

Eksamen Informasjonssikkerhet:

Oppgave 1.

Hvis du ser på ordet 'informasjonssikkerhet', så sier det litt av seg selv. Det betyr å sikre informasjon. Med andre ord så betyr det at man skal passe på at ingen andre, enn de som skal ha informasjonen, får tak i den. Det er også viktig at informasjonen ikke blir endret på av hvem som helst. Men også at den er tilgjengelig til de som trenger informasjonen, til enhver tid.

Det er alt dette CIA står for:

C= Confidentiality (konfidensialitet)

I= Integrity (Integritet)

A=Availability (Tilgjengelighet)

Konfidensialitet i praksis er:

I hovedsak å beskytte dataene(informasjonen). For å beskytte dataene så kan man enten

1. kryptere de slik at ingen kan lese dataene uten å dekryptere de med en hemmelig nøkkel.
2. Ha adgangskontroll på dataen som gjør at man har regler og retningslinjer som gir tilgang til eks. rollen man har i ett selskap. Som er ganske likt som autentisering som er enten rollen du har, eller din identitet (dette er vanlig i nettbanken).

4. Eller ved autorisering som er å bestemme hvem som skal ha tilgang til dataene ut ifra retningslinjene, som er mer fysisk sikring. Som låser på dører, ha serverne med dataene lagret på i ett rom uten vindu og isolasjon mot radiobølger.

Med dette så beskytter man dataene fra alle andre enn de som skal ha tilgang eller fått tillatelse av å se eller ha noe med dataen å gjøre.

Integritet betyr at ingen andre enn de som har fått tilgang kan endre dataene.

Dette vil si at man bør ha backup av all data, som har periodisk arkivering.

Tilgjengelighet betyr at dataene (informasjonen) er tilgjengelig for alle som trenger den, og at man kan få tak i dataene raskt. Men bare de som har tilgang til å endre, kan endre (Jeg har brukt mine notater fra forelesning 1: Østby.B, personlig kommunikasjon, 09.januar 2023).

Oppgave 2.

Som privatperson så blir vi alle overvåket på nett, av store selskaper som Apple, Google, Facebook osv. Selv i nettleseren vi bruker, om det er Firefox, Chrome, Duckduckgo osv. så blir vi overvåket. Noe av det de overvåker er hva vi søker etter på nettet, hva vi liker av innlegg, hva vi deler på våre profiler, posisjonen vår, osv.

En av tingene som blir lagret er når man søker og planlegger f.eks. en ferie. Søket går kanskje utover for å finne ut av hvor man skal dra, og hvor mye det koster for familien. Oppbygningen av setningen blir analysert, for å forstå hvem som søker, og for å finne ut hvilke nettsider som svarer best på det du søker på. Denne informasjonen kan selskapet selge videre, eller ordne slik at du får rettet markedsføring direkte til deg. Som å sette reklame på til bud på reise i din feed på Facebook, Instagram eller kanskje Snapchat. Dette er gjør det vanskelig for privatpersoner å ikke gå på reklamen. De kan også lage en analyse over hvor mange som

bestiller ferie på første søk eller om det er noe forskjell på bestillinger på ulike årstider, og hvor det er mest vanlig at folk drar. Dette var eksempel på ferie.

Dette skjer med våre interesser også. Mange kvinner er interessert i sminke og velvære. Så når vi deler denne informasjonen på våre sosiale medier. Ved å se på sminke videoer, like innlegg, deler bilder at man er på spa. Denne informasjonen om at man bruker sminke og velværeprодукter, eller bare liker slike produkter, blir solgt videre slik at hver person får markedsrettet reklame for å tjene penger på brukerne sine. Med andre ord: *'Hvis du ikke betaler for ett produkt, da er du produktet'* av Østby.B 2023. (Jeg har brukt mine notater fra forelesning 3: Østby.B, personlig kommunikasjon, 23.januar 2023).

Det er større etiske spørsmål her som vi som samfunn ikke har kontroll på. Hvor mye overvåkning er for mye og hvor går grensen? Vi vet at under valgkampen i USA ble det solgt brukerdata fra Cambridge Analytica på omtrent 50 millioner brukere til valgkampanje der de kategoriserte brukerdata til å matche en psykologisk brukerprofil til potensielle velgere. Dette var gjort for å kunne bedre reklamere og dermed påvirke velgerne. Dette endrer helt dynamikken i hele det politiske spillet hvor man nå kan ved bruk av personlig brukerdata kan påvirke valg. Disse selskapene opererer i hovedsak mest i USA. Der bestemmes mye pga. Lobbyvirksomhet og penger fra disse selskapene går til politikere for at selskapene kan få mest mulig frihet til å gjøre det de ønsker. Dermed vil ikke dette bli løst, men kanskje det vil komme retningslinjer etter hvert (Detrow, S. 2018).

En annen overvåkning man ikke tenker over er gjennom Google maps eller Snapchat som bruker GPS på mobilen, som ofte er på. Da lagrer de til enhver tid hvor man har vært, og hvor man er, til all tid. Og ifølge NSB er det ni av ti nordmenn som bruker sosiale medier (Statistisk sentralbyrå, 1.mars 2023).

Det er ikke bare de store selskapene som ønsker informasjon fra privatpersoner. Det flere med mye skumlere baktanker enn reklame, og tjene penger på at man kjøper ting. Det er folk som ønsker å få tak i informasjon som epost som kanskje ikke har så sikkert passord. De bruker ofte informasjonen man har lagt ut på sosiale medier som bursdag, jubileum, første kjæledyr og kjæreste osv. Og basert på dette gjøre det enklere å «brute force» passord, ettersom mange lager passord med datoer og navn på kjæledyr eller kjærester. Dermed kan de fort finne ut passord man bruker, og ta over kontoer man har. Hvis de for eksempel får tak i passordet til Eposten så kan de ha tilgang til alle kontoer man har, til nettbutikker, sosiale medier, bilder og alt du har lagret på den kontoen. Det er skummelt å tenke på.

Det som er positivt i dette er at det gjør hverdagen vår enklere. Ved å bruke for eksempel Google maps og GPS. For personer som ikke har så god retningssans, eller unge som er ett sted for første gang, så kan man ta opp maps og finne veien til nærmeste buss, taxi, tog, legevakt, venner eller bare få adressen der man er for å få noen man kjenner til å hente. Denne teknologien gjør også sporing for politi og etterforskning lettere. Det gjør også det lettere for foreldre med å ha kontroll på sine barn. Med GPS så kan man se hvor barna er, og kan være trygge på at de er hos de vennene, eller kjente som man var enig om.

Nå som AI har kommet stort på banen til å søke om informasjon, så kan man lett få tak i informasjon om ting man lurar på. Selvfølgelig må man være kritisk til alt man leser om. Akkurat slik man er når man søker på nettet. For alt av informasjon som ligger lett tilgjengelig, så ligger det enda mer informasjon som ikke er fakta også.

Alt det som er skrevet tidligere strider imot personvern som er retten til å ha et privatliv, og bestemme over egne personopplysninger. Og for å ivareta personvernet har EU laget personopplysningsloven (*GDPR – General Data Protection Regulation*) for å gjøre det tryggere for privatpersoner med personopplysningene. Denne loven handler om hvordan bedrifter samler inn, tar vare på og bruker personopplysningene. Gjennom denne loven gir privatpersoner rettigheter, som å få innsyn i all informasjon selskapene har om personen. Man har både rett til å endre, slette, protestere og begrense informasjon. Man har også rett på å vite hvordan de behandler informasjonen (*Datatilsynet. Dine Rettigheter*).

Bedriftene har også fått flere plikter på hvordan de skal håndtere informasjonen de får av brukerne sine. Noen av de er å fastsette formålene av personinformasjonen de får av sine brukere. De må også tilrettelegge rettighetene til brukerne (*Datatilsynet. Virksomhetens plikter*).

Selv om det er en lov som skal ivareta personvernet, så kan det være meget vanskelig å få vite informasjonen som er lagret. Et eksempel på dette er Apple som vil vite hvorfor man ønsker informasjonen, og tar veldig lang tid før man får tilbakemelding på hva de har av informasjon. Dermed kan det bli vanskelig å få slettet eller endret informasjon som man ønsker.

For å kunne delta i samfunnet i dag så er man så å si nødt til å være med i den digitale verden uten å måtte bli en «outsider». Herunder bruker man varer og digitale tjenester fra store aktører der man signerer på «terms of service» som man enten ikke helt forstår eller som regel, at man ikke gidder å lese. Det betyr at disse tjenestene har en viss makt over oss som vi ikke er helt klar over hva innebærer. Dette er og tror jeg vil bli et viktig tema ettersom tiden går og vi blir enda mer digitale enn det vi allerede er.

Oppgave 3.

Det er en samling av software som gir tilgang til områder på en datamaskin som angriper ikke har autorisasjon eller adgang til. Rootkit kan manipulere data helt ned i root nivå (Superbruker tilgang, som betyr at den har tilgang til å jobbe nederst i operativ systemet eller andre kontroll systemer, nærmest hardware), som gjør at det kan endre og slette operativfiler. Dermed kan den skule seg veldig godt fra antivirus programmer, og vanskelig å finne den (Jeg har brukt mine notater fra forelesning 4: Østby.B, personlig kommunikasjon, 30.januar 2023).

Rootkit er en teknikk som blir ofte brukt til å skjule spor av malware (som trojanere) og dermed gjøre seg usynlig for maskinen den har infisert (Goodrich, M. & Tamassia, R. 2014).

Når man bruker rootkit så er det med formål å skjule malware, ved å skjule drivere, registeret på PC/MAC eller skjule fysiske filer som er lagret på PC/MAC. Mye av rootkit-angrep er benyttet som spionasjeverktøy. Når man nevner roorkit og espionasje, så må man nesten

nevne Stuxnet og effektivt det kan være for å skjule malware. Kernel mode rootkits går helt til roten av operativsystemet. Atomreaktorene i Iran ble ødelagt som følge av at operatørene ikke oppdaget at noe var galt ettersom rootkiten var såpass effektiv. Dermed klarte CIA med flere sikkerhetstjenester å sette Iran tilbake i prosessen med å anrike uran.

Mye av rootkit-angrep er brukt mot myndigheter, men også mot selskap med formål om å innhente intellectual property/immaterielle eiendeler.

Oppgave 4.

Symmetrisk kryptering betyr at begge parter, som her Alice og Bob, har samme nøkkel til å kryptere og dekryptere filer. Det vil si at nøkkelen de har er hemmelig. Ligningen er: $(C = \text{kryptert tekst}, E = \text{nøkkelen}, M = \text{teksten}, D = \text{dekrypterings nøkkel})$ kryptering av tekst: $C=E(M)$ og dekryptering av tekst: $M=D(C)$. Eksempel på Symmetrisk kryptering er AES.

Asymmetrisk kryptering er at Alice har en privat (hemmelig) nøkkel og en offentlig nøkkel som alle kan bruke. Slik at Bob kan kryptere med Alice sin offentlige nøkkel, men Alice er den eneste som får dekryptert med sin private nøkkel. Ligningen blir det samme som i symmetrisk bare at kryptering av teksten blir E (krypterings nøkkelen) er offentlig nøkkelen og dekryptering av teksten blir D er den private. Eksempel på asymmetrisk kryptering er RSA.

For å bruke både Symmetrisk og asymmetrisk kryptering for å sende over et dokument så sikkert som mulig må Alice bruke RSA for å kryptere sin AES nøkkel til Bob. Slik at de har samme nøkkel til å kryptere og dekryptere dokumentet med. Dette er pga. RSA er veldig tungt å både kryptere og dekryptere. Så man bruker ikke det mer en nødvendig. Etter Bob har fått sin AESnøkkel kan samtalen fortsette med AES kryptering (Jeg har brukt mine notater fra forelesning 2: Østby.B, personlig kommunikasjon, 16.januar 2023).

Oppgave 5.

XSS er eksempel å ha lagt inn malware i inputfeltet på nettsiden. Altså brukt JavaScript på webserver i andres webapplikasjon. Mens CSRF er det motsatte. Da kommer du på en uønsket side samtidig som du logger inn på nettstedet du ville være på eks. når du logger inn på en nettbank. At du blir sendt til en annen side enn det du tror (Jeg har brukt mine notater fra forelesning 8: Østby.B, personlig kommunikasjon, 06.mars 2023).

Oppgave 6.

Noen sårbarheter i IP er:

1. at det ikke er kryptert ved overføringer, så man kan lese og avlyttes hele veien fra sender til mottaker.
2. Alt som er i sendingen kan endres, omdirigeres eller modifiseres. Samt avsenders adresse og dermed vanskelig å spore opp gjerningsmannen (Jeg har brukt mine notater fra forelesning 10: Østby.B, personlig kommunikasjon, 27.mars 2023).

Oppgave 7.

Hvis dataprogrammet er noe originalt og helt nytt, så blir det automatisk beskyttet av åndsverkloven (Altinn, 2022). Og hvis man ikke har snakket om programmet og skiller seg

vesentlig ut enn noe andre program i Norge, og er en løsning på kjent problem, så kan man patentere den. Og da blir oppfinneren enerett på programmet i 20 år. Dette gjør at ingen andre kan produsere, importere eller selge programmet frem til den er offentliggjort eller publisert (Jeg har brukt mine notater fra forelesning 9: Østby.B, personlig kommunikasjon, 13.mars 2023).

Oppgave 8.

Da pandemien traff ble mange sendt hjem på hjemmekontor. Mange måtte da ta med sin arbeids PC eller annen digital infrastruktur hjem. Mange privatpersoner har dårligere nettverksikret og i noen tilfeller åpne nettverksløsninger. Som gjør det mer utsatt for angrep. Det at man måtte økte bruken av digitale verktøy som Zoom, Teams osv. for å holde møter, og personlig bruk. Og all usikkerheten rundt pandemien, kan ha gjort det lettere å svindle gjennom Fishing-angrep og andre svindelforsøk.

På arbeidsplassen har man som regel adgangskort og låste dører med kameraer og overvåkning, mens under pandemien har folk sittet hjemme, eller på offentlige steder. Dette utgjør såkalt fysisk sikkerhetsrisiko. Dette øker risikoen for tyveri, eller å miste datamaskinen, ved å glemme den ett sted.

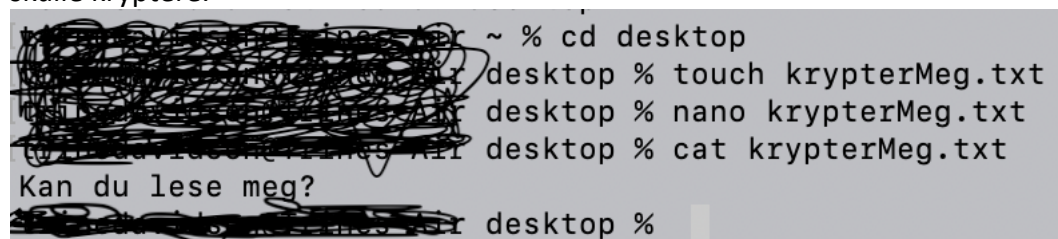
Veldig mange bruker for dårlig passord til innlogginger. Dette gjør det enklere for angriper å komme inn i systemer, nettverk, nettsider, innlogging på PC/MAC osv.

Alle tingene som er nevnt over kan medføre at sensitiv informasjon kommer på avveie. Og utgjøre trussel mot sikkerheten til hele selskapet.

Det som bør endres, dersom det ikke allerede er iverksatt hos de enkelte selskapene er at ansatte bør få opplæring i informasjonssikkerhet, ved å lære om f.eks. nettverkssikkerhet, malware, kryptering, passord sikkerhet, fysisk og digital sikkerhet. For at uvedkommende ikke skal få tilgang på sensitiv informasjon, via fysiske eller digitale sikkerhetsbrudd. Det bør brukes to-faktors-autentifisering iverksettes helst med applikasjon, og ikke meldingsautentifisering. Dette bør iverksettes på alle nettsider eller programmer som inneholder sensitiv informasjon. Og bør kombineres med en VPN-løsning.

Oppgave 9.

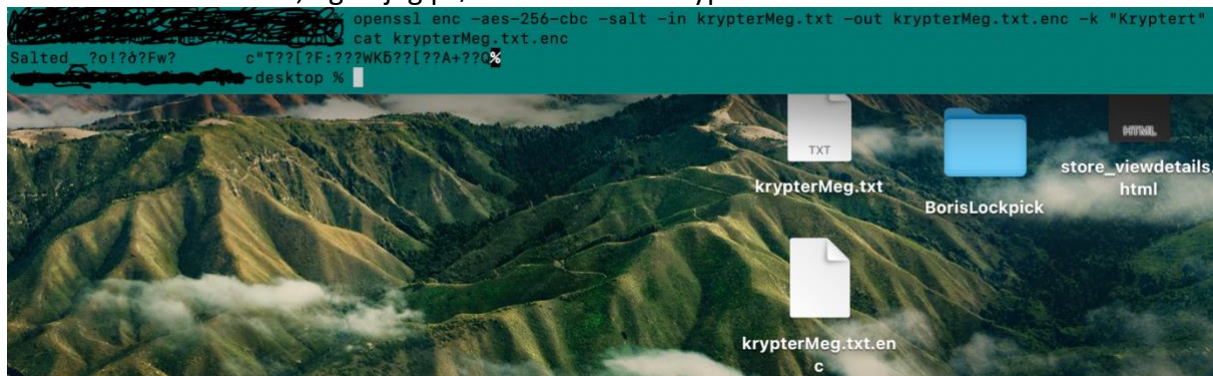
Steg en i prosessen var å lage en fil. Det ble gjort gjennom terminalen. Etter dette ønsket jeg å ha noe skrevet i filen, for å gjøre det enklere for meg selv å finne ut om jeg hadde klart å kryptere. Sjekket også om det ble lagret. Så under tok jeg skjermbilde av stegene frem til jeg skulle kryptere.



```
~ % cd desktop
desktop % touch krypterMeg.txt
desktop % nano krypterMeg.txt
desktop % cat krypterMeg.txt
Kan du lese meg?
desktop %
```

Jeg hadde litt problem med openssl, dermed åpnet jeg en ny terminal, som man ser på bilde 2.

Steg to er å kryptere filen med openssl med aes 256. Ønsket å vise at jeg hadde klart krypter ved å ta bilde av filene, og at jeg prøvde å lese den krypterte filen.



Som jeg forstår det så skulle man bare kryptere filen og ikke kryptere den opp igjen. Hvis man skulle det, er det nesten helt samme prosess som når man krypterte. Da er det å skrive inn i terminalen:

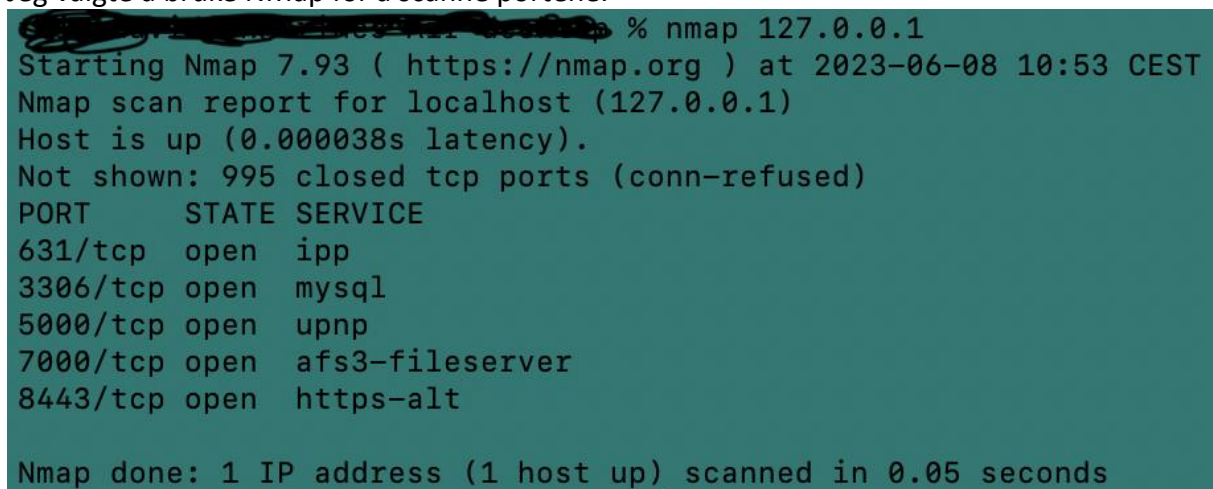
```
openssl enc -aes-256-cbc -d -in krypterMeg.txt.enc -out krypterMeg.d.txt -k "Kryptert"
```

Da skal man få en ny fil som blir helt lik original filen. Og dermed kan lese det som er i den.

(Jeg har brukt mine notater fra øvingsoppgavene: Østby.B, personlig kommunikasjon, 16. januar 2023).

Oppgave 10.

Jeg valgte å bruke NMap for å scanne portene.



Portene som er åpne er:

631 ipp (internet printing protocol) (Wikipedia, 2023) Som jeg forstår pga. At jeg har nettside oppe (Wiseflow), samt port 8443 HTTPS-alt og port 7000 afs3-fileserver er også oppe pga.

Nettleser er oppe på en https side og sender pakker (Audit my PC, 2021).

Port 3306 mysql er også oppe, og det synes jeg var rart, siden jeg hadde avsluttet det programmet før jeg startet eksamenen i dag. Port 5000 er oppe pga. At min MAC prøver å få kontakt med andre apple produkter (Apple, 2022).

Kilder:

- Altinn (22.november.2022) *Opphavsrett* fra:
<https://www.altinn.no/starte-og-drive/starte/rettighetsbeskyttelse/opphavsrett/>
- Apple. (2022, mai) *Developer forums* fra:
<https://developer.apple.com/forums/thread/700989>
- Audit my PC. (2021) *Free internet security audit, UDP 7000* fra:
<https://www.auditmypc.com/udp-port-7000.asp>
- Datatilsynet. (hentet 8.jun.2023) *Dine Rettigheter* fra:
<https://www.datatilsynet.no/rettigheter-og-plikter/den-registrertes-rettigheter/>
- Datatilsynet. (hentet 8.jun.2023) *Virksomhetens plikter* fra:
<https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/>
- Detrow, S. (20. mars 2018) *What Did Cambridge Analytica Do During The 2016 Election?* Fra:
https://www.npr.org/2018/03/20/595338116/what-did-cambridge-analytica-do-during-the-2016-election?fbclid=IwAR3PavVCiWyWxMonlX7XZIK-mGwjPbgMoyOs5h3Qx81GfR6x6l_VjTDgZ54
- Goodrich, M. & Tamassia, R. (2014) *Introduction to Computer Security Pearson New International Edition*, Pearson New International Edition.
<https://archive.org/details/introduction-to-computer-security-goodrich-tamassia-pearson-new-international-edition/page/n1/mode/1up>
- Statistisk sentralbyrå (1.mars 2023) *Ni av ti nordmenn bruker sosiale medier* fra:
<https://www.ssb.no/teknologi-og-innovasjon/informasjons-og-kommunikasjonsteknologi-ikt/statistikk/bruk-av-ikt-i-husholdningene/artikler/ni-av-ti-nordmenn-bruker-sosiale-medier>
- Wikipedia. (2023, 24. Mai). *Internet Printing Protocol*. fra:
https://en.wikipedia.org/wiki/Internet_Printing_Protocol