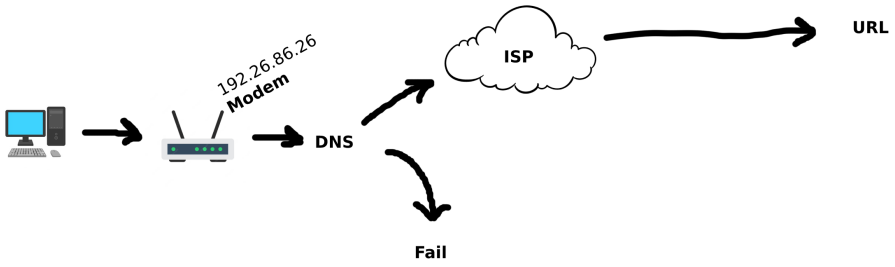
Forelæsningsnoter

Mikkel Boye Rasmussen

02.02.2023

Introduktion til Informationssikkerhed

På tavlen:



modem er årsag til man kan kommunikere med sin Internet service provider (ISP)

Powerpoint præsentation:

Lidt om Karsten:

- Certificeringer - CISO af Exin (ISO27001, ISO27701, GDPR)
- Officielt, lektor på Zealand, guest professor på institut for IT-sikkerhed i Rusland
- indehaver af stealth computing, konsulentvirksomhed indenfor IT-sikkerhed.

ISO - international standard organization
ISO27701 - Udvidet GDPR certificering

Kontaktoplysninger

- kava@zealand.dk
- 50762764 (SMS)

Stealth Computing

- ISO27001 rådgivning og implementering
- Awareness programmer for virksomheder
- GDPR og ISO27701 rådgivning
- Penetration testing, offensive IT security

Fagets emner og mål
Data vs Information - KAVA
Truslen mod vores information/data - KAVA

OS: Kali Linux - ANAC
Python programming for hackers - ANAC
IP Network basics - KAVA

Fagets læringsmål: Viden: Den studerende har viden om og forståelse for

- Grundlæggende programmeringsprincipper
- Grundlæggende netværksprotokoller
- Sikkerhedsniveau i de mest anvendte netværksprotokoller

Færdigheder: Den studerende kan supportere løsning af sikkerhedsarbejde ved at

- Anvende primitive datatyper og abstrakte datatyper
- Konstruere simple programmer der bruge SQL databaser
- Konstruere simple programmer der kan bruge netværk
- Konstruere og anvende tools til f.eks. at opsnappe samt filtrere netværkstrafik
- Opsætte et simpelt netværk.
- Mestre forskellige netværksanalyse tools
- Læse andres scripts samt gennemskue og ændre i dem

Kompetencer: Den studerende kan

- Håndtere mindre scripting programmer set ud fra et it-sikkerhedsmæssigt perspektiv

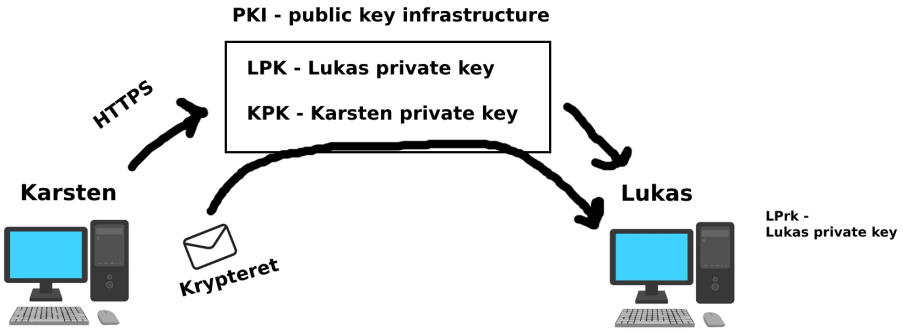
Introduktion til IT-sikkerhed har et omfang på 5 ECTS point.

Definition: data vs. Information

Information er:

- data, der har betydning / giver mening
- data, der giver værdi
- data, der har/giver strukur/kontekst

Teknologi kan behandle, flytte, opbevare og beskytte data



AES - typisk til public keys (længden af Strengen er ikke forudsigelig)

De største trends og kriminalitetens udvikling

Truslen

Den største trusel overfor virksomheder er phishing - udgør 80% af sucessfulde cyberangreb

Heimdal - Endpoint protection

Case: Colonial pipeline attack

Styret af PVC samt OT (operational technology)

På 7.maj 2021 mistede de kontrollen over deres oliesystem, alt benzinlevering blev stoppet, fly og alt anden transport stoppede. Joseph Blount CEO af colonial Pipeline, valgte at betale 32mil danske kroner for at få sit system tilbage.

DarkSide hacker gruppen var bag angrebet, hvilket var heldigt da systemet med garanti blev leveret tilbage af princip fra gruppen, efter betaling.

The good of the bad guys?

CaaS - crime as a service DarkSide falder under CaaS - priser mellem 200.000 og 5.000.000usd. Hacker ikke skoler, hospitaler og nonprofit, samt donerer til velgørenhed. Deres image er vigtigt for dem da det er en stor del af deres salgsmodel.

Top 6 cyber hacks

- Ransomware
- Phishing
- DDoS - Distributed Denial of Service
- MIM - man in the middle
- Sextortion
- Mobile spywar