

Risikovurdering av Devilry



Rapporttittel: Risikovurdering av Devilry
Forfatter: Øivind Høiem
Dato: 25.01.2016

Rapporten er unntatt offentlighet i henhold til Offentleglova § 15 andre ledd.

Innhold

Forord	4
Innledning	5
Tjeneste- /systemprofil	7
Resultat fra risikovurderingen	8
Hovedfunn	8
Risikonivå	9
Konfidensialitet, integritet, tilgjengelighet	10
Risikoområder	10
Anbefalte tiltak	11
Vedlegg A Kopi av ROS-regneark	14

Forord

Alle virksomheter bør ha en egeninteresse i et systematisk arbeid med informasjonssikkerhet. Offentlige virksomheter er også pålagt dette gjennom ulikt regelverk. Det er flere grunner til å foreta risiko- og sårbarhetsvurderinger:

- Overholdelse av rettslige plikter
- Opprettholde tillit til å benytte et system eller en tjeneste
- Beskytte ansatte, studenter, innbyggere o.a.
- Opprettholde kvalitet
- Vedlikeholde oversikt over informasjonseiendeler

Dette er utgangspunktet for alt informasjonssikkerhetsarbeid.

Difi sier at «*Risikovurdering er «hjertet» i internkontrollen. Her identifiseres, analyseres og evalueres risikoer som kan påvirke informasjonssikkerheten. Resultatet av risikovurderingene har betydning for alle de øvrige hovedaktivitetene. Uten risikovurderinger fungerer ikke internkontrollen.*»¹

eForvaltningsforskriften stiller krav om styring og kontroll med informasjonssikkerheten generelt i all informasjonsbehandling som offentlige virksomheter har ansvaret for.

Personopplysningsloven og personopplysningsforskriften har krav til informasjonssikkerhet rundt behandling av personopplysninger i alle typer virksomheter.

Disse kravene utdypes og skjerpes også i Kunnskapsdepartementets tildelingsbrev til institusjonene: «*Kunnskapsdepartementets styringsdokument for arbeidet med samfunnssikkerhet og beredskap i kunnskapssektoren skal ligge til grunn for institusjonens arbeid på dette feltet. Institusjonen skal ha etablert en virksomhetstilpasset risiko- og sårbarhetsanalyse (ROS) på samfunnssikkerhets- og beredskapsfeltet som revideres minimum hvert annet år. ROS-analysen skal følges opp gjennom en egen handlingsplan med tiltak for å redusere risiko og konsekvenser av uønskede hendelser.*

Som offentlig UH-institusjon må UiO ha kontroll på informasjonssikkerheten i sine adgangskontrollsystemer.

¹ <http://internkontroll.infosikkerhet.difi.no/risikovurdering>

Innledning

Bakgrunnen for risikovurderingen (ROSen) av Devilry hos Universitetet i Oslo var følgende:

- etterlevelse av personopplysningsloven, som setter krav om risikovurderinger av systemer som inneholder personopplysninger;
- eForvaltningsforskriften som stiller krav om styring og kontroll med informasjonssikkerheten i all informasjonsbehandling som offentlige virksomheter har ansvaret for
- krav til risiko- og sårbarhetsvurderinger i Kunnskapsdepartementets tildelingsbrev til institusjonene.

ROS-workshopen ble holdt 27. oktober 2015 hos Universitetet Oslo (UiO) Deltakerne var fra enheter som driver med IKT, IT-sikkerhet og informasjonssikkerhet. ROSen ble fasilitert av UH-sektorens sekretariat for informasjonssikkerhet hos UNINETT.

På grunn av man i ROS-rapporten beskriver sensitive forhold vedrørende Devilry og bruken av denne er rapporten unntatt offentlighet i henhold til Offentleglova § 15 andre ledd. Det anbefales at man klassifiserer rapporten som «intern» eller tilsvarende og at kun personer som har tjenstlig behov får tilgang til den.

Rapporten er utarbeidet av seniorrådgiver Øivind Høiem ved UH-sektorens sekretariat for informasjonssikkerhet hos UNINETT med innspill fra deltakerne.

Deltakere

Navn	Rolle	Institusjon
Dag Langmyhr	Systemeier Utdanningsleder, Faglærer	UiO IFI
Kristin Skar	Leder IT-avd IFI. Drift Devilry	UiO IFI
Suhas Govind Joshi	Support Devilry	UiO IFI
Katja Elisabeth Andersson	Studieadministrasjon, eksamen og obliger	UiO IFI
Thomas Hansen	Drift Devilry	UiO IFI IT
Gard Inge Rosvold	Gruppelærer, Devilryansvarlig	INF1000
Michael Glude	Eier Felles studentsystem	UiO LOS/AF/SSD
Espen Grøndal	IT-sikkerhetssjef USIT	UiO USIT
Tor Ivar Johansen	Hovedutvikler	Appresso
Rolf Sture Normann	ROS-fasilitator, Sekretariat for informasjonssikkerhet	UNINETT AS
Øivind Høiem	ROS-fasilitator, Sekretariat for informasjonssikkerhet	UNINETT AS

Tjeneste-/systemprofil

Tjeneste/System	Devilry
Risikoeier	Dag Langmyhr, UiO IFI
Virksomhetsområde	Undervisningssystemer
Utbredelse	It is currently the main delivery management system used at the Department of Informatics, UiO with plans of expanding to span across all departments at the The Faculty of Mathematics and Natural Sciences, UiO.
Beskrivelse	Devilry is a system optimized for delivering and correcting electronic deliveries. Open source and open community. The system can handle all kinds of deliveries from source code to essays. On top a simple and easy-to-use delivery layer Devilry provides a sophisticated interface for examiners and teaching assistants to manage students and deliveries directly in their favorite browser. Course administrators are given a focused interface to be able to easily manage all formalities around course management, from task deadlines to exam lists. Devilry started out in 2008 by a group of students at the Department of Informatics, University of Oslo with a vision to improve the current solutions around deliveries of obligatory assignments. Innlevering av oppgaver, hjemmeeksamen, sensurering, likhetssjekk (fuskesjekk).
Leverandør	devilry.org
Driftes av	UiO IFI IT

Resultat fra risikovurderingen

Hovedfunn

Det ble avdekket 4 administrative og 4 teknisk tiltak. Alle tiltakene retter seg mot uønskede hendelser på risikonivå medium. De uønskede hendelsene er noenlunde jevnt fordelt i forhold til hovedparameterne for informasjonssikkerhet; konfidensialitet, tilgjengelighet og integritet.

Risikoelementene som ble identifisert i workshopen lå på risikonivå lav eller medium. Det ble ikke identifisert risikoelementer med høy risiko.

De fleste risikoelementene som ble identifisert under ROS-workshopen berører kompetanse, ferdigheter og sikkerhetskultur, arbeidsprosesser, anskaffelse, utvikling og vedlikehold av IKT-systemer/tjenester og tilgang- og adgangsstyring. Det anbefales at hoveddelen av tiltakene settes inn på disse områdene.

Det er noen tiltak som ikke ble beskrevet i workshopen. Det er risikoeiers ansvar å beskrive disse hvis man finner det nødvendig.

Risikonivå

Det ble i ROSen identifisert 16 risikoelementer (uønskede hendelser). Fordelingen mellom risikonivåene er vist i tabellen under.

Risikonivå	Høy	Medium	Lav
Antall	0	8	8

Risikoelementet med lav risiko (grønn) vil ikke vurderes spesielt i denne rapporten men tas med slik at de evt. kan vurderes på nytt ved senere risiko- og sårbarhetsvurderinger.

Risikoelementene er for oversiktens skyld markert i matrisen under.

Konsekvens	4 Svært høy				
	3 Høy	4,5,11,13, 14, 15,16			
	2 Moderat	1,2,3,7,9,10			
	1 Liten		8,12		6
		1 Lav	2 Moderat	3 Høy	4 Svært høy
		Sannsynlighet			

Konfidensialitet, integritet, tilgjengelighet

Risikoelementenes konsekvenser ble også vurdert i forhold til de tre hovedparameterne for informasjonssikkerhet;

- **Konfidensialitet:** uvedkommende får tilgang til konfidensiell eller sensitiv informasjon,
- **Integritet:** uønsket endring, sletting eller manipulering av informasjon og
- **Tilgjengelighet:** brukere får ikke tilgang til informasjon når de har behov for det.

Her er en oversikt over fordelingen av risikoelementene i forhold til hovedparameterne. Noen av risikoelementene berørte flere av parameterne.

Informasjonssikkerhetsparameter	Konfidensialitet	Integritet	Tilgjengelighet
Antall	11	13	10

Risikoområder

Risikoelementene som ble identifisert i ROSen berørte understående risikoområder. Områdene er listet opp i prioritert rekkefølge etter antall treff. Noen av risikoelementene berørte flere risikoområder. Antall treff er oppgitt i parentes.

- Kompetanse, ferdigheter og sikkerhetskultur (8)
- Arbeidsprosesser (6)
- Anskaffelse, utvikling og vedlikehold av IKT-systemer/tjenester (6)
- Tilgang- og adgangsstyring (6)
- Håndtering av informasjonsverdier (5)
- Leverandørrelasjoner (4)
- Drift og forvaltning (4)
- Programvare (3)
- Beslutningsprosesser ved IKT-investeringer (2)
- Malware og logiske angrep (2)
- Etterlevelse av lover, regler og avtaler (2)

Anbefalte tiltak

Det er identifisert 8 tiltak. De er også delt opp i tekniske (4) og administrative tiltak (4). Eksisterende tiltak som ble fanget opp under workshopen er tatt med i anmerkningsfeltet.

Tiltakene som er presentert i tabellene ble identifisert under workshopen. Det er noen tiltak som ikke ble beskrevet i workshopen. Det er risikoeiernes ansvar å komme med ytterligere tiltak eller endre de foreslåtte tiltakene.

Tiltakene er sortert etter risikonivå med høyest risikonivå først.

Tiltak nr. 1			
Organisasjon:	UiO	Risiko	Tiltak
Tiltakstype:	Administrativt	Brukerdata blir liggende etter at studenter har sluttet. Brudd på Personopplysningsloven/-forskriften.	Tiltak må sjekkes med Må sjekkes av Martha/Tommy ++
Risikoelement:	6		
Risikonivå:	Medium		
Anm:			

Tiltak nr. 2			
Organisasjon:		Risiko	Tiltak
Tiltakstype:	Administrativt	Uautorisert innlogging. Brukernavn/passord på avveier. Dette utnyttes av annen bruker. På grunn av at uautorisert bruker kan logge seg inn som en annen og se på besvarelser. Manglende logging. Også med retters rolle.	Ikke beskrevet.
Risikoelement:	4		
Risikonivå:	Medium		
Anm:			

Tiltak nr. 3			
Organisasjon:		Risiko	Tiltak
Tiltakstype:	Teknisk	Bruk av felles PC kan føre til at bruker kommer rett inn i en annens sesjon og leverer oppgaver i denne brukers sted. På grunn av timeout på cookiesesjon. Forrige bruker logger seg ikke av.	Vurdere lengde på cookiesesjon.
Risikoelement:	5		
Risikonivå:	Medium		
Anm:			

Tiltak nr. 4			
Organisasjon:		Risiko	Tiltak
Tiltakstype:	Administrativt	Informasjon om fusk/mistanke til fusk kommer uvedkommende i hende. Det kjøres en likhetssjekk mellom innleverte oppgaver.	Sjekker opp med Martha et co om hvordan dette skal håndteres i henhold til POL/POF.
Risikoelement:	11		
Risikonivå:	Medium		
Anm: Eksisterende tiltak er Brukerbegrensning. Samt at ordet "fusk" ikke benyttes. Det sjekkes nøye av personell før vedtak settes.			

Tiltak nr. 5			
Organisasjon:		Risiko	Tiltak
Tiltakstype:	Teknisk	Databasen blir hacket av utro tjener, ekstern (uautorisert) hacker med tilhørende brudd på KIT.	Ikke beskrevet.
Risikoelement:	13		
Risikonivå:	Medium		
Anm: Eksisterende tiltak er segmentering, patching og dirftsrutiner.			

Tiltak nr. 6			
Organisasjon:		Risiko	Tiltak
Tiltakstype:	Teknisk	Feil i kode fra leverandør kompromitterer KIT.	Ikke beskrevet.
Risikoelement:	14		
Risikonivå:	Medium		
Anm: Eksisterende tiltak er automatiserte tester. Koden testes før produksjon. Hver enkelt enhet i systemet testes. Devilry er skrevet i åpen kildekode som gjør det mulig å etterprøve og gjennomgå all programvarekode.			

Tiltak nr. 7			
Organisasjon:		Risiko	Tiltak
Tiltakstype:	Administrativt	Data kommer på avveie som følge av at kopier av databasen (databasedump) blir liggende på bærbare enheter eller eksterne PC utenfor UiOs kontroll.	Avtalte rutiner for hvordan data skal behandles av leverandør.
Risikoelement:	15		
Risikonivå:	Medium		
Anm: Eksisterende tiltak er retningslinjer i sikkerhetshåndboken "Overføring av data til 3. part"			

Tiltak nr. 8			
Organisasjon:		Risiko	Tiltak
Tiltakstype:	Teknisk	Brukerkontoer på avveie på grunn av "bakdør" i Devilry.	Benytte SAML.
Risikoelement:	16		
Risikonivå:	Medium		
Anm: Delvilry benytter ldap og ikke SAML.			

Vedlegg A Kopi av ROS-regneark

Risiko- og sårbarhetsvurdering (ROS)								
Tjeneste/System		Devilry						
Nr.	Risikoelement	Sårbarheter/ svakheter	Eksisterende beskyttelsestiltak	Eksisterende kontrolltiltak	Vurdering			Forslag til tiltak
					S	K	Risiko	
1	Bruker får feil rolle i systemet	Feil data i kildesystemet eller FS			1	2	3	Bedre dokumentasjon av arbeidsprosesser/Ov ergang til WEB services
2	På grunn av feil registrering i FS, kan noen få rollen som "RETTER"	Komplisert registrering i FS (må sjekkes)	Lærer må godkjenne rollen "RETTER"		1	2	3	Opplæring
3	Data i Devilry og tilhørende roller til brukere er feil, disse blir ikke kontrollert, feil/mangledne bruker/roller	Vanskelig å kontrollere hva/hvem som har registrert hva i FS/Nettgrupper			1	2	3	
4	Uautorisert innlogging. Brukernavn/passord på avveier. Dette utnyttes av annen bruker	Uautorisert bruker kan logge seg inn som en annen og se på besvarelser. Manglende logging. Også med retters rolle			1	3	4	
5	Bruk av felles PC, bruker kommer rett inn i en annens sesjon og leverer oppgaver i denne brukerens sted	Timeout på cookiesesjon. Må vurderes lende på denne. Forrige bruker logger seg ikke av			1	3	4	
6	Brukerdata blir liggende etter at studenter har sluttet	Personopplysningsloven/forskriften			4	1	5	Må sjekkes av Martha/Tommy ++
7	En kritisk feil i systemet blir ikke rettet fordi avtalen med utviklerne er terminert/stoppet	Ingen langsiktig avtale med leverandør/utviklere			1	2	3	

8	Manglende support/retting videreutvikling på grunn av sårbarhet hos leverandør	Lite selskap, mange oppgaver, konkurs etc		Open source og vekjent løsning	2	1	3	
9	Manglende support/retting videreutvikling på grunn av at matnat avslutter finansieringen	Deler på kostnader for utvikling av Devilry			1	2	3	Se punkt 7
10	Må skifte leverandør på grunn av lov om offentlig anskaffelse og terskelverdier	Avtalen med leverandør og UiO (matnat) går ut over terskelverdiene			1	2	3	Er ut på anbud, må eventuelt sjekkes ut
11	Informasjon om fusk/mistanke til fusk kommer uvekkende i hende	Det kjøres en likhetssjekk mellom innleverte oppgaver	Brukerbegrensning	Det benyttes ikke ordet "fusk". Det sjekkes nøye av personell før vedtak settes	1	3	4	Sjekker opp med Martha et co om hvordan dette skal håndteres i hht POL/POF
12	Feil manuell registrering av hvilke studenter som er godkjent for eksamen. Inn i FS. Medfører medarbeid og stress	Manuell registrering av studenter som har tilstrekkelig innleverte oppgaver med godkjent resultat blir manuelt skrevet inn i FS			2	1	3	Opplæring/holdning sskapende arbeide
13	Databasen blir hacket med tilhørende brudd på KIT	Utro tjener, ekstern (uautorisert) hacker	Segmentering, patching og dirftsrutiner		1	3	4	
14	Feil i kode fra leverandør kompromitterer KIT	Feilkoding	Automatiserte tester, koden testes før produksjon. Hver enkelt enhet i systemet testes		1	3	4	
15	Data kommer på avveie som følge av at kopier av databasen (db-dump) blir liggende på bærbare enheter eller eksterne PC utenfor UiOs kontroll			Retningslinjer i sikkerhetshåndboken "Overføring av data til 3. part"	1	3	4	Avtalte rutiner for hvordan data skal behandles av leverandør
16	Brukerkontoer på avveie på grunn av "bakdør" i Devilry	Devilry benytter ldap og ikke SAML			1	3	4	Benytte SAML



- ◆ Adresse: 7465 Trondheim
- ◆ Sentralbord: +47 73 55 79 00
- ◆ E-post: postmottak@uninett.no
- ◆ Web: www.uninett.no