IN1020 Obligatorisk innlevering 1: Sikkerhet i praksis

Oppgave 1:

Verdier i dette systemet er elevenes og lærernes personalia, elevenes arbeid, lærernes tilbakemelding til elevene, osv. For eleven vil nok konfidensialitet være viktigere enn for læreren ettersom de kan ønske å holde resultatene sine privat. For lærerne vil nok integritet være viktigere enn for elevene for å bekrefte at deres tilbakemeldinger forblir uendret fra mulige trusselaktører. Sammenlignet med den gjennomsnittlige eleven vil nok den gjennomsnittlige læreren være noe mindre kompetent på datarelaterte områder. Derfor vil nok også tilgjengelighet være viktigere for lærere enn for elever. Sannsynlige trusselaktører i et system med informasjon om standpunktkarakterer kan være elever og foreldre som er misfornøyd med karakterer eller lærers vurdering, eller mindre sannsynlig utenforstående som hacker for moro eller protesterer mot karaktersystemet ved å f.eks. slette alle lagrede karakterer.

Oppgave 2:

Konfidensialitet er relativt viktig for et slikt system for å opprettholde rett til privatliv. I forhold til personalia vil det imidlertid ikke lagres alt for personlig informasjon som kan minke verdien til konfidensialitet. For elevenes innleveringer og tilbakemeldinger vil deres konfidensielle ønsker variere fra person til person, men i slike tilfeller bør man tenke seg verste scenario og heller sikre for mye enn for lite. Mye av tilbakemeldingene og karakterene lagret vil og trolig kun være elektroniske versjoner av tilbakemeldinger eleven allerede har fått av læreren, så hvis en trusselaktør eventuelt hadde endret på karakterer er ikke en slik situasjon nødvendigvis ødeleggende (spesielt ikke med god sporbarhet)

Integriteten bak tilbakemeldingene vil være ganske viktig for å sikre at ingen utenforstående kan sende meldinger autorisert som lærere, eventuelt stoppe trusselaktører fra å sende meldinger til lærere autorisert som elever. Å kunne vite med sikkerhet at karakterene satt for elevene er legitime, altså ikke fra noen andre enn lærerne, vil være veldig viktig.

Tilgjengelighet er alltid noe som er godt å ha, men som ofte må komme på bekostning av andre faktorer. I et slikt system tenker jeg ikke det er lurt å ofre for mye av hverken konfidensialitet eller integritet for å bedre tilgjengelighet.

Oppgave 3:

Sporing for integritet og autentisering for konfidensialitet.

Oppgave 4:

For et slikt system er sporbarhet og autentisering kanskje de viktigste faktorene. Med god sporbarhet og autentisering kan man lett finne frem til hva som var den egentlige tilbakemeldingen i det tilfellet det har vært et systemangrep. Sporbarhet gjør egentlig at hvem som helst angripe systemet når de vil (så lenge det ikke går utover loggen av det som spores) uten at det nødvendigvis har noen effekt for den lagrede informasjonen ettersom man kan finne tilbake til det originale. Man bruker imidlertid autentisering for å gjøre det mer troverdig og oversiktlig. Med god autentisering vil man og kunne minimere sannsynligheten for angrep ved å gjøre det vanskeligere for trusselaktører å kunne endre på informasjon lagret i systemet.

Oppgave 5:

For å implementere dette må det installeres tilgangskontroll. Dette kontrollerer tilgang fra subjekt til objekt. Tjenesten må kunne analysere subjektet, sjekke om de har tilstrekkelig autorisasjon for å gjøre handlingene de forespør og enten gi- eller nekte tilgang. For sporbarhet burde også alle forespørsler loggføres.

Oppgave 6:

For elevers fravær kan det være viktig å sjekke om fraværet er godt begrunnet eller eventuelt ubegrunnet. Det burde for eksempel kanskje skilles mellom legeanmeldt-, selvmeldt-, uanmeldt- eller sykeanmeldt fravær. Årsaken til fraværet kan også være et privat emne som kanskje eleven ikke ønsker å komme på avveie. Det kan derfor være spesielt viktig å innføre tilstrekkelig kryptering og autentisering for å kunne se oversikten over fraværet, dersom denne modulen skulle implementeres. Det kunne også vært gunstig å slette denne informasjonen etter den ikke lenger trengs (etter skoleår eller etter eleven har sluttet på skolen).

Oppgave 7:

Uten kryptering over trådløse nettverk kan hvem som helst lytte inn på nettverkstrafikken og se alt som foregår over nettverket. Dette kan i verste fall være veldig sensitiv informasjon som brukernavn, passord, fødselsnummer, personlige opplysninger, etc. Direkte for dette systemet kan dette misbrukes ved å lytte inn på alle innloggінger til systemet og få tak i innloggingen til andre.

Oppgave 8:

Jeg hadde nok lyttet inn på trafikken gjennom det ukrypterte nettverket frem til jeg fikk innloggings informasjonen til en med administrator tilgang, eller en lærer. Så kunne man enkelt logget seg inn på brukeren deres (Så lenge det ikke er noe 2-stegs bekreftelse) og redigere karakterer. Med administrator-tilgang kunne man også kanskje lagd en sikrere utvei for seg selv ved å gjøre det vanskeligere for de faktisk ansatte å endre tilbake til original karakter. Dette kan være å slette sporingsinformasjonen (mer effektivt hvis læreren ikke har tilbakemelding skriftlig og har glemt karakter), sperre lærere ute fra kontoene sine, endre passordene deres, låse innleveringer, etc. Noen av disse tiltakene kan gjøre det mer åpenbart at det har vært et angrep på systemet, så mest sannsynlig hadde jeg bare fjernet loggen.