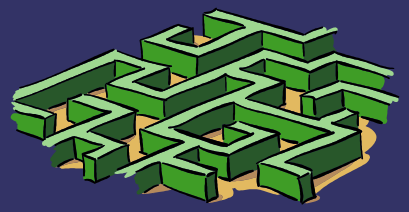
IT-Sikkerhed - en klods om benet eller sund fornuft ?

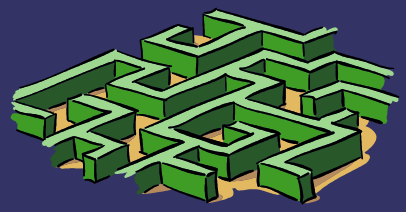
Lars Ole Pedersen OZ5VO

Et dialog foredrag



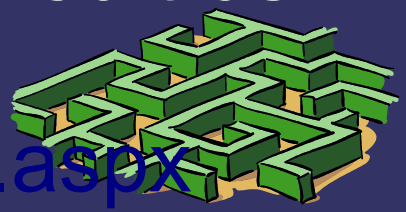
Oversigt

- Introduktion
- Trusselsvurdering – Center for Cybersikkerhed
- Password – sikkerhed og beskyttelse
- Virus/Malware og beskyttelse imod
- Windows Update
- Mail - sikkerhed
- Hackning – skript kiddies - web
- Kryptering
- Hvorledes ”gemmer man sig”
- Diverse og afslutning



Trusselsvurdering
Center for Cybersikkerhed

- Hvem er Center for Cybersikkerhed
- Hvilke opgaver løser CFC
- Hvorledes er samspillet CFC, PET og Politi
- Hvad vedrører det dig ? Er det ikke kun virksomheder og offentlige myndigheder
- Nej – nej og atter nej – dét vedrører os alle der har IT-teknologi (PC, Tablets, mobiltelefoner, hjemmenetværk.
- Vi er alle menneskelige ”FireWall” mod truslen fra Informationsteknologien.
- https://fe-ddis.dk/CFCS/Pages/cfcs.aspx



Aktuel trusselsvurdering

Hovedvurdering – maj 2018

- Truslen fra cyberspionage er MEGET HØJ. Truslen er især rettet mod danske myndigheder, som har oplysninger, der er strategisk, politisk eller økonomisk værdifulde for fremmede stater. Visse stater udfører også cyberspionage mod danske virksomheder. Stater gør generelt mere for at skjule deres cyberspionage.

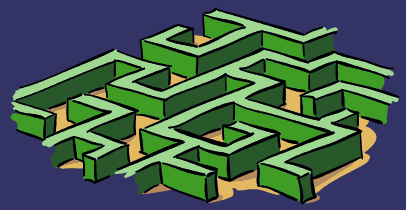
- Truslen fra cyberkriminalitet er MEGET HØJ. Cyberkriminalitet er et globalt fænomen, der også rammer danske myndigheder, virksomheder og borgere. Der er særligt en betydelig trussel fra cyberkriminalitet, der sigter mod at afpresse penge fra myndigheder, virksomheder og **borgere**. Der er cyberkriminelle netværk, der arbejder organiseret og langsigtet, og statsstøttede hackere står sandsynligvis også bag cyberkriminalitet.

- Truslen fra cyberaktsme er MIDDEL. Cyberaktivister retter sjældent fokus på danske myndigheder og virksomheder. Nogle hackergrupper og individer i cyberaktivistiske netværk har dog væsentlige evner og ressourcer til at udføre cyberangreb. Det er sandsynligt, at stater også anvender visse cyberaktivistiske grupper som dække i forsøg på at påvirke meningsdannelsen i andre lande.

- Truslen fra cyberterror er LAV. Militante ekstremister har begrænsede evner og ressourcer til at udføre alvorlige cyberangreb. Selv om de i få tilfælde har ytret interesse for at udføre cyberterror, har de aktuelt ikke kapacitet til dette. • Visse stater bruger cyberangreb til at styrke deres magtposition. Det gælder bl.a. anvendelsen af destruktive cyberangreb og hack og læk af politisk følsomt materiale. Danske virksomheder og organisationer er udsat for en større risiko for destruktive cyberangreb, hvis de er til stede i visse konfliktområder.

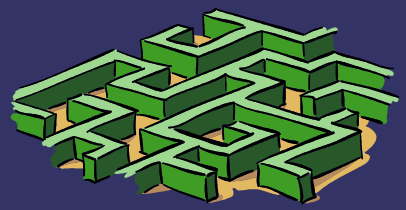
Password
Sikkerhed og beskyttelse

- Password bruger vi alle – og vi har mange.....
- For år tilbage var det anbefalet at password skulle indeholde 8 karakterer – men i dag anbefales det at have 12 karakterer p.g.a. passwords"knækkere" er blevet dygtigere og hastigheden på maskiner er forøget.
- Password – min. 12 karakterer og skal indeholde store og små bogstaver – tal og special tegn og bedst hvis ingen af delene optræde mere end én gang.
- Password skrives ikke ned
- Password må/bør ikke udveksles elektronisk eller via telefon.
- Der findes applikationer som kan opbevare password – vær dog skeptisk.....
- En god måde at danne og gemme password..... vises på tavlen



Password
Sikkerhed og beskyttelse

- Password bruger vi alle – og vi har mange.....
- For år tilbage var det anbefalet at password skulle indeholde 8 karakterer – men i dag anbefales det at have 12 karakterer p.g.a. passwords"knækkere" er blevet dygtigere og hastigheden på maskiner er forøget.
- Password – min. 12 karakterer og skal indeholde store og små bogstaver – tal og special tegn og bedst hvis ingen af delene optræde mere end én gang.
- Password skrives ikke ned
- Password må/bør ikke udveksles elektronisk eller via telefon.
- Der findes applikationer som kan opbevare password – vær skeptisk.....
- En god måde at danne og gemme password..... vises på tavlen

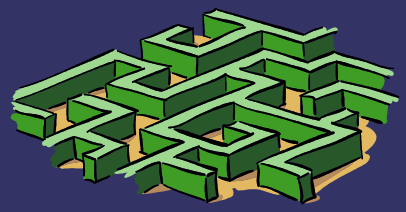


Sikker password

- Sikre password – kan godt skrives ned
- Jehjhbpme20p
- 1951 16 ! [Nøglen]
- Knmkbpme36p?
-
- abcdefghijklmnopqrstuvxyzæøå
- mnopqrstuvxyzæøåabcdefghijkl
- xmåaæxp [lars ole]

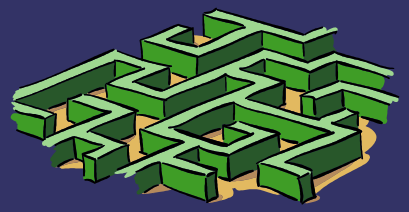
Virus/Malware og Beskyttelse imod

- Beskyttelse mod Virus og Malware er et MUST og kan ikke undervurderes.
- Brug altid anerkendte applikationer hertil – stol ikke blot og alene på Windows10 beskyttelsesforanstaltninger.
- Mange internetudbydere tilbyder gratis eller billige sikkerhedspakker med anti Virus og Malware f.eks. YouSee og andre
- Bl.a. Norton Internet Security og andre – koster penge, men er alle gode og effektive produkter
- Der er jævnligt ”tilbud” på Norton Internet Security ca. 250 kr. for beskyttelse i 18 mdr.
- Skulle man blive ramt af virus/malware har de fleste købeprodukter egenskaber til at kunne rense ud i virus.



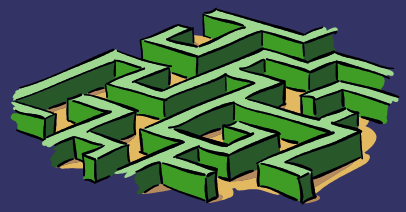
Windows Update

- Microsoft udgiver som regel én gang om måneden – første tirsdag
- Der sker ind imellem updateringer uden for perioden – f.eks. hvis der opdage såbarheder.
- Installer altid de sidste opdateringer – check jævnligt om der ”ligger” opdateringe.
- Pas dog på hvis du får mail som angiver at du skal opdatere – microsoft sender ikke mail om dette – det er spam/fake



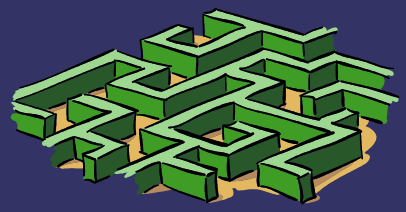
Windows Update

- Microsoft udgiver som regel én gang om måneden – første tirsdag
- Der sker ind imellem updateringer uden for perioden – f.eks. hvis der opdage såbarheder.
- Installer altid de sidste opdateringer – check jævnligt om der ”ligger” opdateringe.
- Pas dog på hvis du får mail som angiver at du skal opdatere – Microsoft sender ikke mail om dette – det er spam/fake



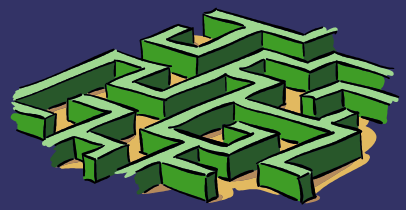
Mail sikkerhed

- Mail bruger vi alle – men pas på.....
- Password til mail-konto – husk sikkerhed
- Vi får alle spammail som forsøger at lokke ting ud af os – f.eks. password og/eller bankkonto oplysninger.
- Vær meget omhyggelig og skeptisk med at klikke på links i mail – se altid efter hvorhen de peger – hvis det er noget du ikke kender eller se mistænkelig ud – spørg en 'ven' f.eks. google - eller SLET direkte.
- Se mit eksempel …….....
- Pas også godt på når du læser mail på telefon
- Pas på ”Shoulder surfing” i offentlig rum
- Pas på offentlige Pcére – biblioteker m.v.



Hackning – skript kiddies - web

- Største trussel fra hackning mod dig og mig – er usikre websider og vores hjemme routere og tilkoblet udstyr.
- Keyboard loggere – stjæler dine oplysninger fra f.eks. net-bank, e-boks, borger.dk
- Altid aktiveret FireWall på routere – altid sikker password på administration af routere – hold øje med loggen
- Altid sikker password på udstyr – videoovervågning, NAS. Udstyr som skal være tilgængelig udefra skal lægges på et DMZ
- Pas på med eksterne TeamViewers eller lign. overtagelse af Desktop - kør aldrig uovervåget.



Kryptering

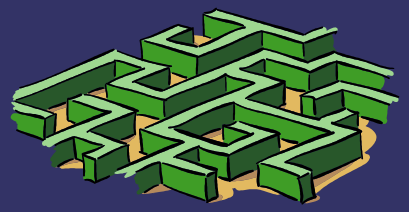
- Den beste mulighed for at holde ting hemmelige er KRYPTERING
- PGP er et af de bedste applikationer til at kryptere – PGP kan fås som Freeware (openPGP) https://www.openpgp.org
- En mulighed er også at anvende ZIP som også er i stand til at kryptere (WinZip) www.Winzip.com
- Kryptering er også mulig bl.a. outlook og gmail.
- Kryptering af HardDisk, USB og USB-diske

Kryptering

- Den beste mulighed for at holde ting hemmelige er KRYPTERING
- PGP er et af de bedste applikationer til at kryptere – PGP kan fås som Freeware (openPGP) https://www.openpgp.org
- En mulighed er også at anvende ZIP som også er i stand til at kryptere (WinZip) www.Winzip.com
- Kryptering er også mulig bl.a. outlook og gmail.
- Kryptering af HardDisk, USB og USB-diske

Hvorledes gemmer man sig....

- Et eksempel vises !
- ALT255
- Direktories >256 niveauer
- Steganography
- http://quickcrypto.com/free-steganography-softw
- Kryptering af HardDisk, USB og USB-diske.
- BiosPassword



Drøftelser, spørgsmål, afslutning

- 1. april 2017 Persondataforordning GDPR
- Alle GDPR-reglerne er vigtige, men her er der 5, som du skal være særligt opmærksom på. Din organisation/forening skal
-
- Føre en fortegnelse.
- Dokumentere at lovgivningens principper for god databehandling efterleves.
- Dokumentere at organisationen har indført passende tekniske og organisatoriske foranstaltninger.
- Oplyse kunder og ansatte om hvordan deres data behandles.
- Bevise, at organisationen efterlever lovgivningen fx hvis der anvendes samtykke, databehandlere, mv.