Oppgave 1 - Generelt

Om vi skal ta et veldig stort begrep og redusere det til essensen, så er informasjonssikkerhet sikringen mot at informasjon er tilgjengelig for andre enn de med godkjent tilgang til den. Ofte brukes begrepet informasjonssikkerhet når man snakker om bedrifter og organisasjoner, men det gjelder all informasjon også på personlig nivå.

Informasjonssikkerhet omhandler like mye din egen dagbok fra barndommen (som du ikke ville familien din skulle lese), som en internasjonal fast food-kjede sin hemmelige saus-oppskrift som ikke må bli kjent til konkurrentene deres.

Når vi snakker om hva informasjonssikkerhet er og hvordan vi kan oppnå det, refererer vi ofte til den engelske CIA-modellen. CIA står for *Confidentiality*, *Integrity* og *Availability* og kan best kan oversettes på norsk til KIT (*konfidensialitet*, *integritet* og *tilgjengelighet)*. Hvert av disse punktene dekker et område innenfor sikring av data, og når man har alle tre kan man si at midtpunktet hvor de overlapper er det nivået av informasjonssikkerhet man optimalt ønsker å oppnå.

- ***Konfidensialitet*** betyr at bestemt informasjon kun er tilgjengelig for de personene som skal ha tilgang på informasjonen. Samtidig sørger for at alle andre hindres fra å få kjennskap til den.
    - Det mest effektive verktøyet for å sikre konfidensialitet er ved å kryptere informasjonen med en hemmelig krypteringsnøkkel. Dette beskytter da informasjonen mot ukjente som uten dekrypteringsnøkkelen ikke kan lese den.
    - Et annet verktøy for å beskytte konfidensialiteten og hindre uvedkommende tilgang er regler og systemer lagd for å stoppe innsyn. Dette kan være digitalt med f.eks. å måtte logge inn i et system, men kan også være fysisk ved å holde informasjonen tilgjengelig kun i et avgrenset område som f.eks. et kontorlokale eller bedriftsbygg.
    - Sikringen av dataen kan også forsterkes ved å legge til autentisering av en person. Dette for å sikre at man har rett på tilgangen med enten noe personen har (f.eks. et nøkkelkort), noe personen vet (f.eks. et passord) eller noe biologisk som er unikt for personen (f.eks. fingeravtrykk, retina-avlesning, DNA, etc.). Disse tre kan videre kombineres for sterkere sikring.
- ***Integritet*** betyr at man skal kunne være sikker på at det ikke har vært noen endringer på informasjonen, så man kan være sikker på at informasjonen presenteres slik den var ment å være.
    - Vi sikrer integriteten med rutiner og verktøy som back-up av informasjonen på jevne tidspunkt og digitale med sjekksummer i filer eller automatiske systemer som sjekker om data har blitt endret på og deretter korrigere den tilbake.
- ***Tilgjengelighet*** betyr at alle som har rett til det skal få tilgang til informasjonen for å kunne lese eller endre på den innen passelig tid.
    - Tilgjengeligheten til data sikres gjennom f.eks. fysiske sikringer som servere og datasenter som sørger for at informasjonen er lett tilgjengelig, eller digitale sikringer og back-ups som gjør at dataen fremdeles kan være tilgjengelig om noe skulle skje med den originale dataen.

Det finnes også andre sikkerhets-modeller som kan brukes når man snakker om informasjonssikkerhet, for eksempel AAA (Assurance, Authenticity og Anonymity), men som oftest er det CIA-modellen som blir brukt.

For å bedre kunne definere informasjonssikkerhet er det også greit å nevne hva informasjonssikkerhet ikke er. Informasjonssikkerhet er ikke det samme som datasikkerhet, men datasikkerhet overlapper området til informasjonssikkerhet så mye at de to begrepene ofte benyttes om hverandre. Hvor informasjonssikkerheten fokuserer på overordnede

prosesser og rutiner rundt sikring av informasjon, dreier datasikkerhet seg mer om metodene og verktøyene innen IKT som benyttes til dette arbeidet. Informasjonssikkerhet er heller ikke cybersikkerhet, da cybersikkerhet har mer fokus på å sikre drift og tilgjengelighet av tjenester og infrastruktur (Nätt & Heide, 2021, p. 350).

Derfor omfatter informasjonssikkerhet veldig mye da det gjelder all sikring av informasjon, uansett medium og nivå. Noe som kan inkludere blant annet risikovurdering, fysisk sikring, planer rundt krisehåndtering om noe oppstår, opplæring av en bedrift sine ansatte og alt lovverk som omhandler det.

Oppgave 2 – Overvåkning

I vår digitale hverdag legger vi igjen mer og mer informasjon på nettet gjennom online forum, sosiale medier, kommentarfelt og andre nettsider. Dette fører til at vi, selv om vi ikke bevisst har ment å gjøre det (eller ikke har tenkt over det), kan legge igjen nok små biter med informasjon om oss selv på internett til at vi gjør det mulig for andre å samle denne sammen og lage en profil av oss over tid. I denne oppgaven vil jeg presentere hvordan jeg mener nasjonale myndigheter fremover kan komme til å bruke digitale spor og informasjon for å kartlegge privatpersoner etter Politiregisterloven §65 ble vedtatt høsten 2023.

3,55 millioner nordmenn over 18 år hadde i slutten av 2023 en brukerkonto på Facebook, 2,86 millioner på Instagram og 2,88 millioner på Snapchat. 78% sier de bruker sosiale medier hver dag mens 90% sier de er innom sosiale medier ukentlig (Chernykh, 2024). Noen sosiale medier er åpne for alle, f.eks. X (tidligere Twitter), og alt som publiserers her er derfor tilgjengelig for alle som ønsker å lese det. På andre sosiale medier som Facebook og Instagram variere det ut ifra hvilke personvernsinnstillinger brukeren har valgt. Fra at det som publiseres kun er tilgjengelig for en selv, tilgjengelig for alle eller deler av en brukers venner eller offentlig åpent for alle som på X. Ofte ønsker vi brukere å holde vår egen informasjon for oss selv og vår lukkede krets, mens kommersielle aktører ønsker det mest mulig åpent for å ha mest mulig aktivitet. Derfor blir til tider standard innstillinger hos aktører endret og har vi ikke gjort egne valg tidligere kan vår brukers innstillinger blir endret til å følge tjenesten sine nye standardinnstillinger. Blir disse da endret til offentlig er dataen vår plutselig åpen for alle (Nätt & Heide, 2021, p. 280). Dette er viktig å snakke om da alt som ligger offentlig teoretisk kan knyttes til oss.

I Politiregisterloven §65 som ble vedtatt ikrafttredelse fra 01.09.2023 åpnes det opp for at politiets sikkerhetstjeneste (PST) kan innhente, behandle og lagre i 5 år (eller mer i noen tilfeller) åpen tilgjengelig data fra internett som kan samles inn ved hjelp av automatiske datasystemer. Denne dataen som samles inn automatisk trenger ikke å følge §6 «Krav til opplysningenes kvalitet» (som omhandler at data skal være relevant, korrekt og ikke lagres lengre enn nødvendig ut ifra formålet) og §7 «Behandling av særlige kategorier av personopplysninger» (at PST kan dersom det er strengt nødvendig ut fra formålet med behandlingen kan hente inn data som rase-/etnisk opprinnelse, politisk, religiøs eller filosofisk overbevisning, fagforeningstilhørighet, genetiske og biometriske opplysninger, helsemessige forhold, seksuelle forhold eller seksuell orientering) (Lovdata, 2023).

Dette betyr at selv om det ikke er lov direkte mot en privatperson, kan PST her samle inn nok informasjon til å kunne bygge en detaljert profil om privatpersoner med å samle sammen datapunkter mange sikkert tror er anonyme når de publiserer. Kravet er at denne informasjonen ligger åpent tilgjengelig uten at det kreves spesifikke handlinger (som passord/innlogging) for å hente den ut og er samlet inn automatisk. Dette er et toegget sverd da det kan brukes til å finne og forebygge angrep mot norske borgere fra f.eks. terrorister eller ekstremister og radikalisering av unge mennesker. På samme tid vil informasjonen også kunne brukes til å vite mer detaljerte og personlige detaljer om privatpersoner som egentlig ligger utenfor lovens håndtering.

For når dataen først er samlet inn, hvordan den lagres og hvem som har tilgang er ikke noe folk flest får vite om. Og hvis regjeringen i fremtiden endrer syn på hva som bør gjøres med denne dataen som er innsamlet, så er det enklere å gjøre endringer på en lov som er i bruk fra før enn å få gjennomslag for en ny. Og denne dataen kan over tid bli veldig detaljert når den hentes fra mange nok datapunkter.

Et enkelt tilfelle jeg ser for meg, er det blir en datalekkasje og en kjeltring finner ut at jeg befinner meg på ferie i utlandet. Hvorfor? Jo fordi at jeg har sjekket inn på en bar i Spania på Instagram (og personverninnstillingen min står til offentlig siden jeg ikke har endret den), har mobilnummeret mitt liggende på 1881.no, har skrevet adressen min i en kommentar til et innlegg fra Telia på Facebook om at nettet er nede og jeg ønsker at de skal fikse det før jeg kommer hjem. Om denne dataen da skulle komme på avveie, så vil en innbruddstyv vite både at huset mitt står tomt (for det står på min Facebook-profil at jeg er singel), hvor huset mitt er og hvor lenge det er til jeg kommer hjem igjen. Så kan de ringe meg på mobilen i Spania, utgi seg å være fra Telia og be om å kunne få komme inn til meg for å fikse feilen. Hvorpå jeg sender dem en engangskode til min digitale dørlås og «vet» da hvem som er i huset mitt når jeg får beskjed at det er bevegelse der, når jeg egentlig blir rundstjelt.

Et annet tilfelle kan være om data om mitt politiske syn eller genetisk informasjon kommer på avveie og blir plukket opp av en kommersiell aktør. Da kan denne bruke informasjonen til å fokusere reklame mer spesifikt rettet mot meg med mål om å tjene penger eller påvirke mitt syn i fremtidige valg.

Med dette i bakhodet er jeg redd vi kan oppleve mulige bivirkninger om denne loven blir mer kjent i allmenheten. At folk føler seg begrenset i hva de tør å skrive og uttrykke seg med i frykt for å bli overvåket, straffet eller oppleve andre negative konsekvenser for det de skriver. I legal kontekst kan dette omtales som en «nedkjølingseffekt» (engelsk «chilling effect») hvor folk føler at deres ytringsfrihet blir begrenset ved at de føler frykt eller usikkerhet som fører til selvsensur. Dette er et brudd på den menneskerettigheten ytringsfriheten er, samt rettigheten til ytringsfrihet som også er gitt i §100 i den norske grunnloven.

Så vi kan si at Politiregisterloven §65 åpner for at denne dataen kan komme Norge til gode ved at PST kan gjøre sin jobb og forsvare landet. Samtidig er det også er mange usikre momenter hvor det kan skje veldig mye negativt om denne dataen som samles inn skulle komme på avveie. Personlig vil jeg nok i fremtiden være mer bevisst på hva jeg skriver eller kommenterer på nett, selv om jeg egentlig ikke føler at det er noe «viktig» det jeg legger ut der og da.

Oppgave 3 – Skadevare

Programvare som når installert (enten den gjør det av seg selv eller ved at en bruker installerer den i god tro) utfører handlinger som er uautoriserte av brukeren (ofte for å skade eller på noen måte skape muligheter for produsenten) kalles malware (**Mal**icious Soft**ware**).

Malware kan grovt deles inn i tre kategorier basert på dens egenskaper: Spredning (den ønsker å spre seg til flest mulig brukere), skjuling (den skjuler at den finnes og hva den kan gjøre) eller nyttelast (den brukes for å utføre en handling med enheten den er innstallert på, og kan være alt fra å «låne» maskinkraft, låse maskinen, stjele identitieten til brukeren, og mer).

Et av de mest kjente malware angrepene i senere tid er Stuxnet, som var en ondsinnet orm som angrep målrettet i 2009-2010 spesifikke Iranske anlegg som hadde tilknytning til det iranske atomprogrammet. Stuxnet ble interessant for både sikkerhetsutviklere og akademia da den var en av de mest kompliserte og avanserte malware man hadde sett tidligere (Falliere et al., 2010, p. 1). Mange mener at gjør det nesten umulig at den er lagd av noen andre enn et lands myndighet (Nachenberg & Standford University, 2012, 02:14). Etter en gjennomgang

av hva Stuxnet var kommer også en drøfting av et potensielt fremtidlig skrekkscenario malware av denne typen kan forårsake.

Stuxnet angrep spesifikt industrielle kontrollsystemer (ICS) fra Siemens og utnyttet flere ukjente bakdører (zero-day vulnerabilities) for å få tilgang til disse systemene.

Stuxnet ble først oppdaget i 2010 når et iransk firma tok kontakt med det hviterussiske sikkerhetsfirmaet VirusBlokAda da de hadde problemer med servere som restartet seg selv. Etter å ha sjekket serverne i en uke kom Sergey Ulasen og hans team frem til at de hadde funnet et rootkit (programvare som skjuler seg ved å endre OS'et så det blir usynlig).

De fant at de tidligste maskinene som var infisert hadde blitt det så tidlig som på sommeren 2009, så et år eller mer før de ble oppdaget. Det som var helt nytt her var at Stuxnet var digitalt signert med et ekte sertifikat fra Realtek som gjorde at det ble godtatt, og det ble etter at sertifikatet ble gjort ugyldig funnet med et nytt sertifikat fra JMicronTechnology.

Det som gjorde Stuxnet så vanskelig å finne var at det begynte som en orm som er forventet å ha kommet inn på et system over en USB-minnepinne, der den deretter delte seg selv ved å kopiere seg over delte fildelingssystemer og WinCC databaserservere. Dette gjorde at den fikk tilgang på datasystemet som etterhvert ikke var tilkoblet det åpne internettet. Når den så installerte seg selv på en ny maskin så ble den liggende i dvale i alt fra 12 timer til flere uker. Når programmet deretter kjørte var logikken satt opp så den sjekket flere punkter for å finne ut om systemet den var installert i var et mål, blant annet:

- Siemens S7-300
- SIMATIC PCS 7 Process Control System
- Kontrollerer minst 33 Variable frequency drivere fra firmaene Vacon (Finland) eller Fararo Paya (Iran)
- Kun motorer med frekvens mellom 807 Hz og 1210 Hz

Om ikke alle punkter var riktig stoppet det og slettet seg selv. Om det var riktig sjekket den deretter om den har administratorrettigheter, hvis ikke brukte den en bakdør for å installere seg. Slik fortsetter den å arbeide til den har sjekket om alle punkter i logikken som var programmert inn som var krevd ble godkjent, hvis ikke avsluttet programmet og slettet seg selv for å fjerne alle spor.

Grunnen til at mange mener at det ikke var mulig for Stuxnet å være lagd av noen andre enn en organisasjon fra et eller flere land var størrelsen og logikken den arbeidet med. Et vanlig malware på denne tiden var som regel rundt 10 kB, mens Stuxnet var på hele 500 kB (hele 50 ganger større). Dette var ikke pga. bilder eller grafikk som det ofte er når malware blir større, men logikken som fortalte hvordan den skulle spre seg og spesifikt hvilke maskiner den skulle infisere og bli liggende på (Nachenberg & Standford University, 2012, 01:45).

Hovedmålet Stuxnet var ute etter er trodd å skulle være industrielle kontrollsystemer (ICS) i det iranske atomprogrammet, og da spesifikt datamaskinene som styrte uran-sentrifugene for uranberikelse, da over 65% av maskinene som ble infisert av ormen befant seg i Iran. Disse ICS'ene er maskiner som ikke er tilkoblet noe nettverk («air gap») for sikkerhets skyld, men programmeres ved å koble til en Windows-maskin, og Stuxnet var programmert til å aktiveres med en gang dette programmet ble kjørt på en maskin som passet kriteriene dens.

Når Stuxnet tilslutt hadde klart å installere seg på en ICS som styrte sentrifuger ville den først sitte stille for å ta opp hva som var normale tall for sentrifugen, før den begynte sakte å kjøre kommandoer som enten gjorde at sentrifugene gikk raskere eller saktere enn det som var normalt. Samtidlig overkjørte den input til menyene som leste av hastigheten som gjorde at operatørene av sentrifugene og ICS'ene ikke så noe galt.

I dagens situasjon med krigen mellom Russland og Ukraina er det lett å tenke seg til hvordan et tilsvarende angrep kunne bli brukt på mye mer kritisk infrastruktur enn atomberikelse, f.eks. strømnettet, transportnettverk, vannforsyninger eller helsesystemer.

Om f.eks. en aktør eller nasjon lagde en malware som var like vanskelig å finne som Stuxnet og rettet seg mot et lands vannforsyninger ville dette få katastrofale følger. (Gulliksen, 2021) skrev i et innlegg om hvordan et hacking-angrep mot Norsk infrastruktur kunne inntreffe:

- **Helsetjenester**: Skulle sykehus bli angrepet og koble ut tjenestene for akutt helsehjelp ville dette skape kaos på kort tid. Men om f.eks. helsenorge sine nettsider ble hacket kunne en angriper skapt livstruende situasjoner om blodprøveresultater, kreftdiagnoser og andre livsviktige helsetjenester ble manipulert.
- **Strømnettet**: Om en angriper kommer seg inn i systemene til kraftstasjonene våre kan de gjøre som Stuxnet og endre hastigheten på turbinene eller sprenge kapsiteten i strømnettet. Dette ville føre til både akutte strømbrudd og på sikt også høyere strømpriser som ville kunne merkes av alle i befolkningen.
- **Vannverk**: Norske vannverk bruker sensorer for å passe på vannet vi får i springen. Her kan man manipulere dataene fra sensorene, på lik linje som at Stuxnet fikk det til å se ut som at sentrifugene fungerte, og dermed få befolkningen til å tro at vannet var forurenset eller i et verre scenario at det var rent etter at noen forgiftet det.
- **Militæret**: Om militær infrastruktur og sentrale systemer blir hacket kan militære hemmeligheter selges eller brukes mot oss. Men det kan like gjerne være leverandører til forsvaret som blir angrepet for å skade fremtidlige leveranser til forsvaret.

Oppgave 4 – Kryptering

Asymmetrisk kryptering er når man har to krypteringsnøkler som trengs for å kunne dekryptere en fil, en offentlig nøkkel (public key) og en privat nøkkel (private key). I motsetning til symmetrisk kryptering som kun bruker en krypteringsnøkkel gir dette en større sikkerhet da Bob og Alice har hver sin nøkkel istedenfor en delt en, men krever med datakraft.

Asymmetrisk kryptering og asymmetrisk nøkkelutveksling er to deler av prosessen med å skulle sikkert dele data mellom to personer når man ikke vil bruke kun symmetriske kryptering med en delt krypteringsnøkkel. Selv om de høres like ut ligger forskjellen i at asymmetrisk nøkkelutveksling er selve metoden for å sikkert utveksle krypteringsnøkler, mens asymmetrisk kryptering er selve prosessen med kryptering og dekryptering av dataen.

For asymmetrisk kryptering bruker vi RSA metoden som eksempel:

- Formelen gitt offentlig nøkkel (e, n) og privat nøkkel (d, n)
  - For å kryptere: $c = m^e \bmod n$
  - For å dekryptere: $m = c^d \bmod n$
- 1. **Generer av nøkler**:
  - Først genererer Bob et par RSA nøkler, en som offentlig han deler med alle og en privat han ikke deler med noen.
  - Bob kommer opp med primtallene $p = 61$ og $q = 53$.
  - Bob regner ut $n = p * q = 61 \times 53 = 3233$.
  - Bob regner ut $f(n) = (p - 1)(q - 1) = 60 * 52 = 3120$
  - Bob velger en eksponent e som gjør at $1 < e < f(n)$ og e er relativt primt til $f(n)$. I dette tilfellet velger vi e = 17.

    - Bob regner ut den private eksponenten d slik at $d * e \pmod{f(n)} = 1$. Her får vi $d = 2753$.
    - Bob har nå offentlig nøkkel $(e, n) = (17, 3233)$ og privat nøkkel $(d, n) = (2753, 3233)$
- 2. **Kryptere meldingen**
    - Alice vil sende Bob en melding med bare en bokstav «B».
    - Hun endrer bokstaven B til tallet 2.
    - Så krypterer hun tallet med bob sin offentlige nøkkel (17, 3233) med formelen $2^{17} \pmod{3233} = 1752$. Så endrer hun tallet til bokstavene de står for så 1752 blir «AGEG» som er den krypterte teksten.
    - Alice sender Bob den krypterte meldingen «AGEG».
- 3. **Dekryptere meldingen**
    - Bob bruker sine privat nøkkel $(d, n) = (2753, 3233)$ for å dekryptere koden.
    - Han endrer «AGEG» til tallene 1752.
    - Så kjører han $1752^{2753} \pmod{3233} = 2$
    - Bob endrer resultatet 2 til «B» og har den krypterte meldingen fra Alice.

Et eksempel på asymmetriske nøkkelutveksling er Diffie-Hellman metoden:

- 1. **Felles verdier:**
    - Denne metoden går ut på at Alice og Bob velger først et stort primtall, p, og et tall kalt en generator, g. Vi bruker her $p = 23$ og $g = 5$.
    - Disse to tallene deler de med hverandre og de blir også fanget opp av Eve som ønsker å spionere på dataen de sender mellom hverandre.
- 2. **Private verdier:**
    - Så velger Alice og Bob tilfeldig hvert sitt hemmelige tall. La oss bruke eksempelet at Alice velger $a = 6$ og Bob velger $b = 15$. Så tar de generatoren, g, opphøyd i sitt private tall, a og b, og moduloen av primtallet, p, for å regne ut sin offentlige nøkkel A og B.
    - Alice beregner $A = 5^6 \bmod 23 = 15625 \bmod 23 = 8$.
    - Bob beregner $B = 5^{15} \bmod 23 = 30517578125 \bmod 23 = 19$.
- 3. **Utveksling av offentlige nøkler**
    - Så deler Alice og Bob disse tallene, deres offentlige nøkkler, med hverandre.
    - Eve fanger opp disse tallene, men kan ikke regne ut de hemmelige tallene a og b basert på bare sluttsummen A og B.
- 4. **Beregning av felles hemmelig nøkkel**
    - Alice og Bob tar nå den andres offentlige nøkkel for å kunne regne ut deres felles hemmelige nøkkel, h.
    - Alice regner ut $h = B^a \bmod p$ ($s = 19^6 \bmod 23 = 47045881 \bmod 23 = 2$)
    - Bob regner ut $h = A^b \bmod p$ ($s = 8^{15} \bmod 23 = 35184372088832 \bmod 23 = 2$)
- Nå har både Alice og Bob den felles hemmelige nøkkelen $s = 2$ uten at Eve har kunne få tilgang til den.

Da asymmetrisk kryptering er ganske resurstungt i motsetning til symmetrisk kryptering er en god måte å sikre kommunikasjon at man først bruker asymmetrisk kryptering, f.eks. Diffie-Hellmann metoden til å skape en felles hemmelig nøkkel. Deretter når man har denne hemmelige nøkkelen går man over til symmetrisk kryptering, f.eks. med AES-metoden, som krever mye mindre ressurser og fortsetter den krypterte kommunikasjonen med AES.

Oppgave 5 – IoT sikkerhet

Selv om det meste av dagens samfunn begynner å bli digitalt, så tenker vi ofte på datamaskiner og internettilkobling er noe som bare utføres av stasjonære datamaskiner, laptoper og mobiltelefoner. De siste 10 årene har derimot flere og flere av tingene vi har i hjemme våre også blitt datamaskiner, fra videospillmaskiner, printere og strømmåleren som mer vanlige eksempler. Men også andre enheter mange ikke tenker på som for eksempel robotstøvsugeren, kjøleskapet, vaskemaskinen og TV'en er datamaskiner. Det meste av digitale enheter vi omgir oss med er i dag å regne som datamaskiner. Alle disse smarthjem-enhetene som også kan kobles opp til internettet er idag å regne som del av tingenes internett (Internet og Things / IoT) (Nätt & Heide, 2021, p. 138).

Problemet med disse produktene er at der hvor man tidligere har hatt fokus på å skulle få mest mulig prosessorkraft ut av små ressurser, så må også produsentene ta seg av sikkerheten når de også kobler disse produktene mot nettet. Dette er dessverre ikke det som har høyest prioritet i kappløpet om kundene. Da blir det viktig at vi forbrukere kjenner til risikomomentene som kan oppstå når vi velger å ta de inn i hjemmene våre.

IoT-økosystemet begynner å bli et veldig stort system med mange komponenter som omgir oss etterhvert i hele hjemmet vårt. Det er sensorer, enheter, nettverk og skytjenester som arbeider sammen eller er koblet opp mot det samme nettverket. Ofte ved at alt skal kunne styres gjennom en app på mobilen enten du befinner deg hjemme eller på jobb. Philips HUE er f.eks. blant de mer populære produsentene innenfor belysning og sensorer. De har lamper, lyspærer og fjernkontroller som kontrolleres med mobilen og som sammen med andre sensorer de selger kan registrere når dører og vinduer er åpne eller lukket, bevegelse i rommet eller i hagen og utføre handlinger basert på disse.

Kappløpet om å hele tiden ha det nyeste på markedet og derfor også få kundene til å kjøpe sine produkter gjør at mange produsenter som nevnt tidligere nedprioriterer sikkerheten på produktene. De setter heller alt inn for å kunne gi gode brukeropplevelser og ekstra funksjoner gjennom internettilkoblingen på produktet (Nätt & Heide, 2021, p. 138).

Utfordringene vi derfor møter når det gjelder informasjonssikkerheten ved disse punktene er blant annet:

- **Svak eller manglende passordbeskyttelse**: Veldig mange IoT-enheter bruker enkle eller standardpassord fra fabrikken for enkelt oppsett. I mange tilfeller er det ikke engang satt opp at man trenger passord for å kunne koble seg opp til enheter som kobles til internettet (Hillestad et al., 2013).
- **Manglende regelmessige oppdateringer**: I takt med at det kommer nye produkter på markedet så er det flere IoT-enheter som ikke får nye oppdateringer, noe som skaper svakheter som kan utnyttes av angripere.
- **Utviklere mangler erfaring:** Når utviklere som før har arbeidet med å skulle få mest mulig ut av ressursene på en liten databrikke for en hvitevare, nå også må passe på sikkerheten ved at hvitevaren er tilkoblet internett, så mangler de erfaringen «eldre» deler industrien som har vært tilkoblet internettet lenger innehar. Dette gjør at «gamle» svakheter som er kjente, men fikset i f.eks. dataindustrien, kan komme tilbake.
- **Usikre datavern:** Når dumme ting som omfatter vår personlige informasjon, f.eks. en badevekt, blodtrykksmåler eller klokke på håndleddet kreves det mye mer av hvordan disse håndtere personopplysningene våre.
- **Input/Output muligheter:** Når høyttaleren og robotstøvsugeren har innebygd mikrofon og baby-monitoren og TV-en har innebygd kamera skaper dette sikkerhetsmomenter hvor lyd eller bilde kan bli tatt opp uten vårt samtykke.

For å sikre oss best mulig som forbruker så vår informasjon ikke kommer på avveie så er det flere punkter vi bør følge.

- **Alltid bruke gode og unike passord** for pålogging til tjenestene som har tilgang til nettet, gjerne ved å bruke en Password-manager som kan lage og spare passordet så vi ikke trenger å huske det (og derfor velge et svakere som er lettere å huske).
- **Endre fabrikkstandarder**. Sjekke om enhetene kommer oppsatt med standard passord og brukernavn og eventuelt endre disse så ikke uvedkommende kan få tilgang bare de vet hvilket merke vi bruker til smarthjemmet vårt.
- **Regelmessig sjekke etter firmware- og sikkerhetsoppdateringer** på enhetene våre for å ikke bli utsatt for kjente sikkerhetsfeil. Og om en produsent slutter å sende ut oppdateringer bør vi skifte ut enheten til en nyere modell eller annet merke.
- **Vurdere om vi trenger at produktet er smart**. Er det nødvendig for oss at babymonitoren har internettilkobling hvis vi vet at det er en (omså liten) sjanse for at naboen kan se bildene vi ser på mobilen av ungen vår som sover?
- **Bruk et eget nettverk for IoT enheter**: For å unngå at det en angriper hacker en enhet og får tilgang til andre og mer private enheter som er tilkoblet nettet, som f.eks. laptopen, mobilen og eksterne harddisker, bør man sette opp et eget nettverk disse enhetene kobles til. Skulle det da bli innbrudd er skaden begrenset til hva angriperen har tilgang på.

Oppgave 6 – Web sikkerhet

Å skulle beskytte en bedrift i dagens samfunn er blitt mye mer enn hva det var for bare 20 år siden. Da holdt det i mange tilfeller å ha gitter foran dører og vinduer på bedriften, låste dører og alarmsystem som ulte om noen gikk i lokalene når bedriften var stengt. Og de kriminelle måtte befinne seg fysisk på stedet der bedriften hadde kontorer, noe som kuttet ned på hvor mange som kunne gjøre noe.

I dag er dette derimot en helt annen virkelighet. Det å sikre IT-systemene til en bedrift er et evig arbeid som aldri blir ferdig, for når sikrer seg mot en ting så kommer det andre og nye svakheter og sikkerhetsfeil som må sikres. Samtidig så gjelder det å ha innsikt i egen business for å vite hvor man kan bli angrepet, hva er det man har av verdier i bedriften som andre kan jakte på. Er det kundedata, forretningshemmeligheter eller kanskje finansiell informasjon en angriper vil være på jakt etter? For vet vi ikke hvor bedriften eksponerer verdiene sine så vet vi heller ikke hvor vi skal rette forsvaret vårt (Netsecurity, n.d.).

En penetrasjonstest (pentest) er en etisk hacking av IT-infrastrukturen hvor man sjekker alle deler av bedriftens infrastruktur for å finne ut hvor det er svakheter som angripere kan misbruke, men før de gjør det. Sikkerhetsarbeidet er prevantivt og proaktivt vinklet, basert på hvordan man tror at en angriper ville gått til verks for å komme til dataen de er på jakt etter. I praksis er det umulig å få en 100% sikker bedrift, og det er derfor viktig å også arbeide med deteksjon og rutiner for hvordan man skal håndtere hendelser som oppstår (Nätt & Heide, 2021, p. 349).

Det finnes sikkerhetsstandarder som omhandler hvordan sikring av en bedrift bør foregå. Det er satt opp prosesser som skal brukes og følges, samt interne og eksterne kontroller for å sjekke om prosessene er utført riktig. Dette gjør at man sparer tid og penger ved å følge et oppsett som er lagd fra før istedenfor å måtte finne ut alt fra bunnen av. ISO/IEC 27000-serien er en samling standarder en bedrift kan betale for å anskaffe seg for å få et system for å sikre virksomhetens informasjon (Nätt & Heide, 2021, p. 365).

LPT (Licenced Penetration Tester) er en metodologi som brukes i penetrasjonstesting og gir en strukturert metode for hvordan pentesten skal utføres, hvilke steg som skal taes i hvilken rekkefølge og forklaringen for dem. De forskjellige fasene er:

1. **Rekognosering**: Her skal man samle all informasjon man kan få tak i fra bedriften man utfører pentesten mot, dette kan være f.eks. IP-adresser, domenenavn og annen data man kan klare å få tak i.

2. **Scanning**: Her identifiserer man aktive systemer og tjenester som kan være mulige angrepsvinkler. Her bruker man ofte programvaren Nmap for å finne åpne porter og kartlegge nettverket.
3. **Sårbarhetsanalyse**: Man søker etter sårbarheter i systemene og bruke automatiske og manuelle verktøy for å finne svakheter.
4. **Eksplisitt utnyttelse:** Nå som man har funnet svakheter og sårbarheter i systemet så utnytter man dem til å prøve å få ut data. Dette kan være alt fra å få tilgang til systemer, passord eller andre data varierende på svakheten.
5. **Post-utnyttelse**: Når man har tilgang til systemet prøver man å utnytte disse for å komme enda lenger og utforske systemet videre. Nå er målet å finne ut hva man kan gjøre med tilgangen man har fått så langt.
6. **Beholde tilgang**: Man prøver å sette opp bakdører eller svakheter i systemet som gjør at man kan beholde tilgangen man har skaffet så langt så man kan få tilgangen senere med mindre arbeid.
7. **Slette spor**: Her skal laget med pentestere gjøre sitt beste for å slette alle spor av at de har vært inne i systemet så det ikke er mulig for andre pentestere eller bedriften å se at de har vært der.
8. **Rapportering**: Til slutt lager man en rapport av hele penetrasjonstesten og hva man fant ut. Denne inkluderer alle svakheter som ble funnet og hvordan man kan utbedre dem.

Oppgave 7 – Nettverk

Transmission Control Protocol/Internet Protocol (forkortet til TCP/IP) er en samling protokoller som brukes for å kunne kommunisere med flere datamaskiner sammen i et nettverk. Protokollene er deretter delt inn i forskjellige lag ut ifra hvordan de kommuniserer med et nettverk og hva deres rolle er. TCP/IP-modellen består av 5 lag, hvor applikasjonslaget er det første laget med protokoller et program er i kontakt med når det skal kommunisere på et nettverk lagd på de lavere lagene med protokoller, enten dette er et lokalt nettverk eller over internett. En svakhet er dessverre at disse protokollene ofte er gamle og ble skrevet på en tid når man ikke tenkte på sikkerheten i kommunikasjonen da det kun var bekreftede enheter som var påkoblet nettverkene som fantes.

Applikasjonslaget inkluderer protokoller som Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP) og Dynamic Host Configuration Protocol (DHCP).

Svakheter og sikkerhetsutfordringer vi har på applikasjonslaget ligger i at kommunikasjonen mellom en nettleser og webserver i utgangspunktet er åpen da kommunikasjonsprotokollene ikke ble lagd med sikkerhet i tankene. Dette betyr at om vi kobler oss til en nettside med HTTP-protokollen eller sender en e-post med SMTP-protokollen så vil hvem som helst som kobler seg til en node mellom oss og serveren vi snakker med kunne lese dataen som sendes og mottaes av oss. Ofte er ikke dette så viktig på de fleste nettsider som har åpen data (som nettaviser, blogger, o.l.), men det betyr også at en hacker kan koble seg på og endre på dataen vi mottar fra serveren og kan derfor manipulere hva vi ser eller lese av e-postene vi sender ut. Et større problem blir derimot når vi kobler oss til webservere med data som er personlig, f.eks. nettbanken vår, eller fyller inn et betalingsskjema med privat info og kortinformasjon. For denne kan også avleses av tredjeparten (Nätt & Heide, 2021, p. 83).

Løsningen for disse problemene på applikasjonslaget blir da å kryptere dataen vår på vår enhet før den sendes avgårde på en måte som kan leses av på serveren som mottar den uten at det er mulig på en tredjepart i midten. Dette gjøres med asymmetrisk kryptering hvor vi bruker private og offentlige krypteringsnøkler med serveren og deretter krypterer all

informasjon som sendes imellom oss. Dette vises som regel med en ekstra S i nettleseren eller kommunikasjonsprogrammet vårt (HTTPS, FTPS, etc.), hvor S'en står for secure og viser til at kommunikasjonen vår er kryptert fra sender til mottaker.

En annen måte som sikrer kommunikasjonen vår med den vi prater med er autentisering av mottakeren. Med autentisering mener vi at vi har sikret at den webserveren vi kommuniserer med er den den sier den er og ikke en tredjepart som prøver å sende oss falsk info eller stjele informasjonen vår. Dette fungerer ved at når vi starter kontakten så sender serveren oss et sertifikat som er utstedt av en pålitelig tredjepart, så sjekker nettleseren vår om sertifikatet stemmer med dataen vi skrev inn og eventuelt stopper oss om den ikke gjør det. Dessverre må vi fremdeles passe på at nettsiden faktisk er den riktige da det er mulig for svindlere å også skaffe seg et sertifikat til en falsk side, da sertifikatet kun sier noe om at du er kommet til en bestemt nettadresse, ikke om nettadressen tilhører en sikker bedrift/tjeneste. Og det er dessverre mulig å forfalske sertifikater også (Nätt & Heide, 2021, p. 84).

Oppgave 8 – Hjemmekontor

Hjemmekontor som en del av dagens verden etter korona har gitt mange ansatte muligheten til å kunne arbeide hjemmefra i ro og mak, men det har også gitt utfordringer for bedriftene når det kommer til hvordan informasjonssikkerheten skal bevares. For en ting er når man har en ansatt på kontoret som har nøkkelkort for å komme inn, eget sikret nettverk, IT-systemer som oppdaterer og installerer sikkerhetspatcher automatisk og teknisk hjelp og opplæring tilgjengelig om noe skulle skje. Saken kan derimot ta en helomvending når den ansatte sitter hjemme i stua på personlig laptop og skal ha tilgang på sensitiv informasjon fra bedriften.

Bedriften mister fort ved hjemmekontor mange muligheter til å sikre at ikke uvedkommende kan få tilgang til informasjonen, siden de ikke lenger har kontroll over mange faktorer (Fortinet, n.d.):

- **Usikre nettverk**: Et av de største farene for avlytting og modifisering av nettverkstrafikk i dag er trådløse nett (WiFi/WLAN) da dette er den mest brukte tilkoblingstypen for bærbare datamaskiner og andre mobile enheter (Nätt & Heide, 2021, p. 150). Her er det ofte at mange ikke endrer standardpassord til trådløse rutere eller oppdaterer software/firmware og skaper mulige sikkerhetsbrudd hvor tredjeparter kan få tilgang til kommunikasjonen mellom bærbare enheter og accesspunktet/ruteren.
- **Ransomware**: Mange ansatte bruker enheter (f.eks. laptop eller mobil) som de får fra jobben til privat formål, eller motsatt (private enheter til jobben), og dette kan åpne opp for å få infisert enheten med ransomware som låser eller blokkerer brukeren fra å kunne få tilgang til dataen. Hovedmålet med ransomware er hovedsakelig å utpresse eller lure brukeren og deles ofte over e-post med en link som man laster ned. Dette kan også skje om andre har tilgang på enhetene, f.eks. samboer eller barn som også bruker f.eks. laptopen for å være på nett.
- **Svake passord**: Om de ansatte bruker svake/usikre eller det samme passordet flere steder kan dette bli et problem. Dette gjør at sikkerhetstiltak som VPN eller andre tiltak blir ubrukelige da hackere kan skrive programvare eller bruke kunstig intelligens til å prøve å komme seg inn i en bedrifts data. Dette kan f.eks. være å sjekke for de mest brukte passordene, eller om brukeren har et passord som er blitt stjålet fra en annen nettside kan de sjekke om de bruker samme passordet til andre kontoer også. Mange bedrifter har også regelmessig endring av passord etter x måneder, men siden mange finner dette vanskelig er det enkelt for mange å bare bruke det samme passordet med en liten endring som å endre et tall på slutten.
- **Private enheter**: Om de ansatte bruker sine egne digitale enheter til å utføre jobben, f.eks. en laptop, så er det ikke sikkert at sikkerheten er på samme nivå som i bedriftens

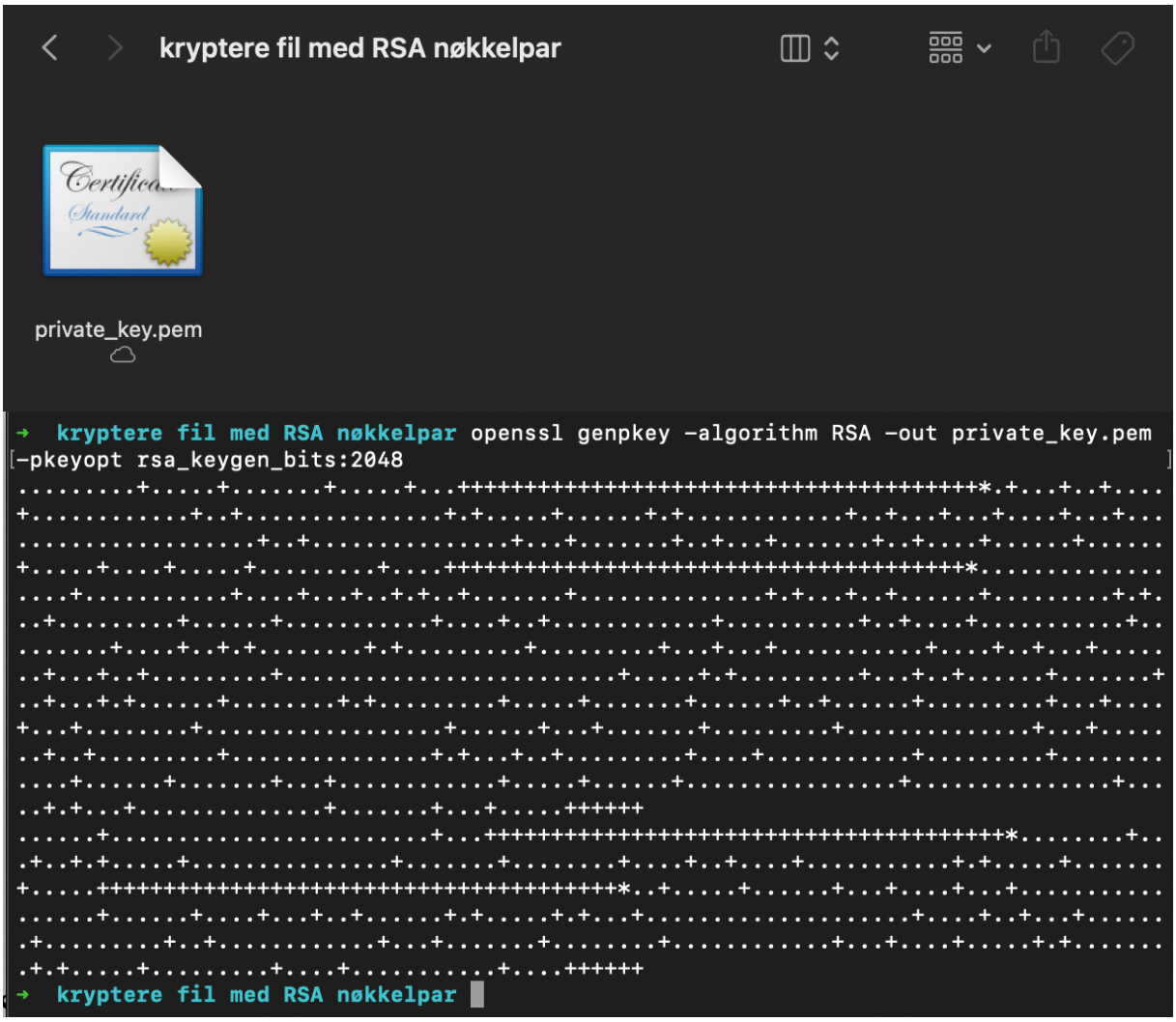
enheter. Manglende oppsett av f.eks. anti-virus eller kryptering av data mellom enheten og bedriftens server kan utgjøre svakheter som kan misbrukes av andre. Det er heller ikke sikker at den ansatte sin enhet er oppdatert til nyeste versjon og kan åpne opp for kjente svakheter som bedriften sine enheter er sikret mot.

- **IoT / Smarte enheter**: I dagens hjem er det blitt mer og mer vanlig med "smarte enheter" som kobles til internett i maskiner som tidligere ikke har hatt dette (IoT eller "Internet of Things"). Dette er alt fra kaffemaskiner, robotstøvsugere og hvitevarer som kjøleskap og vaskemaskiner. Produsentene av disse har tidligere hatt fokus på å få mest mulig ut av begrensede ressurser datasystemene til disse har, det gjør at når de nå får tilkobling til internett så er ikke fokuset like stort på sikkerhet, og kan introdusere "gamle" sikkerhetsfeil som andre bransjer som laptoper og mobiler er sikret mot fra lenge siden. Det er mulig å sette opp et eget nettverk man kobler IoT-enheter til, men det vil ikke stoppe muligheten for f.eks. avlytting om de blir hacket.
- **Fysisk tilgang**: Det kan komme noen på besøk til den ansatte, eller bryte seg inn som leser eller stjeler papirer, notater og digitale enheter med konfidensiell data som tilhører bedriften.
- **Ingen fast plassering**: Selv om man kaller det for "hjemmekontor" så er det ingenting som sikrer at den ansatte sitter hjemme til seg selv. Det er mulig for en ansatt å sitte på en kafe eller et annet offentlig sted og jobbe. Her utsettes man for flere mulige sikkerhetsproblemer som usikre nettverk, at noen andre ser på skjermen over skulderen, at andre overhører telefonsamtaler/online møter hvor man snakker om konfidensiell informasjon.

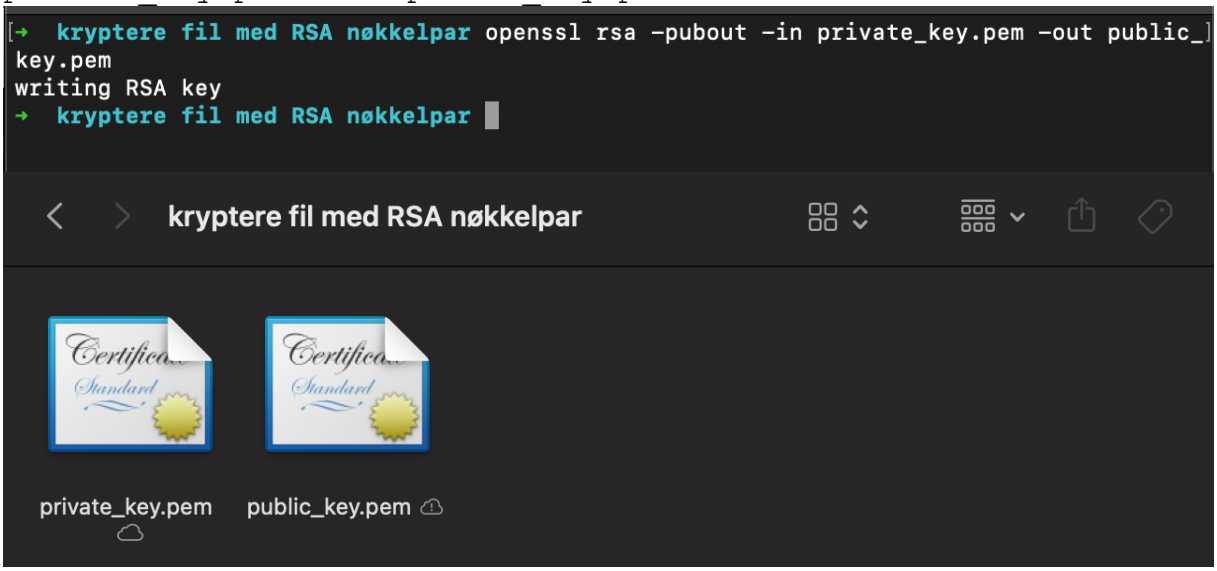
Når hjemmekontor blir mer og mer vanlig i fremtiden så mener jeg at bedrifter best kan sikre seg vil være med å ha mer kontroll over enhetene de ansatte bruker. Om arbeidsplassen er satt opp for å kunne bruke hjemmekontor vil det å ha laptoper og mobiler som den ansatte kan bruke, men som er sikret av bedriftens IT-avdeling med automatisk VPN, antivirus og kontrollert fjernstyrt oppdatering være de punktene som bedriften kan kontrollere. Det er også mulig å gjøre f.eks. innsyn fra andre vanskeligere med skjermbeskytter med innsynsfilter så man bare ser skjermen om man ser rett på den og ikke fra siden. Videre vil regelmessig kursing av testing av ansatte (f.eks. ved å sende ut falske phishing-e-poster for å se om de ansatte trykker på dem), to-faktor-identifisering samt å installere en password-manager så det blir enkelt for en ansatt å bruke sterke, unike passord. Det er også viktig at alle ansatte er klar over prosedyren om det skulle skje dem noe, at de vet hvem de skal kontakte og hvordan de skal oppføre seg så de ikke er redd for å si ifra om de trykker på en link som viser seg å være malware, installerer en ukjent fil eller opplever at noe annet.

Oppgave 9 – Praktisk kryptering

1. Jeg begynner å med generere en RSA privat nøkkel (private key) med kommandoen: `openssl genpkey -algorithm RSA -out private_key.pem -pkeyopt rsa_keygen_bits:2048` (for eksempelets skyld arbeider jeg i en mappe kalt "kryptere fil med RSA nøkkelpar")

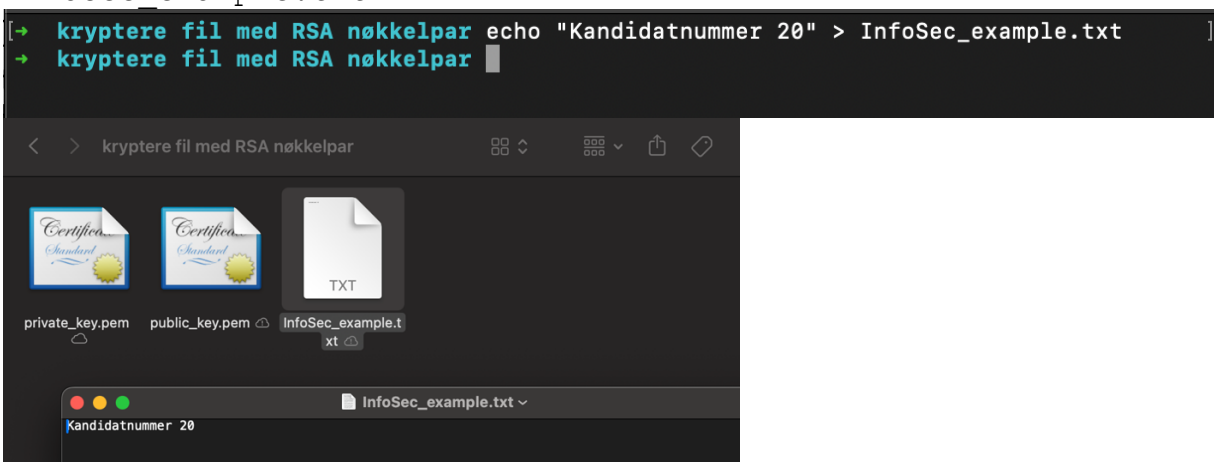


2. Jeg genererer en offentlig nøkkel (public key) med å kjøre kommandoen: openssl rsa -pubout -in private_key.pem -out public_key.pem

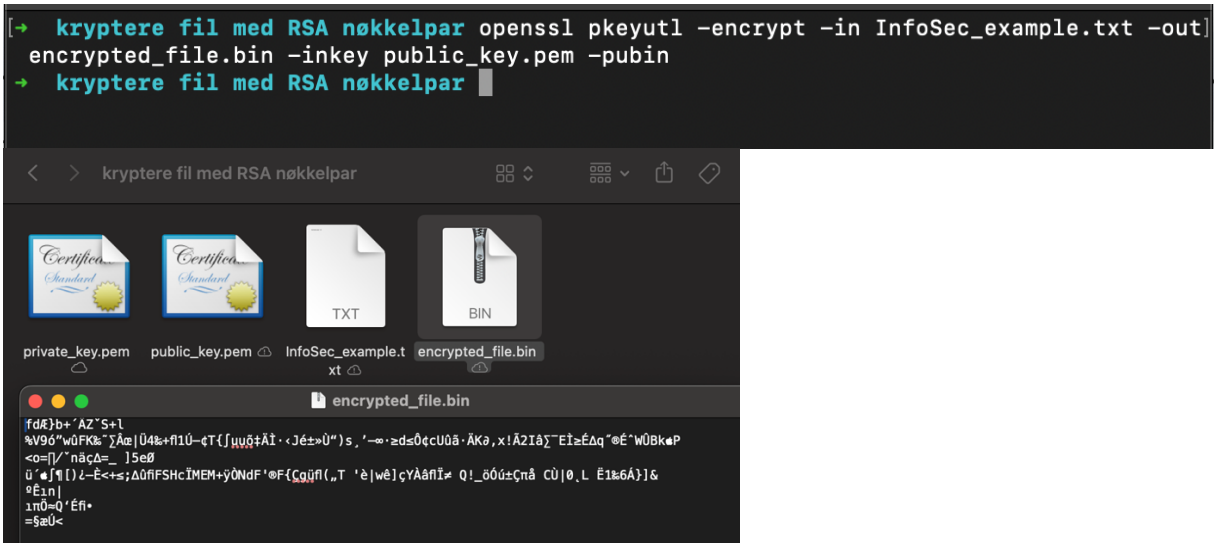


3. Jeg lager en tekstfil jeg kan kryptere som et eksempel med kommandoen: echo "Kandidatnummer 20" >

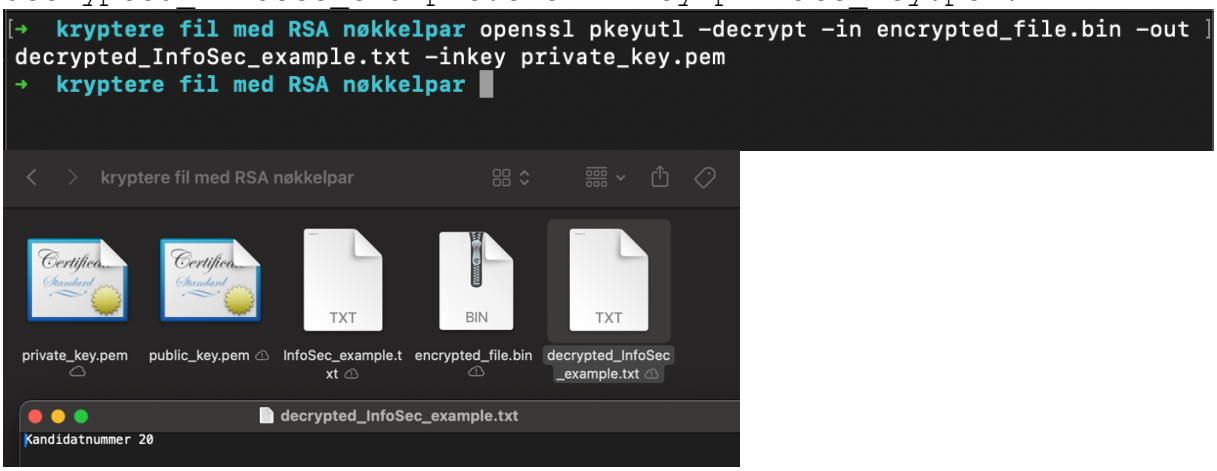
InfoSec_example.txt



4. Jeg bruker den offentlige nøkkelen til å kryptere tekstfilen med kommandoen openssl pkeyutl -encrypt -in InfoSec_example.txt -out encrypted_file.bin -inkey public_key.pem -pubin og får ut en kryptert fil som ikke kan leses:



5. Jeg dekrypterer filen igjen ved å kjøre kommandoen: openssl pkeyutl -decrypt -in encrypted_file.bin -out decrypted_InfoSec_example.txt -inkey private_key.pem.



Oppgave 10b – Praktisk cross-site scripting

1. Jeg bruker Google XSS Game (https://xss-game.appspot.com) for å demonstrere XSS angrep mot en web applikasjon:

2. I søkefeltet på nettsiden skriver jeg inn javascript-koden `<script>alert("Kandidatnummer 20");</script>` og får opp en popup-boks med teksten «Kandidatnummer 20».

Referanseliste

Chernykh, A. (2024, February 5). *Ipsos SoMe-Tracker Q4'23 Norge*. Ipsos. https://www.ipsos.com/nb-no/ipsos-some-tracker-q423

Falliere, N., Murchu, L. O., & Chien, E. (2010). *W32.Stuxnet Dossier* (Version 1.3 (November 2010)). Symantec. https://symantec-enterprise-blogs.security.com/threat-intelligence/stuxnet-dossier-espionage

Fortinet. (n.d.). Work from home: Evolving cybersecurity risks. Retrieved June 4, 2024, from https://www.fortinet.com/resources/cyberglossary/work-from-home-cybersecurity-risks

Gulliksen, G. Ø. (2021, April 5). Når hackerne angriper vannet og strømmen vår. *Avisa OSLO*. https://www.ao.no/nar-hackerne-angriper-vannet-og-strommen-var/o/5-128-77040

Hillestad, L. K., Sadli, E., & Strømman, O. (2013, October 2). Dagbladet fant 2048 norske overvåkings-kameraer på Internett. *Dagbladet*. https://www.dagbladet.no/nyheter/dagbladet-fant-2048-norske-overvakings-kameraer-pa-internett/62718775

Lovdata. (2023, September 1). *Lov om endringer I politiloven Og politiregisterloven (PSTs etterretningsoppdrag Og bruk Av åpent tilgjengelig informasjon)*. Retrieved June 6, 2024, from https://lovdata.no/dokument/NL/lov/2023-04-28-11

Nachenberg, C., & Standford University. (2012, May 8). *Dissecting Stuxnet* [Video]. YouTube. https://www.youtube.com/watch?v=DDH4m6M-ZIU&t=900s

Netsecurity. (n.d.). *Penetrasjonstesting: Derfor bør du teste IT-sikkerheten*. Retrieved June 6, 2024, from https://www.netsecurity.no/fagblogg/derfor-bør-du-jevnlig-teste-bedriftens-it-sikkerhet

Nätt, T. H., & Heide, C. F. (2021). *Datasikkerhet: ikke bli svindlerens neste offer* (2nd ed.). Gyldendal.