BOKMÅL

Høgskolen i Sørøst-Norge

EKSAMENSFORSIDE

Skriftlig eksamen med tilsyn

Emnekode: 6123/6123N	Emnenavn: Informasjonssikkerhet	
Dato: Onsdag 4. Januar 2017	Tid fra / til:	Ant. timer: 4
Ansv. faglærer: Øystein Wendelborg		
Campus: Bø	Fakultet: IØI	
Antall oppgaver: 17	Antall vedlegg: Ett	Ant. sider inkl. forside og vedlegg: 6
Tillatte hjelpemidler (jfr. emnebeskrivelse): Ingen		
Opplysninger om vedlegg: I vedlegget finner du "Figur 1" som det er referert til i oppgave 3e.		
Merknader: Eksamen gjennomføres i Wiseflow. Resultatet vil komme på FS.		

KANDIDATEN MÅ SELV KONTROLLERE AT OPPGAVESETTET ER FULLSTENDIG

Del 1. Definisjoner.

(Vekt: 30%)

1.1. Forklar kort begrepene:
a) Konfidensialitet,
b) Integritet,
c) Tilgjengelighet.

1.2. Sikkerhetsarkitektur.
a) Gjør rede for begrepet "Defense in Depth" i sikkerhetsarkitektur.
b) Begrepet "brannmur" kan forstås på en rekke forskjellig måter innenfor faget informasjonssikkerhet. Nevn minst to ulike typer av brannmur som er aktuelle innenfor sikkerhetsarkitektur og forklar hvilke ulike oppgaver disse typene kan ha i denne sammenhengen.
c) Forklar begrepet "awareness" og
d) forklar med minst to eksempler hvordan menneskene i en organisasjon, i tillegg til tekniske løsninger, er viktige for å etablere en systematisk informasjonssikkerhet.

Del 2 Sikkerhetsarkitektur og internkontroll.

(Teller 40 %).
Www.husefyll.no er dominerende på det norske markedet i salg av interiørdetaljer på nett. Selskapet har både sin egen nettbutikk med over 10000 kundeprofiler, og den drifter samtidig en rekke andre nettbutikker for andre aktører. Bedriften har valgt å eie og drifte sin egen datasentral som dekker funksjonalitet av typen:

- Frontend webtjenere, portal for nettkunder.
- Inngående epost fra eksterne nett.
- Backend Webtjener.
- Systemtjenester for intern DHCP etc.
- Brukerdatabaser, domenekontrollere (AD).
- Filtjener for interne ansatte.
- Kalendersystem.
- Tjener for web-mail.
- Administrasjon av klienter, f.eks. antivirus og lisenser.
- Printer-tjenester.
- Ekstern navnetjener/DNS.
- VPN-tjenester for mobile ansatte.
- Interne tjenere for økonomisystemer, Personalsystemer (HR) og Forskning og Utvikling (FOU).
- Interne tjenere for kunder med særlige krav til lagring av personopplysninger.
- Sak-arkivsystem for kundeporteføljen
- BMC footprints (BMCF) system for helpdesk, tjenesteutvikling og oppfølging av feilsituasjoner. BMCF omfatter også logger som brukes av internrevisjonen.

Kravene til driftsstabilitet og 99 % oppetid er svært høyt, og organisasjonens policydokumenter stiller høye krav til informasjonssikkerhet.

2a) Beskriv en sikkerhetsarkitekturløsning med

- en sikret sone,
- en intern sone,
- DMZ.

I løsningen din skal du fordele tjenestene ovenfor på disse tre alternativene. Hver tjeneste skal forekomme bare en gang i løsningen din. Sammen med løsningen skal du skrive en kort kommentar som begrunner og forklarer hvorfor tjenestene er fordelt slik. Bruk gjerne en figur som du kan referere til i besvarelsen din.
Forklar hva som kjennetegner hver enkelt sone og forklar andre faguttrykk du gjør deg nytte av der det er nødvendig. Du kan gjerne referere til faguttrykk du allerede har definert i del 1.

2b) Beskriv og begrunn relevante sikkerhetsbarrierer for denne løsningen.

2c) Gjør rede for bakgrunnen for at en organisasjon har et internkontrollsystem (IKS), og skisser kort hvordan dette er bygget opp.

Del 3 ROS-analyse.
(Vekt: 30%)
Netspace AS ligger i Lillefjord kommune og leverer tjenester innenfor rådgivning, drift av infrastruktur i bredbåndsnett, lagring og overvåkning. Datasentralen har ca. 2000 kunder ved full kapasitet. Sentralen har rundt 25 ansatte. Stabilitet og oppetid hele døgnet hele året er derfor avgjørende for tilliten mellom kunder og leverandør. Forholdet til kundene er regulert i kontrakter av typen SLA (Service Level Agreement). For de mest krevende og verdifulle kundene er det krav til 99 % oppetid.

Anne Jording arbeider som sikkerhetskonsulent ved Netspace AS. Hennes hovedoppgave er å ha best mulig oversikt over drifts- og informasjonssikkerhet.
Med så høye krav til kvalitet går mye av hennes arbeidstid med til kartlegging og oppfølging av løpende sikkerhetsspørsmål, utforming av planer samt informasjonsarbeid overfor styre, ledelse og kunder. Hun arbeider også med kartlegging og oppfølging av løpende sikkerhetsspørsmål med sikte på en driftssituasjon med færre feil for hvert år som går.

I en rapport fra det lokale elektrisitetsverket som hun nylig har mottatt, går det fram at kvaliteten på strømleveransene gir grunn til uro. Rapporten slår fast at det er:

- 48 % sanns. for minst ett strømutfall på inntil 1-2 minutter i løpet av ett år.
- 21 % sannsynlighet for minst ett strømutfall på inntil 1 time i løpet av ett år.
- 5 % sannsynlighet for minst ett strømutfall på inntil 12 timer i løpet av ett år.
- 1 % sannsynlighet for minst ett strømutfall på inntil 1 døgn i løpet av ett år.

Anne har hatt møte med sentralens styre og ledelse og informert følgende om "ikke varslede strømutfall":

- Strømutfall på 1-2 minutter har ingen konsekvenser i forhold til kontraktene, men det må påregnes at en del kunder vil klage.
- Strømutfall en gang i året på inntil 1 time vil ikke føre til kontraktbrudd eller erstatningsansvar, men vil gjøre det vanskeligere å holde på de mest krevende og lønnsomme kundene på sikt.
- Strømutfall på inntil 10 timer en eller flere ganger i året vil føre til at 10 % av kundene vil si opp kontraktene og gå til andre leverandører.
- Strømutfall på inntil et døgn vil føre til at flere enn halvparten av kundene vil gå til andre leverandører.

Til møtet skrev Anne en rapport med forslag til tiltak og budsjett for tiltakene:

- Oppgradering av strømnett i datasentralen.
- Anskaffelse av 100 KVA dieselaggregat.
- Oppgradering av 4 Online-UPS.

(Anne utarbeidet også budsjett med full oversikt over kostnadene som tiltakene medfører. Det trenger du ikke å bruke tid på her. I besvarelsen din trenger du bare å henvise til budsjett der du selv finner det nødvendig).

Rapporten inneholdt også ROS-analyser som visualiserte disse hendelsene:

- En risikomatrise som viste situasjonen før tiltak.
- En risikomatrise som viste situasjonen etter at forslag til tiltak er implementert.

Anne har argumentert godt, og styre og ledelse bad Anne gjennomføre tiltakene hun har foreslått. Etter at tiltakene er gjennomført og testet og datasentralen er kommet i normal drift igjen er status slik:

- Intern strømtilførsel til kjernenettet i datasentralen er blitt utformet slik at alle vitale deler får strøm fra en sentralisert pool av UPS-er. Det er etablert et eget rom for UPS-er.
- UPS-ene kobler automatisk inn ved strømutfall, og det er ikke nødvendig med automatisk nedkjøring av tjenere.
- Dieselaggregatet er konfigurert slik at det mater 220 v vekselstrøm til UPS-ene. Dieselaggregatet starter automatisk 10 minutter etter utfall av ekstern strømtilførsel, som er godt innenfor tidsmarginene UPS-ene er dimensjonert for.

Oppgaver:

3a Lag en tabell som beskriver sannsynligheter for hendelsen strømutfall *før* Anne gjennomførte tiltakene.

3b Lag en tabell som beskriver konsekvensene av hendelsen strømutfall *før* Anne gjennomførte tiltakene.

3c Lag risikomatrisen som visualiserer sannsynligheter for og konsekvenser av hendelsen strømutfall *før* tiltak. Beskriv akseptkriteriene.

- Bruk grønn farge for å visualisere "ingen konsekvenser".

- Bruk gul farge for å visualisere "noen, men akseptable konsekvenser".
- Bruk rød farge for å visualisere "uakseptable konsekvenser".

3d Skriv en kort vurdering av sannsynlighet for hendelsen strømutfall *etter* at tiltak er satt i verk.

3e Datasentralen har ikke tidligere hatt en sentralisert UPS-løsning. Bruk Figur 1 i vedlegget og begrunn hvorfor dette er viktig, og forklar hvilke fordeler en slik løsning byr på.

3f Beskriv hvordan de tre krafttypene behandles i en slik løsning.

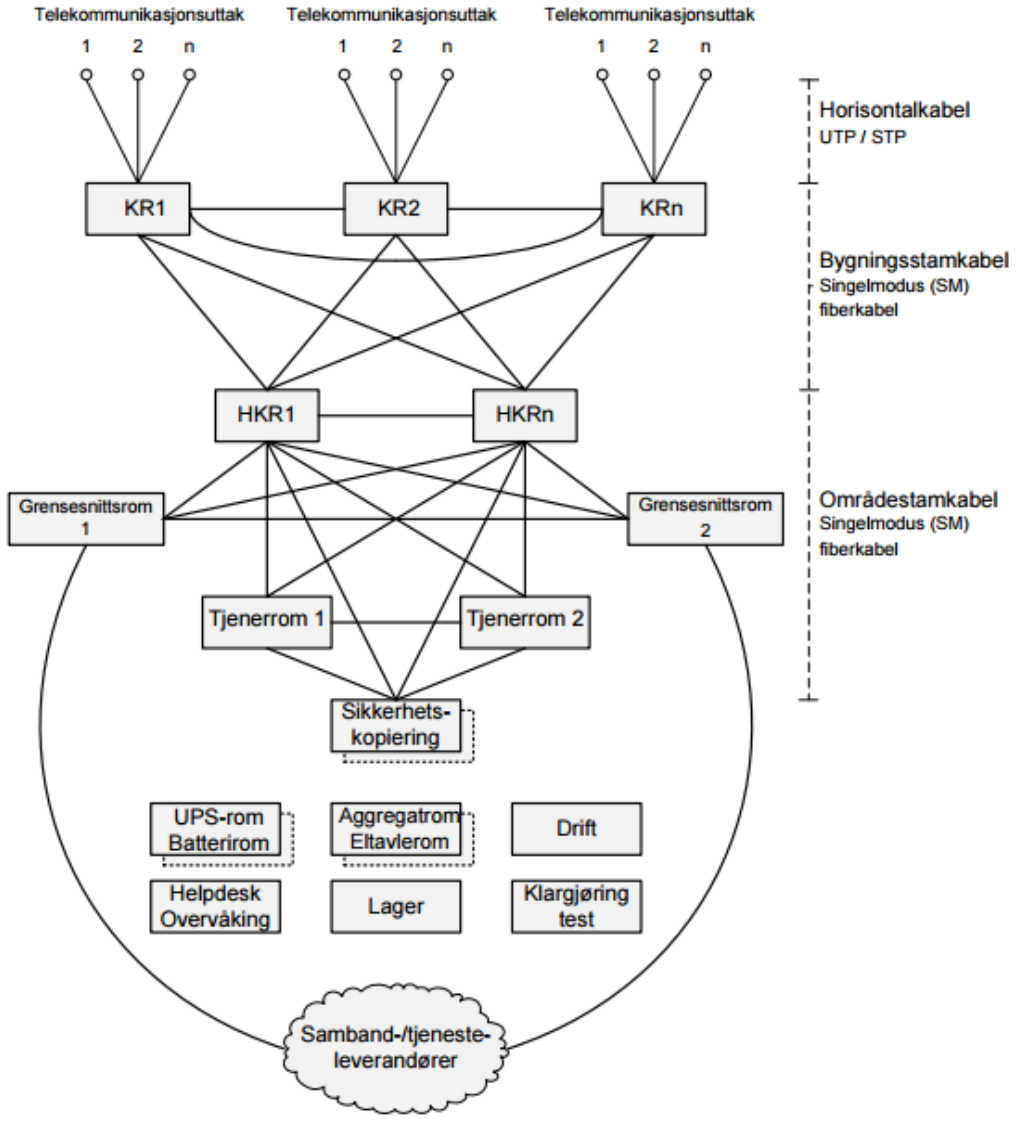
3g Lag risikomatrisen som visualiserer sannsynligheter for og konsekvenser av hendelsen strømutfall *etter* tiltak. Bruk samme fargesymbolikk som i 3c.

Besvarelsen din skal tydelig vise at du har rutine i å bruke ROS-metodikk og relevant terminologi basert på gjennomgått pensum. Velger du å bruke en annen metodikk, skal du oppgi navn og kilder for denne metodikken og forklare den eksplisitte framgangsmåten.

Slutt på eksamenstekst.

Vedlegg 1

FAGSPESIFIKASJON FRA UNINETT



Figur 1. Kjernenettverk. (Hentet fra UFS 103 fra Uninett).