

Øving 7 - GDPR

Deltakere: Pål Karlsen, William Johansen, Ola Grytting

Fagkode: IKT100-G 19H

Dato: 18.11/2019

Oppgave 1

Gjør Følgende øvelse:

- a. **Identifiser alle virksomhetene som i dag har personopplysninger om deg lagret.**

Det er veldig vanskelig å kunne peke på absolutt alle virksomhetene som har personopplysninger om oss lagret. Nærmere umulig å kunne si, men vi kan si noen virksomheter som har det. Disse vil være virksomheter som vi har registrert oss på ved å bruke personopplysningene våres: Facebook, Google, UiA, Bank (DNB etc..), Steam, etc..

- b. **Legg til hva slags informasjon dette er (opplysninger, personopplysninger, sensitive personopplysninger etc.) og tenk over hva virksomhetene benytter denne informasjonen til.**

Banken har alle personlig informasjon som navn, bankId, fødselsnummer, saldo, alle bankkontoer, osv. Denne informasjonen er privat og banken har ingen rettigheter til å dele denne informasjonen til andre selskaper eller institusjoner uten min godkjenning, men den kan bli brukt innenfor banken og blir ofte brukt til å gi meg tilbud eller godkjenning av lån.

Google har alle søkene mine som vi har brukt igjennom dem og siden jeg bruker Google chrome som nettleser så har de alle nettsøkene mine selv om jeg ikke bruker google. Denne informasjonen kan brukes til tilrettelagt reklame spesifisert for meg og hva jeg eventuelt kan tenke meg og kjøpe.

Facebook har personlige informasjon som jeg har skrevet til venner. Denne informasjonen kan brukes på lik linje som med googles informasjon, til reklame.

UiA har alle personlig informasjon som jeg har gitt de som tidligere karakterene, fødselsnummer, kurs jeg har eller tar på UiA, karakterer jeg får i dei kursa, osv. Denne informasjonen kan bli brukt av andre selskap til hyring av nye ansatte.

Alle statlige institusjoner har privatopplysninger om meg som er relevant for de. Denne informasjonen har de ingen rett til å gi ut uten min godkjenning, men denne informasjonen kan bli brukt til f.eks. godkjenning av lån av statenslånekaske eller av politiet for pass.

c. Hva har du gitt ditt samtykke til?

Gav UiA informasjon om mine tidligere prestasjoner fra videregående, og videregående fikk informasjon fra ungdomsskolen, osv. Har gitt facebook tillatelse til da de kreve at du godkjenne for å bruka siden deres, samme med google. For og vær helt ærlig vet jeg ikke helt hva da innebære. Har skreve under et par kontrakter fra banken ikke da at jeg huske hva det var for noe. Har nok gitt samtykke til et par andre sider og institusjoner i tillegg, men kan ikke huska hva da var om eller hvem det er.

d. Tenk gjennom og noter hvilke konsekvenser det har dersom denne informasjonen kommer på avveie.

Konsekvensene kan være mange. Hvis bank opplysningane mine går på avveie kan det bli brukt til identitetstyveri.

Facebook har masse personlig informasjon om meg og de jeg har snakket med som kan i verste fall bli brukt som "blackmailing" ikke da at eg er redd for noko av den informasjonen. Google har masse informasjon om kva eg kjøper, ser på og alle sider jeg besøker så den informasjonen kan bli brukt til tilrettelagt angrep mot meg som

spearphishing. Staten har meir informasjon om meg enn banken så den informasjonen hadde vært katastrofale om den hadde blitt stjålet. De har alt fra personnummeret mitt, medisinske journaler, adresser, skoler jeg har gått på, osv. Dette er informasjon som kan bli brukt til identitetstyveri, men kan også bli brukt for å få tilgang til f.eks. eposten min. [1]

Oppgave 2

Hvordan kommer data på avveie? Tenk gjennom og diskutere ulike scenarier.

Data kan komme på avveie på mange ulike måter, lekkasje, angrep, eller uvitenhet som f.eks. helse sør-øst gav tilgang og utvida rettigheter til datasystemet deira til utenlandske IT-arbeidere. Dette gav dei rettighet til å personopplysninga til 2,8 milliona nordmenn. [2]

Dei seier at menneske er det svakeste lenka i sikkerhet og da med god grunn. Mesteparten av svakheter i firmaer ligg i at arbeiderne er uvitende om faren og tar kanskje en infisert privat pc til jobb og sprer malware på jobben uten og vite det.

Hydro ble angrepet i år av et løsepengevirus og dei fann ut at dei kun var uheldige siden sensoren ikke var tilkoblet, men sånn små feil som det er som oftest menneskelig feil, som f.eks. glemmer å skru på sensorer eller alarmer vist en jobber seint ein kveld. Om det er en menneskelig feil veit eg ikkje, men mest sannsynlig så er det da. [3]

Oppgave 4

Diskuter og forklar sikkerhetsbegrepene:

- Konfidensialitet: sikre at informasjon og informasjonssystemer bare er tilgjengelig for de som skal ha tilgang.
- Integritet: å sikre informasjon og informasjonssystemene er korrekte, gyldige, og fullstendige.

- Tilgjengelighet: sikra informasjon og informasjonssystemer er tilgjengelig innenfor dei tilgjengelighetkrava som er satte.
- Sporbarhet: er ein metode som knytter informasjon til ein Ident. F.eks. bankbrikken din.
- Personvern: er ein måte å verne enkeltpersoner mot krenkelser av personvernet gjennom bruk av personopplysninger.

Oppgave 5

Personopplysninger og personvern. Ta utgangspunkt i datatilsynets artikkel og beskriv

Hva er en personopplysning?

Personopplysninger all informasjon som kan knyttes til en spesifikk person som f.eks. fødselsnummer, gateadresse, bilde av personen som kan bli gjenkjent, bil, telefonnummer, e-post, osv. Personopplysning kan være mangt, men så lenge det kan knyttes opp mot en spesifikk individuell person så blir det regnet som en personopplysning. IP-adresser vil også være definert som personopplysninger siden de er knytte til en enhet som er knyttet til en enkeltperson f.eks. en mobiltelefon. [4]

Hva er personvern?

Personvern er retten til et privat liv uten innblanding fra staten eller andre enheter/mennesker. Det vil si en har rett til at personlig informasjon skal være privat og så lenge noen andre vil bruke den informasjonen så må det være godkjent av deg. Det som er problemet med dette er f.eks. Facebook. Kor mange har lest kva opplysninger facebook har lov å samle om seg? Kor mange har godkjent dette? Sider som facebook spør om tillatelse, men hvis du nekter så får du ikke brukt siden deres. Dette blir et større og større problem når sider som blir brukt av millioner av mennesker går uten kontroll og oppsyn. Kva burde vært lov og samle og kven skal ha tilgang til denne informasjonen? [5] [6]

Case: Test av helsedata

HelseApp er i ferd med å utvikle en applikasjon som måler blodtrykk og hjerterefrekvens for å forutsi alvorlige hendelser som slag.

For å teste applikasjonen under utvikling har HelseApp satt sammen et utvalg «test-pasienter» for å teste nøyaktighet og pålitelighet i appen. Data har begynt å komme inn, og resultatene er solide.

HelseApp begynner å få dårlig tid for å nå fristene for release av første versjon av applikasjonen. For å hjelpe med utviklingen har HelseApp engasjert AppButikken, som er et lokalt basert firma som har 10 utviklere lokalisert i India.

- Drøft fordeler og ulemper med å engasjere utviklere lokalisert utenfor EU

Fordelen med dette er jo at det er billigere arbeidskraft, men ulempene er mye større enn fordelene. Regler på data er en stor forskjell mellom EU og India. hva kommer denne informasjonen og bli brukt til? Er de sikre på at det er kun test-data de har tilgang til? Er ikke første gang en sånn feil har blitt gjort i helse Norge. Er det noen som sjekker arbeide de har gjort? Selv om det er billig arbeidskraft for oss, så er det en risikoen for at de finner veier inn eller får med et uhell tilgang til mer sensitiv informasjon.

- **Hvordan kan HelseApp bruke utviklere utenfor EU på en sikker måte?**

De kan begynne med å ha folk til å se gjennom alt arbeid de har gjort og konstant passe på kva informasjon så blir gitt ut. Dei kan minske kva de har tilgang til og kun ha produksjonen som kan være en risiko, her til lands.

- **Hva slags data kan utviklerne og andre aktører ha tilgang til?**

For å lage en sånn app som dette så må en ha tilgang til litt informasjon, trenger ikke å være sann, men uansett. Dette kan skape en risiko for kven veit kva som blir kodet inn hvis ingen går inn og sjekker. Kanskje de lager ei bakluke inn i appen.

- **Hvordan kan man bruke reelle kliniske data i test?**

Ved å gjøre alle dataene til pasienter anonyme. Ikke ha noen navn på datasett (Ha en ID uten at den kan bli sporet tilbake til en person).

Referanser

- [1 A. Zaharia, «All About (Concealed) Data Leakage for Users Like You and Me,» Heimdalsecurity, 8 September 2016. [Internett]. Available: <https://heimdalsecurity.com/blog/all-about-data-leakage/>. [Funnet 18 November 2019].
- [2 A. C. Remen og L. Tomter, «Helse Sør-Øst: Innrømmer at utenlandske IT-arbeidere fikk tilgang til sensitive pasientdata,» NRK, 3 Mai 2017. [Internett]. Available: https://www.nrk.no/norge/helse-sor-ost_innrommer-at-utenlandske-it-arbeidere-har-hatt-tilgang-til-pasientjournaler-1.13478443. [Funnet 18 November 2019].
- [3 Aftenposten, «NSM: Uheldig at Hydro hadde koblet seg fra varslingssystem for dataangrep,» Aftenposten, 20 Mars 2019. [Internett]. Available: <https://www.aftenposten.no/norge/i/XwxleE/nsm-uheldig-at-hydro-hadde-koblet-seg-fra-varslingssystem-for-dataangrep>. [Funnet 18 November 2019].
- [4 Datatilsynet, «Hva er en personopplysning?,» [Internett]. Available: <https://www.uio.no/studier/emner/matnat/ifi/IN1020/h19/dokumenter/hvaerenpersonopplysning.pdf>. [Funnet 18 November 2019].
- [5 Datatilsynet, «Hva er personvern?,» Datatilsynet, [Internett]. Available: <https://www.uio.no/studier/emner/matnat/ifi/IN1020/h19/dokumenter/hvaerpersonvern.pdf>. [Funnet 18 November 2019].
- [6 T. Neset, «Alt dette «stjeler» Facebook fra deg,» Dinside, [Internett]. Available: <https://www.dinside.no/data/alt-dette-stjeler-facebook-fra-deg/69892710>. [Funnet 18 November 2019].