Oblig 1

Ulrikso

Oppgave 1

Noen verdier:

Personopplysninger

Tilbakemeldinger

standpunktskarakterer

Personvern er viktig for elevene, siden informasjon om deres adresse, mobilnummer, navn og fødselsdato blir lagret på skolens datasystemer.

Standpunktskarakterer er viktige for elevene for elevene fordi det påvirker mulighetene for å komme opp i høyere utdanning.

Tilbakemeldinger er viktig for eleven fordi de viser faglig utvikling underveis.

For en elev kan standpunktskarakterer og tilbakemeldinger være en viktig verdi. Mens for enn lærer er personopplysninger om lærerne.

Trusselaktører:

En ondsinnet elev.

Oppgave 2

KIT-målene

Vurder viktigheten og hva som kan utgjøre en trussel.

Viktigheten av verdiene avhenger av hvilken situasjon det omhandler. For personopplysninger vil konfidensialitet og tilgangskontroll være svært viktig. Mens med nuclear launch codes er integritet langt viktigere. Mens for en facebook post er tilgjengelighet viktigere for alminnelige den personen.

For skole situasjonen er konfidensialitet noe viktig, men integritet svert viktig, siden utdanningsforløpet vil avhenge av tallene i systemet. Tilgjengelighet er og greit å ha, men kommer under de andre i viktighet.

En trussel mot konfidensialitet vil for eksempel være dårlig kryptering, generell sikkerhet eller tilgangskontroll så hackers eller elever enten med vilje eller uhell får tilgang til elevers informasjon.

En trussel mot integritet vil for eksempel være mangel av backup, i tilfelle brann eller annet tap av data.

En trussel mot tilgjengelighet vil for eksempel være et ddos angrep.

Oppgave 3

sikkerhetstiltak:

Sikkerhetstiltak som kan bidra til konfidensialitet er for eksempel two-factor authetication, autentisering med flere lag for å øke sikkerhet

1. Two-factor authentication, kryptering
2. Sikkerhetskopi, info puttet på blockchain

Oppgave 4

De er begge like viktige.

I nesten hvilket som helst datasystem, i dette tilfellet en videregående skole, der det er brukere skal ha tilgang til data gjennom internettet er både sporbarhet og autentisitet ekstremt viktige sikkerhetsmål. Sporbarhet og autentisitet henger sammen med hverandre til en stor grad. Sporbarhet; å spore hendelsene på et gitt system og å kunne tilknytte de hendelsene til en identitet. Autentisitet innebærer å vite om en gitt identitet er *autentisk*, at en person er den de påstår å være. For en elev på denne videregående skolen ville dette innebært en innlogging(brukerautentisering) som krever et brukernavn(identifikator) og passord(autentiseringsfaktor). For å oppnå sporbarhet må systemet ha oversikt på alle identiteter og handlinger, dette krever at autentisitet allerede er oppnådd. Så må handlingene loggføres slik at de kan i etterkant bli analysert. Uten at de fungerer sammen ville det ikke vært mulig å identifisere trusler før eller etter de allerede har skjedd.

Oppgave 5

Det trengs en liste over brukere og forespørsler, så må forespørslene bli godkjent eller avvist i forhold til policy, brukeren blir deretter autorisert til riktig tilgangsnivå. Deretter trengs et system som kan autentisere en bruker som den de er, som bank id, eller liknende. Her kan flerfaktorautentisering tas i bruk. På nettet kan man bruke epost eller sms som indifikator.

Så må informasjon deles ut i henhold til tillatelsene.

Oppgave 6

Siden man ikke vet hva begrunnelsen kan inneholde, burde alle behandles som om de inneholder besyttede personoplysninger. Systemet må derfor forsikre at informasjonen er trygt lagret (kryptert) og har streng kontroll over tilgang.

Man kunne bedt elev/forelder notere hvilket nivå personoplysninger det er snakk om, men dette fører til mer arbeid, stress for bruker og potensielle sikkerhetshull.

Oppgave 7

Det er viktig å kryptere trådløs nettverkdata (wifi/WLAN) fordi ukryptert data, selv om det blir filtrert ut av mange nettverkskort, er fortsatt åpen for de med riktig utstyr(kort med promiscuous mode). En trusselaktør kan enkelt bruke en laptop for å se på nettverkstrafikken din på et ukryptert trådløst nettverk. Dette er et relativt åpenbart sikkerhetsproblem. I forhold til å la elever og lærere dele trådløst nettverk er det tenkelig at en elev kan se på nettverkstrafikken lese andre elevers innleveringer på en prøve ved å sniffe packets.

Oppgave 8

Jeg hadde laget en klassisk phishing scam, altså en login nettside som er helt lik skolens login side(feks som feide) som lagrer brukernavn og passord. Jeg sender linken til læreren i det faget jeg har lyst til å endre karakter i (eller alternativt en sysadmin om det ikke fungerer). Hvis det fungerte er det bare å logge inn med lærerens brukernavn og passord for å utnytte tilgangen til å endre informasjon i systemet.