Velkommen!

Datateknologi og sikkerhet 1
01. september 2021

(Hanne-)Kristin S. Leiros
hkleiros@ifi.uio.no

Plan for dagen

- Info
- Repetisjon av pensum
- Case oppgave: Twitter Hack
- Jobbe med ukesoppgaver

Om gruppetimen

- Lavterskeltilbud, lov å ikke delta så aktivt, men også lov å avbryte og stille spørsmål :)
- Repetisjon av ukas pensum
- Prøve å få diskusjon
- Tenkte å ha (frivillig) breakoutrooms etterhvert for å kunne diskutere oppgaver og oblig
  - Send privat melding om dere ikke vil delta, eller om dere vil ha et fra starten av timen for å samarbeide
- Blir ikke tatt opp
- Ikke mulig å bytte gruppetime før 13. september
  - Lov å gå på alle digitale timer, men ikke fysiske man ikke er satt opp på

! Kan hende tidspunkt på denne timen flyttes, dere får mail og blir oppdatert

Nyttige kontakter i faget

- Meg! Kan svare på spørsmål direkte, sende spørsmål videre, utsettelse, hjelp…
  hkleiros@uio.no
  @hkleiros på mattermost om epost er for formelt

- Mattermost
  https://mattermost.uio.no/

- Studieinfo
  studieinfo@ifi.uio.no
  - Full oversikt:
    https://www.mn.uio.no/ifi/studier/kontakt/

- Ofte stilte spørsmål på IFI
  https://www.mn.uio.no/ifi/studier/ofte-stilte-sporsmal.html

Plattformer

- Semestersiden
  https://www.uio.no/studier/emner/matnat/ifi/IN1020/h21/
- Ukesoppgaver
  https://www.uio.no/studier/emner/matnat/ifi/IN1020/h21/ukeoppgaver/
  - Ikke obligatorisk å gjøre, men de er pensum

- Devilry:
  https://devilry.ifi.uio.no/
- Mattermost
  https://mattermost.uio.no/ifi-in1020/channels/town-square

Andre nyttige linker

- Mine studier
  https://minestudier.uio.no/student
  - Timeplan uke til uke, samla beskjeder, snarveier

- Outlook
  https://mail.uio.no/

- Nettside med rom på Ole Johan Dahls hus
  http://magnus.li//ifirooms/
  - Kan søke opp rom å få kart over bygget

- Nettside for printing:
  https://mobilprint.uio.no/
  - Info om vanlig oppsett av printer
    https://www.uio.no/tjenester/it/utskrift/hjelp/med-kortleser/windows/forstegang.html

Læringsmål etter uke 1

- Kunne forklare for andre begrepene *sikkerhet* og spesielt *informasjonssikkerhet*.
- Forstå viktighet av fokus på *sikkerhetsarbeid* også i en digital omgivelse, og ikke minst som en del av de samfunnsmessige utfordringene knyttet til digitalisering.
- Være i stand til å på et overordnet nivå identifisere *verdier*, *trusler* og *trusselaktører*.
- Kjenne de ulike *sikkerhetsmålene*, kunne betydningen deres og vite hvorfor de er sentrale.
- Vite hva et *sikkerhetstiltak* er, og sammenhengen mellom sikkerhetsmål og sikkerhetstiltak.

Hvorfor lære om sikkerhet?

- Det første som kuttes når det er tidspress
  - Ledelse ser ikke vitsen
- Ny utvikling, nye sårbarheter
  - Kriminalitet følger nye tjenester
  - Stadig flere tjenester er på nett
- Forbrukere bruker mer ny teknologi
- Utvikles mer effektive angrepsverktøy
- Økende antall trusler
  - Lettere å true når vi har flere verdier
- Ettertraktet kompetanse

Hva er sikkerhet?

- Safety – trygghet
  - Følelse
- Secutrity - sikkerhet
  - Ikke-statisk tilstand, fravær av uønskede hendelser
- Certainty – visshet
  - Handler om overbevisning

Handler om å beskytte verdier mot skade og ødeleggelse

Hva er en verdi?

Hva er viktig for deg?

Hva er viktig for en virksomhet?

Hva er viktig for samfunnet?

Digital sikkerhet

- Informasjonssikkerhet
  - Beskytte informasjon, eller data
  - Både fysiske og digitale
- Datasikkerhet
  - Sikring av IKT-tjenester og datamaskiner
- Cybersikkerhet
  - Roboter
  - Selvkjørende kjøretøy
  - Infrastruktur

Trusler og Trusselaktører

- En trussel er noe som vil skade eller ødelegge en verdi
  - Det kan være både tilsiktete og utilsiktede hendelser
  - Situasjonsbetinget

- En trusselaktør er; den som kan tenktes å utføre en potensielt skadelig handling
  - «Hackere»
  - Aktivister
  - Kriminelle
  - Virksomheter
  - Nasjonalstater

Hvorfor?

- Økonomisk vinning
- Uautorisert tilgang
  - Forretningshemmeligheter
  - Forskning
- Svekke konkurrenter
  - Virksomheter
  - Stater
- Tilgang til konfidensiell informasjon
  - Sabotasje
  - Maktutøvelse
- Ideologi
- Anerkjennelse
- Nysgjerrighet?

Sikkerhetsmål vs. Sikkerhetstiltak

- En egenskap man kan ønske å oppnå
- Overordnet
- Uavhengig av implementering

- De konkrete tiltakene
- Verktøy for å oppnå målene
- Spesifikk implementering
- Kan brukes for å forebygge, oppdage, eller gjenopprette

KIT-målene

De tre opprinnelige målene fra ISO standarden

- Konfidensialitet
  - Kun de som skal ha tilgang på informasjon, har tilgang på den
  - Hindre at uvedkomne får tilgang
- Integritet
  - Sikre at informasjon bevares i sin helhet
  - Alltid korrekt, ikke endres eller slettes utilsiktet
- Tilgjengelighet
  - Å sikre at informasjon er tilgjengelig når det skal være tilgjengelig

Autentisitet, uavviselighet, sporbarhet

- Autentisitet
  - Vite at noen eller noe er det de utgir seg for å være
    - F.eks.: bruker, system, opprinnelse til data
- Uavviselighet
  - Hindre fornektelse av at data er sendt eller mottatt
    - Uavviselig opphav
    - Uavviselig mottak
  - Skaper er behov for et «bevis» som kan bekreftes av en tredjepart
- Sporbarhet
  - Å kunne knytte en gitt identitet til en gitt hendelse

Personvern

- Personvernopplysninger er alle opplysninger og vurderinger som er mulig å knytte til deg som enkeltperson
- Alminnelige personopplysninger
- Særlige eller sensitive personopplysninger
- Regulert i Norge av personopplysningsloven
  - Brudd fører til bøter

- https://www.datatilsynet.no/rettigheter-og-plikter/personopplysninger/

Kategorier av sikkerhetstiltak

Fysiske tiltak

- Dører
- Låser
- Overvåking
- Tilgangskontroll

Teknologiske tiltak

- Tilgangskontroll
- Autentieringsmekanisker
- Sikkerhetskopiering
- Sikkerhetsoppdatering
- Kryptografi

Administrative tiltak

- Opplæring
- Retningslinjer
- Prosedyrer
- Hendelseshåndtering

Sikkerhetstiltak i ulike tilstander

- Viktig å beskytte data i alle tilstandene
  - Når den lagres
  - Under overføring
  - Når den er i bruk
- Forskjellige tilstander krever forskjellige tiltak

Sikkerhetstiltak i ulike tidsfaser

- Forebyggende tiltak
  - Forhindre og avskrekke angrepsforsøk
- Detekterende tiltak
  - Varsle angrep som forsøkes eller som allerede er skjedd
- Korrigerende tiltak
  - Gjenopprette skade på informasjonsressurser etter angrep

- Må kombineres for å opprettholde dekkende beskyttelse
- Gjerne flere lag som overlapper

Sikkerhetsmål og sikkerhetstiltak

- Konfidensialitet
- Integritet
- Tilgjengelighet
- Autentisitet
- Uavviselige
- Sporbarhet
- Personvern

- Tilgangskontroll
- Opplæring
- Kryptering
- Sjekksumalgoritmer
- Digital signatur
- Skallsikring

Case-oppgave:
Twitter Hack

1. Les artikkelen: https://edition.cnn.com/2020/07/17/tech/former-twitter-employees-sleuthing/index.html
2. Diskuter: Hva gikk galt her? Hvilke verdier ble satt på spill?
3. Er det noen flere trusler som kan oppstå som følge av dette, annet enn bitcoin scammen?
4. Hvilke sikkerhetsmål ble ikke tatt hensyn til?
5. Hvis dere nå hadde fått jobbe i Twitter for å unngå at dette kunne skje i fremtiden, hvilke tiltak ville dere foretatt?
6. Hvor stor rolle spiller sikkerhet når det kommer til sosiale medier? Hvilke verdier kan bli satt på spill?
7. Hvordan kan man balansere sikkerhet og brukervennlighet i en sitasjon som dette? Hva burde prioriteringene være?

Ukesoppgaver

- https://www.uio.no/studier/emner/matnat/ifi/IN1020/h21/ukeoppgaver/uke2-oppgaver.pdf

Oblig 1

- Publiseres i morgen 2. september
- Innleveringsfrist 15. september 23:59:00

- Handler om Sikkerhet og Datanettverk

- Jeg kan gi opptil 3 dagers utsettelse hvis dere SPØR før fristen
  - Kontakt studieinfo@ifi.uio.no hvis dere trenger mer enn tre dager

Sees neste uke!

Spørsmål? hkleiros@uio.no