Eksamen Digital teknologi

Grafikk: Coursera, 2023a

Eksamen i Digital teknologi

Gokstad Akademiet

Cybersikkerhet

Vinter 2023

Innholdsfortegnelse

Innledning

Aldri før har det vært lettere å lagre sin personlige informasjon, og ikke minst sikkerhetskopiere viktige digitale hendelser. Bilder av barna da de var små, videoer fra eksotiske sommerferier, eller viktige dokumenter, er plutselig blitt til digitale spor med noen få tastetrykk på din digitale enhet. Slike datalagringstjenester er nå en del av vår digitale kultur, men hvordan kan disse skytjenestene virke så enkle og lett håndterlige? Når det egentlig ligger så mye teknologisk innovasjon og digital infrastruktur bak? Hvordan har digital teknologi som massive serverparker, milevis lange optiske fiberkabler og tusenvis av datamaskiner blitt en så viktig del av vår digitale kultur, så raskt?

Del 1 i denne eksamen vil omhandle viktige temaer nettopp innenfor digital teknologi. I oppgave 1 vil jeg beskrive forskjellen mellom digital teknologi og digitalisering, deretter forklare binære tall og hvordan disse representeres i en datamaskin. Så defineres begrepene bit og byte, hvor jeg deretter forklarer deres rolle i en datalagringssammenheng. Videre ser jeg på hvordan koding og ASCII kan brukes til å representere tekst i datamaskiner.

Oppgave 2 omhandler komponentenes samspill i en datamaskin, hvor jeg blant annet forklarer grunnleggende datamaskinoperasjoner. Videre presenterer jeg de viktigste faktorene som påvirker datamaskinens ytelse. Til slutt i denne oppgaven går jeg inn på driverens funksjon, og fremhever hvordan den bygger en bro mellom operativsystemet og maskinvaren i en datamaskin.

Oppgave 3 vil forklare hva virtualisering er og hvordan hypervisor type 1 og type 2 fungerer. Deretter vil jeg forklare forskjellen mellom en switch og en ruter i en nettverkssammenheng. Til slutt fremstiller jeg hva en brannmur er, og hvordan denne bidrar til nettverkssikkerhet.

I del 2 vil jeg gå i dybden på CIA-triaden og presentere eksempler på hendelser hvor konfidensialitet, integritet og tilgjengelighet ble kompromittert. Videre diskuterer jeg etiske utfordringer knyttet til bruk av digital teknologi og personvern, med eksempler både fra kunstig intelligens og cybersikkerhet. Til slutt presenterer jeg forslag til hvordan organisasjoner kan balansere informasjonssikkerhet og personvern, ved å jobbe etter GDPR og implementere ulike sikkerhetsmodeller.

Oppgave 1: digital teknologi

Forskjellen mellom digital teknologi og digitalisering

For å forstå forskjellen mellom digital teknologi og digitalisering, kan det være nyttig å definere data og informasjon. Eie (2020:156) har en relativt enkel definisjon på data, som passer fint inn i denne oppgaven: “data kan defineres som mengder med verdier og individuelle elementer av det som utgjør informasjon." Som regel samles inn store mengder data, for å kunne gi mening i form av informasjon. I denne sammenhengen kan vi da definere informasjon som mengden data som blir samlet inn for å kunne gi oss en mening og forståelse for hva vi har samlet inn. Data består av digitale signaler, og gir oss ikke noe særlig mening uten at vi klassifiserer den (Eie, 2020:156).

Bringer vi inn begrepet digital teknologi, betyr dette å bruke avansert teknologi for innsamling, lagring, analysering og deling av informasjon (Rahimi, 2023a). Dette kan være enkle eksempler som å bruke en smarttelefon til å surfe på nettet, helt opp til Big Data-analyser i store organisasjoner. Nye typer teknologier påvirker oss hele tiden, alt i fra kunstig intelligens som endrer måten vi bruker chatbots, til smarte enheter som kan snakke med hverandre og IoT (Internet of things) med sine smarte enheter tilkoblet Internett som gjør at vi kan smartlade bilen vår for å spare strøm.

Begrepet digitalisering derimot, kan vi forklare som prosessen med å konvertere informasjon, innhold eller data fra en analog (fysisk) form til en mer digital (elektronisk form). Informasjon blir i dette tilfellet representert som tall og symboler en datamaskin kan behandle og forstå. Et godt eksempel på dette er et digitalt bilde kontra et fysisk gammelt bilde, det digitale bildet blir lagret som en elektronisk fil og ikke som en fysisk fotoutskrift (Rahimi, 2023a).

Sagt på en litt annen måte benytter en digital teknologi i dag i et kommunikasjonsnettverk for håndtering og lagring av store mengder data. Digitalisering skjer først når digitalisert informasjon brukes til å forbedre eller forenkle forskjellige prosesser. Teknologi har blitt en integrert del av vårt samfunn og innehar stor makt over oss både privat og på jobb. Derfor bør det ikke komme som en overraskelse på oss at kompetanse innen digital sikkerhet er helt nødvendig (Windvik, 2020:22). Digital sikkerhet er et stort tema, og i denne oppgaven vil jeg omtale cybersikkerhet som “en tilstand med fravær av uønskede hendelser, frykt og fare"

(Windvik, 2020:22). Begrepet kan også benyttes som et tiltak for å forbedre en slik tilstand. I en perfekt verden ønsker man totalt fravær av uønskede hendelser, frykt og fare, samt redusere disse til et akseptabelt nivå. Sjeldent medfører et datainnbrudd noe fare for liv og helse, men gitt den økende mengden bruk av teknologier der ute, kan dette muligens endre seg dramatisk i fremtiden (Windvik, 2020:22).

Binære tall i datamaskiner

Utenfor datamaskinenes verden bruker vi titallsystemet, også betegnet som desimaltall, når vi snakker om tall. I dette systemet bruker vi ti ulike siffer eller symboler, rangert fra 0 til 9. I datamaskinens verden derimot, brukes et annet system som kalles for totallsystemet eller det binære tallsystemet. Her forstår vi tall på bare to måter, nemlig 0 og 1. Det vil si at alle operasjoner som involverer tall i digitale teknologier kan stå som en rekke av disse to tallene (Rahimi, 2023a).

Drar vi begrepet binært litt lenger kan en hevde at det finnes kun to mulige statuser, ja eller nei, av eller på. Datamaskiner inneholder flere trillioner av disse binære knappene om du vil, som alle indikerer statuser av eller på. Det finnes flere måter å representere en binær status, en av de kan vi hente fra programmering når vi snakker om verdien *boolean.* Disse verdiene er enten sanne eller falske, som eksempelet til Winnie (2016b) viser ved “å ha flere enn tre penner". Svaret på dette er enten sant eller usant. Binære tall har en sterk sammenheng med datalagring i datamaskiner, fordi alt av tekst, bilder, video og programmer representeres av binære tall. 0 og 1 i databehandling gjør det lettere for datakommunikasjon og gir en mer presis overføring samt mottak (Rahimi, 2023a).

Måten binære tall benyttes i sammenheng med datamaskiner kan for eksempel være lagring og kommunikasjon av informasjon ved å bruke statusene av eller på, lagringsenheter som kan endre og lagre binære statuser for å kunne få tilgang til de senere, eller et nettverk som kommuniserer ved hjelp av signaler som defineres ut ifra om de er av eller på. En binær status som involverer et signal, kalles for en bit (Winnie, 2016b). Dette vil jeg fokusere nærmere på i det neste avsnittet.

Bit, byte og deres roller i datalagring

Bit er den minste mengden av lagring som kan måles. Benytter man denne enheten, kan en bygge større og mer kompliserte representasjoner av informasjon. Enheten muliggjør også at vi kan ta helt hverdagslige ting vi gjenkjenner hver dag, og representere dem ved hjelp av en liten verdi som en bit er (Winnie, 2016a). I det binære tallsystemet kalles derfor den grunnleggende enheten for informasjon en bit, som er en forkortelse for *binary digit.* For å fremvise meningsfull informasjon kan en kombinere flere biter. 8 biter blir tradisjonelt sett brukt til å representere en enkelt bokstav. Dette gir 256 mulige kombinasjoner som igjen kalles for en *byte*, som ofte kan forkortes med en stor B (Rahimi, 2023a).

En byte er veldig vanlig å benytte som en målenhet for data, som vi faktisk bruker hver dag. Byte måles i kilobyte, megabyte, gigabyte og terabyte (Winnie, 2016a). Disse brukes i sammenheng med lagringsenheter, som for eksempel harddiskene HDD (hard disk drive) eller SSD (solid state drive). Mulig din egen datamaskin har en harddisk som kan lagre 1 terabyte med data? Da vil denne harddisken inneholde nesten ni millioner bits. Hver enkelt av disse bitsene holder en av eller på status, som igjen representerer en liten del av et større stykke informasjon. For eksempel et enkelt nummer, en type tekst vi kaller for *string*, et dokument, et bilde, en sang, en film eller et dataprogram. Alle disse tingene vi bruker hver dag blir oversatt til bits som igjen blir lagret, overført, oversatt av datamaskiner og nettverk. Prosessen ved å ta kjente ting vi har i dag, og konverterer disse til binære tall, kalles for *encoding* (Winnie, 2016a). Dette skal jeg forklare nærmere i neste avsnitt.

Koding og ASCII som tekst i datamaskiner

Encoding på engelsk, som jeg heretter bare betegner som koding, kan som nevnt betegnes som prosessen med å konvertere informasjon eller data fra en form til en annen. Til eksempel kan dette være å konvertere menneskelig forståelig tekst over til en binær kode for lagring (Rahimi, 2023a). Det handler altså om å ta noe mennesker kan forstå, og konvertere disse ved hjelp av en spesifikk prosess til binære tall som igjen kan bli lagret, prosessert og overført til en datamaskin eller et nettverk. Snur du hele prosessen på hodet, og konverterer binære tall tilbake til informasjon som vi kan forstå som mennesker, kaller vi dette for de-koding (Winnie, 2016a). Her kan vi introdusere begrepet protokoll, som ofte kan betegnes som et sett med regler for

hvordan bits blir overført og definerer basisen for hvordan digital kommunikasjon fungerer (Winnie, 2016a).

Et eksempel som blir relevant for cybersikkerhet, kan for eksempel omhandle et personnummer eller en e-postadresse. Begge disse består av tall eller tegn, som igjen er kodet som strenger av binære tall. Uansett format kan det være lett å kopiere en slik form for identifikator. For ondsinnede er det også lett å benytte en kopiert identifikator. Er ikke sikkerheten på plass vil det da være lett å misbruke en slik kopiert identifikator, som igjen kan gi et grunnlag for økt fare for svindel (Køien, 2020:65).

ASCII er en tegnkodingsstandard, forkortet ned fra *American Standard Code for Information Interchange*. Den representerer ofte teksttegn med 7 eller 8 biter, hvor hvert enkelt tegn som for eksempel symboler, desimaltall eller bokstaver, har en unik binærkode i seg. Systemet følger en fastsatt tabell, som gjerne begynner med symbolet A, som blir det samme som desimaltallet 65 og det binære tallet 01000001 (Rahimi, 2023a). Siden mengden av karakterer og symboler har økt såpass mye med årene, finnes det nå en ny standard ved navn *Unicode* som benytter flere bytes til å representere denne økte mengden av symboler fra mange ulike språk rundt omkring i verden. Denne standarden spiller en nøkkelrolle slik at vi alle kan kommunisere hver dag ved hjelp av brev, symboler, glyfer og ikke minst representere disse i et digitalt format ved hjelp av binære bits. Også som en standard protokoll slik at hver enkelt datamaskin kan lese og forstå den (Winnie, 2016c).

Oppgave 2: komponentenes samspill i en datamaskin

Grunnleggende datamaskinoperasjoner

Skal vi forstå grunnleggende datamaskinoperasjoner, kan det være nyttig først og fremst å forstå en datamaskin som en elektronisk enhet. Denne enheten behandler, lagrer og sender ut informasjon ved hjelp av forhåndsprogrammerte instruksjoner, typisk i form av programvarer (Rahimi, 2023). Bill Nichols (1988:627) har en litt mer filosofisk og teknologisk deterministisk definisjon: “The computer is more than an object: it is also an icon and a metaphor that suggests new ways of thinking about ourselves and our environment.”

En datamaskin er bygget opp av de fysiske delene prosessoren ofte betegnet som en CPU (Central Processing Unit), lagringsenheter (HDD/SSD), minne (RAM), hovedkort og I/O-enheter (Coursera, 2023d). Programvare derimot kan vi betegne som et hvert virtuelt program som kjøres på datamaskinen. Dette kan inkludere for eksempel operativsystemet, programmer som Word eller Internett-nettlesere. I et bredt perspektiv kan vi skille mellom applikasjonsprogramvare og systemprogramvare. Datamaskinens maskinvare bestemmer for eksempel hvilke applikasjonsprogramvarer, for eksempel Word, som skal kjøres og hvor de skal kjøres i systemet. Systemprogramvare relateres og kjøres direkte mot maskinvaren, for eksempel drivere eller operativsystemer som Windows eller Mac (Coursera, 2023f).

Fire følgende funksjoner kan brukes til å beskrive en datamaskin: input, lagring, prosessering og output av ønsket informasjon. Handlingen, altså input, kan utføres av en rekke enheter for eksempel mus, tastatur eller skjerm. Et tastetrykk på tastaturet medfører at et signal blir konvertert og sendt bestående av binære tall til lagringsstasjonen på din datamaskin. I/O-enheter vil videre kommunisere med ulike programvarer i din maskin ved hjelp av ulike drivere. Her kommer også minnet inn i bildet, for når datamaskinen mottar en input lagres denne omgående i minnet. Som regel er minne klassifisert som enten flyktig eller ikke-flyktig, der RAM er flyktig fordi dataene lagres ikke permanent mens maskinen er i bruk. Ikke-flyktig minne kan være som en tilnærmet permanent lagringskapasitet for eksempel i en harddisk (Coursera 2023d).

CPU-en sørger videre for at dataene som har blitt lagret, prosesseres. Dette gjøres av de to delene i CPU-en, nemlig kontrollenheten og aritmetikkenheten. Selve kontrollenheten mottar instruksjonen, dekoder denne og sender deretter signalene videre basert på resultatet av dekodingen. Funksjoner som er hittil nevnt, omtales som tiden det tar å utføre et program. Aller siste steget kan vi forklare som det som faktisk vises på din datamaskin, altså selve outputen. Kort forklart aktiveres input-enheten gjerne av noe fysisk, menneskelig interaksjon konverteres så til digitale signaler som lagres i korttidsminnet, før det starter opp en prosess videre mot CPU-en, som til slutt vil generere en output (Coursera 2023d). Et godt menneskelig eksempel på dette er når vi bruker munnen til å kommunisere en tanke vi har fra hjernen vår. For en datamaskin, kan det være å programmere inn den ikoniske teksten *Hello World!* som printes ut i lesbar tekst på en digital skjerm.

Faktorer som påvirker datamaskinens ytelse

Tidligere i oppgaven nevnte jeg de viktigste delene en datamaskin er bygget opp av, altså selve prosessoren betegnet som en CPU (Central Processing Unit), minne (RAM), lagringsenheter (HDD/SSD), hovedkort og I/O-enheter (Coursera, 2023d). I denne delen vil jeg fokusere på enhetene CPU, RAM og lagringsmedium for å beskrive faktorer som påvirker datamaskinens ytelse.

Hvor rask og bra en CPU er, blir ofte målt etter hvor fort den kan gå, med andre ord hvor rask klokke-hastigheten er. Dette gjøres i betegnelsen gigahertz, og som regel kan en CPU bestå av opptil flere kjerner hvor disse kan utføre en oppgave sammen (Coursera 2023b). CPU-en er ikke lager for å kunne holde på minne, dette utføres av RAM-brikkene. Mengden RAM kan måles i gigabyte (GB) og sier noe om hvor mye en datamaskin klarer å prosessere på en gang.

En datamaskin er som et velsmurt maskineri. Begynner en komponent å svikte, kan dette påvirke ytelsen til de andre og datamaskinen blir tregere. For å få en lettere forståelse av de enkelte komponentene, kan en si at CPU-en hovedsakelig bestemmer programmenes og operativsystemenes hastighet. Desto mer RAM du har, desto flere oppgaver klarer datamaskinen å utføre samtidig. Lagringsmediet sin hovedoppgave er å lagre informasjonen, men spesielt en SSD vil også kunne påvirke ytelsen til en datamaskin og hvor raskt for eksempel et dataspill starter opp og flyter. Her er det ikke mengden lagringskapasitet som gjelder med tanke på ytelse, men hvor rask for eksempel lese- og skrivehastigheten er på harddisken.

Grafikkortet (GPU) står for den visuelle kraften, og behandler som regel de grafiske, synlige og visuelle oppgavene i en datamaskin. Hovedkortet er et kretskort som kobler alle enhetene sammen og som gjør at de kan kommunisere med hverandre (Rahimi, 2023b). Et solid hovedkort er viktig med tanke på ytelsen, fordi den bestemmer hvilke prosessorer, RAM-brikker, lagringsenheter og grafikkort som er mulig å koble til. Noen hovedkort støtter til og med avanserte prosessorer og overklokking for å få maksimal ytelse ut av datamaskinens enheter.

Driver: en bro mellom operativsystemet og maskinvaren

Som tidligere nevnt består en datamaskin av både programvare og maskinvare. En viktig enhet for at I/O-enheter skal fungere optimalt, er drivere som kommuniserer med denne programvaren

(Coursera 2023d). Vi kan betegne en driver som en spesialprogramvare, og uten denne vil ikke forskjellige enheter som mus, tastatur og skjerm fungere optimalt (Rahimi, 2023b). Har du ervervet deg en ny datamaskin eller oppgradert din nåværende med ny maskinvare, behøver du kanskje også å installere nye drivere. Dette kan være en manuell prosess, alt ettersom hvilken datamaskin eller ny maskinvare du skal installere. Likevel kan det være en automatisert prosess, for eksempel gjøres dette automatisk i Windows for mange ulike drivere.

Et godt eksempel på samspillet mellom operativsystemet, driveren og maskinvaren finner man innenfor gaming. Grafikkort byttes ut hyppig for å sikre mest mulig ytelse og konkurransefortrinn spesielt innenfor grafikk-krevende spill. Likeså må drivere oppdateres kontinuerlig, for å sikre optimal ytelse og eventuelle feil mellom spillet og det installerte grafikkortet patches.

For eksempel maskinvarer som PCI-, PCI-Express og generelt USB-enheter identifiserer seg i maskinen ved hjelp av *Vendor ID* som viser til produsentnavnet og *Device ID* som henviser til en spesiell maskinvaremodell. Dette gjør at enheten indentifiseres slik at operativsystemet klarer å koble seg mot den korrekte driveren (Bårdgård, 2021). Enheter du kobler til kommuniserer med BIOS under oppstart, som står for *Basic Input Output System* som vi kan betegne som maskinens startveileder (Rahimi, 2023b). Enhetene kommuniserer videre med operativsystemet, og enheter som kobles til mens maskinen er på blir hentet opp av egne prosesser og får en driver tilknyttet mens maskinen er i gang (Bårdgård, 2021). Slike identifikatorer er viktig innenfor cybersikkerhet, et tema jeg kommer tilbake til i dybdeemnet.

Oppgave 3: virtualisering og nettverk

Virtualisering og hypervisor

Virtualisering kan vi betegne som en type teknologi som kjører flere såkalte virtuelle maskiner (VM-er) på én fysisk maskin. Hver enkelt maskin fungerer da som en uavhengig datamaskin med sitt eget operativsystem og applikasjoner (Rahimi, 2023b). Dette tillater bedre utnyttelse av datamaskinressurser siden flere VM-er kan dele den samme fysiske maskinvaren uten å interferere med den andre. Virtualisering gir større fleksibilitet og skalerbarhet, noe som er veldig nytt for eksempel for en bedrift som raskt kan justere deres behov for datamaskinkraft.

Sikkerheten økes også fordi en kan isolere VM-er fra hverandre, som igjen minimerer risikoen for trusler som kan spre seg på tvers av systemer (Coursera, 2023g).

For å kunne styre og opprette VM-er, benytter man ofte en programvare som kalles for hypervisor. Dette muliggjør at flere operativsystemer kan kjøres samtidig på en enkelt maskin. En hypervisor lager en virtuell versjon av en fysisk ressurs, for eksempel virtuelle CPU-er, minne og lagringsplass. Som regel skilles det mellom to ulike hypervisorer, type 1 (ofte kalt *Bare-Metal Hypervisor*) kjøres direkte på den fysiske maskinen til vertssystemet og har ikke et behov for et underliggende operativsystem (Rahimi, 2023b). Type 1 brukes ofte i ulike datasenter og hos store bedrifter fordi disse gir økt sikkerhet og isolasjon enn type 2 hypervisors (Coursera, 2023g). Vanlige programvarer for type 1 er VMware eller Microsoft Hyper-V. Type 2 (ofte kalt *Hosted Hypervisor*) kjører mot eksisterende operativsystem, i motsetning til type 1. Noen vanlige programmer for denne typen er WMware Workstation eller Oracle VirtualBox (Rahimi, 2023b). Type 2 brukes ofte til skrivebordsvirtualisering, testmiljøer og personlig bruk. Og i denne typen er det lett å kjøre for eksempel Windows inne i Linux eller i Mac OS, eller vice versa (Coursera, 2023g).

Forskjellen mellom en switch og ruter i et nettverk

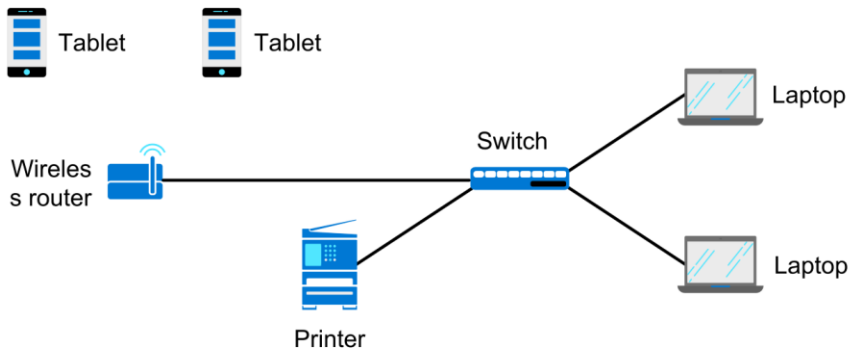
Sett med enkle øyner er en switch et teknologisk apparat som mottar signaler fra flere inngående linjer for deretter å sende disse videre på en eller flere utgående linjer etter egne bestemte regler (Rossen, 2023). Switchen gjør det mulig å koble flere ulike verter sammen, akkurat som en hub eller bro. Måten switchen er bygget opp på rent teknisk, gjør at den kan inspisere mottatt trafikk og deretter gjøre beslutninger for viderekobling. Sett i et nettverksperspektiv, vil en switch håndtere dataflyten ved å undersøke innkommende MAC-adresser og sende data videre til den påtenkte verten (Study-CCNA, 2023).

I et nettverk er det avgjørende at mange enheter kan kommunisere på samme tidspunkt, dette er switchen sin oppgave. I en hub tillates det å kun gi en fysisk enhet tilgang om gangen, mens i en switch gis hver datamaskin en dedikert ressurs som ikke er delt (Coursera, 2023c). Betegnelsen på en ruter derimot, kalles for en spesialisert datamaskin som har mulighet for å kontrollere forbindelsen mellom to eller flere nettverk. En av ruterens viktige oppgaver er å lese adressene til de ulike pakkene som passerer igjennom nettverket. Disse sjekkes så opp mot ferdiglagde

rutingtabeller og sender disse videre på sin rette vei (Liseter, 2023). Drar vi inn en metafor til å forenkle konseptet, brukes ruteren til å dirigere og navigere trafikk igjennom et nettverk. Den inneholder også ulike transport-teknologier, som kan være både kablede og trådløse tilkoblinger. Både ruter og switch er viktige enheter å beskytte i et nettverk, fordi datatrafikken som går igjennom de er svært utsatt for hacking. Uønskede personer bruker ofte ulike teknikker for å stjele til seg brukerdata, og dette kan for eksempel innebære data-manipulering, phishing, skadevare eller avlytting (Coursera, 2023h).

Dagens rutere er såpass moderniserte, at de av og til kan inneholde både en modem-del, ruter-del og ethernet-porter som kan oppføre seg lignende som en switch. For å forklare forskjellen nærmere, kan vi se på illustrasjonen nedenfor som viser et enkelt oppsett av et nettverk. I dette tilfellet består nettverket av en trådløs ruter, switch, kablet tilkoblet printer og totalt fire endepunkter (to tablets og to laptops). I dette tilfellet ville ikke nettbrettene kunne ha koblet seg opp mot det trådløse nettverket uten en ruter, og printeren vil ikke kunne kommunisert med resten av enhetene uten en kablet tilkobling til switchen.

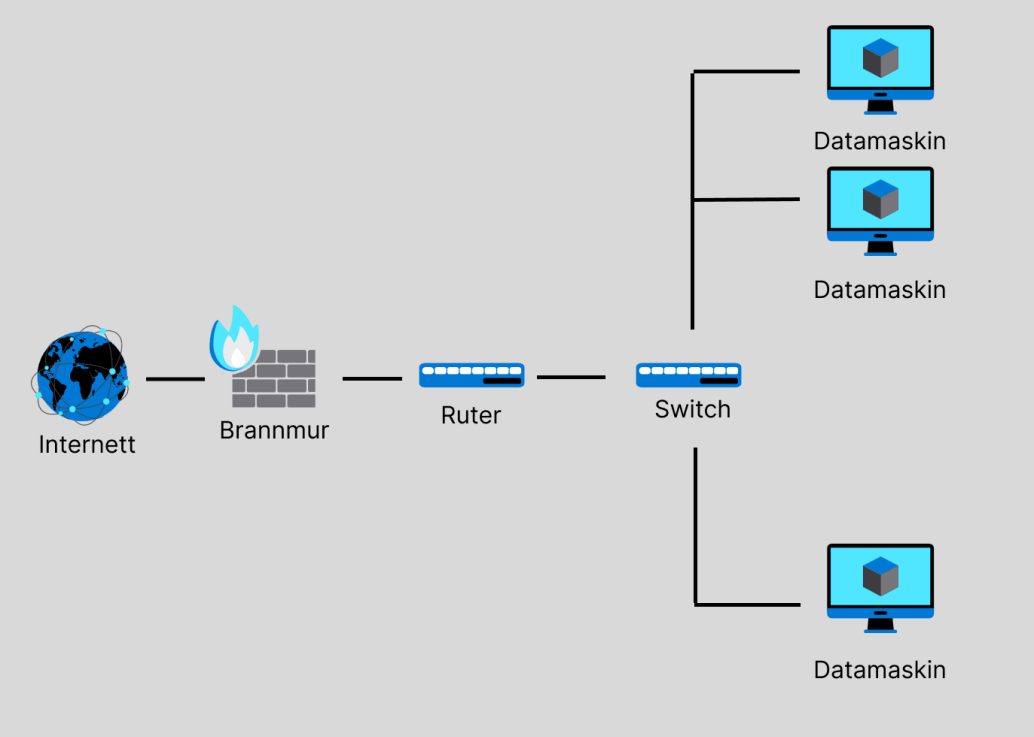
Fra bedrift til bedrift kan det være store variasjoner, men i dette tilfellet har bedriften valgt å kable datamaskinene og printeren, mens nettbrettene kommuniserer over Wi-Fi. I et sikkerhetsperspektiv ville en mulig løsning vært å ha printeren på eget nettverk, nettbrettene på sitt eget trådløse nettverk og la datamaskinene være kablet i et annet nettverk. Slik spres risiko og gjør det mye vanskeligere for potensielle hackere å flytte seg fra nettverk til nettverk, hvis de først skulle ha kommet seg inn.



Grafikk: (Coursera, 2023e)

Brannmur og nettverkssikkerhet

En essensiell og viktig del for å sikre et nettverk er en brannmur. Denne kan vi kalle for en sikkerhetsenhet, som ofte befinner seg mellom et godkjent nettverk og et ikke-godkjent nettverk til eksempel Internett (Coursera, 2023e). Drar vi med oss det enkle eksempelet fra forrige oppgaven, er brannmuren veldig viktig dersom vi skulle koblet et lokalt nettverk (LAN) til et mye større nettverk (WAN). Dette gjelder mange bedrifter som ønsker å skalere sin virksomhet, for eksempel å utvide nettverket sitt til et annet kontor i en annen by. Et annet eksempel er om det ene lokale kontoret skulle ønske å tilkoble seg Internett, som grafikken under viser.



Grafikk: (Haukeberg, 2023), laget i Figma.

En veloptimalisert brannmur bør plasseres foran nettverket, og bør kun åpne visse nødvendige nettverksporter. Dette kan være komplisert, for blokkerer man for mye nettverkstrafikk kan dette forstyrre produktiviteten i en bedrift. På denne måten reduseres andre aktørers mulighet til å kunne utnytte sårbarheter i tjeneren (Eie, 2020:149). Brannmuren fungerer som en beskyttende barriere mellom ulike trusler og aktørers mulighet for å komme seg inn på nettverket. Dette gjøres for eksempel ved å analysere all innkommende og utgående trafikk, og basert på denne analysen vil enheter enten gis tilgang eller ikke basert på pre-definerte sikkerhetsregler. Ideelt sett tillater brannmuren all legitim trafikk, mens den blokkerer all ondsinnet trafikk. I et standard oppsett blokkeres all innkommende trafikk og filtrerer utgående trafikk helt til administratorer konfigurerer hva som skal tillates og ikke. Brannmuren sjekker hver enkelt datapakke for å definere om visse tilstander er oppfylt, før trafikken får lov til å passere igjennom. Dette kan for eksempel være spesifikke IP-adresser, nettverksprotokoller, nettverksporter eller en kombinasjon av alle disse (Coursera, 2023e).

Dybdeemne 4: Informasjonssikkerhet

CIA-triaden

CIA-triaden er en informasjonssikkerhetsmodell ofte brukt i sammenhenger når man skal lage sikkerhetspolicyer. Modellen har en lang og rik bakgrunn, som strekker seg helt tilbake til 1998. Den lange historien er fordi modellen har sitt utspring i eldre scenarioer innenfor for eksempel filhåndtering, opptak og lagring. Triaden består av tre seksjoner, konfidensialitet (confidentiality), integritet (integrity) og tilgjengelighet (availability). Modellen skiller seg fra andre tradisjonelle modeller med individuelle seksjoner, CIA-triaden opererer heller som en kontinuerlig syklus. I enkelte tilfeller kan alle tre elementer overlappe hverandre, og dersom et element mangler vil de to andre elementene være ubrukelige. Har du en sikkerhetspolicy som ikke tar høyde for disse tre seksjonene, vil nok ikke dette være en særlig effektiv sikkerhetsløsning (TryHackMe, 2023). I de neste avsnittene vil jeg gå mer i dybden på disse tre elementene.

Konfidensialitet

Dette elementet handler om beskyttelsen av data fra uønsket tilgang og misbruk (TryHackMe, 2023). Windvik (2020:22) forbinder det mer som en hemmelighet underlagt en taushetsplikt når han diskuterer begrepet i sammenheng med informasjonssikkerhet. Målet er altså at informasjon ikke skal bli kjent for uvedkommende. Spionasje kan være et eksempel på ødelagt konfidensialitet, mens kryptografi brukes til å bidra å styrke konfidensialitet. For en bedrift handler det mye om å beskytte sine sensitive data lagret i sine systemer, sagt på en litt annen måte, å skape konfidensialitet handler om å beskytte data fra andre aktører de ikke er tiltenkt til (TryHackMe, 2023).

Et godt eksempel på et klart brudd på konfidensialitet, finner vi i Snowden-avsløringene. Edward Snowden, en amerikansk IT-tekniker, omtaler seg ofte som en selverklært «varsler». I mai 20213 valgte han å si opp jobben sin i etterretningsorganet National Security Agency (NSA) og publisere gradert informasjon om NSA (Blindheim og Strømman, 2013). Hans hovedfokus var å belyse utfordringene med etterretningsprogrammet PRISM, som avslørte et hemmelig samarbeid mellom NSA og store selskaper som Google, Yahoo, Apple, Facebook og Microsoft.

Samarbeidet handlet om hvordan NSA drev masseovervåkning av internasjonal tele- og datatrafikk (Greenwald, 2014:119).

Senere skulle det også vise seg at NSA ikke engang trengte direkte tilgang til disse selskapene sine servere, informasjonen ble regelrett bare hentet direkte ut fra selskapenes fiberoptiske kabler (Stavenes, 2013). Disse avsløringene la grunnlaget for en stor og verdensomspennende debatt rundt trusselen i massiv elektronisk overvåking, og ikke minst hvor viktig personvernet er i den digitale tidsalderen (Greenwald, 2014:10). Etterretningstjenestene skjulte seg bak frykten for terror, for å blant annet kunne samle data om privatpersoner. Likevel blir det et brudd på konfidensialitet hos privatpersoner, fordi vi har sverget vår tillit til disse gigantene og at de passer på at dataene ikke faller i feil hender.

Integritet

Elementet integritet i CIA-triaden handler om tilstanden hvor informasjon holdes korrekt og konsistent, med mindre autoriserte endringer blir gjort. Integriteten opprettholdes når informasjonen holder seg uforandret både under lagring, transport og at bruken ikke inneholder modifikasjoner av informasjonen. Sikkerhetstiltak bør være på plass i dette elementet også, spesielt for å sikre at data ikke kan bli endret eller modifisert av uautoriserte personer (TryHackMe, 2023). Teknikker som enveis hashing-algoritmer er med på å beskytte dataintegritet, som igjen vil generere et unikt fingeravtrykk av dataene som vil sikre at disse ikke har blitt tuklet med under transport (Coursera, 2023c).

Noen eksempler på brudd på sikkerhetsmålet integritet kan for eksempel være endringer eller tukling med kontrakter, e-poster og helseopplysninger innenfor en helseorganisasjon hvor helsedata krever utstrakt beskyttelse. Kanskje et av de mest imponerende dataangrepene i nyere historie, ifølge sikkerhetseksperter, er Stuxnet (Windvik 2020:22). Dette var en dataorm som ble laget for å angripe anlegget Natanz i Iran 2010. Denne skadevaren ble fraktet inn til anlegget ved hjelp av en minnepinne eller laptop. Målet var å spre seg til datamaskinene som styrte turbinene som hadde ansvar for å utvinne uran. Senere analyser av Stuxnet viste at flere lot seg imponere over hvor avansert den var laget og hvordan den kunne ødelegge disse turbinene. Det er vanskelig å si hvilke konsekvenser dette hadde for Iran, men en ting er sikkert, dette var et brudd

på deres integritet. Ikke bare hadde aktørene endret på dataprogrammene deres, men de hadde også forårsaket fysiske ødeleggelser (Windvik 2020:22).

Tilgjengelighet

Det siste elementet i CIA-triaden kalles for tilgjengelighet, som omhandler prinsippet hvis data skal være nyttig må det også være tilgjengelig for brukeren. Et viktig prinsipp i triaden er at informasjon må være tilgjengelig når autoriserte brukere har behov for tilgang til den (TryHackMe, 2023). Enkle eksempler på dette kan være et problem med innlogging i nettbanken din, eller at du får et virus som krypterer alle bildene på din datamaskin. Da kaller vi dette et brudd på sikkerhetsmålet tilgjengelighet. Sikkerhetstiltak som bidrar til å forsterke tilgjengelighet kan for eksempel være sikkerhetskopiering av informasjon og sørge for at en internettjeneste har tilstrekkelig båndbredde (Windvik 2020:23).

Det danske rederiet Maersk fikk i 2017 kryptert sine filer av et løsepengevirus. Angrepet var svært omfattende, og selskapet endte opp med et tap på over 200 millioner dollar. Viruset kom seg inn i systemene til Maersk via en ukrainsk programvareleverandør. Det interessante i denne saken var at oppdateringene fra leverandøren spredte viruset til Maersk (Windvik, 2020:22). Slike løsepengevirus kan være former for brudd på prinsippet om tilgjengelighet. Et annet eksempel er såkalte distribuerte tjenestenekt-angrep (Distributed Denial of Service, DDoS) ofte omtalt som DDoS-angrep. Tusenvis av datamaskiner eller servere vil da overbelaste offerets IT-systemer ved å drastisk øke trafikken. Disse angrepene skjer ofte, og det er mange virksomheter i Norge som har blitt utsatt for dette. Begge eksemplene kan være brudd på sikkerhetsmålet tilgjengelighet, fordi Maersk for eksempel ikke hadde tilgang til sine egne filer i en periode (Windvik, 2020:22).

CIA-triaden inneholder elementer for å kunne øke den digitale sikkerheten nettopp for å oppnå ønskede sikkerhetsmål. Dette kan for eksempel være kryptering av dokumenter på bedriftenes enheter for å sikre konfidensialitet, benytte seg av digitale signeringsmetoder for integritet og sikkerhetskopiere dokumenter for å bedre tilgjengeligheten for flere i bedriften (Windvik, 2020:22).

Etiske utfordringer ved bruk av digital teknologi

Etikk innenfor digital teknologi ligner i mange tilfeller på vanlig etikk, altså vi ønsker å ta en vurdering på hva som er rett, galt, redelig og rettferdig. På mange måter er etikkens formål å undersøke hvordan en bør handle korrekt, samt hvordan vi kan evaluere ulike handlinger og utfallet av handlingene. Innenfor utviklingen av ny teknologi kommer vi ikke utenom etikk ved bruk av digital teknologi og de etiske problemstillingene som følger. I enkelte tilfeller er det også vanlig å koble inn begrepet makt, fordi innføringen av ny teknologi endrer ofte på maktbalansen i et samfunn (Dalsaune, 2021).

Den digitale og teknologiske utviklingen i samfunnet vårt har naturlig nok en del med historien til digital etikk å gjøre. Etikk er på mange måter ikke noe nytt, men spesielt etikk innenfor digital teknologi er det mange likheter mellom gamle og nye etiske dilemmaer. Rundt 1960 ble dataprosessering normalisert, og "eldre" etiske dilemmaer som datasikkerhet, personvern og makt igjennom informasjon ble adressert. En kan hevde i dag at digital etikk innebærer en rekke "nye" dilemmaer som for eksempel tidligere nevnt, med Snowden-avsløringene og overvåking. Helt frem til dagens dato kan vi også finne eksempler innenfor bruk av automate våpen, søkemotorer, automatisert beslutningstaking eller menneskelig eksistensiell risiko fra kunstig intelligens (Müller, 2022).

Diskusjon rundt personvern under koronapandemien er et godt eksempel på en utfordring ved bruk av digital teknologi. Myndighetene ønsket å bruke en sporingsapplikasjon, som skulle gjøre det enklere å drive med smittesporing av innbyggere. Mange hevdet at appen var et klart brudd på vårt personvern, med en argumentasjon om at vårt samfunnsvern og beskyttelse mot sykdom skal vektes høyere enn vårt eget personvern. Organisasjoner opptatt av personvern, som for eksempel Amnesty International, var ikke enig i en slik beslutning. I dette tilfellet kan det være riktig at samfunnsvern skal vektes høyere enn personvern, dette for å forhindre dødsfall særlig blant utsatte grupper. Samtidig er det veldig viktig å ha en debatt om slike etiske problemstillinger, slik at premissene både blir veid for og imot.

Det finnes også eksempler på etiske dilemmaer i utviklingen av kunstig intelligens, fordi spesielt store språkmodeller som ChatGPT endrer måten vi jobber med informasjon på. Store og tunge tjenester innenfor AI krever enormt mye datakapasitet som igjen krever en del energi. Legger vi til et bærekraftperspektiv, kan en hevde at det er mer riktig å gjøre et enkelt Google-søk enn å

bruke en mer energikrevende ChatGPT. Store språkmodeller krever også en del manuelt arbeid fordi de trenger å språkvaskes for usanne og uhyggelige temaer. Dette gjøres ofte av arbeidere i u-land og timeprisen for en sånn type arbeid er ofte svært lavt.

Bruk av digital teknologi og cybersikkerhet er tett sammenknyttet, spesielt innen risikovurdering. I en slik digital-etisk evaluering er målet ofte å gjenkjenne og begrense risiko, samtidig som man søker å optimalisere og avdekke fordelene og potensialet innen teknologien. Det dreier seg ofte om å redusere forskjellige trusler, både når det gjelder misbruk og tapt potensiale (Bergsjø, 2020:54).

Vurderinger knyttet til digital etikk kan utføres parallelt med sikkerhetsvurderinger i en bedrift. Dette inkluderer muligheter som å identifisere potensielle risikofaktorer, implementere tiltak for risikoredusering og deretter gjennomføre en nøye evaluering. Bergsjø (2020) hevder at dette kan utrykkes som digital-etisk risiko i forholdet mellom verdi, trussel og sårbarhet. Modellen antyder at en reduksjon i en av faktorene vil føre til en nedgang i den samlede risikoen. Etikk kan også benyttes for å identifisere både interne og eksterne trusler i en organisasjon, og dette er kritisk for å kunne måle helheten i risikobildet til en virksomhet. Det kan være fornuftig å differensiere mellom digital sikkerhet spesielt rettet mot beskyttelse av verdier, for å gjøre etiske verdier kjent for alle, både internt og eksternt. På samme måte kan det være relevant å evaluere trusler mot organisasjonens verdier samt identifisere spesifikke sårbarheter som krever ekstra beskyttelse (Bergsjø, 2020).

Har en ambisjoner om å bli en etisk hacker, også kjent som penetrasjonstester, er dette et ypperlig eksempel på hvor etikk innen digital teknologi verdsettes høyt. I denne rollen vil du bli utfordret med oppgaver som å identifisere sikkerhetsfeil i programvare og konfigurasjoner i en organisasjons datasystemer (Jaatun, 2020:225). Suksess i en slik rolle avhenger i stor grad av din evne til å forstå forskjellen mellom rett og galt, samt integritet og uærlighet. Manglende evne til å håndtere slike moralske dilemmaer kan føre til en kort karriere, spesielt hvis du ikke klarer å motstå fristelsen av for eksempel å utnytte funnene du gjør til fordel for ondsinnede aktører.

Informasjonssikkerhet og personvern

Informasjonssikkerhet som begrep har flere likhetstrekk til CIA-triaden, nettopp fordi det handler om at informasjon ikke skal bli kjent for uvedkommende, at den ikke skal kunne bli endret utilsiktet og at den er tilgjengelig for autoriserte ved behov. Enkelt forklart består informasjonssikkerhet både av informasjon i IKT-systemer, men også om informasjon utenfor, som for eksempel viktige fysiske papirer som et pass (Gundersen, 2020:114). Begrepene informasjonssikkerhet og personvern har en tendens til å overlappe hverandre, men de har også ulike formål. Som tidligere nevnt handler informasjonssikkerhet mye om vern av typer informasjon når det gjelder brudd på konfidensialitet, integritet og tilgjengelighet. For eksempel forretningshemmeligheter, personopplysninger, finansielle opplysninger eller statshemmeligheter. Personvern derimot, handler mer om å beskytte personlig integritet når det kommer til behandling av opplysninger om oss, både autorisert og uautorisert (Gundersen, 2020:114).

Et etisk utfordrende eksempel på dette er for eksempel bedrifter som har aktivert loggsystemer i alle sine IT-systemer for å forhindre industrispionasje. I tillegg analyseres alle logger for å avdekke mistenkelig aktivitet. I en seksjon av denne automatiserte analysen, vil det være mulig å se når og hvor brukere logger seg inn, og om innloggingen skiller seg ut fra det vanlige innloggingsmønsteret til brukeren (Gundersen, 2020:114). Da kan det diskuteres om dette er lovlig og nødvendig, fordi dette er en behandling av personopplysninger. Lovlig og nødvendig kan tolkes dersom dette er et legitimt tiltak for å sikre virksomhetens verdier. Brukes disse opplysningene til å undersøke om de ansatte faktisk er på jobb når de skriver timer, vil dette fort bli et brudd på regelverket for personopplysninger. Dette er fordi det ikke er et nødvendig eller proporsjonalt tiltak å avdekke om ansatte jukser med timelister. Likevel er det ikke å anse som et informasjonssikkerhetsbrudd heller, siden informasjonen ikke er utlevert, endret eller slettet (Gundersen, 2020:114).

For å kunne balansere informasjonssikkerhet og personvernet kan organisasjoner benytte seg av prinsippene i personvernforordningen (GDPR). Denne sier at en virksomhet skal ta vare på persondata etter trusselbildet, gjeldende lovverk og tilgjengelig teknologi. Første prinsipp handler om at personopplysninger skal behandles lovlig, åpent og rettferdig. Bedrifter må behandle persondata korrekt og lovlig, privatpersoner skal kunne vite at det behandles

opplysninger som de og bruke sunn fornuft ved å behandle data rettferdig. Andre prinsippet er formålsberegning, altså at personopplysninger skal samles inn etter spesifikke og berettigede formål. Tredje prinsippet betyr at det kun skal samles inn opplysninger som strengt tatt kun er nødvendig for å nå formålet med behandlingen, også kalt for dataminimering. Har vi behov for å identifisere noen, kan det i mange tilfeller holde med kun navn og fødselsdato, ikke fødselsnummer (Gundersen, 2020:114).

Prinsipp nummer fire handler om at opplysninger skal behandles som både oppdaterte og korrekte data opp mot de formålene de behandles for. Dette er svært viktig for et helseforetak, da legen må kunne gi korrekt helsehjelp ut ifra en antagelse om at opplysningene om pasienten er korrekte. Femte prinsipp betegner varigheten på lagringen av data, når formålet er nådd skal opplysningene enten slettes eller anonymiseres. Prinsipp nummer seks fokuserer på integritet og fortrolighet, altså kjente begreper fra CIA-triaden hvor personopplysninger skal vernes mot tap av konfidensialitet, integritet og tilgjengelighet. Det siste prinsippet, nummer syv, beror på at den behandlingsansvarlige dokumenterer og overholder alle personvernsprinsippene (Gundersen, 2020:117).

Bygges det videre på elementene fra CIA-triaden kan organisasjoner sikre sin informasjon ved hjelp av et lagvis forsvar. For å sikre konfidensialitet kan brukernes passord beskyttes, bruke kryptering for ulike sensitive data og sikre innhold i e-poster. Bruke biometriske innloggingsmetoder, for eksempel fingeravtrykk, kan sikre integriteten i organisasjonenes systemer. For å sikre tilgjengelighet kan organisasjoner bygge inn mekanismer som failover-protokoller og ved å spre sine data og systemer over flere geografiske områder i for eksempel en sky-tjeneste (Coursera, 2023c).

Første laget i dette forsvaret handler om å beskytte data, som ofte er primærmålet til ondsinnede aktører. Her må organisasjoner sørge for at databaser, lagringsenheter, skylagring, SaaS-applikasjoner sikres etter regulatoriske krav. Det andre laget fokuserer på å sikre applikasjoner siden disse ofte kan gi tilgang til selve dataene. Selv når applikasjoner blir utviklet, bør en tenke sikkerhet og implementere tiltak helt fra starten av. Tredje laget handler om computering, altså å sikre virtuelle maskiner og endepunkter. Dette kan for eksempel være tilgangsstyring, endepunktsbeskyttelse og holde ulike systemer oppdaterte og patche når det kommer sikkerhetsoppdateringer (Coursera, 2023c).

Deretter kommer nettverkslaget, som naturlig nok fokuserer på nettverk hvor det kontrolleres og begrenser tilgang for å forhindre uautorisert adgang og muligheten til å forflytte seg via interne nettverk. Tilgangskontroll og nettverkssegmentering kan implementeres for å begrense kommunikasjonen til kun det som er nødvendig. Så har du permiter-laget hvor du skal beskytte nettverket ditt fra stor-skala angrep fra utsiden. Dette kan for eksempel være å implementere tiltak mot DDoS-angrep og benytte en brannmur som kan identifisere, mitigere og alarmere potensielle angrep (Coursera, 2023c).

Etter dette laget kommer laget for identitet og tilgang. Her styres tilgang til selve infrastrukturen og vil monitorere eventer og mulige endringer eller unormale forhold. Teknologier som SSO (single sign-on), for å redusere antall påloggінger og unike passord som kreves, eller MFA (multi-factor authtentication) som krever to eller flere former for autentisering, sikrer at kun autoriserte individer får tilgang til ønskede ressurser. Til slutt følger det fysiske laget, som omhandler å forhindre uvedkommende fysisk tilgang til organisasjonene sine systemer. Ved å implementere sikkerhet i flere lag og forsvar i dybden, kan organisasjoner signifikant øke deres motstand mot cyber-trusler (Coursera, 2023c).

En annen litt nyere sikkerhetsmodell er Zero Trust-modellen. Formålet med denne modellen er å alltid stille spørsmålet, hvem kan du egentlig stole på når det gjelder dine egne data? Denne nye måten å forholde seg til datasikkerhet på kan deles opp i tre prinsipper, hvor første prinsippet handler om å verifisere eksplisitt, for eksempel en ansatt i en bedrift bekrefter sin identitet uansett hva vedkommende skal gjøre (Coursera, 2023i). Det andre prinsippet er å bruke minst privilegert tilgang som betyr å begrense brukertilgang innenfor visse tidsrammer og gjennom nok retningslinjer for tilgang. Det kan for eksempel være å sette restriksjoner på hva som er behov for å bruke av systemer innenfor en gitt oppgave, som igjen vil redusere mulige innbrudd. Det siste prinsippet er å anta at et brudd har skjedd, altså å implementere en defensiv strategi ved å minimere angrepsområdet til organisasjonen, segmentere tilgang, verifisere ende til ende-kryptering og bruke analyser til å bedrive trusselbeskyttelse. I denne modellen inngår seks elementer som må sikres for å skape en god Zero Trust-modell, for organisasjoner som ønsker å implementere denne modellen gjelder dette identiteter, enheter, applikasjoner, data, infrastruktur og nettverk (Coursera, 2023i).

Avslutning

I denne oppgaven belyste jeg viktige temaer innenfor emnet digital teknologi, hvor jeg i oppgave 1 beskrev forskjellen mellom digital teknologi og digitalisering, forklarte binære tall i en datamaskin, definerte begrepene bit og byte, og til slutt presenterte hvordan koding og ASCII kan brukes til å representere tekst i datamaskiner. Oppgave 2 handlet om komponentenes samspill i en datamaskin, grunnleggende datamaskinoperasjoner, datamaskinens ytelse og til slutt hvordan driverens funksjon bygger en bro mellom maskinvaren og operativsystemet i en datamaskin. Måten datamaskinen fungerer på er svært fasinerende, for hvem blir vel ikke glad av å se teksten *Hello World!* printet ut i konsoll på en digital skjerm. En herlig symbiose hvor menneske møter datamaskin.

I oppgave 3 forklarte jeg hva virtualisering er, samt hvordan type 1 og type 2 hypervisor fungerer. Deretter forklarte jeg forskjellen på en switch og en ruter i en nettverkssammenheng. Til slutt fremstilte jeg hva en brannmur er, og hvordan denne bidrar til nettverkssikkerhet. I del 2 gikk jeg i dybden på CIA-triaden og presenterte eksempler på hendelser hvor konfidensialitet, integritet og tilgjengelighet ble kompromittert. Deretter diskuterte jeg etiske utfordringer knyttet til bruk av digital teknologi og personvern, med eksempler både fra kunstig intelligens og cybersikkerhet. Til slutt presenterte jeg forslag til hvordan organisasjoner kan balansere informasjonssikkerhet og personvern, ved å jobbe etter GDPR og implementere ulike sikkerhetsmodeller.

Dersom organisasjoner har en god forståelse og oversikt over GDPR, vil dette bidra til å implementere en balanse mellom personvern og digital sikkerhet. Et grunnleggende krav til digital sikkerhet handler om risikostyring, altså proporsjonal sikring av opplysninger. Både sikkerhetsloven og GDPR ønsker at opplysninger og systemer skal sikres i samsvar med de verdiene en organisasjon forvalter. Sikkerhetsloven fokuserer på et "forsvarlig sikkerhetsnivå", mens GDPR betegner dette som "egnet sikkerhetsnivå". Det kan være vanskelig å tolke begge disse, og hva som ligger i disse begrepene bør avgjøres av organisasjonen selv på bakgrunn av hvilke verdier som forvaltes og de truslene de står ovenfor (Gundersen, 2020:122).

Referanser

Bergsjø, L.O. (2020) *Sikkerhet i et digital-etisk perspektiv*, i Bergsjø, Håkon Windvik, Ronny Øverlier, Lasse (red.) Digital sikkerhet: en innføring. Oslo: Universitetsforlaget, side 54.

Bårdgård, T. (2021). *Drivere*. NDLA. Tilgjengelig fra: https://ndla.no/article/28031 Hentet 10.12.2023.

Blindheim, A.M. og Strømman, O. (2013) *Dette er Snowden-saken.* Dagbladet. Tilgjengelig fra: http://www.dagbladet.no/nyheter/dette-er-snowden-saken/61924440 Hentet: 12.12.17

Coursera (2023a) *Evolution of encryption.* Tilgjengelig fra: https://www.coursera.org/learn/cybersecurity-threat-vectors-and-mitigation/supplement/fRcax/evolution-of-encryption Hentet: 04.12.2023.

Coursera (2023b) W*hat is a computer and what is inside it?* Tilgjengelig fra: https://www.coursera.org/learn/introduction-to-computers-and-operating-systems-and-security/lecture/390nf/what-is-a-computer-and-what-is-inside-it Hentet: 09.12.2023.

Coursera (2023c) *Defense in depth.* Tilgjengelig fra: https://www.coursera.org/learn/cybersecurity-threat-vectors-and-mitigation/lecture/rGdsD/defense-in-depth Hentet: 08.12.2023.

Coursera (2023d) *How does a computer operate?* Tilgjengelig fra: https://www.coursera.org/learn/introduction-to-computers-and-operating-systems-and-security/lecture/dbpon/how-does-a-computer-operate Hentet: 09.12.2023.

Coursera (2023e) *Firewalls*. Tilgjengelig fra: https://www.coursera.org/learn/introduction-to-networking-and-cloud-computing/lecture/cYM9m/firewalls Hentet: 08.12.2023

Coursera (2023f) *Hardware versus software.* Tilgjengelig fra: https://www.coursera.org/learn/introduction-to-computers-and-operating-systems-and-security/supplement/6Fsxl/hardware-versus-software Hentet: 09.12.2023.

Coursera (2023g) *What is virtualization?.* Tilgjengelig fra: https://www.coursera.org/learn/introduction-to-networking-and-cloud-computing/lecture/D3kNz/what-is-virtualization Hentet: 12.10.2023

Coursera (2023h) *Physical and logical topology* Tilgjengelig fra: https://www.coursera.org/learn/introduction-to-networking-and-cloud-computing/supplement/uzQwS/physical-and-logical-topology Hentet: 12.12.2023.

Coursera (2023i) *Zero Trust Model.* Tilgjengelig fra: https://www.coursera.org/learn/cybersecurity-threat-vectors-and-mitigation/lecture/HFpTH/zero-trust-model Hentet: 15.12.2023.

Dalsaune, K.A. (2021) *Digital etikk.* Tilgjengelig fra: https://ndla.no/article-iframe/nb/urn:resource:6ada7fc5-9642-4675-9c93-c771b3baba9e/30237 Hentet: 13.12.2023

Eie, K.M. (2020) *Trusler og etterretning* i Bergsjø, Håkon Windvik, Ronny Øverlier, Lasse (red.) Digital sikkerhet: en innføring. Oslo: Universitetsforlaget, side 156.

Greenwald, Glenn (2014) *Overvåket. Edward Snowden, NSA og overvåkningsstaten.* Norsk utgave, oversatt av Eivind Lilleskjæret og Gunnar Nyquist. Oslo: Cappelen Damm.

Gundersen, Gullik (2020) *Lover og ansvar* i Bergsjø, Håkon Windvik, Ronny Øverlier, Lasse (red.) Digital sikkerhet: en innføring. Oslo: Universitetsforlaget, side 114.

Jaatun, M.G. (2020) *Programvaresikkerhet* i Bergsjø, Håkon Windvik, Ronny Øverlier, Lasse (red.) Digital sikkerhet: en innføring. Oslo: Universitetsforlaget, side 225.

Køien, G.M. (2020) *Identifikasjon, autentisering og aksesskontroll* i Bergsjø, Håkon Windvik, Ronny Øverlier, Lasse (red.) Digital sikkerhet: en innføring. Oslo: Universitetsforlaget, side 65.

Müller, V.C. (2022) *The history of digital ethics*, in Carissa Véliz (ed.), Oxford handbook of digital ethics. Oxford: Oxford University Press.

Nichols, Bill (1988) *The Work of Culture in the Age of Cybernetic Systems*, i Fruin, N.W. og Montfort, Nick (red.) The New Media Reader. Cambridge, Massachusetts: The MIT Press, side 627.

Rahimi, Fawad (2023a) *Innføring i Digital teknologi.* Tilgjengelig fra: https://gokstadakademietas.sharepoint.com/:b:/r/sites/23-25Cybersikkerhet-nett/Delte%20dokumenter/Emne%203%20-

%20Digital%20teknologi/UKE%2047/innf%C3%B8ring%20i%20digital%20teknologi.pdf?csf=1&web=1&e=bH3zPu Hentet 08.12.2023.

Rahimi, Fawad (2023b) *Grunnleggende om datamaskiner*. Tilgjengelig fra: https://gokstadakademietas.sharepoint.com/:b:/r/sites/23-25Cybersikkerhet-nett/Delte%20dokumenter/Emne%203%20-%20Digital%20teknologi/UKE%2047/Grunnleggende%20om%20datamaskiner.pdf?csf=1&web=1&e=FBiwWd Hentet 09.12.2023.

Rossen, Eirik (2023) *svitsj i Store norske leksikon på snl.no.* Tilgjengelig fra: https://snl.no/svitsj Hentet 12.12.2023.

Stavenes, Erik Grasaas (2013) *Et kaos av spionkabler*. Klassekampen, 1. november. Tilgjengelig fra: https://klassekampen.no/utgave/2013-11-01/et-kaos-av-spionkabler Hentet: 12.12.2023.

Study-CCNA (2023) *TCP/IP vs OSI Model.* Tilgjengelig fra: https://study-ccna.com/osi-tcp-ip-models/ Hentet: 12.12.2023.

TryHackMe og cmnatic (2023) *Principles of Security: The CIA-triad.* Tilgjengelig fra: https://tryhackme.com/room/principlesofsecurity Hentet 12.12.2023.

Liseter, Ivar M. (2023) *ruter - i datanettverk i Store norske leksikon på snl.no.* Tilgjengelig fra: https://snl.no/ruter_-_i_datanettverk Hentet 12.12.2023.

Windvik, Ronny. (2020) *Introduksjon til digital sikkerhet* i Bergsjø, Håkon Windvik, Ronny Øverlier, Lasse (red.) Digital sikkerhet: en innføring. Oslo: Universitetsforlaget, side 22.

Winnie, Doug (2016a) *Binary and bits.* Tilgjengelig fra: https://www.linkedin.com/learning/computer-science-principles-digital-information/binary-and-bits?resume=false&u=171076145 Hentet 09.12.2023.

Winnie, Doug (2016b) *Yes and no answers with binary*. Tilgjengelig fra: https://www.linkedin.com/learning/computer-science-principles-digital-information/binary-and-bits?resume=false&u=171076145 Hentet 09.12.2023.

Winnie, Doug (2016c) *ASCII and Unicode*. Tilgjengelig fra: https://www.linkedin.com/learning/computer-science-principles-digital-information/ascii-and-unicode?resume=false&u=171076145 Hentet 09.12.2023.