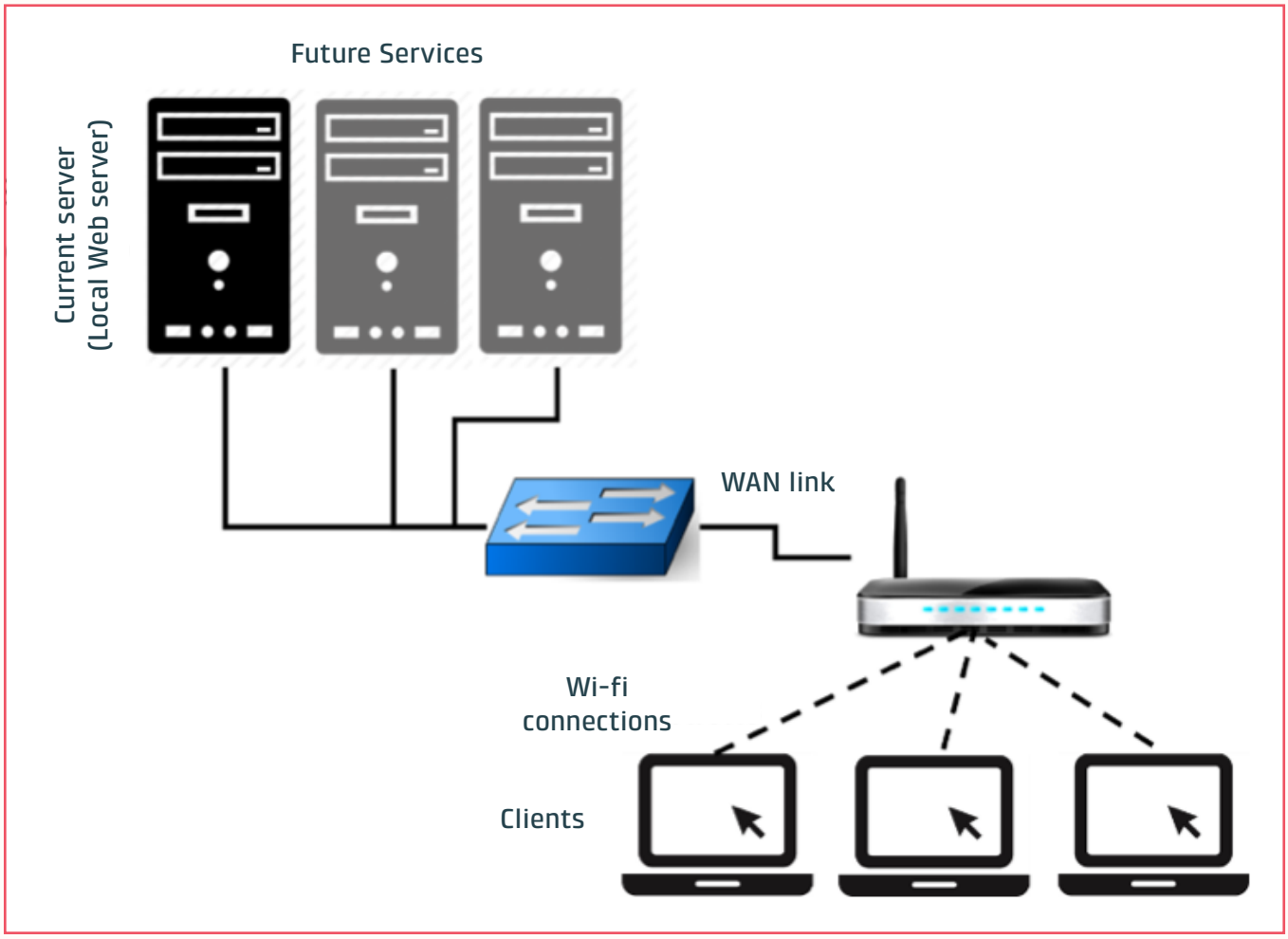
CYBERSIKKERHED



GRUNDEJERNES
INVESTERINGSFOND

CIU
Center for
it i undervisningen

TEKNOLOGISK
INSTITUT

CYBERSIKKERHED

Læsemål: Sikkerhed og Adfærd

I dette hæfte skal du lære om: Cybersikkerhed

Logisk sikkerhed · Fysisk sikkerhed · Dataangreb
Beskyttelse af virksomhedens data

Både som privatperson og som medarbejder behandler du data hver eneste dag.

For dig som ansat i en virksomhed er der med indførelsen af GDPR den 18. maj 2018 blevet strammet op omkring, hvordan du skal håndtere data. Derfor skal vi i dette kapitel bl.a. arbejde med emner som:

- Cybersikkerhed - håndtering af virksomheders, kunders og brugeres digitale data
- Erhvervsrettet brug af data - sammenhængen mellem Cybersikkerhed og lovgivning

Med andre ord skal dette kapitel klæde dig på til databehandling i dit fremtidige job.

Logisk sikkerhed

Login · Rettigheder · Logning

LOGIN

Adgang til pc'erne i netværket styres ved hjælp af login, hvor du indtaster brugernavn og adgangskode for at logge på netværket.

Det svageste led i sikkerheden er vores adgangskode. IT-afdelingen opstiller derfor ofte regler for adgangskoden fx:

- Hvor mange tegn adgangskoden skal bestå af
- Hvor ofte adgangskoden skal skiftes
- Hvor mange gange adgangskoden må tastes forkert

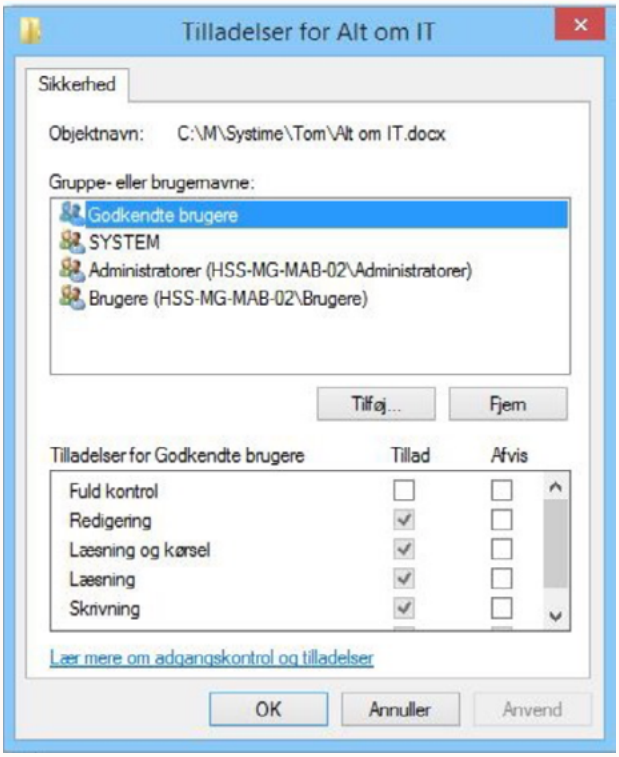
Det hjælper også på sikkerheden, hvis uvedkommende ikke kender brugernavnene på netværkets brugere.

RETTIGHEDER

Ud over login er det er en god idé kun at give brugerne de rettigheder, der er nødvendige for at udføre arbejdsopgaverne og ikke mere. For eksempel skal:

- En medarbejder i HR- afdelingen have adgang til lønsystemet, men ikke til salgsafdelingens kundesystem
- Ledelsen have de nødvendige informationer for at tage beslutninger, men har ikke nødvendigvis forstand på at overføre løn

Selv om medarbejderne i IT-afdelingen har adgang til alle virksomhedens informationsnetværk, bør de ikke kende brugernes adgangskoder.



GODE RÅD OM ADGANGSKODER

- Lær adgangskoden udenad
- Brug forskellige adgangskoder til forskellige enheder og systemer
- Skift adgangskoden med jævne mellemrum
- Brug en kombination af bogstaver og tal, men pas på med Æ, Ø, Å og andre mærkelige tegn
- Brug lange adgangskoder: Mindst 8 tegn og gerne 20 tegn – jo flere tegn, jo bedre
- Brug både store bogstaver, små bogstaver og tal
- Brug tilfældige tegn, som hverken helt eller delvist er rigtige ord
- Brug evt. en passwordmanager
- Slå to-faktor godkendelse til

RETTIGHEDER - FORTSAT

For ikke at miste data eller komme i konflikt med Persondataloven, skal der tildeles forskellige rettigheder til brugerne afhængig af deres myndighed og ansvar i virksomheden. Typisk inddeler virksomheden de ansatte, både ledere og medarbejdere, i grupper med de samme rettigheder: *READ*, *WRITE*, *EXECUTE*

Read: Adgang til at læse data
Write: Adgang til at ændre data
Execute: Adgang til at uploade eller slette data

Som du kan se i dette eksempel med en Word-fil, kan du selv bestemme, om andre skal have rettighed til ændre i dit dokument:
Eks. På rettigheder - er det her færdigskrevet?

LOGNING

Teknologien gør det muligt for virksomheden at registrere, hvad brugerne foretager sig på virksomhedens netværk. Dette kaldes logning og er en passiv form for sikkerhed.

Hvis der sker en fejl eller noget ulovligt, har virksomheden via logningen mulighed for at gå tilbage og se, hvad der er sket. Det svarer til at have et overvågningskamera i en butik, hvor videoen med overvågningen kun tages i brug i tilfælde af tyveri.

Fysisk sikkerhed

Beskyttelser af serverrum · Spejling · Strømsvigt

Virksomhedens informationsnetværk skal være funktionsdygtige for, at ledere og medarbejdere kan løse deres arbejdsopgaver. Fysisk sikkerhed handler om, hvordan virksomheden beskytter sit fysiske netværk mod:

- Tyveri
- Hærværk
- Brand
- Vand
- Røg
- Varme
- Strømsvigt

BESKYTTELSER AF SERVERRUM

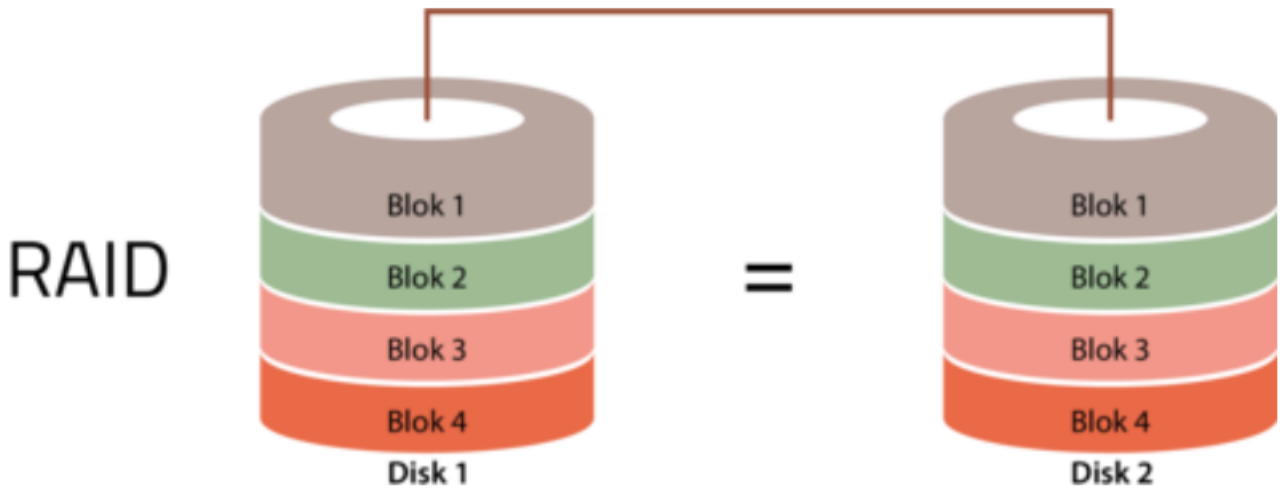
I et client/server-netværk afhænger alle virksomhedens aktiviteter af serveren. Serverrummet skal derfor være et af de bedst sikrede rum i virksomheden. Kun vedkommende medarbejdere må have adgang til serverrummet og skal kunne styre temperaturen i rummet. Virksomheden skal anskaffe sig særligt udstyr til brandslukning, der ikke skader IT-udstyr.

SPEJLING

IT-udstyr slides og går i stykker på de mest uheldige tidspunkter. Derfor installerer mange virksomheder ofte to enheder af hver slags hardware, især serverne som er livsnerven i virksomheden. Fx anvender mange virksomheder et RAID-system med to harddiske, hvor den ene harddisk er en spejling af den anden harddisk.

Dataene og ændringer i dataene bliver altså hele tiden gemt på begge harddiske på én gang. Det er meningen, at reserveenheden overtager opgaven, når et stykke IT-udstyr går i stykker, uden at brugerne oplever forsinkelser eller problemer.

Figur 01 RAID-system



STRØMSVIGT

Selv om vi i Danmark ikke oplever strømsvigt så tit, skal der tages forbehold for det alligevel. Når strømmen forsvinder, forsvinder dataene på skærmen (RAM-lageret), som ikke er gemt på harddisken. De fleste programmer kan indstilles til automatisk at tage en sikkerhedskopi. I Word kan man fx indstille programmet til at gemme sit dokument med et bestemt antal minutters mellemrum.

Nogle virksomheder fx sygehuse sikrer sig med en nødgenerator, der kan levere strøm, hvis den normale strømforsyning svigter. Der kan også ske uheld, hvor fx en ledning falder ud, hvis ikke den er skubbet ordentligt på plads. Derfor har mange virksomheder skruer eller clips til at sætte IT-kablerne ordentligt fast.

UPS (UNINTERRUPTIBLE POWER SUPPLY)

Virksomheden kan også vælge at benytte en UPS. UPS (Uninterruptible Power Supply) er et stort batteri, der automatisk slår til, hvis strømmen svigter.

UPS'en placeres mellem computeren og stikkontakten, og står typisk i server-rummet. Den har normalt strøm til at holde serverne i gang i ca. 10-15 minutter, hvilket burde være nok til at gemme data og tage de nødvendige backups. Hvis strømmen ikke vender tilbage til tiden, bruges den sidste strøm på UPS'en til at lukke serverne ordentligt ned.

Figur 02 UPS

Firewall

En firewall har mange funktioner. Fx skal den:

- Fungere som en brandmur mellem virksomhedens lokale netværk (LAN) og eksterne netværk fx internettet
- Kontrollere dataene, inden den afviser eller lader dem få adgang til virksomhedens netværk
- Hjælpe med at forhindre, at hackere eller skadelig software som fx virus og orme får adgang til virksomhedens netværk via internettet

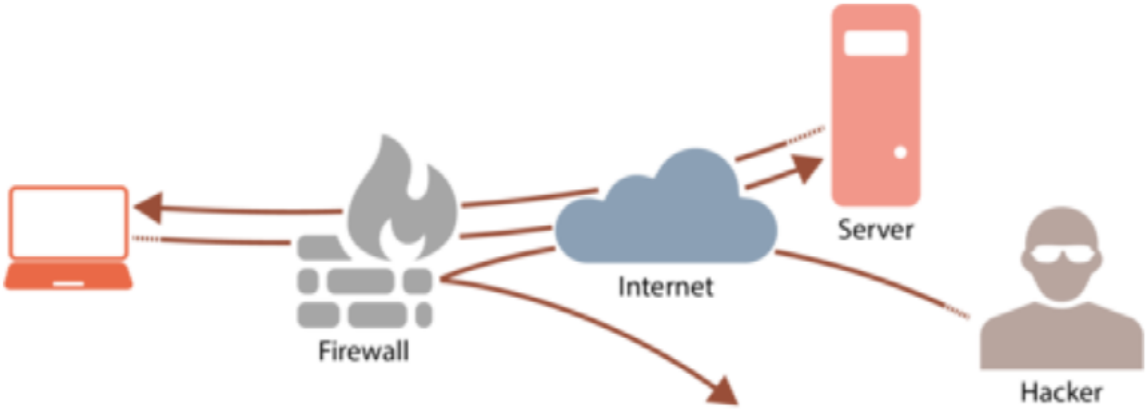
Firewall'en kan også stoppe din computer i at sende skadelig software til andre computere i virksomhedens netværk. Eller indstilles til at frasortere bestemte hjemmesider fx porno, Facebook, YouTube eller programfiler.

En firewall installeres på en af virksomhedens servere, og serveren er den eneste computer, der kan ses udefra. Derfor har virksomheder kun én IP-adresse, nemlig den til firewall-serveren.

Mange routere har en indbygget firewall, og der følger også en firewall med mange styresystemer fx Windows.

HUSK at en firewall ikke er det samme som et antivirus program!

Virksomheden skal have et antivirusprogram der beskytter den mod alle de trusler du har lært om i afsnittet Trusler fra nettet.



Figur 03 Firewall

Antivirusprogram

Et antivirusprogram er et program der forhindrer skadelig software i at komme ind på din pc / virksomhedens netværk.

De fleste antivirusprogrammer har en "realtime" beskyttelse mod vira og andre trusler, og en scanner som bruges til at afsløre og fjerne den skadelige software, som er kommet ind i computerne i virksomhedens netværk som bl.a.:

- Vira
- Orme
- Trojanske heste

Antivirusprogrammer fra fx AVG, Symantec og Norton arbejder med en liste af kendte vira og andre trusler, som den bruger til at sammenligne med computernes filer. Da der hele tiden kommer nye trusler til, er software-udviklere altid lidt bagud med at udvikle en kur imod den skadelige software. Derfor er det vigtigt altid at have et opdateret antivirusprogram.

I virksomheden bruger man typisk antivirus programmer på hver device der bliver centralt styret fra en server. Medarbejderne kan ikke selv ændre på indstillingerne.

VIRUS

En virus er et program, der prøver at overføre kopier af sig selv til andre computere, uden at brugeren opdager det.

ER ANTIVIRUS STADIG NØDVENDIG TIL WINDOWS?

Windows 10 er på mange måder en stor opgradering i forhold til de forrige versioner af Windows styresystemet.

Det kommer nu med en god indbygget beskyttelse mod malware og virus i form af programmet Windows Defender Antivirus. Det scanner systemet løbende og kan også foretage løbende sikkerhedsovervågning af brugerens aktivitet på nettet, ligesom andre kendt antivirus programmer. Så på din egen Windows pc behøver ikke egentlig betale for et tredjepartsprogram. Det er dog en god ide også at have et anti malware program.

KUN ÉT ANTIVIRUSPROGRAM

Det er meget vigtigt, at du ikke anvender flere antivirusprogrammer samtidig. Fordi programmerne arbejder på nogenlunde samme måde vil de skabe konflikter med hinanden.

VPN FORBINDELSE

En VPN-forbindelse giver mulighed for, at medarbejdere hjemmefra kan få adgang til virksomhedens harddisk og ERP-systerm på en sikker måde.

At logge sig på sin pc derhjemme via en VPN-forbindelse svarer til at logge sig på en computer i virksomhedens netværk på arbejdspladsen. Det vil sige, at du på din pc derhjemme har adgang til nøjagtig de samme drev og IT-systemer, som hvis du sad på arbejdspladsen. Hvis du bruger VPN-forbindelsen til at logge på virksomhedens netværk hjemmefra, kan du ikke være på internettet på samme tid.

VPN

VPN står for Virtual Private Network, og er en sikker privat punkt-til-punkt tunnel fra medarbejderens pc til virksomhedens informationsnetværk gennem et offentligt netværk fx internettet.

Kryptering

Hvis du køber noget i en webshop, bliver oplysningerne om betalingen med kort fx din adresse, dit telefonnummer og dit kreditkortnummer krypteret for at øge beskyttelsen af disse data.

Desuden skifter de fleste websider fra protokollen http til protokollen https. Kryptering beskytter altså os almindelige forbrugere ved betaling via internettet.

Ligesom vi som privatpersoner gerne vil beskytte vores data, er virksomhederne heller ikke interesserede i, at deres data falder i de forkerte hænder. Derfor krypterer virksomhederne også deres data fx:

- Strategiplaner
- Regnskaber
- Personaledata

Så de ikke kan læses af andre end de ansatte i virksomheden. Kryptering er især vigtigt, hvis virksomheden:

- Vil beskytte sine data ved lagring i skyen hos en ekstern udbyder af lagerplads
- Gør brug af VPN- forbindelser eller trådløse netværk

Omvendt kan kriminelle og terror-organisationer også kryptere deres data, så politiets arbejdsopgaver bliver sværere at løse.

KRYPTERING

Kryptering er en matematisk teknik til kodning af data. Kryptering øger sikkerheden af en meddelelse eller en fil ved at kryptere indholdet, så det kun kan læses af den, der har den rigtige krypteringsnøgle.

Figur 04 Kryptering af digital post

Backup

Server · Cloud · Medier

Større mængder af data udfordrer den måde, man gemmer data på. Da man ikke kan forudse, hvor mange data der skal gemmes, vælger virksomhederne ofte cloud løsninger, som kan tilpasses efter behov.

Der er mange virksomheder som fx Athena og Global-Connect, der har servere til den daglig drift og backup. Fordelene ved at outsource IT-driften kan være:

- Fleksibel løsning
- Højere oppetid
- Større sikkerhed
- At virksomheden ikke skal beskæftige sig med IT

Video: *Sådan redes data ud af ødelagte harddiske*

SERVER

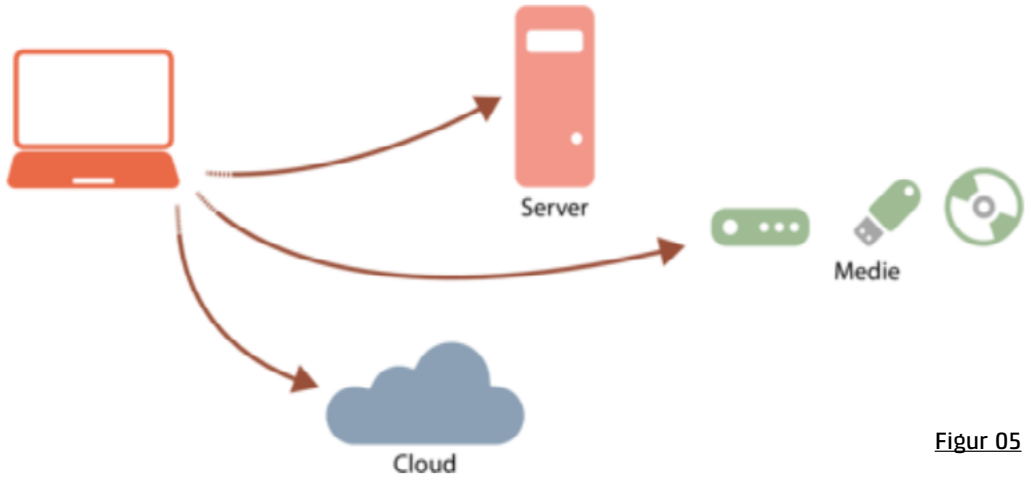
En af mulighederne for backup er en spejling af virksomhedens servere eller harddiske, hvor dataene i virksomhedens informationsnetværk er gemt.
Ved denne backup-løsning vil alle data stadig være i den samme bygning.

CLOUD

Virksomheden kan også vælge en cloud backup-løsning hos et datacenter, der udbyder lagerplads på deres store server-systemer. Det er en fleksibel løsning for virksomheden, for datacentret kan nemt ændre på den lagerplads, virksomheden har til rådighed hos dem.

Når data gemmes i skyen, er det vigtigt at kryptere virksomhedens data, inden de sendes ud af huset, så de er ulæselige for uvedkommende.

Virksomheden er ikke afhængig af datacentrets geografiske placering, men nogle lande kan være politisk ustabile eller oplever ofte naturkatastrofer, derfor er virksomheden nødt til at tage højde for, hvor i verden datacentret er placeret, hvis de vælge en backup-løsning i skyen.



Figur 05

MEDIER
Virksomheden kan også vælge at bruge medier fx et USB-stik, en DVD eller en ekstern harddisk. Kapaciteten er dog ikke så stor som server- og cloud-løsningen, derfor bruges medier kun til backup af de vigtigste data.

VPN
Der skal selvfølgelig være sammenhæng mellem virksomhedens behov for backup og prisen for back-up-løsningen. Ellers er det en dårlig forretning for virksomheden.

For dig som privatperson er det også vigtigt at tage backup. Ligesom en virksomhed skal du tage stilling til, hvordan du vil tage backup af de vigtigste data i din smartphone og pc. Der er mange muligheder for at tage backup, og alligevel er vi rigtige dårlige til at tage backup.

Forestil dig at:
- Du har brugt 6-8 timer på en afleveringsopgave
- Du tænder for din pc for at printe opgaven ud, men skærmen er helt sort, og din pc er fuldstændig død
- Du ikke har taget backup, så du er nødt til at lave hele opgaven om

Mega nederen ikk'? Så husk at tage backup af dine vigtigste data!

Medie	Kapacitet
USB	1 – 256 GB
DVD og Blu-ray disc	700 MB – 128 GB
Ekstern harddisk	120 GB – 6 TB
Tape streamer og bånd	200 – 15 TB
Server	I teorien er der ingen begrænsning
Cloud (i skyen)	I teorien er der ingen begrænsning

Figur 06 Medier og kapacitet