Høgskolen i Sørøst-Norge

EKSAMEN

6123

INFORMASJONSSIKKERHET

03.05.2017

Tid:	4 timer (10-14)
Målform:	Norsk
Sidetal:	9 (inkludert denne)
Hjelpemiddel:	Ingen
Merknader:	Ingen
Vedlegg:	

Sensuren finner du på StudentWeb.

1 Del 1 Flervalgsoppgaver (teller 20%)

Poengberegning flervalgsspørsmål:

- Oppgaven består av 15 flervalgsspørsmål.
- Hvert spørsmål har 4 svaralternativ.
- Kun 1 alternativ er riktig.
- Du kan velge å «gardere» ved å svare på flere enn ett alternativ.
- Du får 3 poeng for riktig svar, -1 poeng for hvert galt svar og 0 poeng for spørsmål som ikke er besvart.
- Oppgi svar på formen: Spørsmål 1. a (Spørsmål 1.a,d om du garderer) (ikke gjenta ordlyden i spørmål eller svar)
- Hvis a er riktig og d er feil får du 3-1=2 poeng på dette spørsmålet.
- For å få maksimalt antall poeng (3) må du altså svare med kun ett (korrekt) alternativ.

1.1 Et av temaene i datasikkerhet er konfidensialitet. Hva mener vi med dette begrepet?

a) At informasjon alltid er tilgjengelig for rette vedkommende.
b) At datasikkerheten er underlagt et kvalitetssystem.
c) At informasjonen ikke er tilgjengelig for uvedkommende.
d) At brukerne av informasjon kan stole på at informasjonen er riktig.

1.2 Et annet tema i datasikkerhet er integritet. Hva mener vi med dette begrepet?

a) At informasjon alltid er tilgjengelig for rette vedkommende.
b) At personopplysninger på avveie ikke skal skade en persons omdømme.
c) At informasjonen ikke er tilgjengelig for uvedkommende.
d) At brukerne av informasjon kan stole på at informasjonen er riktig.

1.3 Hva menes med begrepet autentisering?

a) Med autentisering mener vi metoder for å kunne identifisere hvem som prøver å logge seg på.
b) Med autentisering mener vi metoder for å spore aktivitet i et system.
c) Med autentisering mener vi å gi rette personer tilgang til de rette ressursene.
d) Med autentisering mener vi at påloggingsinformasjonen blir behandlet kryptert.

1.4 Hva menes med begrepet phishing?

a) Phishing betyr å forsøke å få sensitiv informasjon fra en bruker ved å sende ham/henne en e-post, eller lure ham/henne inn på en falsk nettside, som ser ekte ut.
b) Phishing betyr å komme seg forbi sikkerhetsmekanismene til et system og infisere dette med skadevare.
c) Phishing betyr å benytte en annens identitet, for eksempel i forbindelse med bestilling av en vare eller tjeneste.
d) Phishing betyr å sende en melding som skal få noen til å tro på noe usant, f.eks. at vedkommende har blitt infisert av skadevare på sin maskin.

1.5 Hva kaller vi skadevare som låser maskinen for bruk eller krypterer data på disken og hvor svindleren krever løsepenger for å frigjøre maskinen eller data?

a) Rootkit.
b) Hijacking.
c) Ransomware.
d) Hoax.

1.6 Hva menes med begrepet «mail spoofing»?

a) Med «mail spoofing» mener vi å forfalske innholdet i en e-post.
b) Med «mail spoofing» mener vi å sortere e-post slik at «spam» havner i søppelpostmappen.
c) Med «mail spoofing» mener vi å forfalske avsender av e-post.
d) Med «mail spoofing» mener vi å manuelt skrive og sende e-post ved hjelp av SMTP-kommandoer.

1.7 Skadevare består av flere ulike komponenter som hver har sin oppgave. Hvilke fire komponenter er dette normalt?

a) Trojaner, virus, ormer og makrovirus.
b) Stridshode, spredning, kamuflasje og utpressing.
c) Nyttelast, kamuflasje, infeksjon og inkubasjonstid.
d) Stridshode, spredning, kamuflasje og nyttelast.

1.8 For å oppdage skadevare benyttes ofte signaturbasert deteksjon. Hva betyr dette?

a) Det betyr at det tas et "bilde" av systemet i ren tilstand og gjøres en vurdering av endringer som avviker fra bildet.
b) Det betyr at det letes etter egenskaper som er karakteristisk for skadevare.
c) Det betyr at det finnes en liste med sekvenser av kode som kjennetegner kjent skadevare. Ved å lete gjennom maskinkode etter disse sekvensene kan skadevare oppdages.
d) Det betyr at signerte sertifikater bekrefter at skadevare ikke finnes og at du kan være trygg på at overføring av data ikke kan avlyttes.

1.9 Hva mener vi med «metamorfe virus»?

a) Virus som endrer sin egen kode hver gang en ny fil blir infisert.
b) Virus som kun infiserer metadatene til et objekt eller en fil.
c) Skadevare som på egenhånd er i stand til å finne nye ofre og spre seg til disse via internett.
d) Skadevare som utgir seg for å være et nyttig program.

1.10 Hvorfor bør vi benytte kredittkort når vi handler på nett?

a) Fordi det da alltid vil være dekning på kortet/kontoen.
b) Fordi nettbutikken ikke kan misbruke informasjonen, da kredittkort er knyttet opp mot bankID.
c) Fordi personopplysningsloven §49 sier at den behandlingsansvarlige skal erstatte skade som er oppstått som følge av at personopplysninger er behandlet i strid med loven.
d) Fordi finansavtaleloven §54 gir rett til å fremme pengekrav for mangelfull vare eller tjeneste mot den som har gitt kreditten.

1.11 Hvorfor benytter svindlere ofte linker med kortadresser på nettet?

a) Fordi en kort nettadresse virker mindre mistenkelig enn en lang nettadresse.
b) Fordi kortadresser vil alltid sende oss videre til en nettside som inneholder skadevare.
c) Fordi vi ut fra nettadressen ikke kan se hvor linken sender oss.
d) Fordi det er vanskeligere for politiet å finne ut hvem som står bak nettadressen.

1.12 Hvilken oppgave har en brannmur, når vi snakker om sikkerhetsarkitektur?

a) Brannmuren stopper all nettverkstrafikk ut og inn fra et nettverkssegment.
b) Brannmuren kontrollerer utgående nettverkstrafikk.
c) Brannmuren stopper all nettverkstrafikk inn til et nettverkssegment.
d) Brannmuren kontrollerer inngående og utgående nettverkstrafikk.

1.13 Hva er formålet med personopplysningsloven?

a) Loven skal forhindre at sensitive opplysninger lagres elektronisk, slik at personvernet ikke blir krenket.
b) Loven skal beskytte den enkelte mot at personvernet blir krenket og bidra til at personopplysninger behandles i samsvar med personvernhensyn.
c) Loven skal sørge for at alle som registrerer personopplysninger har konsesjon og at ikke sensitive opplysninger overføres til utlandet.
d) Loven skal sørge for at Datatilsynet kan nekte adgang til bruk av fødselsnummer ved registrering av personopplysninger, slik at personvernet ikke blir krenket.

1.14 En virksomhet som behandler personopplysninger er pålagt å etablere internkontroll. Hva skal virksomheten gjøre dersom personopplysninger håndteres i strid med fastlagte rutiner?

a) Da skal virksomheten umiddelbart avslutte behandlingen av personopplysninger.
b) Da skal virksomheten gjennomføre en risikovurdering av informasjonssystemet.
c) Da skal virksomheten iverksette avviksbehandling.
d) Da skal virksomheten kartlegge behandlingen av personopplysninger.

1.15 Hva er en demilitarisert sone (DMZ)?

a) DMZ er en ytre sikkerhetsbarriere som er plassert mellom intern/ekstern sone og eksternt nettverk, hvor sistnevnte alt er under virksomhetens fysiske kontroll.
b) DMZ er et nettverkssegment som kun tillater kommunikasjon fra sikret sone mot intern sone.
c) DMZ er et nettverkssegment som benyttes til å isolere tjenester og styre trafikk mellom sikkerhetssoner ved hjelp av teknisk utstyr.
d) DMZ er et nettverkssegment som inneholder en VPN-forbindelse mellom avdelingskontor og intern sone,

2 Del 2 – Grunnleggende begreper (teller 40 %)

2.1 HTTPS

Forklar forskjellen mellom HTTP og HTTPS og beskriv hva HTTPS beskytter brukeren mot.

2.2 To-faktor autentisering

Forklar hva to-faktor-autentisering er.

2.3 Social engineering

Forklar begrepet social engineering og nevn minst tre menneskelige egenskaper som svindlere ofte utnytter i den forbindelse.

2.4 DNS-server (Domain Name System)

Forklar hva en DNS-server er og hvordan hackere kan påvirke DNS-oppslagene.

2.5 Internkontroll

Personopplysningsloven §14 stiller krav til internkontroll for den som behandler personopplysninger. Forklar hva internkontroll er og hvilke tre hovedelementer internkontroll består av.

2.6 Sikkerhetsstrategi

Forklar hva vi mener med begrepet sikkerhetsstrategi.

2.7 Systemteknisk sikkerhet - soner

Datatilsynet mener at sikkerhetsarkitekturen skal deles inn i adskilte soner. Forklar hvilke soner man bør ha og hvordan disse kan skilles fra hverandre.

3 Del 3 – Risikovurdering av informasjonssystem (teller 40 %)

Case

Bumpibump barnehage AS er en ganske stor privat barnehage med 120 barn fordelt på 3 avdelinger inndelt etter alder. Styrer i barnehagen er Berit Berg. Barnehagen har 35 ansatte, noen av dem arbeider deltid. Barnehagen holder til i moderne lokaler og har i tillegg fine utearealer. Barnehagen har ulike tilbud om oppholdstid; inntil 10 timer per uke, inntil 20 timer per uke, inntil 30 timer per uke og inntil 40 timer per uke.

Barnehagen har en IT-løsning som kjører på en av barnehagens PC-er. Her lagres all informasjon som er nødvendig for driften av barnehagen. Eksempelvis inneholder løsningen bilde av barnet, informasjon om barnets navn, fødselsnummer, adresse, avtale om oppholdstid, avtale om pris, avtale om betalingsmåte, avtale om frukt-/melk-ordning mm. Her finnes også informasjon om barnet har allergier eller andre sykdommer som barnehagen må være klar over og om barnet ikke skal spise spesiell mat av religiøse eller andre grunner. I tillegg finnes her navn på foresatte med adresse, email, telefon, arbeidssted, inntekt o.l. Det kreves passord for å benytte programvaren, men dataene i løsningen blir lagret ukryptert på katalogen C:\\Dokumenter\bhgsys\....
Sikkerhetskopiering kjøres automatisk daglig og lagres på en ekstern harddisk tilknyttet PC-en. Den lagres i en skuff i skrivebordet der PC-en står.

IT-løsningen håndterer også søknadsprosessen på web, månedlig fakturering av dem som har plass i barnehagen og har automatisk overføring av bilag/transaksjoner til regnskapskontoret som barnehagen benytter. Barnehagesatsen varierer utfra familiens totale inntekt.

I løsningen finnes gode muligheter for å lage rapporter og statistikker. Det er også muligheter for enkelt- og masseutsendelser av SMS og e-post. Dette benyttes til å informere foreldrene om planleggingsdager, lusesmitte mm.

PC-en er stasjonert på personalrommet. PC-en er ikke passordbeskyttet og den brukes av alle ansatte i barnehagen ved behov, f.eks. til å skrive brev eller meldinger til foreldre.
I barnehagen har man et trådløst lokalt datanett(LAN), som også er tilknyttet internett. Dette nettet er ikke sikret med passord, da det er praktisk at foreldre og andre som er på besøk får tilgang til internett.

Printeren står på personalrommet. Etter oppstart på høsten skrives det ut rapporter som ligger på personalrommet, slik at de ansatte skal få oversikt over barna. Lister med navn på barn med matallergi og barn som ikke skal spise spesielle matvarer av religiøse eller andre grunner, er hengt opp ved kjøleskapet i spiserommet slik at man f.eks. skal være trygg på at barn ikke får allergiske reaksjoner. Det er ofte foreldre og andre besøkende sammen med barna når de spiser og foreldremøter blir også ofte holdt i spiserommet.

Oppgave

Du arbeider som konsulent innen informasjonssikkerhet. Styreren i Bumpibump barnehage AS, Berit Berg, har tatt kontakt med deg for å gjennomføre en risikovurdering av IT-løsningen. Hun vet at det er spesielle krav til informasjonssikkerheten ved behandling av personopplysninger. En av foreldrene har tatt opp med henne at hun synes ikke noe om at alle

som er på spiserommet kan se at hennes barn lider av nøtte- og glutenallergi, hun lurer også på om barnehagen er like «slumsete» med personopplysninger på andre områder. Berit Berg ønsker å følge regelverket og vil derfor gjennomføre en risikovurdering.

Du kjenner Personopplysningsforskriftens §2-1, der det står at sikkerhetstiltakene skal stå i forhold til sannsynlighet og konsekvens av sikkerhetsbrudd og at arbeidet med å avdekke risiko ikke bør være mer omfattende eller formalisert enn strengt tatt nødvendig. Ha dette i bakhodet når du besvarer spørsmålene nedenfor.

(I oppgavene nedenfor blir du bedt om å lage noen tabeller. Tabellverktøy finner du på verktøylinja i Wiseflow. Velg «Table» – «insert table»)

3.1 Du skal gjennomføre planlegging av risikovurdering

Beskriv kort mål(hypotese), bakgrunn og avgrensninger for risikovurderingen.
Nevn hvilke personer/roller du vil ha med i en slik prosjektgruppe.
Du kan gjerne sette dette opp i en tabell.

3.2 Du skal gjennomføre kartlegging av personopplysninger

Lag en tabell over hvilke personopplysninger som behandles. Dersom du ikke har nok opplysninger i teksten ovenfor, tar du egne forutsetninger.

Tabellen bør inneholde følgende kolonner:

- Informasjonstype
- Formål med behandlingen
- Hjemmel for behandling
- Melde-/konsesjonsplikt
- Sensitivitet
- Taushetsplikt
- Omfang
- Sikkerhetsbehov

Hjemmel for behandling av personopplysninger om barn i barnehage finnes i barnehageloven. Unntak fra melde- og konsesjonsplikt jf. Personopplysningsforskriften §7-21.

3.3 Du skal designe en tabell som viser mulige konsekvenser, kvantitativt og kvalitativt.

Ta utgangspunkt i målet om å sikre personopplysninger. Bruk fire nivå.

3.4 Du skal designe en tabell som viser sannsynlighet for sikkerhetsbrudd.

Gjør gjerne sannsynlighetsvurdering ut fra motivering. Bruk fire nivå.

3.5 Du skal identifisere uønskede hendelser som berører personvernet.

Velg deg ut 3 hendelser. Lag en tabell som inneholder hendelse, årsak, mulig konsekvens, type sikkerhetsbrudd, type hendelse, sannsynlighet, konsekvens, risiko og akseptabel risiko.

Sammen med Berit Berg har du kommet frem til et akseptabelt risikonivå:
Risiko < 4 akseptabel risiko, ingen tiltak
Risiko = 4 tiltak må vurderes
Risiko > 4 uakseptabel risiko, tiltak må iverksettes.

3.6 Lag en risikomatrise for å beskrive risiko.

Plassér hendelsene i en risikomatrise. Risikomatrisen må også vise akseptabelt risikonivå.

(For å endre farge på celler i tabellen velger du «table» – «cell/row properties» – «advanced» – «background color». Fargen angis med den engelske betegnelsen, f.eks. «red»)

3.7 Beskriv aktuelle tiltak for å håndtere risiko.

Lag en tabell over de viktigste tiltakene som barnehagen kan sette i verk for å håndtere risiko.

3.8 Forutsatt at barnehagen har implementert dine forslag til tiltak. Lag en risikomatrise (etter tiltak) med de samme hendelsene som tidligere.

Plassér hendelsene på nytt i en matrise. Vis at tiltakene har medført at risiko nå er innenfor akseptabelt risikonivå.

Lykke til!

1 Del 1 Fleirvalsoppgåver (tel 20 %)

Poengrekning fleirvalsspørsmål:

- Oppgåva består av 15 fleirvalsspørsmål.
- Kvart spørsmål har 4 svaralternativ.
- Berre 1 alternativ er rett.
- Du kan velje å «gardere» ved å svare på fleire enn eitt alternativ.
- Du får 3 poeng for rett svar, -1 poeng for kvart gale svar og 0 poeng for spørsmål som ikkje er svart på.
- Oppgje svar på forma: Spørsmål 1. a (Spørsmål 1.a,d om du garderer) (ikkje gjenta ordlyden i spørmål eller svar)
- Dersom a er rett og d er feil får du 3-1=2 poeng på dette spørsmålet.
- For å få maksimalt tal på poeng (3) må du altså svare med berre eitt (korrekt) alternativ.

1.1 Eit av temaa i datasikkerheit er konfidensialitet. Kva meiner vi med dette omgrepet?

a) At informasjon alltid er tilgjengeleg for rette vedkomande.
b) At datasikkerheita er underlagt eit kvalitetssystem.
c) At informasjonen ikkje er tilgjengeleg for uvedkomande.
d) At brukarane av informasjon kan stole på at informasjonen er rett.

1.2 Eit anna tema i datasikkerheit er integritet. Kva meiner vi med dette omgrepet?

a) At informasjon alltid er tilgjengeleg for rette vedkomande.
b) At personopplysingar på avvege ikkje skal skade ein person sitt omdømme.
c) At informasjonen ikkje er tilgjengeleg for uvedkomande.
d) At brukarane av informasjon kan stole på at informasjonen er rett.

1.3 Kva meiner vi med omgrepet autentisering?

a) Med autentisering meiner vi metodar for å kunne identifisere kven som prøver å logge seg på.
b) Med autentisering meiner vi metodar for å spore aktivitet i eit system.
c) Med autentisering meiner vi å gi rette personar tilgang til dei rette ressursane.
d) Med autentisering meiner vi at påloggingsinformasjonen blir behandla kryptert.

1.4 Kva meiner vi med omgrepet phishing?

a) Phishing tyder å forsøke å få sensitiv informasjon frå ein brukar ved å sende han/henne ein e-post, eller lure han/henne inn på ei falsk nettside, som ser ekte ut.
b) Phishing tyder å kome seg forbi sikkerheitsmekanismane til eit system og infisere dette med skadevare.
c) Phishing tyder å nytte ein annan person sin identitet, til dømes i samband med bestilling av ei vare eller teneste.
d) Phishing tyder å sende ei melding som skal få nokon til å tru på noko usant, til dømes at vedkomande har blitt infisert av skadevare på si maskin.

1.5 Kva kallar vi skadevare som låser maskina for bruk eller krypterer data på disken og kor svindlaren krev løysepengar for å frigjere maskina eller data?

a) Rootkit.
b) Hijacking.
c) Ransomware.
d) Hoax.

1.6 Kva meiner vi med omgrepet «mail spoofing»?

a) Med «mail spoofing» meiner vi å forfalske innholdet i ein e-post.
b) Med «mail spoofing» meiner vi å sortere e-post slik at «spam» hamnar i søppelpostmappa.
c) Med «mail spoofing» meiner vi å forfalske avsendar av e-post.
d) Med «mail spoofing» meiner vi å manuelt skrive og sende e-post ved hjelp av SMTP-kommandoar.

1.7 Skadevare består av fleire ulike komponentar som kvar har si oppgåve. Kva for fire komponentar er dette normalt?

a) Trojaner, virus, ormar og makrovirus.
b) Stridshovud, spreiing, kamuflasje og utpressing.
c) Nyttelast, kamuflasje, infeksjon og inkubasjonstid.
d) Stridshovud, spreiing, kamuflasje og nyttelast.

1.8 For å oppdage skadevare nyttar vi ofte signaturbasert deteksjon. Kva tyder dette?

a) Det tyder at det takast eit "bilete" av systemet i rein tilstand og gjerast ei vurdering av endringar som avvik frå biletet.
b) Det tyder at det leitast etter eigenskapar som er karakteristisk for skadevare.
c) Det tyder at det finnast ei liste med sekvensar av kode som kjenneteiknar kjend skadevare. Ved å leite gjennom maskinkode etter desse sekvensane kan skadevare oppdagast.
d) Det tyder at signerte sertifikat bekreftar at skadevare ikkje finnast og at du kan være trygg på at overføring av data ikkje kan avlyttast.

1.9 Kva meiner vi med «metamorfe virus»?

a) Virus som endrar sin eigen kode kvar gong ei ny fil blir infisert.
b) Virus som berre infiserer metadataa til eit objekt eller ei fil.
c) Skadevare som på eigen hand er i stand til å finne nye offer og spreie seg til desse via internett.
d) Skadevare som utgjev seg for å være eit nyttig program.

1.10 Kvifor bør vi nytte kredittkort når vi handlar på nett?

a) Fordi det då alltid vil være dekning på kortet/kontoen.
b) Fordi nettbutikken ikkje kan misbruke informasjonen, då kredittkort er knytta opp mot bankID.
c) Fordi personopplysingslova §49 seier at den behandlingsansvarlege skal erstatte skade som er oppstått som følgje av at personopplysingar er behandla i strid med lova.
d) Fordi finansavtalelova §54 gjev rett til å fremje pengekrav for mangelfull vare eller teneste mot den som har gjeve kreditten.

1.11 Kvifor nyttar svindlarar ofte linkar med kortadresser på nettet?

a) Fordi ei kort nettadresse verkar mindre mistenkjeleg enn ei lang nettadresse.
b) Fordi kortadresser vil alltid sende oss vidare til ei nettside som inneheld skadevare.
c) Fordi vi ut frå nettadressa ikkje kan sjå kor linken sender oss.
d) Fordi det er vanskelegare for politiet å finne ut kven som står bak nettadressa.

1.12 Kva for oppgåve har ein brannmur, når vi snakkar om sikkerheitsarkitektur?

a) Brannmuren stoppar all nettverkstrafikk ut og inn frå eit nettverkssegment.
b) Brannmuren kontrollerer utgåande nettverkstrafikk.
c) Brannmuren stoppar all nettverkstrafikk inn til eit nettverkssegment.
d) Brannmuren kontrollerer inngåande og utgåande nettverkstrafikk.

1.13 Kva er føremålet med personopplysingslova?

a) Lova skal forhindre at sensitive opplysingar lagrast elektronisk, slik at personvernet ikkje blir krenkt.
b) Lova skal beskytte den einskilde mot at personvernet blir krenkt og bidra til at personopplysingar blir behandla i samsvar med personvernomsyn.
c) Lova skal sørgje for at alle som registrerer personopplysingar har konsesjon og at ikkje sensitive opplysingar blir overført til utlandet.
d) Lova skal sørgje for at Datatilsynet kan nekte tilgjenge til bruk av fødselsnummer ved registrering av personopplysingar, slik at personvernet ikkje blir krenkt.

1.14 Ei verksemd som behandlar personopplysingar er pålagt å etablere internkontroll. Kva skal verksemda gjere dersom personopplysingar blir handtert i strid med fastlagte rutiner?

a) Då skal verksemda straks avslutte behandlinga av personopplysingar.
b) Då skal verksemda gjennomføre ei risikovurdering av informasjonssystemet.
c) Då skal verksemda sette i verk avviksbehandling.
d) Då skal verksemda kartlegge behandlinga av personopplysingar.

1.15 Kva er ei demilitarisert sone (DMZ)?

a) DMZ er ei ytre sikkerhetsbarriere som er plassert mellom intern/ekstern sone og eksternt nettverk, kor sistnemnde alt er under verksemda si fysiske kontroll.
b) DMZ er eit nettverkssegment som berre tillét kommunikasjon frå sikra sone mot intern sone.
c) DMZ er eit nettverkssegment som nyttast til å isolere tenester og styre trafikk mellom sikkerhetssoner ved hjelp av teknisk utstyr.
d) DMZ er eit nettverkssegment som inneheld eit VPN-samband mellom avdelingskontor og intern sone.

2 Del 2 – Grunnleggjande omgrep (tel 40 %)

2.1 HTTPS

Forklar skilnaden mellom HTTP og HTTPS og beskriv kva HTTPS beskyttar brukaren mot.

2.2 To-faktor autentisering

Forklar kva to-faktor-autentisering er.

2.3 Social engineering

Forklar omgrepet social engineering og nemn minst tre menneskelege eigenskapar som svindlarar ofte utnyttar i samband med dette.

2.4 DNS-server (Domain Name System)

Forklar kva ein DNS-server er og korleis hackere kan påverke DNS-oppslaga.

2.5 Internkontroll

Personopplysingslova §14 stiller krav til internkontroll for den som behandlar personopplysingar. Forklar kva internkontroll er og kva for tre hovudelement internkontroll består av.

2.6 Sikkerhetsstrategi

Forklar kva vi meiner med omgrepet sikkerheitsstrategi.

2.7 Systemteknisk sikkerhet - soner

Datatilsynet meiner at sikkerheitsarkitekturen skal delast inn i åtskilde soner. Forklar kva for soner ein bør ha og korleis desse kan skiljast frå kvarandre.

3 Del 3 – Risikovurdering av informasjonssystem (tel 40 %)

Case

Bumpibump barnehage AS er ein ganske stor privat barnehage med 120 barn fordelt på 3 avdelingar delt inn etter alder. Styrar i barnehagen er Berit Berg. Barnehagen har 35 tilsette, nokre av dei arbeider deltid. Barnehagen held til i moderne lokaler og har i tillegg fine uteareal. Barnehagen har ulike tilbod om opphaldstid; inntil 10 timar per veke, inntil 20 timar per veke, inntil 30 timar per veke og inntil 40 timar per veke.

Barnehagen har ei IT-løysing som køyrer på ein av PC-ane i barnehagen. Her lagrast all informasjon som er naudsynt for drifta av barnehagen. Til dømes inneheld løysinga bilete av barnet, informasjon om barnets navn, fødselsnummer, adresse, avtale om opphaldstid, avtale om pris, avtale om betalingsmåte, avtale om frukt-/melk-ordning mm. Her finnast og informasjon om barnet har allergi eller andre sjukdomar som barnehagen må være klar over og om barnet ikkje skal ete spesiell mat av religiøse eller andre grunnar. I tillegg finnast her navn på føresette med adresse, email, telefon, arbeidsstad, inntekt o.l. Det krevjast passord for å nytte programvara, men dataa i løysinga blir lagra ukryptert på katalogen C:\\Dokumenter\bhgsys\....
Sikkerheitskopiering blir køyrt automatisk dagleg og blir lagra på ein ekstern harddisk knytt til PC-en. Den blir lagra i ein skuff i skrivebordet der PC-en står.

IT-løysinga handterer og søknadsprosessen på web, månadleg fakturering av dei som har plass i barnehagen og har automatisk overføring av bilag/transaksjonar til rekneskapskontoret som barnehagen nyttar. Barnehagesatsen varierer ut frå familien si totale inntekt.

I løysinga finnast gode mogelegheiter for å lage rapportar og statistikkar. Det er og mogelegheit for enkelt- og masseutsendingar av SMS og e-post. Dette blir nytta til å informere foreldrene om planleggingsdagar, lusesmitte mm.

PC-en er stasjonert på personalrommet. PC-en er ikkje passordbeskytta og den blir bruka av alle tilsette i barnehagen ved behov, t.d. til å skrive brev eller meldingar til foreldre.
I barnehagen har dei eit trådlaust lokalt datanett(LAN), som og er knytt til internett. Dette nettet er ikkje sikra med passord, då det er praktisk at foreldre og andre som er på vitjing får tilgjenge til internett.

Printeren står på personalrommet. Etter oppstart på hausten skrivast det ut rapportar som ligg på personalrommet, slik at dei tilsette skal få oversyn over barna. Lister med navn på barn med matallergi og barn som ikkje skal ete spesielle matvarer av religiøse eller andre grunnar, er hengt opp ved kjøleskåpet i spiserommet slik at ein t.d. skal væra trygg på at barn ikkje får allergiske reaksjonar. Det er ofte foreldre og andre vitjande saman med barna når dei et og foreldremøter blir og ofte halde i spiserommet.

Oppgave

Du arbeider som konsulent innan informasjonssikkerheit. Styraren i Bumpibump barnehage AS, Berit Berg, har tatt kontakt med deg for å gjennomføre ei risikovurdering av IT-løysinga. Ho veit at det er spesielle krav til informasjonssikkerheita ved behandling av personopplysingar. Ein av foreldrene har tatt opp med henne at ho ikkje synast noko om at alle

som er på spiserommet kan sjå at hennar barn lid av nøtte- og glutenallergi og ho lurar på om barnehagen er like «slumsete» med personopplysingar på andre område. Berit Berg ynskjer å følgje regelverket og vil difor gjennomføre ei risikovurdering.

Du kjenner Personopplysingsforskrifta §2-1, der det står at sikkerheitstiltaka skal stå i forhold til sannsynlegheit og konsekvens av sikkerheitsbrudd og at arbeidet med å avdekkje risiko ikkje bør være meir omfattande eller formalisert enn strengt tatt naudsynt. Ha dette i bakhovudet når du svarar på spørsmåla nedanfor.

(I oppgåvene nedanfor blir du bedd om å lage nokre tabellar. Tabellverktøy finn du på verktøylinja i Wiseflow. Velg «Table» – «insert table»)

3.1 Du skal gjennomføre planlegging av risikovurdering

Beskriv kort mål(hypotese), bakgrunn og avgrensingar for risikovurderinga.
Nevn kva for personar/roller du vil ha med i ei slik prosjektgruppe.
Du kan gjerne setje dette opp i ein tabell.

3.2 Du skal gjennomføre kartlegging av personopplysingar

Lag ein tabell over kva for personopplysingar som blir behandla. Dersom du ikkje har nok opplysingar i teksten ovanfor, tek du eigne føresetnader.

Tabellen bør innehalde følgjande kolonner:

- Informasjonstype
- Føremål med behandlinga
- Heimel for behandling
- Melde-/konsesjonsplikt
- Sensitivitet
- Teieplikt
- Omfang
- Sikkerheitsbehov

Heimel for behandling av personopplysingar om barn i barnehage finnast i barnehagelova. Unntak frå melde- og konsesjonsplikt jf. Personopplysingsforskrifta §7-21.

3.3 Du skal designe ein tabell som viser mogelege konsekvensar, kvantitativt og kvalitativt.

Ta utgangspunkt i målet om å sikre personopplysingar. Bruk fire nivå.

3.4 Du skal designe ein tabell som viser sannsynlegheit for sikkerheitsbrudd.

Gjer gjerne sannsynlegheitsvurdering ut frå motivering. Bruk fire nivå.

3.5 Du skal identifisere uønskte hendingar som rører ved personvernet.

Velg deg ut 3 hendingar. Lag ein tabell som inneheld hending, årsak, mogeleg konsekvens, type sikkerheitsbrudd, type hending, sannsynlegheit, konsekvens, risiko og akseptabel risiko.

Saman med Berit Berg har du kome fram til eit akseptabelt risikonivå:
Risiko < 4 akseptabel risiko, ingen tiltak
Risiko = 4 tiltak må vurderast
Risiko > 4 uakseptabel risiko, tiltak må setjast i verk.

3.6 Lag ei risikomatrise for å beskrive risiko.

Plassér hendingane i ei risikomatrise. Risikomatrisa må og vise akseptabelt risikonivå.

(For å endre farge på celler i tabellen vel du «table» – «cell/row properties» – «advanced» – «background color». Fargen angjev du med den engelske nemninga, f.eks. «red»)

3.7 Beskriv aktuelle tiltak for å handtere risiko.

Lag ein tabell over dei viktigaste tiltaka som barnehagen kan setje i verk for å handtere risiko.

3.8 Føresett at barnehagen har implementert dine forslag til tiltak. Lag ei risikomatrise (etter tiltak) med dei same hendingane som tidlegare.

Plassér hendingane på nytt i ei matrise. Vis at tiltaka har medført at risiko nå er innanfor akseptabelt risikonivå.

Lykke til!