Slides med info til it-sikkerhed

Passwords

Lav stærke kodeord:

- **Langt** – Mindst 12 tegn
- **Unikt** – brug ikke det samme kodeord flere steder
- **Kombineret** – brug symboler, tal samt store og små bogstaver
- **Dit og kun dit** – del ikke dit kodeord med andre

Kodeordet må gerne være nemt at huske

- I2018spistejegmangeis!
- **P**iraten**E**r**R**2D2? (Per)

Beregningsopgave omkring passwords

Hastigheder (forudsætninger)

- En normal computer 100.000 passwords i sekundet
- En (lille) supercomputer 1.000.000.000 passwords i sekundet
- Den hurtigste computer på jorden: 76.000.000.000 passwords i sekundet

Udregn hvor lang tid det tager at bryde følgende passwords:

- **Passwords kun af tal på 8 karakterer**
- **Passwords kun af bogstaver (26 forsk.)**
- **Passwords af store og små bogstaver (52 forsk.)**
- **Passwords af store, små og tal (62 forsk.)**
- **Passwords af store, små, tal og symboler (96 forsk.)**

Beregningsopgave - løsning

Udregn hvor lang tid det tager at bryde følgende passwords:

- **Passwords kun af tal på 8 karakterer:**
  100.000.000 muligheder 10^8 => knækkes på 17 min på en pc og øjeblikkeligt på en supercomputer
- **Passwords kun af bogstaver (26 forsk.):**
  200 mia muligheder 26^8 => knækkes på 24 dage på en pc og på 3 ½ minut på en supercomputer
- **Passwords af store og små bogstaver (52 forsk.):**
  53 billioner muligheder 52^8 => knækkes på 17 år på en pc og på 15 timer på en supercomputer
- **Passwords af store, små og tal (62 forsk.):**
  218 billioner muligheder 62^8 => 70 år på PC og 60 timer på supercomputer
- **Passwords af store, små, tal og symboler (96 forsk.**):
  7,2 trillioner muligheder 96^8 => 2200 år på pc og 84 dage på supercomputer – 26 timer på verdens hurtigste computer

Personlige oplysninger

Personoplysninger:

Fx navn, adresse, fødselsdato, eksamen, sygedage, familieforhold, synlige skader

Eks. ”Lasse har brækket benet og skal derfor ikke være med til idræt”

Du må kun videregive personoplysninger og følsomme personoplysninger til dem, de er relevante for. De skal deles via sikre, krypterede kanaler, fx e-boks.

Følsomme oplysninger

Følsomme personoplysninger:

Fx sociale problemer, race, poli0sk eller religiøs overbevisning, sygdomsforløb, diagnoser, seksualitet, fagforenings0lknytning, gene0ske data

Eks. ”Lasse har fået konstateret ADHD – I bedes være ekstra opmærksomme”

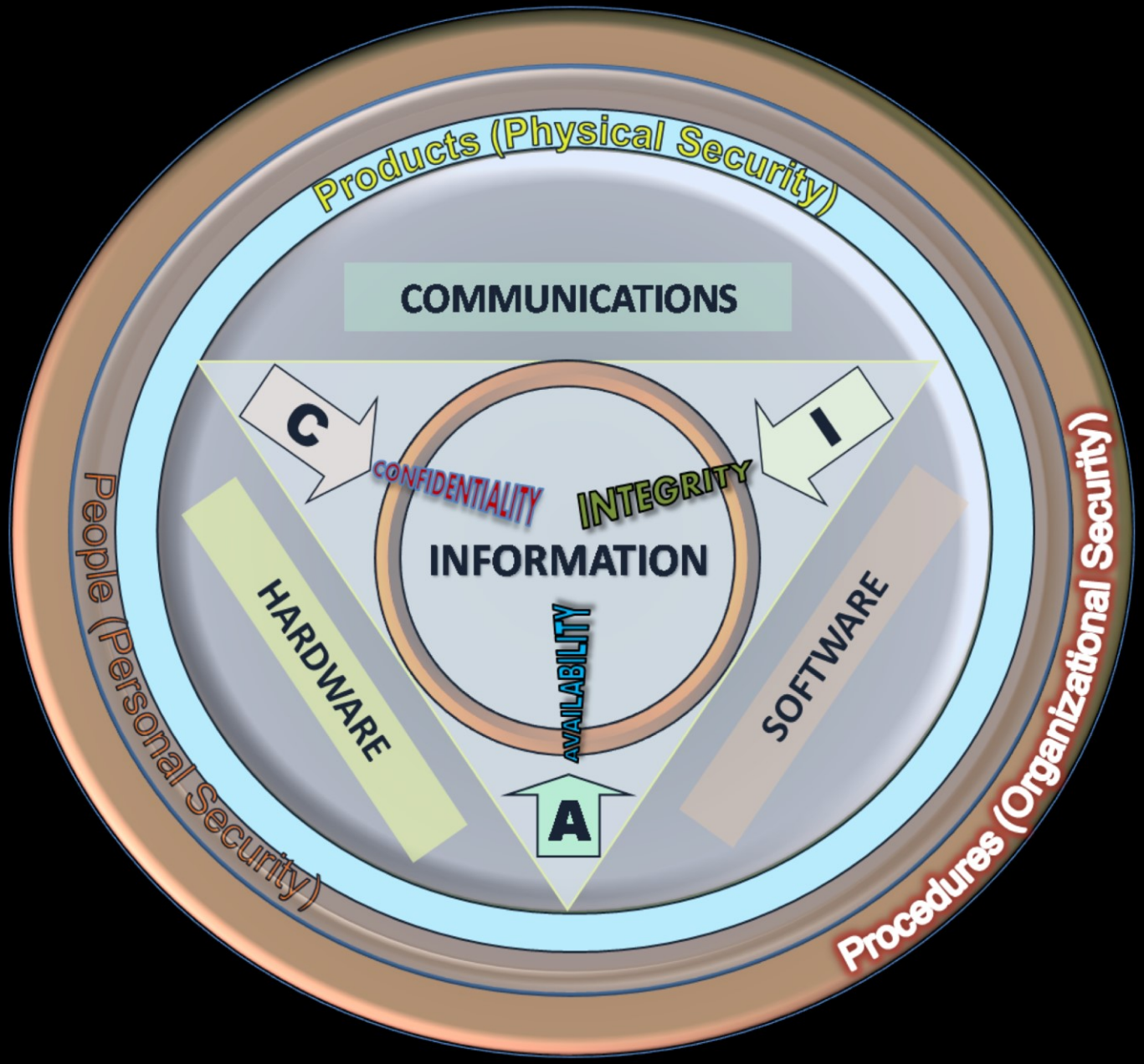
Du må kun videregive personoplysninger og følsomme personoplysninger 0l dem, de er relevante for. De skal deles via sikre, krypterede kanaler, fx e-boks.

IT-sikkerhed

Normalt skelner man mellem 3 overordnede typer af informationsbeskyttelse:

- *Fortrolighed*: Kun personer og systemer, der er autoriseret til at læse informationen, har adgang til informationen.
- *Integritet*: Kun personer og systemer, der er autoriseret til at ændre eller slette informationen, har adgang til informationen.
- *Tilgængelighed*: Alle personer og systemer, der er autoriseret til at læse og/eller ændre informationen, kan komme til det.

CIA modelle


Products (Physical Security)
COMMUNICATIONS
C
I
CONFIDENTIALITY
INTEGRITY
INFORMATION
HARDWARE
SOFTWARE
AVAILABILITY
A
People (Personal Security)
Procedures (Organizational Security)

CIA eksempel - Netbank

- Et banksystem beskytter en kundes konto, herunder hendes kreditkortnummer og saldo.
- *Fortrolighed* er, at kun kunden og hans bankrådgiver kender til kontooplysningerne – og ikke afslører det til tilfældige personer på gaden.
- *Integritet* er, at hendes saldo er "som den bør være": Saldoen bliver kun ændret, hvis hun sætter penge ind eller hæver penge på kontoen, og saldoen bliver i så fald opdateret korrekt.
- *Tilgængelighed* er, at hun kan hæve og indsætte penge – og på andre måder tilgå sin konto – når hun har ret til og brug for det.