

Oppgave 1.

Informasjonssikkerhet er det å holde informasjon sikker. Her vil da sikker bety at uvedkommende ikke har tilgang til å lese, bruke, ødelegge eller endre informasjon eller data. Dette kan være alt fra bedrifts-hemmeligheter til personvern. Ettersom det finner flere nivåer på hvor alvorlig det er hvis informasjon kommer ut er det også flere nivåer med sikring av informasjonen. Her kommer da CIA-modellen inn som retningslinjer for hvordan en skal praktisere informasjonssikkerhet best mulig.

CIA-Modellen:

Confidentiality (Konfidensialitet)

Konfidensialitet handler om at informasjonen kun skal være tilgjengelig for brukere med riktig autorisasjon. Her er målet å hindre at brukere uten riktig autentisering ikke skal kunne få tilgang. Dette kan oppnås ved flere metoder. Det første steget for å holde informasjon konfidensiell er å kryptere data som blir sendt. Dette vil si at informasjonen vil være en melding, en kryptert melding og en nøkkel som låser opp og gir tilgang til den krypterte meldingen. Dette vil sikre dataene i meldingen i å bli plukket opp av noen som muligens lytter på datastrømmen på nettverket.

En annen god regel er at alt skal være på et need-to-know basis. Dette vil si at vi holder informasjonen konfidensiell ved at vi kun gir tilgang til informasjon ettersom de har bruk for tilgang. Et eksempel på dette kan være at alle ansatte ved et firma starter med minimal fysisk tilgang, si for eksempel kun adgang til fellesområder. Dette vil hindre at den nyansatte vaskehjelpen kan ta seg inn i server-rommet eller andre steder hvor data kan kompromittert. Videre blir de tildelt tilgang til vaskerommet på nøkkelkortet, da dette er et behov for akkurat denne brukeren.

En siste måte å sikre konfidensialitet på er å bruke verktøy for å vise, til så stor grad som mulig, noen identitet. Dette blir ofte delt inn i tre parter:

Noe en person **har**: Adgangskort, nøkler, bank-id.

Noe en person **vet**: Personlig kode, personlig passord.

Noe en person **er**: Fingeravtrykk, ansikt eller iris-avlesning.

For å bygge på videre på forrige eksempel; så vil vaskehjelpen ha et adgangskort som er tildelt kun seg selv med en personlig pin-kode for å komme seg inn i bygget. Dette vil hindre at dersom andre vil få tak i kortet eller kopiere det vil de ikke nødvendigvis få tilgang til bygget. Dette kan videre gjøres sikrere dersom det også er systemer på plass for å sjekke for noe personen er; fingeravtrykk e.l.

Integrity (Integritet)

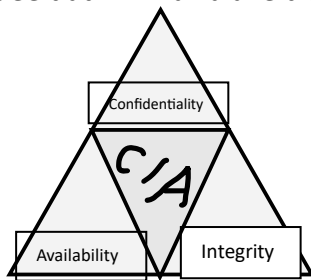
Integritet handler om at informasjon skal være så nøyaktig og komplett som mulig, og at vi vet om informasjonen har blitt endret på. Her er målet å hindre at det blir gjort uautoriserte endringer av informasjonen eller manipulasjoner av uvedkommende. Dette kan oppnås ved bruk av digitale signaturer, logging av endringer, å ta back-up av data. Dersom informasjonen blir sendt fra A til B kan en også ta i bruk sjekksummer. Her vil vi se på om

dataene som ble sendt og dataene som ble mottatt har samme sjekksum. Dersom de er forskjellige vil dataene ha blitt endret underveis, muligens av en uvedkommen tredjepart.

Availability (Tilgjengelighet)

Tilgjengelighet i forhold til CIA modellen er at det skal være enkelt for de som skal ha tilgang på informasjonen skal lett kunne få tilgang på og kunne endre informasjonen. Her er tanken at selv om informasjonen skal være sikker, så skal dette ikke gå på bekostning av produktiviteten til arbeidet som blir utført.

Avslutningsvis kan vi se på CIA modellen som en trekant. Vi kan tenke oss at vi vil at informasjonen vår skal være så sikker som mulig at vi vil ha maksimal konfidensialitet og integritet. Hvis vi for eksempel har en harddisk med kritisk informasjon, og for å bevare denne så plasserer vi den i en safe som vi plasserer i en sementkloss og kaster i sjøen. Vi vil da ha forsikret oss om at denne informasjonen ikke vil bli endret på. Informasjonen vil heller ikke være tilgjengelig for uvedkommende slik at de kan ødelegge eller manipulere dataene på harddisken. Problemet her er at de som skal ha tilgang på denne dataen ikke har enkel tilgang når de trenger det, så viktigheten av de andre faktorene faller bort. Det er derfor ideelt at vi vi av alle tre faktorene.



Oppgave 2.

Dersom en privatperson er koblet til internett i noen som helst grad, blir de trolig eksponert for overvåking og forbrukeranalyser av store internasjonale selskaper. En god tommelfingerregel å ha med tanke på internett er: Om produktet er gratis, er du produktet.

Internettaktivitet: Allerede fra du starter opp nettleseren din begynner du å etterlate deg informasjon. Nettlesere og nettsider samler inn data fra nettleserloggen, informasjonskapsler (veldig mange nettsider nå til dags tar i bruk «Cookies» straks noen er inne på en nettside for å samle informasjon om brukeren). Disse store selskapene, for eksempel Google, om en bruker Google sin søkemotor eller Google Chrome, samler inn informasjonen å tilpasse anbefalinger og reklame tilpasset til brukeren. Du har kanskje lagt merke til at straks du var inne og søkte etter nye joggesko, begynte du å få annonser for lignende varer? Dette er et resultat av at selskaper samler inn informasjonen du legger igjen på internett for å så bruke videre i markedsføring.

Sosiale medier: Stadig flere sosiale medier dukker opp og stadig flere brukere benytter seg av dem. Selv om det blir flere tilfeller av premium versjoner av sosiale medier er de i hovedsak gratis. Her kommer tommelfinger-regelen inn i spill igjen. Når du bruker sosiale

medier som for eksempel Facebook eller Instagram, samler disse selskapene inn informasjon om deg og analyserer det. Dette kan være informasjon du selv legger inn for å bygge en profil, interaksjoner med andre eller delinger og likes. Ved hjelp av denne informasjonen bygges det en profil rundt deg som blir brukt til å tilpasse markedsføringen mot deg eller solgt videre.

Smarte enheter: Smarte enheter blir mer og mer vanlig i hjem og hverdag og blir markedsført med at de gjør hverdagen enklere. De fleste i dag har en smarttelefon, kanskje en klokke med GPS eller til og med smart-høytalere. Disse kan brukes til å samle inn data om alt fra plassering, bruk og aktiviteter om brukeren. Flere av disse kommer også med stemmegjenkjenning og lydopptak, slik at en kan snakke til enheten og kommunisere med tale. Disse digitale assistentene og talekontrollsystemene kan ligge i bakgrunnen og lytte uten at de er i bruk, mens de venter på aktivisering. Her har det ofte allerede blitt opprettet en profil på systemet for å kjenne igjen brukeren, og systemet kan også ta videre opptak uten at brukeren er klar over det. Smarte enheter kan være en risiko for personvern hvis data eller lydopptak blir lagret uten samtykke, spesielt da det kan være andre personer til stede som ikke er klar over funksjonen til noe av teknologien i rommet.

Handlevaner: Når en forbruker benytter seg av et bankkort, kredittkort eller handler på nett registreres informasjonen om kjøpet. Dette gjelder ikke kun på nett, det finnes flere eksempler på tjenester som en forbruker selv velger å laste ned, som gir fordeler ved å lese av handlevanene til forbrukeren. Noen av disse er Rema1000 sin Æ-app eller Trumf bonus. Disse lagrer informasjon om varer du handler og vaner du har, for å så tilpasse sine tilbud til deg. Det viser seg at denne informasjonen også kan bli plukket opp gjennom bongdata og banktransaksjonsdata.

«Gjennom bongdata og banktransaksjonsdata, ville SSB hatt opplysninger om hva en betydelig andel av befolkningen handler av dagligvarer. Dette ville igjen kunne kobles opp mot sosioøkonomiske data slik som husholdningstype, inntekt og utdanningsnivå.»
(Datatilsynet.no, 2023)

Som det kommer frem i Datatilsynets, 2023 *Forbud mot behandling av personopplysninger for SSB*, da de valgte å gripe inn mot SSB sin innsamling av statistikk fra kunder.

Med så stor bruk av overvåking og analysering av forbrukere skaper det flere trusler mot privatpersonens personvern. Ettersom det er såpass mye informasjon som blir samlet inn fra flere forskjellige aktører kan det blir vanskelig og overveldende å ha kontroll på egen personlig informasjon. Dette fører til at en ikke vil ha kontroll på hvilke profiler og hvilken informasjon som blir lagret om deg og hvordan det blir brukt.

Det er også stor verdi i en stor ansamling med data og dette er stadig et attraktivt mål for data-angrep og misbruk. Avhengig av hvilken informasjon som blir samlet inn, kan denne dataen i feil hender bli brukt til både identitetstyveri og svindel.

Lovverket rundt datasikkerhet og personvern er i stadig utvikling. I 2018 innførte Europa et lovverk som gjelder alle EU- og EØS-land, kalt General Data Protection Regulation (GDPR). Formålet med dette lovverket er at hver enkelt privatperson skal ha tilgang på nødvendig informasjon og ha muligheten til å velge om de skal gi samtykke til hvordan virksomheter samler inn og bruker informasjon som blir delt med dem.

Hovedtrekkene i reglementet er at forbruker skal bli informert om et tydelig formål med innsamlingen av dataen. Brukeren har deretter muligheten til å frivillig gi et samtykke til hvilken informasjon som skal bli samlet inn, og skal ikke bli nektet adgang dersom de velger å ikke gi samtykke. Dette samtykket skal også kunne trekkes tilbake uten videre. Det er også innført krav til dokumentasjon fra virksomhetens side, for å loggføre samtykker fra forbrukerne. Dersom selskapene hadde allerede eksisterende databaser, var disse nødt til å oppdateres i henhold til de nye kravene til GDPR.

Oppgave 3.

Rootkit er en form for skadevare som legger seg helt ned på OS nivået til et system (derav navnet «root» som er en administrator på Unix systemer og «kit» er verktøypakken). Siden denne skadevaren har muligheten til å legge seg på nederste nivået av systemet sin programvare har den også muligheten til å endre atferden til systemet. Dette vil blant annet gi muligheten for skadevaren til å skjule seg selv dersom enheten prøver å scanne seg selv for skadevare. Ved hjelp av dette vil et rootkit kunne gi angriperen en varende tilgang til systemet uten å bli fanget opp av antivirus eller administratorer som monitorerer enhetene.

Hensikten med et rootkit er å gi angriperen full adgang til et system, over lengre tid, uten å måtte ha de tillatelsene som vanligvis er nødvendig, med minimal risiko for å bli oppdaget. Angriperen kan da bruke denne tilgangen til å installere eller manipulere allerede eksisterende programvare, deaktivere antivirusprogram eller overvåke systemet.

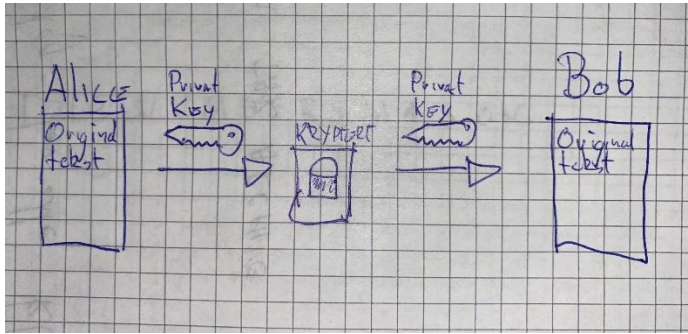
En kan bli infisert med en rootkit skadevare gjennom flere forskjellige metoder, som spam e-post, korrupte nedlastinger (ofte piratkopier) eller USB-enheter. Når en først har blitt infisert vil et rootkit kunne bruke flere forskjellige metoder for å få tak i det de vil på systemet. Et rootkit kan starte med å skjule sin egen tilstedeværelse for å så begynne å laste inn annen skadevare som den også skuler. Dette kan være å installere key-loggers (et program som leser av tastetrykk), stjele log-in informasjon og skru av sikkerhetstjenester. Et rootkit kan også ligge skjult og vente i bakgrunnen uten å gjøre noen handlinger mens den venter på at tiden er riktig. Dette betyr at maskiner kan være infisert med et rootkit lenge før de begynner å gjøre skadelige endringer.

Oppgave 4.

«Symmetrisk kryptoalgoritme; en matematisk funksjon som basert på en felles kryptonøkkel krypterer eller dekrypterer.» (Forskrift om informasjonssikkerhet, 2001 §1-2)

Symmetrisk kryptering er når samme nøkkelen blir brukt for både kryptering og dekryptering. Her vil avsender og mottaker ha tilgang til den samme nøkkelen. Dette gjør symmetrisk kryptering til en rask og effektiv metode, men veldig sårbar da dersom du skal dele nøkkelen med flere personer og nøkkelen kommer på avveie kan hvem som helst som får tak i nøkkelen få tilgang til dataene.

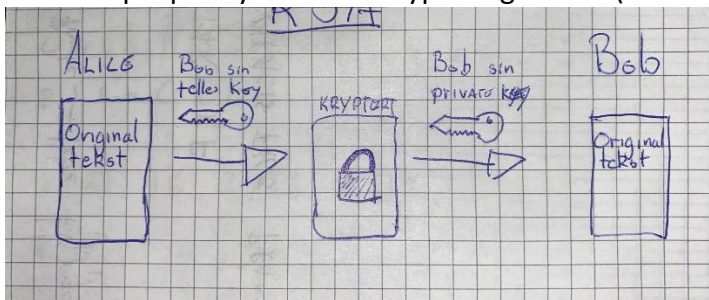
En populær symmetrisk kryptering er AES (Advanced Encryption Standard).



«Asymmetrisk kryptoalgoritme; en matematisk funksjon basert på et kryptonøkkelpar der den ene nøkkelen benyttes til kryptering og den andre til dekryptering, hvorav den ene hemmeligholdes og den andre er offentlig.» (Forskrift om informasjonssikkerhet, 2001 §1-2)

Asymmetrisk kryptering benytter seg derimot av to par med nøkler. En offentlig nøkkel og en privat nøkkel. Her vil den offentlige nøkkelen til mottakeren brukes til å kryptere dataene, men kun den private nøkkelen til mottakeren kan bli brukt til å dekryptere dataen igjen. Denne metoden gjør det derfor enkelt å dele ut den offentlige nøkkelen uten at en risikerer at nøkkelen for dekryptering kommer på avveie og uvedkommende får tilgang til dataene.

Et eksempel på asymmetrisk kryptering er RSA (Rivest-Shamir-Adleman).



For å kombinere både sikkerheten fra asymmetrisk kryptering og effektiviteten til symmetrisk kan vi benytte oss av hybrid kryptering.

Hvis vi sier at Alice er personen som starter med å skulle sende dokumentet til Bob, starter hun med å opprette en asymmetrisk nøkkel for denne økten. Denne nøkkelen vil Alice kryptere ved bruk av Bob sin offentlige nøkkel, slik at han kan dekryptere den med sin private nøkkel (RSA). Når Bob har mottatt og dekryptert nøkkelen vil han ha mottatt den symmetriske nøkkelen fra Alice. Nå kan Bob sende en bekreftelse på mottatt nøkkel som er kryptert med den symmetriske nøkkelen fra Alice. Dersom Alice klarer å dekryptere den mottatte meldingen med sin symmetriske nøkkel, vet hun at Bob mottok nøkkelen og den fungerer og de kan bytte til raskere symmetrisk kryptering (AES).

Ved å gjøre dette har de brukt sikkerheten til asymmetrisk kryptering for å utveksle en symmetrisk nøkkel som de kan bruke resten av økten de skal kommunisere, slik at de får effektiviteten til en symmetrisk kryptering. Straks de er ferdig med å kommunisere vil denne nøkkelen bli kastet og de oppretter en ny en neste gang de skal kommunisere.

Oppgave 5.

XSS og CSRF er to forskjellige nettangrep som blir benyttet i sårbare applikasjoner. Den prinsipielle forskjellen på de to er at ved Cross Site Scripting, vil en angriper utnytte en sårbarhet i en legitim nettside til å kjøre skadelig kode ved hjelp av input eller for eksempel skadelige annonser. Cross Site Request Forgery derimot er når en angriper lurer brukeren til å trykke seg inn på en ikke-legitim nettside, ved for eksempel å konstruere falske e-poster eller SMS 'er.

Cross Site Scripting fungerer ved at en angriper bruker en sårbarhet i en nettapplikasjon, som for eksempel ikke har et godt nok sikkerhetsfilter i sine input-felter. Her kan en angriper bruke muligheten til å kjøre skadelige script eller kode som deretter vil kjøre denne koden på nytt igjen når andre brukere laster inn applikasjonen fra sin egen enhet. Dette kan da brukes for å stjele informasjon fra brukere, lese keystrokes eller videresende brukeren til en skadelig nettside.

Cross Site Request Forgery fungerer ofte ved at en angriper, gjerne ved hjelp av manipulering som phishing eller spoofing, lurer et offer til å trykke på en lenke som fører til en skadelig nettside. For eksempel kan dette være at en angriper utgir seg for å være en bank-tjeneste, og at offeret får en e-post om at de må fikse noe på kontoen sin. De blir sendt til en falsk nettside hvor de blir bedt om å logge inn med sin konto-info, og dermed så har angriperen fått tak i bankopplysningene til offeret. Dersom offeret allerede har et forhold mellom nettleseren og den autentiske nettsiden som den stoler på, kan angriperen få tak i alle informasjons-kapslene til den autentiske nettsiden bare ved at offeret åpner den skadelige nettsiden.

Oppgave 6.

TCP/IP ble utviklet med tanke på at hovedoppgaven er å flytte informasjon mellom to endepunkter, uten tanke på sikkerhet. Hvis vi tar utgangspunkt i CIA modellen finner vi umiddelbart flere feil. Det er ingen krav til konfidensialitet. Svak integritet ettersom det er mulig å endre og lytte til pakker som blir sendt. Sjekksummer vil gi en grad av pålitelighet, men er ikke en garanti mot endring. Tilgjengeligheten har vært fokuset, men har vist seg vanskelig å skalere opp.

Det finnes flere kjente nettverk-angrep som utnytter svakheter ved TCP/IP modellen.

Denial of Service (DoS): Siden TCP/IP modellen ble kun sørget for å overføre data i riktig rekkefølge til riktig maskin, er det mulig for et DoS angrep. Dette er et angrep hvor angriper har som formål å gjøre et nettverk eller en maskin utilgjengelig for andre brukere. Her vil angriperen utnytte TCP/IP sin «three-way-handshake» som består av tre meldinger: SYN, SYN/ACK og ACK. Angriperen sender en forfalsket SYN pakke til en motpart, som da vil svare med en SYN-ACK pakke adressert til en adresse som ikke eksisterer. Ved å gjøre dette vil systemet bli stående og vente på den siste ACK meldingen den tror den skal motta. Ved å kontinuerlig sende ut disse pakkene vil systemet ende opp med flere pakker som står i vent i portene til systemet og det vil ikke være noen ledige porter for andre brukere grunnet overbelastning. I noen tilfeller så setter dette maskinen eller nettverket ut av drift midlertidig eller permanent. Dette angrepet er mulig siden, uten ekstra tiltak, regulerer ikke TCP/IP modellen hvilken data som vil bli tatt opp av et system.

Man-in-the-Middle (MitM): Her vil en angriper endre data-strømmen til to parter og plassere seg selv i midten. Partene vil tro at de kommuniserer direkte med hverandre, men i realiteten sitter angriperen i midten og lytter til samtalen (Eavesdropping), eller i andre tilfeller endrer på hva som blir sendt mellom partene.

Botnet: En angriper har i dette tilfellet tatt over flere usikrede datamaskiner og kan fjernstyre dem. Ofrene er gjerne uvitende om at maskinen deres er kompromittert og angriperen vil dermed over tid få tilgang til et eget nettverk av datamaskiner. Disse blir som regel brukt til ondsinnede handlinger. Et botnet kan blant annet utføre et DoS angrep, slik at det vil bli et enda kraftigere Distributed Denial-of-Service angrep, stjele data og dyrke skadevare.

Masquerading (Spoofing): Her vil en angriper imitere en annen bruker sin identitet. Her kan angriperen få tilgang til sensitiv informasjon ved at ofre tror de gir ut informasjon til en person de stoler på. Et vanlig tilfelle av dette er at angriperne kan sende ut phishing e-poster for å virke legitime ovenfor ofrene.

Spoofing kan også bli brukt i et DoS angrep, slik nevnt tidligere. En bruker kan da utgi seg for å være en annen enhet som ikke eksisterer, og deretter sende flere pakker til et system. Siden angriperen later som om den er en annen adresse vil alle svarene bli sendt til denne falske adressen og overbelaste systemet da den aldri får noe svar.

Oppgave 7.

I Norge blir eierskap over dataprogram beskyttes av Åndsverksloven og patentering.

Åndsverkloven:

«Den som skaper et åndsverk, har opphavsrett til verket, og betegnes som opphaver. Med åndsverk forstås i denne loven litterære eller kunstneriske verk av enhver art, som er uttrykk for original og individuell skapende åndsinnsats, slik som

l. datamaskinprogrammer»

(Åndsverkloven, 2018 §2)

Her regnes dataprogrammer som åndsverk og blir derfor beskyttet av Åndsverkloven i Norge. Ifølge loven vil opphavsmannen automatisk bli tildelt opphavsrett i eget dataprogram så straks det er skapt.

Patentering: I noen tilfeller kan et dataprogram, eller deler av et dataprogram være patenterbart. For å være kvalifisert til dette er det nødt til å innfri noen krav. Oppfinnelsen må ha oppfinnelseshøyde. Det vil si at oppfinnelsen, i dette tilfellet den tekniske fremgangsmåten og apparater i dataprogrammet, må skille seg vesentlig fra tidligere oppfinnelser. Det skal ikke være en logisk videreføring av en kjent teknikk.

(Den europeiske patentkonvensjonen, 2000)

Oppgave 8.

Hjemmekontor kan by på flere utfordringer innen sikkerhet for et selskap. Flere hjem har blant annet sårbare hjemmenettverk. Dersom ansatte skal bruke sine personlige nettverk til å koble seg på et selskap sine systemer dens data må det stilles krav til sikkerheten.

Hjemmenettverk er ofte usikre og mangler korrekt oppsett og blir heller ikke overvåket slik som nettverket til et firma ville vært. Her vil de ansatte bli nødt til å forsikre seg om at nettverket er satt opp med et annet passord enn fabrikkinnstillingene, og sørge for at det er sterkt. Det burde også settes opp kryptering og regelmessig sørge for at alle oppdateringer på maskin og rutere er lastet ned da dette ofte har utarbeidet svakheter. I noen tilfeller kan også bedrifter levere ut maskiner som er ferdig satt opp og administrert av en sakkyndig IT ansatt. Her burde det da stilles krav til at personlig og arbeidsutstyr skal skilles.

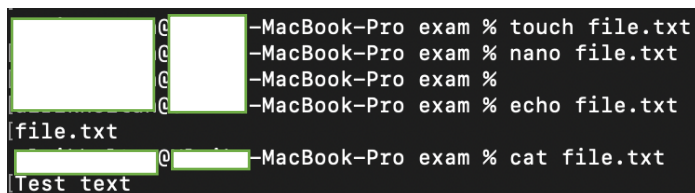
Ved hjemmekontor er det ikke bare det elektroniske som kan by på problemer. I et kontorlandskap er det ofte kontrollerte forhold med begrenset adgang for uvedkommende. En vil ofte trenge spesiell tilgang for å komme seg inn i bygget og de forskjellige rommene. Ved hjemmekontor kan det være varierende sikkerhet i selve boligen. Avhengig av livssituasjonen til en ansatt kan det være samboere, barn, håndverkere eller vaktmestere og huseiere som har tilgang til boligen. Dersom en er ikke personlig er til stede, kan det hende at andre som du vanligvis har grunn til å stole på, eller deg selv, har glemt å låse en dør å uvedkommende kan ta seg inn i en bolig å få tilgang til fysisk eller elektronisk sensitiv informasjon. Det kan derfor stilles krav til at en skal ha låsbare skap i bolig dersom en ikke selv er til stede for å hindre dette.

Når ansatte jobber hjemmefra kan dette føre til at de er mindre oppmerksomme på sosial manipulasjon eller phishing forsøk. Det kan her være vanskelig å følge med på nyansatte i firmaet når en ikke har en personlig relasjon med dem. Ved et fysisk oppmøte vil en lettere legge merke til nye ansikter, og dersom det er nye ansikt kunne identifisere dem ved hjelp av for eksempel adgangs-kort. Uten dette kan en lettere falle for forfalskede e-poster eller lignende og det burde trolig terpes på identifisering av phishing forsøk og rapportering av mistenkelig aktivitet.

Oppgave 9.

Jeg startet først med å lage en tekstfil som heter file.txt.

Dette gjorde jeg med touch, deretter la jeg til tekst i filen med nano, så leste jeg innholdet ut i terminalen.



```
@ -MacBook-Pro exam % touch file.txt
@ -MacBook-Pro exam % nano file.txt
@ -MacBook-Pro exam %
@ -MacBook-Pro exam % echo file.txt
file.txt
@ -MacBook-Pro exam % cat file.txt
Test text
```

Neste steg brukte jeg openssl til å kryptere filen (enc) med aes 256 og bruk av salt, og valgte at dette skulle lagres i out filen file.txt.enc med et passord. Vist slik:


```
@MacBook-Pro exam % openssl enc -aes-256-cbc -salt -in file.txt -out file.txt.enc -k "password"
@MacBook-Pro exam % ls
file.txt      file.txt.enc
@MacBook-Pro exam % cat file.txt.enc
Salted__?(?X?{???v
??#??M???A?
@MacBook-Pro exam %
```

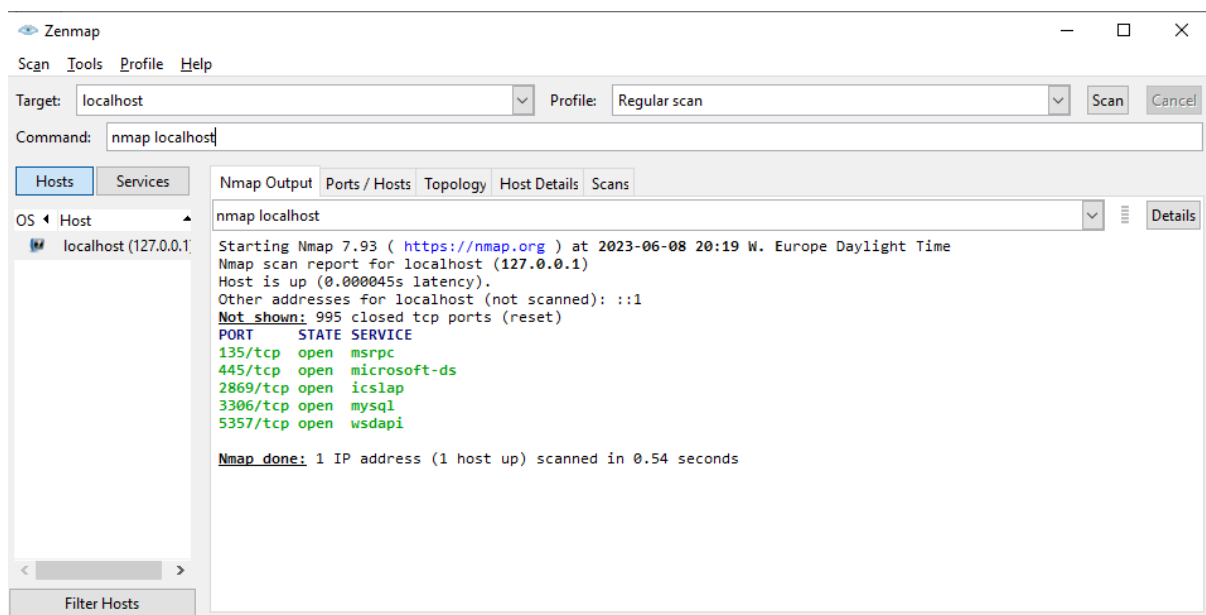
Etterpå prøvde jeg å lese av filen med cat, og fikk et kryptert svar.

Dermed fikk jeg vite at krypteringen fungerte. Da gikk jeg videre til å dekryptere, med bruk av openssl og å bytte ut -salt kommandoen med -d for decrypt. Valgte at den nye filen skulle hete file.decrypt.txt. Jeg leste av filen med cat igjen og fikk resultatet «Test text» som er innholdet i den originale filen. Dermed fungerte både krypteringen og dekrypteri

```
@MacBook-Pro exam % openssl enc -aes-256-cbc -d -in file.txt.enc -out file.decrypt.txt -k "password"
@MacBook-Pro exam % ls
file.decrypt.txt  file.txt      file.txt.enc
@MacBook-Pro exam % cat file.decrypt.txt
Test text
@MacBook-Pro exam %
```

Oppgave 10.

Nmap localhost



Regular scan av localhost. Her scanner jeg hvilke porter som er tilkoblet og tilgjengelige for min egen maskin. Her får jeg opp 5 åpne porter.

Port 135. Msrpc, dette er en åpen port som kommuniserer med Microsoft.

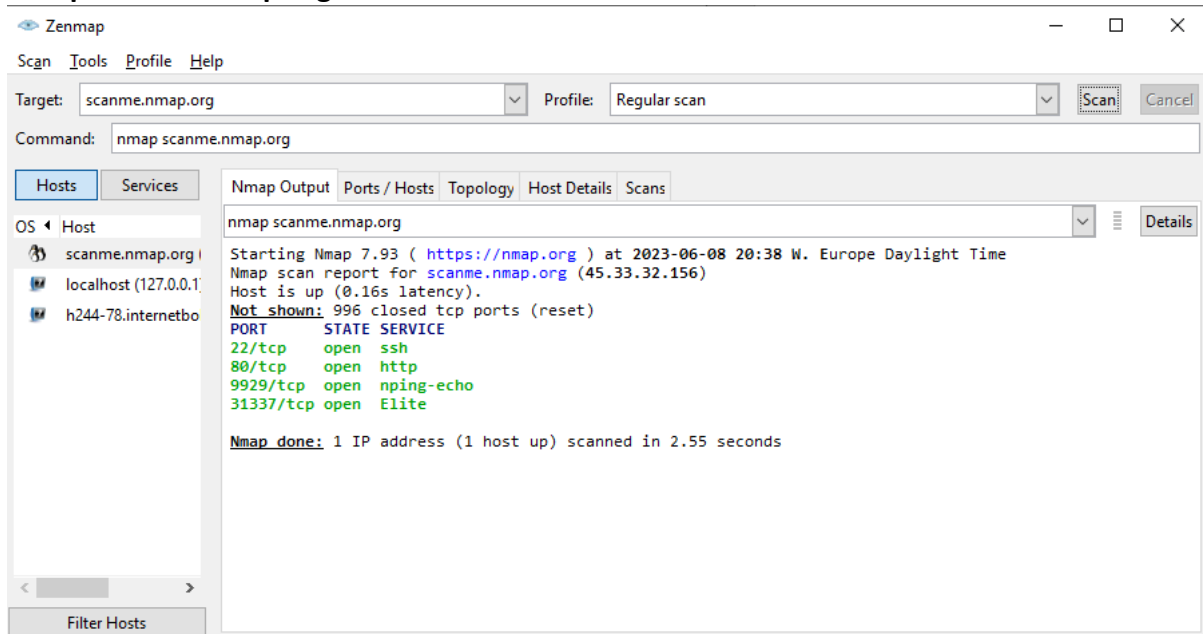
Port 445. Dette er også en port som kommuniserer med Microsoft.

Port 2869. Dette er en port for internet, windows firewall eller local network deling.

Port 3306. Dette er porten som mysql kjører på.

Port 5537. Denne porten kontrollerer blant annet printere, scannere og prosjektorer.

Nmap scanme.nmap.org



Her kjørte jeg en vanlig port-scan av nmap sin dedikerte nettside for port-scanning. Her får vi opp 4 åpne porter som da er i bruk:

Port 22 som kjører ssh. Denne porten blir brukt til fjernstyrt administrasjon ved hjelp av SSH. Port 80. Dette er en port som er koblet til en usikker, ukryptert http nettside. Dette er en sårbar port.

Port 9929. Denne kjører nping.

Port 31337. Denne porten er en referanse til 1337, som betyr Elite på hacker-lingo. Denne er ofte brukt som en bakdør.

Referanser:

Datatilsynet.no. (2023, 02. Mai) Forbud mot behandling av personopplysninger for SSB
<https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/avgjorelser-fra-datatilsynet/2023/forbud-mot-behandling-av-personopplysninger-for-ssb/>

Forskrift om informasjonssikkerhet. (2001). *Forskrift om informasjonssikkerhet* (FOR-2001-07-01-744). Lovdata. <https://lovdata.no/LTI/forskrift/2001-07-01-744>

Lov om opphavsrett til åndsverk mv. (åndsverkloven). (2018) *Åndsverkloven* (LOV-2018-06-15-40). Lovdata. <https://lovdata.no/lov/2018-06-15-40>

Den europeiske patentkonvensjonen 2000 som vedtatt ved Forvaltningsrådets beslutning av 28. juni 2001, (TRAKTAT-2000-11-29-23) Lovdata. <https://lovdata.no/traktat/2000-11-29-23>