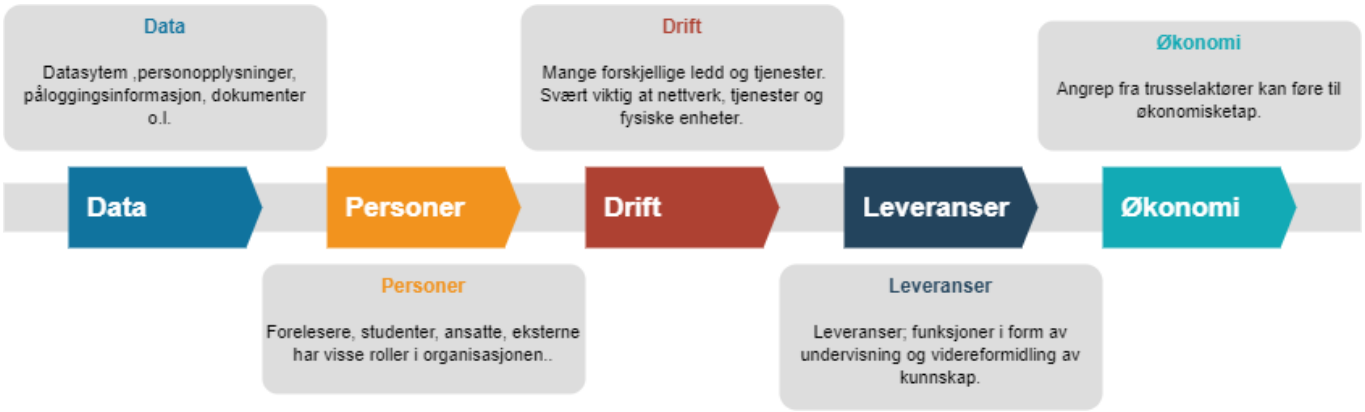
Risikoanalyse og beredskapsplaner

Del 1 – Risikoanalyse

Kartlegging

Kartlegging av Høgskolen i Østfold sine hoveddeler vil gi en bedre forståelse og et lite innblikk i de forskjellige leddene som den består av. Deretter er det nødvendig å trekke forskjellige underledd i disse delene i verdivurderingen. Disse verdiene vil i hovedsak være det som er i fokus og generelt det som skal sikres med tanke på datasikkerhet. I modellen under er det valgt å trekke frem fem essensielle hoveddeler som denne organisasjonen har.



Data

I en slik organisasjon omgår det store mengder av forskjellig data, blant annet personopplysninger, påloggingsinformasjon, dokumenter o.l. For at sensitiv data ikke skal komme på avveie i trusselaktørens hender er det viktig å sørge at konkrete personer har nok basis kunnskap om håndtering av sensitiv data og om personlig datasikkerhet på nett.

Personer

Høyskolen er bygd av en rekke avdelinger og det innebærer en mengde personer rundt de. Forelesere, studenter, ansatte, eksterne, alle har visse roller i organisasjonen. Det er essensielt at deres informasjon er sikker og konfidensiell.

Drift

Drift av en utdanningsinstitusjon er en omfattende prosess som består av mange forskjellige ledd og tjenester. Svært viktig at nettverk, tjenester og diverse driftsrelaterte fysiske enheter er i drift, med minimalisert nedtid.

Leveranser

Leveranser i denne sammenhengen er tenkt å være funksjoner i form av undervisning og videreformidling av kunnskap i alle former. Som hovedfunksjon av en utdanningsinstitusjon er det en selvfølge at dette alltid leveres i høyest mulig grad.

Økonomi

Selv om en høyskole har ikke direkte materielle verdier, eksisterer det fortsatt en rekke trusler og risiko som kan forårsake økonomiske tap. Slike trusler kan være angrep fra trusselaktører. Svært viktig å sikre seg fra slike angrep for å minimisere finansielle utfordringer.

Verdivurdering

Før risikoanalysen settes i gang er det nødvending å kartlegge verdier som er viktige og er mest verdifulle for organisasjonen. I denne tilfellen vil det i stor grad være snakk om immaterielle verdier i form av funksjoner som drifter organisasjonen i sin helhet. Følgende verdier er definert etter viktighetsgrad for høgskolen og ikke til etter verdi for trusselaktøren.

ID	Verdi	Beskrivelse	Viktighets grad	Klassifisering KIT-triangelet	Konsekvens
V.1	Nettverk	Den mest essensielle delen av drift i en høgskole. Organisasjon er svært avhengig av denne. Nettverk i form av internett gir mulighet å utføre leveranser både for studenter og ansatte. Alle tjenester og systemer er i større eller mindre grad koblet opp mot internett.	Svært høy	Tilgjengelighet	Leveranser, drift, økonomi
V.2	Personopplysninger	Personopplysninger om studenter, ansatte og andre personer som er relatert til Høgskolen er viktige å oppbevare på en sikker måte.	Svært høy	Konfidensialitet, Integritet	Omdømme, økonomi,

		Dette bør oppbevares og behandles i hht. Personvernloven og sikkerhetsloven som er pålagt til en skole av NSM sin internkontroll.			
V.3	Utføring av undervisning	Undervisning er blant de sentrale verdiene i organisasjonen. Det drifter organisasjonen. Undervisning er avhengig av en del andre verdier.	Svært høy	Konfidensialitet	Økonomi, drift, leveranser
V.4	Databaser	Riktig og oversiktlig struktur som står bak alle tjenestene og funksjonene er grunnleggende for en flytende drift av tjenester og systemer.	Høy	Tilgjengelighet, Integritet, Konfidensialitet	Drift
V.5	Sikkerhetskopier	Sikkerhetskopier av all data, dataservere er viktige for en sikker drift av en virksomhet.	Høy	Tilgjengelighet, Integritet	Økonomi, drift
V.6	Sensitive dokumenter	Rutiner og prosedyrer, undervisnings relaterte dokumenter, plantegninger, rapporter o.l. er informasjonen som er «drivstoff» til en høgskole.	Høy	Konfidensialitet, Integritet	Drift, leveranser
V. 7	Kompetansen til forelesere/lektorer	Forelesere og personell som gjennomfører undervisning er blant det meste verdifulle for en utdanningsinstitusjon. Alle leveransen stammer fra denne «verdien». Kompetansen til disse personene er verdifullt for virksomheten.	Høy	Integritet	Økonomi, drift
V.8	Strømforsyning	Uten strøm er det umulig å levere noe som helst fornuftig tjeneste i vår tid. Svært avhengig av denne. Avhenger også av fysisksikring og leverandøren.	Høy	Tilgjengelighet	Drift, leveranser
V.9	Fysiske enheter – svitsjer, datamaskiner, rutere.	Kartlegging og oversikt i så stor grad som mulig over alle fysiske enheter i bygget er viktig for å kunne sikre og herde sikkerhetshull.	Moderat	Tilgjengelighet	Drift
V.10	Logger	Mulighet for oppslag av logger gir bedre ettersporing av	Moderat	Tilgjengelighet	Drift

		hendelser og bearbeiding av denne informasjon bidrar til minimalisering av sannsynlighet for at uønskede hendelser oppstår igjen.			
V.11	Eksterne tjenester	Tjenester som Office360, Canvas, Exchange, Inspera o.l.	Moderat	Tilgjengelighet	Leveranser
V.12	Administrative oppgaver	Drift av organisasjonen er avhengig av utføring av administrative oppgaver. Dette innebærer utføring av blant annet hierarkibaserte administrative oppgaver; HR får nye ansatte, styret kommer med nye innføringer osv. Det at dette fungerer som det skal er kritisk.	Moderat	Integritet	Drift
V.13	Støttetjeneste IKT	Mulighet for råd og hjelp ved oppståtte problemer for både ansatte og studenter er en essensiell tjeneste.	Moderat	Konfidensialitet, Tilgjengelighet	Drift

Som tabellens viktighetsgradering viser, de viktigste verdiene i organisasjonen er verdier knyttet til undervisning og det som dreier seg rundt de. Videre steg er å se på mulige trusler som kan påvirke sikkerhet rundt disse verdiene og kan forårsake vanskelighet rundt leveranser av funksjoner og tjenester i forbindelse med dem.

Trusselmodellering

Det finnes en stor mengde måter, teknikker og motivasjoner for trusselaktører å utføre nettangrep. I denne trusselmodelleringen vil det tas utgangspunkt i «CWE top 25» liste av de mest kjente og vanlige angrep. Det skal trekkes frem det som kan spesielt ramme Høgskolen i Østfold, i ulik grad og måte, med utgangspunkt i både tekniske og fysiske risikoer.

ID	Navn	Beskrivelse	Verdi i fare	Årsak

T.1	Phishing	Phishing er kanskje den mest vanlige måten av nettangrep som kan være rettet mot Høgskolen i Østfold. Phishing går gjennom falske sider, linker, e-poster som framstiller seg selv som troverdige. Phishing	V.2, V.6., V.12	Dårlige og ikke oppdaterte spam-filtre i e-post tjenester. Manglende opplæring og kunnskap hos ansatte.
T.2	Ransomware	Ransomware er skadelig programvare som blir installert på offerens datamaskin med mål om å låse data på maskinen og få en gevinst i form av en pengesum mot en «nøkkel».	V.2, V.4, V.6, V.10, V.12	Manglende overvåking av systemer. Sikkerhetstiltak Manglende sikkerhetskopier
T.3	DDoS angrep	DDoS angrep overbelaster dataservere med store menge av trafikk som fører til ustabil drift av disse tjenestene. Dette kan ha en kritisk påvirking på utføring av leveranser i organisasjonen.	V.1, V.3, V.11, V.12, V.13	Manglende DDoS beskyttelse på nettverk og servere.
T.4	"Man in the middle" angrep	"Man in the middle" er angrep med avlytting av informasjon mellom to eller flere parter. Trusselaktøren er da «en mann i midten» som stjeler denne dataen uten om at partene vet det.	V.1, V.2, V.6	Manglende virusbeskyttelse, systemovervåking.
T.5	SQL-injeksjoner	SQL-injeksjoner er injeksjon av skadelig kode inn i SQL databaser som kan føre til tap av data.	V.1, V.4, V.10	Dårlig skrevet kodebase som lar trusselaktører å utføre sql-injeksjoner. Manglende «parametirized statements». Utdaterte database drivere. Manglende sikkerhetskopier.
T.6	Feil tillatelsestildeling for kritiske ressurser	Tillatelsestildeling til kritiske ressurser bør tildeles kun til brukere som har behov for det. Dersom færre brukere har viktige tilganger vil minske sjansen for uvedkommende å få tak i viktig data o.l.	V.2, V.4, V.6, V.10, V.12	Feil tillatelsestiledeling.
T.7	Feilkonfigurasjon av innstillinger/regler sikkerhet i systemer og tjenester	Feilkonfigurering av sikkerhetsinnstillinger kan gi uvedkommende tilgang til sensitive deler av systemet og data.	Konfidensialitet	Feilkonfigurasjon av regler for sikkerhet.
T.8	"Zero-day exploits"	Exploits i systemer som har blitt meldt til å være sikkerhetshull, men har ennå ikke blitt oppdatert og sikret hos de som bruker disse systemene.	V.2, V.6, V.11, V.12	Manglende oversikt over kjente angrep hos sikkerhetsansvarlige. Utdatert programvare.

T.9	CSRF	Forfalsking av forespørsler på tvers av tjenester (spesielt nettjenester).	V.2, V.6	Upålitelige anskaffelser. Utdaterte nettløsninger og programvare.
T.10	"Path traversal"	Feil begrensning i programvaren. Programvare som gir mulighet for inntasting av kode syntaks kan føre til at trusselaktøren får mulighet til å endre «basen» i programvaren og stjele data eller installere skadelig programvare.	V.6, V.11	Bruk av programvare som ikke tar hensyn til kritiske sikkerhetsaspekter. Upålitelige anskaffelser. For mange unødvendige funksjoner i programvaren.
T.11	Manglende autentisering til kritiske funksjoner	Alle viktige funksjoner bør kontrollere om tillatelser til en bruker har nok rettighet til å se innholdet. Sikring av innhold basert på brukertyper.	Tilgjengelighet	Manglende eller feil gradering av brukertyper

Trusselaktører kan ha en god del grunner og motiver til å utføre nettangrep. Det mest attraktive for dem i en organisasjon som Høgskolen i Østfold er oftest mengden av relativt ubeskyttede fysiske mobile enheter som studenter og ansatte har i sin disposisjon, blant annet smarttelefoner, nettbrett, bærbare PC-er o.l. Hver eneste av de enhetene kan potensielt brukes som en inngangsdør inn i datasystemene til høgskolen. Motiver er oftest uklart, med mindre trusselaktørene selv annonserer om hva de ønsker å oppnå, for eksempel utnyttelsen av ransomware for en gevinst. Andre motiver kan være kompromittering og tyveri av data som forskningsdata, personopplysninger og sensitive dokumenter.

Oftest er det umulig å 100% beskytte seg selv og andre mot nettangrep, særlig dersom de er et stort angrep. Enkle tiltak, som opplæring av ansatte. Store bedrifter bør også ha ansatte som er ansvarlige for datasikkerhet i organisasjonen. Disse skal alltid holde seg oppdatert med de alle aktuelle angrep som kan potensielt ramme høgskolen. «CVE-identifiers», oppdatering av programvare og gode beskyttelsestiltak vil i større eller mindre grad beskytte mot mest vanlige nettangrep.

Risikovurdering

I denne delen er det valgt å utføre en kvalitativ risikovurdering, som er det mest fornuftige i denne sammenhengen. Grunnen til valget av denne fremgangsmåten er mangel av reelle tall og verdier for å kunne måle eksakt risiko og sannsynlighet. Andre grunner er også at de fleste risikoer som er nevnt i tabellen under er knyttet til funksjonsbaserte og immaterielle verdier. Sannsynlighetsvurdering er i denne delen en subjektiv sannsynlighetsvurdering basert på forhåndskunnskap og erfaring.

Hendelse	Kategori (KIT)	Konsekvens	Sannsynlighet	Risiko	Vurdering
H.1 – Ansatt følger en falsk «phishing» lenke i en e-post.	K+I	Mulig tap an personopplysninger, påloggingsinformasj	Høy	Middels	Ikke akseptabelt

		on o.l., dersom personen taster inn informasjonen i den falske nettsiden. Tilgang til andre deler av systemet, andre tjenester.	Veldig vanlig måte å stjele informasjon, stor sannsynlighet at ikke alle brukere kontrollere nettsidens troverdighet.		
H.2 – Ansatt/student laster ned en skadelig fil med ransomware på en datamaskin på høgskolens lokaler.	T	Datamaskinen blir låst og blir utilgjengelig. Dette kan medføre tap av data, informasjon og ekstra arbeid for IKT-hjelp tjenesten. Dette kan også medføre infisering av flere andre enheter på nettverket.	Høy Lett å falle i denne fellen, svært få av ikke datasikkerhetsanvendte personer som sjekker filens opprinnelse og troverdighet.	Middels	Ikke akseptabelt
H.3 – Trusselaktør angriper Inspera-tjenesten med et «DDoS» angrep.	T	Tjenester blir ustabil eller utilgjengelig. Vansker rundt gjennomføring av eksamen. Dårlig omdømme, frustrasjon, mistet tillitt.	Middels Relativt enkelt å utføre og lite sporbarhetsmuligheter, derfor veldig fristende for trusselaktører å utføre.	Høy	Ikke akseptabelt
H.4 – Mellommann kompromitterer en e-post samtale mellom en student og ansatt og får tak i et sensitivt forskingsdokument.	K+I	Tap av sensitive dokumenter, personopplysninger og påloggingsinformasjon. Dårlig omdømme om virksomheten i media.	Lav Krever store sikkerhetshull for å klare gjøre slikt og derfor lavt sannsynlighet for denne hendelsen.	Høy	Ikke akseptabelt
H.5 – Ny anskaffelse(programvare) hos høgskolen blir kompromittert med et «sql-injection» som en	I+T	Database med viktig informasjon blir slettet. Informasjon på avveie.	Lav Svært lite sannsynlig i store systemer som har kode som sikrer seg mot dette.	Høy	Ikke akseptabelt

følge av dårlig systemdesign.					
H.6 – Uvedkommende får tak i en student brukerkonto og gjennom den får tilgang til en svakt sikkerhetskonfigurert tjeneste.	K+I	Tilgang til sensitive dokumenter. Trusselaktør får tilgang til andre deler av nettverket	Lav Mange barrierer, en brukerkonto alene gir ikke så mange muligheter dersom det finnes 2 faktor auth o.l.	Lav	Akseptabelt
H.7 – Media annonserer at flere virksomheter har blitt rammet av et angrep som følge av en exploit i felles programvare. Høgskolen er litt sen med å oppdatere programvaren og blir offer av «zero-day-exploit».	K+I+T	Dårlig omdømme i media. Mulig tap av finanser.	Høy Buggfrie systemer og kode eksisterer ikke, slike feil har stor sjanse for å oppstå.	Høy	Ikke akseptabelt
H.8 – Studentkonto ved en feilkonfigurasjon får tilgang til administrator verktøy i programvaren og med uhell sletter et emneside.	K+I+T	Dårlig tillitt til virksomheten fra ansatte/studenter. Deler av tjenesten blir utilgjengelig, kan medføre frustrasjon hos brukere og drift.	Lav	Lav	Akseptabelt
H.9 – Trusselaktør fysisk installerer en avlytter (Key logger) på en svitsj/ruter på høgskolens lokaler.	I	Dårlig omdømme i media. Dårlig tillitt til virksomheten fra ansatte/studenter.	Lav Stor sannsynlighet for virksomheten å spore trusselaktøren, og derfor har det for stor risiko kontra gevinst.	Lav	Akseptabelt
H.10 – Upålitelig anskaffelse selger informasjonsdump av brukere og deres personopplysninger som er knyttet til høgskolen.	K+I	Dårlig omdømme i media. Store tap av finanser, ved eventuelt endring til en annen system. Katastrofale konsekvenser i	Lav Krever at anskaffelsen blir kjøpt fra en utroverdig og lite kjent aktør, som er lite sannsynlig.	Høy	Ikke akseptabelt

		forhold til personvern. Søksmål mot høgskolen.			

Som tabellen viser er det en stor mengde funksjonsbaserte risikoer, men samt en del menneskefaktor feil som kan oppstå i en virksomhet. Oppsummert, det absolutt verste og det som vil medføre størst menge med konsekvenser er risikoer som innebærer tap og tyveri av personopplysninger. Grunnen til det er at tap av sensitiv informasjon og personopplysninger er ikke noe som kan fikses og trekkes tilbake. Jeg ville satt størst fokus på etablering av tiltak for minskning av disse risikoene. Resten av risikoer har relativt enklere tiltak som innebærer tekniske løsninger, som blant annet overvåking, etablering av nye tjenester og fjerning av risikoer. Videre i neste del av risikoanalysen vil det bli listet opp noen forsalg til tiltak om mulige løsninger.

Tiltak

Rapporten forutsetter at utgangspunktet for levering, etablering og fristene trer i kraft fra og med 2. november. Det har blitt forsøkt å aggregere flere hendelser og trusler under felles tiltakspakker, for å minske kostander og tid for gjennomføring av tiltakene.

Hendelse ID	Tiltak	Kostnad	Test og måling	Frist
H.1, H.2, H.4, H.11	Etablering av en form for opplæring av ansatte i henhold til datasikkerhet og trusler. Dette kan for eksempel gjennomføres som e-læringskurs. Kurs vil da kreve jevnlig testing av ansatte, for eksempel kursbevis er gyldig i 1 år, deretter må den gjennomføres på nytt og fornyes. Opplæring i datasikkerhet vil øke oppmerksomhet, bevissthet for hendelser og kritisk	Lav	Etablering av jevnlig kompetansetesting av ansatte. Innføring av krav til levering av beståtte kurs.	4 uker + jevnlige gjentagelser.

	tenkning, samt gi basis kunnskap i faget. Dette tiltaket vil minske feil i forbindelse med menneskefaktor ved håndtering av e-poster, linker, filer.			
H.3, H.5	Opprettelse av DDoS responsplan, samt kjøp av større og bedre bandwidth. Endring av oppbygning av infrastruktur til systemet/databasen, tilføring av redundans. Benyttelse av «DDos mitigation» utvidelser/systemer med det nåværende systemet. Opprette honeypots, som vil minske trafikk av angrep fra trusselaktørene mot hovedservere. Risikofjerning ved byttet til andre tjenester.	Middels	Overvåking og logging av servere. Jevnlig forbedring av infrastruktur	2 uker på de tekniske implementasjonene + kontinuerlig overvåking.
H.6, H.8, H.5	Innstramming av sikkerhet for brukertyper. Gjennomgang av omvurdering av eksisterende tilganger knyttet til brukere. Gjennomgang av logger for eventuell	Høy	Sikkerhetstesting rettet mot systemet/tjenesten. Kjøp av pentesting/red team.	4 uker

	oppdagelse av flere samme type sikkerhetshull i relevante tjenester som er tilgjengelige for brukeren.			
H.9	Forbedring av fysisksikring og minskning av tilgjengelighet til fysiske enheter på lokasjonen for uvedkommende. Etablering av logging og endrings deteksjonssystem.	Middels	Gjennomgang av alle fysiske enheter i virksomheten/lokasjonen.	~3 måneder
H.7	Etablering av programvarepakker som tvinger kritiske oppdatering på lokale datamaskiner og systemer, samt hvitlisting av tillatte programvare.	Middels	Enkle tester som forsøk å installere ikke hvitlistet programvare på gjeldende enheter.	2 uker for etablering + 1 uke testing

Del 2 – Beredskapsplaner

Kriseteam

Følgende informasjon er hentet fra hiof.no sin side for beredskapsplan og krise. Som definert av HiØ, kriseteam skal styrkes:

- Ved hendelser der studenter er berørt styrkes kriseteamet med direktør for studentsamskipnaden.
- Ved hendelser der ansatte er berørt styrkes kriseteamet med Bedriftshelsetjenesten.
- Ved behov kan kriseteamet styrkes med leder for eiendomstjenester, bibliotekleder, IKT-direktør og/eller dekan ved berørt avdeling.

Kriseteam består av følgende kontaktpersoner (nevnt kun relevante personer til denne risikoanalysen):

Funksjon	Navn	For kommunikasjon
Høgskoledirektør	Carl-Morten J.	Telefon
Rektor	Lars-Petter J.	Telefon
Prorektor	Annette V. D.	Telefon
Studiedirektør	Frid S.	Telefon
Økonomidirektør	Henrik B.	Telefon
Informasjonssjef	Tore Petter E.	Telefon
Direktør for organisasjons- og tjenesteutvikling	Elin C.	Telefon
Leder for campustjenester	Jan-Lorang B.	Telefon
IKT-direktør	Jørgen G.	Telefon
Sikkerhet- og beredskapsrådgiver	Lars-Erik Å.	Telefon
HMS rådgiver	Ruth Å. L.	Telefon

Eksterne

Funksjon	Navn	For kommunikasjon
Kontaktperson Inspera	Ingrid Inspera	Telefon
Kontaktperson Canvas	Christian Canvas	Telefon

Samhandling i kriseteam (Ansvar, Roller, Varsling)

Samhandlingen er inndelt og beskrevet på følgende måte (hente fra hiof.no):

Hvem varsler internt/eksternt om hva:

- Rektor vurderer hvilken informasjon det kan være aktuelt å formidle forøvrig, og rådfører seg med Østfold politidistrikt om innhold og tidspunkt for info.
- Informasjons- og kommunikasjonssjef bistår rektor, meddeler info via HiØs internettside/kriseweb, og organiserer evt. pressekonferanser som kan være aktuelle i tillegg til politiets.

Organisering av informasjonstiltak:

- Informasjons- og kommunikasjonssjef er ansvarlig for etablering av krisekommunikasjonsteam.
- Informasjons- og kommunikasjonssjef er ansvarlig for etablering av kriseweb.
- Leder for IT-drift er ansvarlig for etablering av pårørendetelefon.
- HR-direktør er ansvarlig for å etablere pårørendesenter.

Hvem har ansvar for dokumentasjon:

- Ansvarlig sekretær som er en del av kriseteamet ved en krisesamling er ansvarlig for dokumentering av kriseteamets diskusjoner, hendelser og tiltak
- Overvåkingssystemet er påkrevd å inneholde logger over driften i minst de siste 48 timer. For enkelt oppslag og gjennomgang av logger skal man bruke funksjon «logg» i overvåkingssystem X.

Kriseteamets oppgaver er nærmere beskrevet i krisestøtteverktøyet CIM.

Dokumentasjon

Sekretær rollen har ansvar for å skrive møtereferat og dokumentere hver eneste diskusjon, forslag og beslutninger som blir nevnt i et kriseteammøte.

Sekretær har ansvar for å gjennomføre og dokumentere følgende:

- Sjekklister
- Møtereferat
- Dokumentere forslag, beslutninger og hendelser
- Sortere, gruppere og laste opp dokumentasjonen for tilgjengelighet for andre ansatte
- Sende ut møtereferat og dokumentasjon til ansatte i pårørte avdelinger.

Dokumenter skal legges under felles ansvarsområde i serveren og skal ha følgene dokumenter og struktur:

Dokumentnavn	Beskrivelse
Situasjonsbeskrivelse	Beskrivelse av krisesituasjon
Møtereferat <dato> <klokkeslett>	Møtereferatet skal inneholde en dokumentert kronologisk rekkefølge av spørsmål, diskusjoner o.l. som har oppstått under det møtet.
E-post til ansatte	E-post med informasjon om krisen for ansatte.
E-post til studenter	E-post med informasjon om krisen for studenter.
E-post til leverandør	E-post med informasjon om krisen for den aktuelle leverandøren.
Ferdigutført gjennomgang av beredskapsplan	Dokument som er utført i hht. Beredskapsplan med tiltak, sjekklister o.l.
Endelig beslutnings dokument med tiltak og beslutninger	Dokument som inneholder en endelig beslutning for håndtering av krisesituasjonen. Samt etterbehandlingstiltak.

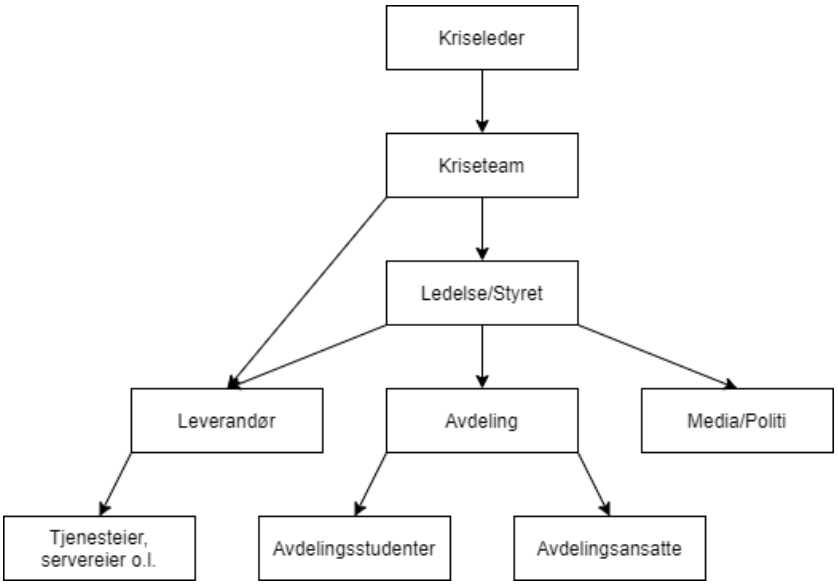
I tillegg er det nødvendig å ta snapshots av systemer i ulike tidspunkter for å kartlegge og identifisere tidspunkter når angrepet startet for å eventuelt finne ut hvilket sikkerhetskopi som skal brukes for å gå tilbake til normalsituasjon. Disse snapshots blir også blir brukt i etterbehandling av krisen for å gjennomføre etterkontroll og trekke noen punkter som kan bidra til hindring av gjentagelse av slike hendelser, samt lærdom av dem.

Kommunikasjon

Kommunikasjons- og informasjonssjef har ansvar om å varsle studenter og ansatte om et pågaende krisesituasjon og bør vurdere å benytte følgende kommunikasjonskanaler:

- Legge ut en varselsmelding på Hiof.no sin hovedside og under «aktuelle nyheter» med informasjon om at det jobbes med løsning til situasjonen som har oppstått.
- Sende ut epost/ til krisekommunikasjonsteam ved bruk av mal «krisesituasjon_typesituasjon.doc»
- Kommunikasjons- og informasjonssjef skal vurdere situasjonen og vurdere om relevante personer ved sære nødsituasjoner skal kontaktes direkte på telefon.

Kommunikasjonen ved en krisesituasjon skal fungere etter følgende prinsipp (kontaktinformasjonen til relevante personer/avdelinger er nevnt i kontaktlisten):



Behandling

Ved spesifikke hendelser skal kriseteamet sette i gang og benytte hendelsesspesifikke beredskapsplaner. Følgende er eksempler for slike hendelser, se «Beredskapsplan for situasjon 1 – DDoS angrep mot Inspera» og «Beredskapsplan for situasjon 2 – Informasjon potensielt på avveie som følge av en phishing e-post».

Beredskapsplan for situasjon 1 – DDoS angrep mot Inspera

Kriseleder varsler nærmeste kontaktpersoner, blant annet sikkerhets- og beredskapsrådgiver, HMS rådgiver, Eksamenskontoret, IKT-direktør, representerende kontaktperson for «Inspera» om en

pågående krisesituasjon. Kriseteamet møtes på møterom X i høgskolens lokaler, andre personer uten mulighet for fysisk oppmøte eventuelt blir med gjennom videoløsninger som Zoom, Skype o.l.

Beskrivelse av krisen

Kriseleder/områdeansvarlig skal ved en krisesituasjon varsle kriseteamet og gi en kort briefing av hendelsen, slik at alle deltakerne har oversikt og forståelse av omfanget på situasjonen. Det skal typisk være en kort beskrivelse av situasjonen, bruk følgende tabell som eksempel for å varsle om DDoS angrep.

(Referer til hendelse med ID H.5 i risikoanalysen.)

Hva er hendt	Potensielle konsekvenser
Overvåkingssystemet IDS/IPS til virksomheten har varslet om et pågående DDoS «Application layer» angrep mot HiØ sine tjenester. Særlig påvirket av angrepet er eksamensgjennomføringsverktøyet «Inspera». Som følge av angrepet er tjenesten utilgjengelig og svært ustabil. Studenter i visse tilfeller får ikke startet eksamen, i andre tilfeller er det umulig å gå videre i eksamen, samt levering av eksamen er utilgjengelig. Gjennomføring av eksamen for studenter i dette tilfelle er i stor fare og tvil, og det vurderes løsninger til saken.	Utilgjengelig og svært ustabil tjeneste. Forskyving av eksamensgjennomføring, eksamen starter senere enn oppvist tid. Avlysning av eksamen for den dagen det gjelder. Store kostnader som følge av avlysning. Høgskolen er nødt til å utvikle ny eksamensoppgave, skaffe nye sensorer, eksamensvakt og eksaminatorer. Etablering av alternative eksamensgjennomførings løsninger dersom angrepet varer over lengre tid. Eksamensgjennomføring på papir istedenfor digitaleksamen. Media blir informert om hendelsen og skriver et negativt innlegg om høgskolen. Omdømme om HiØ som utdanningsinstitusjon blir påvirket.

Forslag for å komme gjennom krisen

Etter første steg skal kriseteamet være informert om hendelses omfang og skal vurdere følgende tiltak for å finne løsninger til situasjonen. Bruk følgende forslag, eller utarbeid egne basert på situasjonen.

Tiltak	Kommentar
Forslag A:	Kontakte Inspera for å finne ut om tiltak er satt i gang.

HiØ er i kommunikasjon med leverandør Inspera om benyttelse av backup i form av «redundant site», «hot site», «warm site» eller «cold site».	
Forslag B: Kriseteamet sammen eksamenskontoret vurderer å kjøre i gang endring av gjennomføringsform av eksamen. Forslaget er å gjennomføre eksamen på papir istedenfor digital eksamen. Eksamen kjøres fortsatt samme dag.	Det må vurderes om eksamen er gjennomførbar på papir, samt om eksamenskontoret klarer å hente ut eksamensoppgaven samme dag og skrive ut flere kopier for studenter å bruke.
Forslag C: Kriseteamet sammen eksamenskontoret gir forslag om å forskyve eksamen med et par timer samme dag i håp om at situasjonen løser seg i løpet av den tiden.	Bør vurderes dersom Inspera gir klar beskjed om at de klarer å stabilisere driften av tjenesten på antall oppgitte timer.
Forslag D: Kriseteamet gir forslag om å finne alternative tjenester for eksamensgjennomføring midlertidig. Tatt utgangspunkt i at angrepet strekker seg over lengre tid.	Svært vanskelig å implementere og kjøre ut denne løsningen på så kort tid. Kun mulig dersom HiØ allerede har leverandør Y tilgjengelig.
Forslag E: DDoS angrepet stopper ikke og kriseteamet gir forslag om å avlyse eksamen og sette opp en ny eksamensdato.	Dette er en stor og viktig avgjørelse, for at det vil medføre store kostnader ved produksjon av ny eksamensoppgave, nye eksamensvakt og sensorer.

Behandling av krisen

Kriseteam er nødt til å reagere kjapt og velge reaktive beslutninger ved slike situasjoner, samt vurdere forslag til tiltak fra tabellen over.

Etter å ha gått gjennom alle mulige forslag skal kriseteamet velge et punkt og kjøre den i gang for å løse situasjonen. Hvis det viser seg at DDoS angrepet er mer omfattende enn det var tidligere tenkt, så er kriseteamet nødt til å ta avgjørelsen om å avlyse eksamen og heller sette opp en annen eksamensdato. Da skal kriseteamet gå over til forslag E, sekretær skal dokumentere dett underveis.

Tjenesteansvarlig skal da ta vare på relevant informasjon av situasjonen, blant annet snapshots og logger. Det skal også tilkalles parter som vil utføre overvåking og følge med på situasjonens utvikling og gi beskjed dersom flere IT-systemer blir berørt. Det må også vurderes umiddelbare tiltak som stans av servere for å begrense skadeomfang.

Kriseleder skal videreformidle denne beslutningen og informasjonen til eksamenskontoret og ledelsen. Høgskolen skal informere involverte parter, studenter og ansatte, om at eksamen er avlyst og at ny eksamensdato kommer fortløpende. Dette kan gjøres gjennom et utvalg kommunikasjonskanaler; sms mal «eksamen avlyst», innlegg på hiof.no, epost til vedrørte studenter og gjennom muntlig beskjed i eksamenslokaler.

Eksamenskontoret da skal sette i gang produksjonen av en ny eksamensoppgave. Hendelsens alvorlighetsgrad involverer også at ledelsen anmelder denne til Politiet for etterforskning.

Etterbehandling av krisen

I etterbehandlingen av en krisesituasjon skal leder sammen kriseteamet kartlegge, gå gjennom og vurdere informasjonen som har blitt samlet igjennom hendelsen og møtet. I dette tilfellet skal man gå gjennom denne sjekklisten for å kartlegge denne informasjonen.

Hendelsesorientert sjekkliste

Spørsmål	Ja	Nei	Ukjent	Kommentar
Har angrepet stoppet?				
Er tjenesten tilbake til normaldrift?				
Nye forsøk på angrep?				
Er mottiltak av gjentagende forsøk satt i gang?				
Er ledelsen informert?				
Er det observert noen følger av angrepet? Blackmailing?				
Er hendelse sikkerhetstruende?				
Tatt snapshots av systemet?				
Er nødvendig dokumentasjon om hendelsen samlet?				
Sikkerhetsbrudd? Er KIT påvirket?				
Har varslingssystemet fungert bra?				
Er hendelsen grunnet avvik?				
Hendelse grunnet ikke oppdatert programvare?				
Begrenset funksjonalitet? Nettverks sperringer som følge av DDoS?				

Organiserings sjekkliste

Spørsmål	Ja	Nei	Ukjent	Kommentar
Fungerer eksisterende rutiner for sikkerhet og internkontroll?				
Reforhandling av kontrakt med leverandør?				
Vurdere bytte leverandør?				
Skal sikkerhetskrav oppdateres?				
Er trusselbildet kjent godt nok?				

Trenger trusselbildet oppdatering?				
Har risikoanalysen vært aktuell og nyttig?				
Er ansatte kjent med prosedyrer og er opplært?				
Har ansatte utført prosedyrer godt nok?				
Er krisehåndteringssteg tilfredsstillende?				
Er beredskapsplanen god nok?				

Etter dette skal kriseleder ta avgjørelsen om å avslutte møtet. Hvert eneste kristeammedlem da skal evaluere behandling av krisen. Sekretær skal sende ut mal «evaluering_kriseteam.doc» til kriseteamet. Videre, skal kriseleder samle en rapport til ledelsen med vurdering av gjennomføring og eventuelt forbedringer av rutinene, kriseteamet.

I etterbehandlingfasen er det nødvendig for IKT-tjenesten og Inspera å kontrollere utførelsen av alle aktuelle oppdateringer av systemet, servere og utføre vedlikehold for å kontrollere at situasjonen er virkelig løst.

Beredskapsplan for hendelse – Informasjon potensielt på avveie som følge av en phishing e-post til ansatt.

Beskrivelse av krisen

I en situasjon der involverte parter oppdager at en e-post eller andre aktiviteter virker å være mistenksomme, er den selv ansvarlig om å gi beskjed til sin nærmeste leder. I en annen situasjon der tap av informasjon som følge av phishing e-post har oppstått, skal overvåkingssystemet varsle om dette. Deretter skal nærmeste ansvarlig for overvåkingssystemet gi beskjed til sin leder. Videre skal kriselederen og informasjonsansvarlig kontaktes for evaluering av situasjonen. Et eksempel på en slik beskjed kan formuleres som i tabellen under.

Referer til hendelse med ID H.1 i risikoanalysen

Hva er hendt	Potensielle konsekvenser
Ansatt har fått en phishing e-post som vedkommende har trykket på og fulgt lenken. Der etter har ansatt tastet inn påloggingsinformasjon som samsvarer med påloggingsinformasjon til andre virksomhetens tjenester og kan potensielt misbrukes.	Personopplysninger på avveie. Innloggingsinformasjon på avveie. Identitetstyveri som følge av tap av personopplysninger.

Som følge av dette har overvåkningssystemet merket mistenksom aktivitet knyttet til denne brukeren og varslet om dette. Nærmeste IKT-sikkerhetsansvarlig som har fått dette varselet, kontaktet kriseledelsen.	Uvedkommende får tilgang til andre kritiske virksomhetens systemer.

Forslag for å komme gjennom krisen

I en hendelse som innebærer en god del usikkerhet rundt motiver og videreutvikling av situasjonen som følge av en phishing e-post kan disse tiltak vurderes:

Tiltak	Kommentar
Forslag A: Stenge den aktuelle brukeren ut av systemet	For å hindre videre handlinger for uvedkommende kan systemansvarlig sperre brukerkontoen.
Forslag B: Overvåke aktivitet knyttet til den aktuelle brukeren	I en situasjon der det uklart om hvor dypt trusselaktøren har klart å komme seg inn i systemene til virksomheten. Overvåk utviklingen.
Forslag C: Kjøre i gang bytte av passord for alle brukere	Denne skal vurderes dersom det er mistenkt at uvedkommende har klart å lure flere enn bare en person.
Forslag D: Slå av aktuell tjeneste og utfør umiddelbart vedlikehold og feilsøking	Dersom det er klart at det gjeldende systemet har blitt kompromittert trenger det umiddelbare handlinger. Kriseteamet skal kontaktes.

Behandling av krisen

Ved oppdaget hendelse skal IKT-rådgiver og Sikkerhets- og beredskapsrådgiver kontaktes. Videre er det nødvendig å evaluere hendelsen og kartlegge omfanget på hva som er berørt av hendelsen. Basert på evalueringene skal behandlingen bestemmes på følgende:

Behandling av denne hendelsen kan deles inn i to typer:

- Kriseteam ikke involvert.
  - Dersom det blir valgt forslag A, B, C fra tiltakslista.
- Kriseteam involvert.
  - Dersom det blir valgt forslag D fra tiltakslista, og andre tiltak som krever reaktive umiddelbare handlinger.

Hvis situasjonen ekskluderer kriseteamet skal det settes i gang tiltak som overvåker konkrete brukere og deler av systemet som er berørt. Aktuelle involverte parter skal kontaktes og varsles om den oppståtte situasjonen, for eksempel i form av e-post, felles innlegg på hovedsiden eller sms. Videre utvikling av

situasjonen bestemmer om situasjonen er løst eller om det trengs å involvere kriseteam. Som mottiltak er det anbefalt å sette i gang bytte av passord for ansatte som kan være berørt av situasjonen.

Hvis situasjonen involverer kriseteamet, skal de umiddelbart samles til et møte. Basert på logger og utvikling av situasjonen skal omfanget av situasjonen og mulige konsekvensene vurderes. Dersom komprimerte brukeren utfører skadelig aktivitet, skal den sperres ut av systemet. Dersom flere brukere blir infisert gjennom den ene komprimerte brukeren, skal systemet tas snapshot av, tas ned og rulles tilbake til siste sikkerhetskopi. Andre ansatte skal varsles om et pågående innsending av falske e-poster.

Etterbehandling av krisen

I etterbehandlingen av en krisesituasjon involverte parter kartlegge, gå gjennom og vurdere informasjonen som har blitt samlet igjennom hendelsen og møtet. I dette tilfellet skal de gå gjennom denne sjekklisten for å kartlegge denne informasjonen.

Hendelsesorientert sjekkliste

Spørsmål	Ja	Nei	Ukjent	Kommentar
Er situasjonen løst?				
Er den involverte aktuelle brukeren informert?				
Har det oppstått tap av personopplysninger?				
Har det oppstått tap av påloggingsinformasjon?				
Er phishing e-posten kjent?				
Er resten av ansatte varslet om en potensielt farlig e-post?				
Er overvåking av systemet satt i gang?				
Har det oppstått mer mistenksom aktivitet knyttet til den aktuelle brukeren?				
Har det oppstått mer mistenksom aktivitet knyttet til andre brukere?				
Er andre systemet berørt?				
Er det samlet inn spor?				

Organiserings sjekkliste

Spørsmål	Ja	Nei	Ukjent	Kommentar
Fungerer eksisterende rutiner for sikkerhet og internkontroll?				
Skal sikkerhetskrav oppdateres?				
Er trusselbildet kjent godt nok?				
Trenger trusselbildet oppdatering?				

Har risikoanalysen vært aktuell og nyttig i sammenheng med hendelsen?				
Er ansatte kjent med prosedyrer og er opplært?				
Har ansatte utført prosedyrer godt nok?				
Er krisehåndteringssteg tilfredsstillende?				
Er beredskapsplanen god nok?				

Dersom kriseteam er involvert, kriseleder skal ta avgjørelsen om å avslutte møtet. Hvert eneste kristeammedlem da skal evaluere behandling av krisen. Sekretær skal sende ut mal «evaluering_kriseteam.doc» til kriseteamet.
Videre, skal kriseleder samle en rapport til ledelsen med vurdering av gjennomføring og eventuelt forbedringer av rutinene, kriseteamet. Hendelsen meldes til politiet.

Dersom kriseteam er ikke involvert, skal involverte parter rapportere hendelsen til ledelsen. Logger og relevante dokumenter som ble aggregert i løpet av situasjonen skal oppbevares. Uten politianmeldelse.

Kriseøvelser

Høgskolen skal gjennomføre øvelser med jevnlige intervaller, for å opprettholde kompetansen til ansatte og evnen til å håndtere krisesituasjoner. Sikkerhetsansvarlig er ansvarlig for arrangering av øvelsene. Plan for utføring av kriseøvelser er definert i tabellen under:

ID	Navn	Kommentar	Intervall
K.1	Teoretiske øvelser (skrivebordsøvelser)	Inkluderer kurs for ansatte og forskjellige informasjonsskriv for øking av kompetanse innenfor IT sikkerhet.	6 måneder
K.2	Simuleringsøvelser	Simulering av angrep som involverer at ansatte bidrar. Gjennomføres i et simulertmiljø.	2 år
K.3	Fullskala øvelser	Involverer anskaffelse av pen-testere og redteam-testere for å teste reelle systemer og tjenester som er i drift i virksomheten.	1-3 år (basert på frekvensen av angrep)

Ressurser

- *CWE top 25, hentet 10.22.2020 - https://cwe.mitre.org/top25/archive/2020/2020_cwe_top25.html*
- *Nsm håndbook for verdivurdering av informasjon hentet 26.10.2020 - https://nsm.no/getfile.php/133657-1592813304/Demo/Dokumenter/Veiledere/handbok-i-verdivurdering-av-informasjon---032020.pdf*
- *Beredskapsplan HiØ, hentet 30.10.2020 - https://www.hiof.no/om/hms/sikkerhet/beredskapsplan/*
- *NorSIS krise- og beredskapspplan v.0.3 – hentet 28.10.2020 - https://nettvett.no/krise-og-beredskapsplan/*