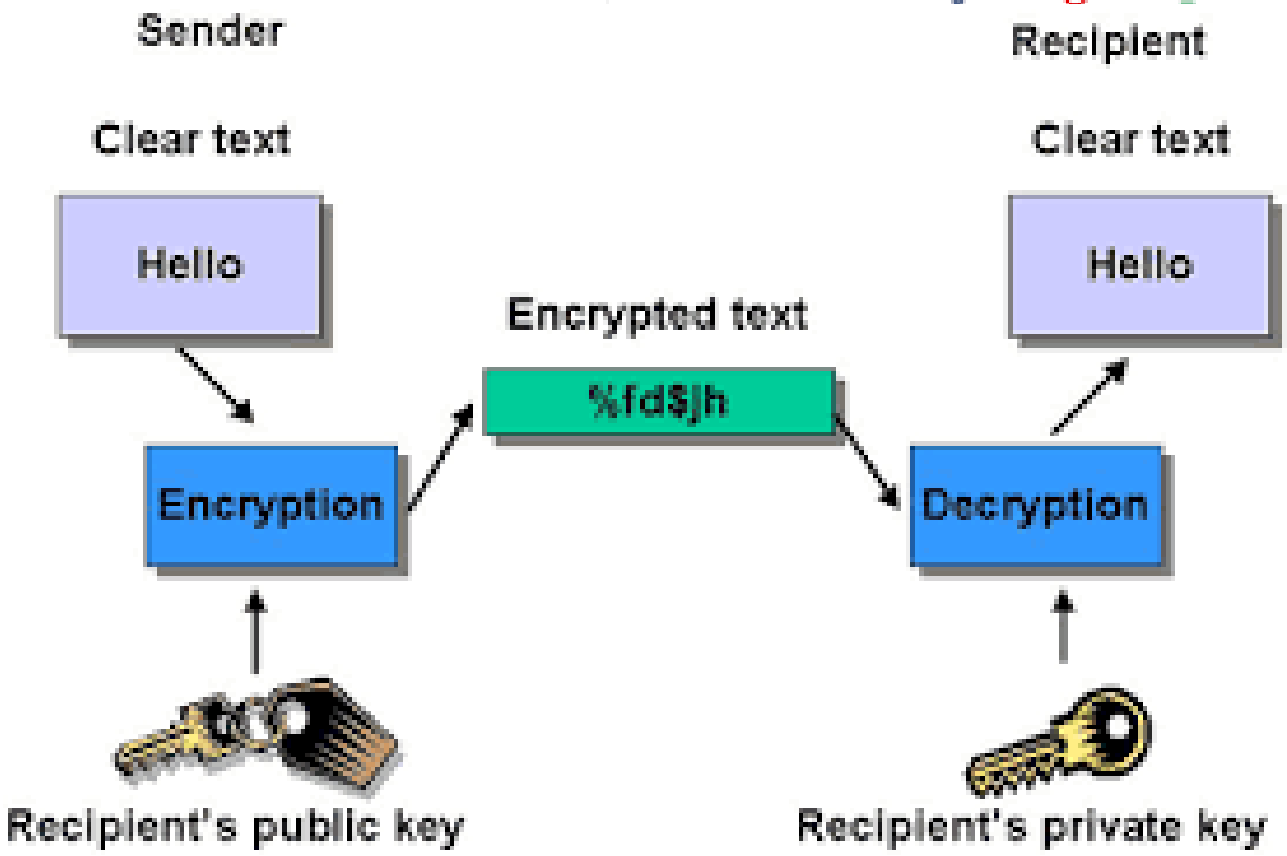
THC-Hydra

Langkah-langkah keselamatan - proses

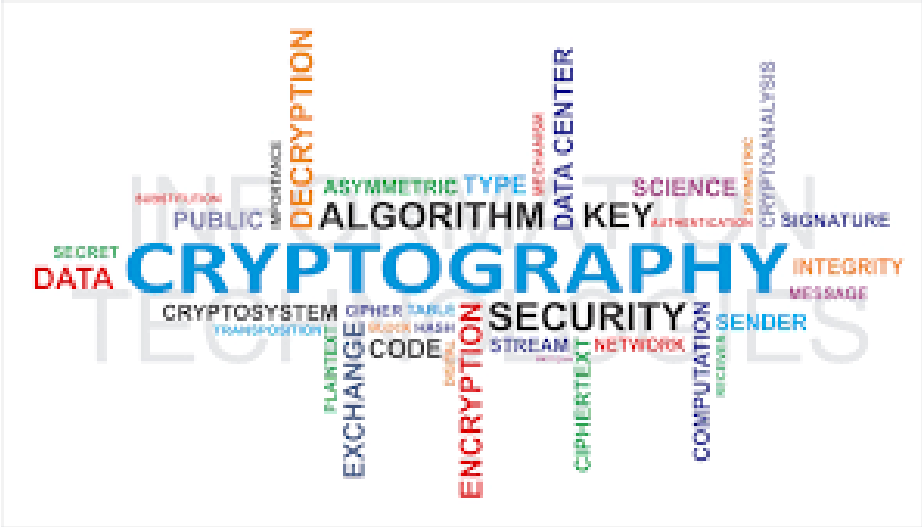
- Sistem pengurusan kata laluan yang efisen
- Amalkan policy kata laluan yang kuat
- Perisian original bukan cetak rompak
- Jangan memuatturun perisian yang diragui
- Jauhi dari menjadi backdoor
- Pastikan perisian sentiasa dikemas kini (Patch update)



Langkah keselamatan Encryption



Langkah keselamatan Encryption



- Aku
- Suka
- Kamu

- Akakugu
- Sukukaga
- Kakamugu

- Aku
- Suka
- Kamu

Public key:
lepas vowel isi k if awal isi g if akhir and tambah vowel yang sebelumnya

Teknologi: Perisian Antivirus

Produk Keselamatan Siber

IAM, Encryption, DLP, Risk and Compliance Management, IDS/IPS, UTM, Firewall, Antivirus/Antimalware, SIEM, Disaster Recovery, DDOS Mitigation, Web Filtering dan Security Services

KASPERSKY
ENDPOINT SECURITY
FOR BUSINESS

COMODO
Endpoint Security
Manager

DDoS
Distributed Denial of Service
Protection


Bomb
DIVING
Hat
Adware
DUMPSTER
Black
Door
HACKER
Spyware
Keylogger
Botnet
Cracker
Gray
Phreaker
MALWARE
PHISHING
ENGINEERING
Virus
Trojan
Worm
Adware
threat
security
protect
crime
protection
attack
danger
breach
conflict
internet
network
online
searching
alert
computer
identity
information
theft
surveillance
vulnerability
encryption
defense
password
software
leak
confidential
firewall
secrecy
antivirus
symbol
burglar
concept
person
spy
aggression
business
risk
criminal
virus
unlock
data
cyber
privacy
bomb
stealing
hacker
hacked
chief

Usaha sama

- Pelbagai agensi yang bergabung usaha
  - ITPSS
  - BruCERT
  - AITI
  - AGC (Criminal Justice Division)
  - Royal Brunei Police Force
  - Jabatan Sekolah-Sekolah di bawah Kementrian Pendidikan
- Kempen Kesedaran melalui “Talks”
- Risalah kesedaran
  - Secure Verify Connect
  - Digibytes

Forum Keselamatan Siber (RBTS, 2015)

- Royal Brunei Technical Services (RBTS)
- 5 Februari 2015
- Tema: Combating Cyber Security Threats
- Objektif
  - mendedahkan kesedaran korporat terhadap keselamatan siber & memastikan organisasi dilengkapi dengan pengetahuan keselamatan online
- Take away message:
  - **Ancaman dunia siber meningkat dengan perkembangan pengunaan ICT**
  - **Kepentingan usaha sama dlm membasmi dan membenteras ancaman siber**

Antara jenayah & hukuman

Jenayah Siber	Tahun	Hukuman
Hacking & Mencuri data	2010	28 bulan penjara
Rogol – 13 tahun - chat	2011	14 tahun penjara 14x sebatan
Cyber bullying	2012	10 bulan penjara
Rogol – sexual grooming, facebook	2015	9 tahun penjara, 6 x sebatan
Ancaman terroris	2015	Dalam sekatan

APCERT
Asia Pacific Computer Emergency Response Team

OIC-CERT
Computer Emergency Response Team

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

SingCERT
Singapore Computer

PakCERT
Pakistan Computer Emergency Response Team

RU-CERT

BRUCERT
BRUNEI COMPUTER EMERGENCY RESPONSE TEAM

aeCERT
Computer Emergency Response Team
فريق الإستجابة لطوارىء الحاسب الآلي

Technology, IT etc.
HKCERT
means
Hong Kong Computer Emergency Response Team
by acronymsandslang.com

computer emergency response team CERT-EU
for the EU institutions, bodies and agencies

CERT-GH
Ghana Computer Emergency Response Team

KZ-CERT

عمان الرقمية
e.oman

Oman National CERT
Towards a safe cyber environment

CERT IS A MARK OWNED BY CARNEGIE MELLON UNIVERSITY
CERT
AUTHORIZED TO USE CERT

Satu strategi diperlukan bagi mengabung semua usaha menjadi satu usaha yang koherent, komprehensive dan mapan (ITU, 2016)

TERIMA KASIH