Universitetsstyret
Universitetet i Bergen

Arkivkode:

Sak nr.: 2009/7019

Styresak: 111

Møte: 03.12.2009

Revisjon av IKT- reglement og IKT- sikkerhetspolitikk

Bakgrunn

Universitetets IKT- reglement ble sist revidert i 2002. Siden den gang er IT-driftstjenestene ved universitetet blitt samlet i en sentral IT-avdeling. Endret organisering og endringer i lover og forskrifter, gjør det nødvendig å gjennomgå reglementet. Som del av arbeidet med å utforme en revidert sikkerhetspolitikk, er det gjennomført en undersøkelse av tekniske forhold knyttet til IT-sikkerheten.

IKT- reglementet

IKT-reglementet gjelder både ansatte og studenter. Alle som får tildelt IT-konto, må sette seg inn i reglementet. Forslaget til revidert reglement (vedlegg 1) har samme oppbygging som det eksisterende, men er tilpasset ny organisering av IKT-tjenestene og endringer i lov- og regelverk.

Vedtaket av *Forskrift om endring i forskrift om behandling av personopplysninger* (personopplysningsforskriften), e-postforskriften har betydning for reglementet. Forskriften regulerer arbeidsgivers rett til å gjennomsøke, åpne eller lese e-post i arbeidstakers e-post, blant annet ved begrunnet mistanke om at arbeidstakers bruk av e-post medfører grove brudd på plikter som følger av arbeidsforholdet, eller kan gi grunnlag for oppsigelse eller avskjed (§9-2).

Det foreslås endrede prosedyrer ved opphør av brukerkonto i universitetets IKT-anlegg. *Studenter* foreslås å kunne beholde brukerkonto i to semestre etter siste registrering som student,en samordning med studierettsreglementet. Ved opphør av *ansettelsesforhold*, foreslås det at det gis varsel om sperring av brukerkonto 14 dager før sluttdato, gitt i lønns- og personalsystemet. Pensjonister foreslås, i henhold til retningslinjer for tildeling av brukerkonto ved universitetet, mulighet til å beholde sin e-postkonto, dersom det er ønskelig.

Reglementet har regler for *utestenging* av fra universitetets IT-anlegg. Slik utestenging skal bare brukes dersom det er strengt nødvendig. Kortvarige utestenginger brukes for å sikre tid til nærmere undersøkelse eller for å avverge eller redusere skade. Lengre utestenginger vil ha preg av sanksjon mot regelbrudd. I slike tilfeller skal det vurderes om andre tiltak er bedre egnet enn utestenging etter IKT-reglementet. For studenter må det for eksempel legges vekt på at utestenging vil være hinder for å fortsette studiene og dermed kan grense opp mot utestenging etter universitets- og høyskoleloven.

Ved omorganisering til en sentral IT-avdeling ble funksjonen som IKT-driftsansvarlig ved enhetene borte. Noen punkt i de tidigere retningslinjene for IKT-driftsansvarlige er tatt med videre, men *Retningslinjer for IKT*- driftsansvarlige foreslås slettet.

Universitetets IKT- sikkerhetspolitikk

Den gjeldende IKT- sikkerhetspolitikken ble styrebehandlet i 2004 (sak 17/04). Den erstattet IKT-sikkerhetspolitikken fra 1993. Nye retningslinjer fra sentrale myndigheter ble innarbeidet i dokumentet i 2004. I vedlegg 2 er nytt forslag til dokumentet om IKT-sikkerhetspolitikk

I 2004 var det en IKT- sikkerhetssjef ved institusjonen, det er det ikke lenger. Samtidig er det langt flere administrative informasjonssystemer enn tidligere, det krever formalisert ansvar og tydelige ansvarslinjer, samt tydeliggjøring av krav til ansattes bruk av universitetets IKT-anlegg. Disse forholdene ligger til grunn for gjennomgangen av IKT-sikkerhetspolitikken fra 2004 og gjenspeiles i forslaget til revidert IKT-sikkerhetspolitikk.

Uønskede hendelser, som sikkerhetsbrudd, kan ha mange årsaker og være påvirket av mange faktorer. Noe kan påvirkes, andre forhold er det mulig å beskytte mot, og noen faktorer er det urealistisk å påvirke eller beskytte mot – institusjonen må leve med risiko. Men det bør ikke være tilfeldig risiko, og det er nødvendig å foreta risikovurderinger og å redusere risiko der det er mulig.

Dagens informasjonssystemer er komplekse og har mange brukere. Kontinuerlig foregår det utviklings-, drifts- og vedlikeholdsarbeid, både av ansatte og av eksterne leverandører. Det er ikke mulig å ha feilfrie (og sikre) systemer. Selv om de færreste med vilje vil ønske å skape uønskede hendelser, kan menneskelige feil gi risiko for at dette skjer. Videre kan noen være motivert til å foreta handlinger som fører til uønskede hendelser. IKT- sikkerhetspolitikkens mål er å medvirke til at sikkerheten i informasjonssystemene er god og tilpasset det enkelte informasjonssystemet. Risikoen og sårbarheten må være akseptabel med de kostnadene relevante sikkerhetstiltak har.

Gjennomgang av IT-sikkerheten ved UiB
Som oppfølging etter flere internrevisjoner av IT-systemer ved UiB, ble konsulentselskapet Avenir engasjert for å gjennomføre en teknisk gjennomgang av universitetets IKT-infrastuktur sommeren 2009. Hovedformålet var å gjennomføre en ekstern vurdering av hvordan den tekniske sikkerheten blir ivaretatt. Det var den delen av IKT-infrastruktur den sentrale IT-avdelingen har ansvaret for som ble undersøkt. Vedlagt følger IT-avdelingens rapport, med oppsummering fra revisjonsrapporten fra Avenir (vedlegg 3). Sikkerheten knyttet til universitetets felles IKT-ressurser er i hovedsak meget godt ivaretatt. Det er ikke avdekket noen alvorlige sikkerhetssvakheter, og IT-avdelingen har gode rutiner og kompetanse for å opprettholde en forsvarlig sikker IKT-infrastruktur. Avenir påpeker svakheter ved regimet for passord ved UiB, særlig hvordan passord tidligere ble satt sammen og det at det ikke er foretatt et tvunget passordskifte. Alle nye passord følger god passordstandard, og det planlegges at alle ansatte og studenter med eldre passord skifter dette. Avenir har også pekt på utfordringer med dokumentasjon av rutiner og hvordan IKT-tjenestene er bygd opp.

Universitetsdirektørens kommentarer
I det vedlagte forslaget til nytt IKT-reglement (vedlegg 1) for universitetet er det to tema som krever særlig oppmerksomhet. Det ene gjelder regler for utestenging fra IT-anlegget og det andre gjelder institusjonens håndtering av den nye forskriften om innsyn i ansattes e-post.

Det understrekes at det skal være en høy terskel for utestenging fra IT-anlegget, enten det gjelder studenter eller ansatte. Den det gjelder skal alltid varsles, og for utestenging over en viss tid skal det foreligge beslutning om dette fra univeristetsdirektøren.

Universitetet i Bergen har og vil ha en restriktiv politikk for innsyn i ansattes e-post slik at det bare helt unntaksvis skal være grunnlag for å be om innsyn. Tidligere kunne ansatte som var IKT-driftsansvarlige gå inn i ansattes e-post og hjemmekatalog ved mistanke om uønsket adferd. I forslaget til revidert IKT-reglement skjerpes regelverket inn, slik at det også blir strengere enn det den nye forskriften om behandling av personopplysninger gir rom for. Innsyn skal alltid være saklig begrunnet og gjelde mistanke om særlig alvorlige brudd på de pliktene som følger av arbeidsforholdet, eller kan gi grunnlag for oppsigelse eller avskjed av arbeidsforholdet. Det er bare aktuelt å be om innsyn hvis det er begrunnet mistanke om at arbeidstakers bruk av e-post kan gi grunnlag for oppsigelse eller avskjed, for eksempel

mistanke om at e-posten benyttes til å sende innhold som er i strid med norsk lov, trakassering eller til utsending av spam. Arbeidstaker skal varsles og få anledning til å uttale seg før det gjennomføres innsyn. I varselet skal universitetet begrunne hvorfor vilkårene for innsyn anses å være oppfylt og det skal orienteres om arbeidstakers rettigheter etter denne bestemmelsen.

Det foreslås at det bare er de ulike avdelingenes leder, sammen med personaldirektør og aktuell systemeier, som kan be om innsyn i ansattes e-post (jf. forskrift av 29.01.09 om endring i forskrift av personopplysninger). Eventuell beslutning om innsyn skal fattes av universitetsdirektøren.

IKT- sikkerhetspolitikken skal gjenspeile universitetets egenart og være i samsvar med dets overordnete mål og verdier. Universitetets IKT- anlegg er integrert i virksomheten. For at regelverket skal være hensiktsmessig, må det oppdateres i tråd med gjeldende lover og regler og med endringer i organisering. Ansvaret for IKT-sikkerhet følger universitetets linjeorganisasjon. Gjennomgående administrative informasjonssystemer nødvendiggjør større oppmerksomhet om ansvaret for systemene. Den reviderte IKT-sikkerhetspolitikken (vedlegg 2) har dette perspektivet med seg.

Revisjonsforslaget til nytt IKT-reglement og IKT-sikkerhetspolitikk har vært til høring hos fakultetene og de administrative avdelingene. I høringsrunden kom det kommentarer fra Universitetsbiblioteket (vedlegg 4), og disse er i hovedsak innarbeidet i forslagene eller de tatt med i den videre tekniske utviklingen av tjenestene.

Gjennomgangen av den generelle IT-sikkerheten ved institusjonen vurderes som nyttig for å oppnå tilstrekkelig sikkerhet i vår infrastruktur (vedlegg 3). Rapporten viser ikke umiddelbar risiko for eventuelle sikkerhetsbrudd, men noen områder bør utvikles og arbeides videre med. Det er gledelig at flere områder karakteriseres som godt IT-sikkerhetsmessig ivaretatt.

Universitetsdirektøren legger frem følgende forslag til

Vedtak:

1. Universitetsstyret godkjenner det reviderte forslaget til IKT-reglement ved UiB.
2. Universitetsstyret godkjenner det reviderte forslaget til IKT-sikkerhetspolitikk ved UiB.
3. Universitetsstyret tar rapporten om IT-sikkerhet ved Universitetet i Bergen til orientering.

19.11.2009 / CEO/THEV/PEH

Vedlegg:
1. IKT- reglement for Universitetet i Bergen
2. Overordnet IKT-sikkerhetspolitikk ved UiB
3. IT-sikkerhet ved Universitetet i Bergen
4. Høringsuttalelse fra Universitetsbiblioteket

IKT- reglement for Universitetet i Bergen

1. Virkeområde og organisering

1.1

Dette reglement gjelder for bruk av IKT-anlegg (Informasjons- og kommunikasjons teknologi anlegg) ved institusjonen. Med IKT-anlegg menes maskiner, sluttbrukerutstyr (også enheter som mobiltelefon og lomme-PC), nettverk, programmer, data m.v. som stilles til disposisjon av institusjonen - inklusive lokale, nasjonale og internasjonale nettverk, eller andres anlegg som det gis tilgang til gjennom slike ressurser. Reglementet gjelder også, for brukerens private IKT-anlegg eller andre IKT-anlegg i den utstrekning dette benyttes til å utføre oppgaver for institusjonen. Dette gjelder om anlegget er plassert i institusjonens lokaler eller andre steder.

1.2

Reglementet gjelder for arbeidstakere, studenter og andre som får tilgang til IKT-anlegg, heretter kalt brukere.

1.3

Ansvaret for institusjonens ulike IT-systemer som er i bruk enten i hele organisasjonen eller ved enkelte enheter, knyttes til systemeier. Med systemeier menes øverste leder ved den enheten som er ansvarlig eier av de enkelte systemene og løsningene. Systemeieren har ansvar for alle sider ved forvaltningen av IT-systemene eid av enheten. Dette gjelder både utvikling, oppgradering, drift, brukerstøtte og opplæring. En oversikt over systemeiere og gjennomgående fagsystem i organisasjonen skal være tilgjengelig. Systemeier kan gi utfyllende regler for bruk av det aktuelle IT-systemet

2 Formålet med bruk av institusjonens IKT-anlegg

Institusjonens IKT-anlegg og fagsystem skal nyttes til å utføre oppgaver knyttet til forskning, utdanning og formidling, samt til nødvendig drift og administrasjon. Alle bestemmelser i reglementet skal forstås ut fra dette formålet.

3 Lojal og ansvarlig bruk

3.1

Systemeier kan kreve at brukeren skal identifisere seg med navn, egen brukeridentitet og eget passord, eller på annen måte.

3.2

Brukeren har et medansvar for at IKT-anlegg og fagsystem utnyttes best mulig. Brukeren skal la sin bruk være til minst mulig ulempe for andre og ikke misbruke felles ressurser. Bruk som ikke direkte er knyttet til institusjonens formål, som reklame og kommersiell bruk, er bare tillatt dersom dette er bemyndiget av institusjonen.

3.3

Brukeren har plikt til å følge systemeiers anvisninger om bruk av anlegg eller tjenester knyttet til anlegget.

3.4

Det er brukerens ansvar at den informasjonen som skapes, lagres eller formidles på institusjonens IKT-anlegg ikke er i strid med dette reglementet, eller rettsregler for øvrig. Utover dette skal brukeren avholde seg fra bruk av IKT-anlegg som utsetter institusjonen for vesentlig risiko for tap av omdømme.

3.5.

Brukeren er selv ansvarlig for ytringer og informasjon som formidles gjennom IKT-anlegget. Det skal fremgå hvem som er ansvarlig for den aktuelle informasjonen.

Informasjon om annet enn institusjonens virksomhet skal ha en form som gjør at den ikke kan forveksles med offisiell informasjon fra institusjonen.

3.6

Brukeren skal ikke uautorisert endre eller modifisere IKT-anlegget eller på annen måte forårsake at IKT-anlegget virker på en annen måte enn forutsatt.

3.7

Alle ansatte har et ansvar for å lagre arbeidsrelatert materiale på områder der det jevnlig tas back-up (det vil si på avdelingens fellesområder eller den ansattes eget filområde på universitetets nett).

3.8

Ved opphør av ansettelsesforhold gis det varsel om sperring av brukerkonto 14 dager før sluttdato, slik denne fremkommer i lønnssystemet eller er satt av leder ved den ansattes enhet. Konto sperres på sluttdato og ligger sperret i ett år for så å bli slettet. Ved opphør av studentforhold sendes varsel om sperring av brukerkonto en måned før konto sperres. Sperrevarsel sendes det 3. semesteret etter at en student sist var registrert som student (betalte semesteravgift). Konto slettes automatisk ett år etter at sperring inntreffer. Ved opphør av ansettelses-, studie- eller brukerforhold er brukeren ansvarlig for at kopier av data, programmer og annet som eies eller disponeres av universitetet sikres slik at dette kan være tilgjengelig for ettertiden. Andre filer og annet som er lagret under brukerens navn, brukeridentitet eller lignende, skal brukeren selv slette. Skjer dette ikke innen ett år, kan øverste leder ved enheten slette slike filer. Dette gjelder både for ansatte og studenter.

Ved dødsfall skal personlig e-postkasse og private filer som hovedregel slettes, med mindre offentlige myndigheter har krevd innsyn eller dødsboet har gjort gjeldende rett til materialet. Av hensyn til slike eventuelle krav og rettigheter, slettes ikke noe før ett år etter dødsfallet. Ved dødsfall kan universitetsdirektør beslutte at det skal foretas innsyn for å finne fram til virksomhetsrelatert e-post. Slikt innsyn vil bli gjennomført i samarbeid mellom enhetens leder og Personal- og organisasjonsavdelingen.

4 Informasjon , opplæring og krav til kunnskap

4.1

Reglementet og eventuelle utfyllende bestemmelser, skal være tilgjengelig på institusjonens web-sider. Brukeren av IKT-anlegg plikter å holde seg informert om det til enhver tid gjeldende IKT-reglement og eventuelle supplerende bestemmelser til dette.

4.2

Brukeren har plikt til å sette seg inn i bruksanvisning, dokumentasjon m.v. på forsvarlig måte slik at risikoen for driftsforstyrrelser eller tap av data, programmer eller utstyr ikke blir unødig stor.

5 Datasikkerhet

5.1

Brukeren plikter selv å treffe de tiltakene som er hensiktsmessige for at tap av data, programmer eller lignende skal få minst mulig følger gjennom sikkerhetskopiering, forsvarlig oppbevaring av media og anbefalte rutiner for bruk av nettet. Nærmeste overordnete skal opplyse om institusjonens rutiner og tiltak for å sikre brukernes data. Brukeren er kjent med at ingen IKT-anlegg kan være helt sikre og vil legge dette til grunn når en sikkerhetsløsning skal velges.

5.2

Brukeren plikter å ikke gjøre personlige passord kjent for andre.

5.3

Brukeren har et ansvar for å innrette seg slik at uautoriserte personer ikke får tilgang til bruk av nettet, adgang til anlegg eller tilgang til rom hvor utstyr er tilgjengelig, og ellers på annen måte bidra til å hindre at uautoriserte personer får tilgang til utstyret.

5.4

Brukeren plikter å være oppmerksom på at programmer eller data kan inneholde uønskede elementer ("virus"e.l.) og selv treffe hensiktsmessige tiltak for kontroll.

5.5

Brukeren plikter straks å rapportere forhold som kan ha betydning for IKT-anleggets sikkerhet eller integritet til nærmeste overordnete eller til IT-avdelingen.

6 Respekt for andre brukere, personopplysningsvern

6.1

Brukeren må ikke søke å oppnå uautorisert tilgang til andres data, programmer m.m., eller søke å gjøre seg kjent med andres passord.

6.2

Brukeren plikter å gjøre seg kjent med lover, forskrifter og regler som gjelder for bruk av IKT-anlegg, særlig for behandling av personopplysninger. Personal- og organisasjonsavdelingen kan gi veiledning om hvordan brukere skal forholde seg ved behandling av personopplysninger.

6.3

For å oppfylle reglementets formål, Jf.§2, er IKT-anlegg tilrettelagt med blant annet sporing (logging) og sikkerhetskopiering.

7 Rettigheter

7.1

Brukeren forplikter seg til å respektere opphavsrett eller lignende rettigheter til datamaskinprogrammer og til data (tekst så vel som samlinger av opplysninger som databaser, musikk, bilder og film). Det er brukerens ansvar å gjøre seg kjent med de gjeldende reglene om slike rettigheter, enten de fremgår av lov eller av avtale med vedkommende rettighetshaver (lisensavtaler). Slike avtaler vil være tilgjengelige hos systemeier.

8 Tjenestekvalitet, erstatningsansvar

8.1

Brukerne har selv ansvaret for bruk av opplysninger, programmer m.v. som gjøres tilgjengelige gjennom anlegget. Institusjonen fraskriver seg ansvar for økonomisk tap eller annen ulempe som følge av feil eller mangler i programmer, data, bruk av opplysninger fra tilgjengelige databaser eller andre opplysninger innhentet gjennom nettet m.v.

9 Arbeidsgivers rett til å søke tilgang til reserverte områder

9.1

Arbeidsgivers rett til innsyn i ansattes e-post m.v. er regulert i forskrift av 29. januar 2009 om endring i forskrift om behandling av personopplysninger. Universitetet i Bergen skal bare be om innsyn i når det er særlig presserende og den ansatte skal alltid varsles. Forskriften gjelder også for innsyn i studenters e-post. Begjæring om innsyn fremmes av av øverste leder ved enheten (ved institutt, fakultet eller avdeling i sentraladministrasjonen) i samråd med Personal- og organisasjonsavdelingen og aktuell systemeier. Den ansatte skal varsles om begjæringen. Beslutning om innsyn skal fattes av universitetsdirektøren. Begjæring om innsyn i studenters e-postkasse fremmes av leder av fakultet i samråd med

Utdanningsavdelingen og aktuell systemeier. Beslutning fattes av universitetsdirektøren.

9.2

I tilfeller som er beskrevet i punkt 9.1, skal bruker varsles og få anledning til å uttale seg før det gjennomføres innsyn. Bruker skal så langt som mulig gis anledning til å være tilstede under gjennomføringen av innsynet og har rett til å la seg bistå av tillitsvalgt eller annen representant. Innsynet skal gjennomføres på en slik måte at dataene så langt som mulig ikke endres og at de frembrakte opplysninger kan etterprøves.

Viser innsyn i e-postkassen at det ikke foreligger dokumentasjon som UiB har rett til innsyn i, vil e-postkassen og dokumenter i denne straks bli lukket. Eventuelle kopier slettes.

9.3

Hvis bruken av arbeidsstasjon, terminal eller annet sluttbrukerutstyr på grunn av driftssikkerhet eller av andre hensyn overvåkes, skal dette opplyses med merke på enheten eller på annen hensiktsmessig måte.

10 Sanksjoner

10.1

Overtredelse av reglementets bestemmelser kan føre til at bruker nektes tilgang til hele eller deler av institusjonens IKT- anlegg. I tillegg kan det medføre sanksjoner etter andre regler, så som disiplinærreaksjoner etter tjenestemannslovgivningen, advarsel eller utestenging fra studier og eksamen etter universitets- og høyskoleloven, erstatningsansvar, straffeansvar o.a.

10.2

Midlertidig utestenging, i inntil 5 virkedager, på grunn av overtredelse, eller mistanke om overtredelse, kan besluttes av øverste leder ved enheten (ved institutt, fakultet eller i avdeling i sentraladministrasjonen), eventuelt i samråd med systemeier. Slik utestenging kan bare skje dersom det er grunn til å anta at:

- brukeren har gjort seg skyldig i alvorlige overtredelser, eller
- brukeren utgjør en vesentlig trussel for IKT-sikkerheten (brudd på konfidensialitet, integritet eller tilgjengelighet), eller
- brukerens IKT-utstyr utgjør en vesentlig trussel for IKT-sikkerheten

10.3

Vedtak om utestenging gjøres av universitetsdirektøren når utestengingsperioden er lengre enn 5 dager, men ikke lengre enn seks måneder. For øvrig gjøres vedtak av styret. Det skal legges vekt på overtredelsens grovhet, om brukeren tidligere har overtrådt reglementet, hvilke følger en utestenging vil få for brukeren og forholdene ellers.

Dersom sanksjoner etter reglementet her vedtas i et slikt omfang at det må likestilles med ordensstraff eller andre disiplinærsanksjoner etter tjenestemannsloven, ev. med advarsel eller utestenging etter universitets- og høyskolelovens § 4-8, skal saken behandles etter disse lovenes regler om saksforberedelse m.v.

10.4

Klage på vedtak truffet med hjemmel i tjenestemannsloven, universitets- og høyskoleloven og forvaltningsloven følger disse lovenes regler om klage.

Andre vedtak etter punkt 10 kan påklages innen 3 uker til nærmeste overordnede instans, jf.punkt 1.3.

Overordnet IKT- sikkerhetspolitikk ved UiB

1. Formål

- IKT-sikkerhetspolitikk ved Universitetet i Bergen skal bidra til å støtte opp under institusjonens mål, verdier og hovedoppgaver
- Som rammeverk for sikkerhetspolitikken er standarden NS-ISO/IEC 17799 benyttet og gjelder som utfyllende bestemmelser så langt formuleringene passer på forholdene ved UiB.

2. Begrep og definisjoner

- Informasjonssikkerhet: Beskyttelse av informasjonens konfidensialitet, integritet og tilgjengelighet.
  - Konfidensialitet: Å sikre at informasjonen er tilgjengelig bare for dem som har autorisert tilgang.
  - Integritet: Å sikre at informasjonen og behandlingsmetodene er nøyaktige og fullstendige.
  - Tilgjengelighet: Å sikre autoriserte brukeres tilgang til informasjon og tilhørende ressurser ved behov.
- Risikovurdering: Vurdering av trusler opp mot, virkninger på og sårbarheten til informasjonen og informasjonssystemene, og sannsynligheten for at sikkerhetshendelser kan inntreffe
- Risikostyring: Prosessen med å identifisere, kontrollere og redusere eller eliminere sikkerhetsrisikoer som kan påvirke informasjonssystemer, innenfor en akseptabel kostnadsramme
- Systemeier er den øverste lederen ved den enheten som er ansvarlig for de enkelte systemene og løsningene. Systemeier har ansvar for alle sider ved forvaltningen av IT-systemene enheten har ansvar for, det gjelder utvikling, oppgradering, drift, brukerstøtte og opplæring
- Behandlingsansvarlig: rektor er behandlingsansvarlig etter lov om behandling av personopplyninger. Operative oppgaver er delegert til systemeier slik det fremkommer i fortsettelsen, IKT-reglementet ved Universitetet i Bergen, samt etter Sikkerhetsmål og sikkerhetsstrategi for behandling av personopplysninger i administrative system og Sikkerhetsmål og sikkerhetsstrategi for behandling av personopplysninger som ledd i forskning.

3. Sikkerhetspolitikk

- Sikkerhetspolitikken skal søke å oppnå en langsiktig tilpasning mellom reelle sikkerhetstrusler og de kostnadene sikkerhetsbrudd kan medføre sammenholdt med de sikkerhetstiltakene som iverksettes
- Risikovurderingen skal baseres på en konkret vurdering av trusler og utfordringer for UiB. Videre skal direkte og indirekte vurderinger i lover, forskrifter, pålegg eller avtaler med tredjepart, god IT-skikk og etiske normer legges til grunn
- For systemer som er virksomhetskritiske, skal det være utarbeidet sårbarhets- og risikoanalyser

4. Ansvar og myndighet

Overordnet ansvar

- Universitetsdirektøren har etter delegasjon fra Universitetsstyret og i samråd med rektor overordnet ansvar for IKT-sikkerheten ved UiB.

Operativt ansvar

- IT-direktøren har overordnet ansvar for operativ IKT-sikkerhet med fullmakt til å treffe tiltak for å hindre skade og forebygge fare for skade, samt å iverksette tiltak med sikte på bevissikring og koordinere tiltak for å utbedre eventuelle skader.

- Administrativ leder ved fakultet (fakultetsdirektører eller dekaner ved enhetlig ledelse og ledere for administrative avdelinger eller de disse utpeker på sine vegne) har det operative ansvar for IT-sikkerhetsarbeidet (er IT-sikkerhets-ansvarlige) innenfor sine respektive ansvarsområder. Grunnenheter kan utpeke IT-sikkerhetskoordinatorer dersom virksomheten ved enheten gjør dette hensiktsmessig.
- Ansvaret uttrykkes ledernes stillingsbeskrivelser
- Sammen med universitetsledelsen har systemeiere ansvar for fastsetting av sikkerhetsnivået i systemene og kontroll av at sikkerheten ivaretas. Der det ikke er utpekt en systemeier, regnes den som har utviklet eller anskaffet systemet for bruk ved UiB, som systemeier. IT-direktøren systemeier for anlegg for datalagring og sikkerhetskopiering (backup), e-postsystemet og nettverk. Systemeier skal foreta årlig sikkerhetsrevisjon av informasjonssystemer som behandler personopplysninger, jf personopplysningsforskriften § 2-5 og "Rutiner for sikkerhetsrevisjon av informasjonssystemer ved Universitetet i Bergen (ikke vedtatt).

Ansvar tillagt tilsatte og studenter

Alle brukere av systemene ved UiB har ifølge IKT-reglementet et ansvar for å ivareta sikkerheten i forbindelse med utførelsen av eget arbeid; dette gjelder både den informasjon som behandles på systemene så vel som systemene i seg selv.

5. Klassifisering og sikring av informasjon

- Universitetet er underlagt bestemmelser om klassifisering og sikring av informasjon som fremgår av personopplysningsloven, offentleglova, helseregisterloven, helsepersonelloven, helseforskningsloven, beskyttelsesinstruksen, universitets- og høyskoleloven, lov om offentlige arkiv og andre bestemmelser for statsforvaltningen.
- Forskningsvirksomhet som er klausulert vil kunne kreve at informasjon skal beskyttes særskilt.

6. Personellsikkerhet

Krav til personellsikkerhet ivaretas gjennom den generelle aktsomhetsplikt som forutsettes blant annet ved tilsetting og innleie av personell.

7. Fysisk og miljømessig sikkerhet

Det forutsettes at alt IKT-utstyr som benyttes som basis for fellesfunksjoner (servere, datalager, nettverkstjenere m.m) er plassert i lokaler som er fysisk sikret mot tilkomst for uvedkommende.

8. Kommunikasjons- og driftsadministrasjon

- Den enkelte systemeier skal påse at enhetene som er involvert i drift av systemet har dokumenterte driftsprosedyrer.
- Driftsenheter skal alltid ha en generell beskyttelse mot virus og andre former for angrep som kan påvirke systemenes stabilitet, integritet og konfidensialitet, samt rutiner for forebygging av de mest forekommende feilsituasjoner.
- I samråd med systemeiere skal driftsenhetene oppta og analysere hendelseslogger og foreta sikkerhetskopiering. For systemer som utveksler informasjon skal de respektive systemeierne påse at de involverte driftsenhetene tar hensyn til dette i sine driftsrutiner.
- For systemer med omfattende utbredelse som e-post, web-portaler, saksbehandlersystem og IKT-baserte undervisningsopplegg, skal sikringstiltak dokumenteres.

9. Tilgangskontroll

- Tilgang til informasjon og tjenester og prosesser for IKT-behandling skal styres i samsvar UiBs virksomhets- og sikkerhetsbehov. Alle studenter og ansatte skal etter personlig aksept av reglene i IKT-reglementet, autoriseres for tilgang til generell informasjon relatert til studenter eller ansatte.

- Tilgang til andre IKT-systemer skal være basert på en vurdering av hvilke legitime behov som foreligger i forbindelse med utføring av oppgaver som er pålagt av institusjonen.
- IKT-tjenester rettet mot publikum skal normalt ikke kreve autorisasjon. Personer som ikke er tilsatt eller er student ved UiB kan tildeles autorisasjon til IKT-tjenester i samsvar med en konkret vurdering av systemeier.
- For å motvirke misbruk av en autorisasjon, kan systemeier etablere ordninger for sikring, for eksempel ved hjelp av passord, eller en fysisk identifikator.
- Systemeier skal utarbeide egne rutiner for tilgang til det enkelte informasjonssystem.
- IT-avdelingen har hovedansvar for kontroll med tilgang til UiBs nettverk og generelle IKT-tjenester, også for bærbart utstyr og utstyr som benyttes utenfor UiB.

10. Systemutvikling og vedlikehold

Alle sikringskrav, inkludert behovet for reserveløsninger, identifiseres i forbindelse med kravspesifikasjon og skal godkjennes og dokumenteres som en del av driftsavtalen. Systemeier i samråd med driftsenheten(e) skal etablere system for kontroll av produksjonsprogramvare og testdata, med endringer og oppdateringer.

11. Kontinuitetsplanlegging

- Basert på en vurdering av relevante risikoer for driftsavbrudd, skal systemeier påse at det utarbeides planer og iverksettes tiltak som kan redusere avbrudd ved sikkerhetssvikt til et akseptabelt nivå. Det skal utføres realistiske kontroller av for å verifisere effektiviteten av de tiltakene som er iverksatt.
- Driftsenhetene i samråd med systemeiere har ansvaret for å sikre at systemet og informasjon i systemet kan gjenopprettes. Der det ikke er utpekt systemeier, er det den enkelte brukers ansvar å foreta en hensiktsmessig kontinuitetsplanlegging, blant annet det å sikre at vital informasjon ikke går tapt ved utilsiktede hendelser.

12. Overensstemmelse med eksterne bestemmelser og krav

- Som statsinstitusjon skal UiB følge retningslinjer og bestemmelser som gjelder virksomhet i Norge og for statsinstitusjoner innenfor forskning og undervisning. Systemeier skal dokumentere hvilke eksterne bestemmelser og krav som er retningsgivende for informasjonssystemet.
- UiB skal ha klare regler og praksis for håndtering av informasjon som andre har lovbeskyttede rettigheter eller disposisjonsrett til, dette gjelder også programvare, datasamlinger og IKT-baserte løsninger knyttet til forskning og undervisning.
- Informasjonssystemene er etablert for virksomhetsformål og bruken av systemene skal autoriseres av ledelsen i samsvar med formålet. Bruk av systemene for ikke-virksomhetsrelaterte formål uten godkjenning av ledelsen, er utilbørlig bruk. Informasjonssystemene skal tilrettelegges slik at normale krav til bevisførsel ved lovbrudd og avvik fra interne rutiner og regler (som eksamensfusk) skal kunne tilfredsstilles.
- Det skal foretas systematiske gjennomganger (internkontroll) som verifiserer at UiBs og eksterne myndigheters krav til IKT-sikkerhet er ivaretatt og fungerer etter sin hensikt.

IT-sikkerhet ved Universitetet i Bergen

Thomas Evensen, IT-avdelingen

19. oktober 2009

Innhold

1 Innledning

Denne rapporten oppsummerer den generelle IT-sikkerheten ved Universitetet i Bergen som den sentrale IT-avdelingen har ansvaret for. Det henvises og til UiB IKT-reglementet og IKT-sikkerhetspolicy i UiB regelsamling for ytterligere dokumentasjon om ansvar og regler for bruk av UiB IKT. Begrepet IT-sikkerhet

kan defineres til å omfatte kontinuitetsløsninger, sikring av data, tilgjengelig til data, fysisk sikring osv. IT-sikkerhet i denne rapporten har primært fokus på ytre trusler fra internett men diskuterer og indre trusler. Hovedtema i rapporten er hvordan den sentrale IT-avdelingen ved UiB håndterer disse trusler for å minimalisere og redusere risikoen for at:

- UiB som institusjon og
- ansatte/studenter som enkeltindivider

skal bli utsatt for uønskede hendelser som følge av et ondsinnet angrep fra internett. Ondsinnet angrep er benyttet som et samlebegrep for de trusler man som person og organisasjon blir utsatt for ved eksponering på internett.

1.1 Ingen garantier

Det er ikke mulig å gi noen garantier for at UiB i fremtiden ikke vil oppleve at et ondsinnet angrep blir "vellykket" gjennomført. Nye sårbarheter oppdages jevnlig, og det tar tid før det er utviklet oppgraderinger som eliminerer sårbarheten. Hovedpoenget med rapporten er å dokumentere både styrker og svakheter ved forvaltning av UiB IT-sikkerhet for å kunne bedre forvaltningen og redusere risikoen for "vellykkede" angrep. God og tilstrekkelig IT-sikkerhet ved UiB er en kompleks og sammensatt utfordring, og det forutsetter både fokus og ressurser.

1.2 Ekstern sikkerhetsrevisjon

Konsulentselskapet Avenir ble sommer 09 engasjert for å gjennomføre en teknisk sikkerhetsrevisjon av UiB IKT-infrastruktur. Hovedformålet med oppdraget var å gjennomføre en ekstern revisjon av hvordan den tekniske sikkerheten blir ivaretatt ved UiB. Omfang for undersøkelsen var den del av UiB IKT-infrastruktur som den sentrale IT-avdelingen har ansvaret for. Revisjonen hadde og en teknisk vinkling. Hovedkonklusjonen fra revisjonen er referert i denne rapporten.

1.3 Oppbygging av rapporten

Rapporten inneholder ingen tekniske detaljer eller detaljerte beskrivelser. Alle skisser er overordnede, og hovedhensikt med rapporten er å gi en generell status på sikkerhet. Hvilke områder som har et forbedringspotensiale og hva er forutsetningene for å opprettholde en forsvarlig sikkerhet (totalt sett). Rapporten er bygd opp som følger:

1. generell informasjon om hva som oppfattes som sikkerhetstrusler fra internett (seksjon 2 på neste side)
2. generell informasjon om hvordan UiB IKT-infrastruktur er bygget opp (seksjon 3 på side 6)
3. informasjon om løpende- og organisatoriske tiltak for å minimalisere risiko for angrep (seksjon 4 på side 8)

4. informasjon om status IKT-sikkerhet ved UiB(seksjon 5 på side 11)
5. forslag til forbedringstiltak (seksjon 6 på side 12)

2 Trusselbildet

Trusselbildet har endret seg over tid. De første hackere (datasnoker) brøt seg inn på websider og la igjen bevis på at de hadde vært inne. Utover et redusert selvbilde til den lokale IT-avdeling eller IT/webansvarlig var det liten skade ved slike angrep. Hovedandelen av angrepene i dag er gjennomført av *organiserte kriminelle*. Det betyr og at skaden etter et eventuelt vellykket angrep i dag er langt mer alvorlig enn tidligere[1]. Det er forsatt innbrudd/datasnoking/hacking av den "gamle sorten". Observasjoner tyder nok på at det meste av dette er politisk orientert og blir f.eks utført når to parter er i konflikt med hverandre (enten for å spre politiske budskap eller DoS/DDoS[2] angrep). Det antas at militære installasjoner og etterretningsorganisasjoner (som f.eks Pentagon og CIA i USA) er mest utsatt for forsøk på innbrudd og tapping av informasjon.

2.1 Ytre og indre trusler

I IT-sikkerhetssammenheng brukes ofte begrepene *ytre/indre* trusler. De ytre trusler er representert ved at organisasjonens nettverk eksponert for internett. De indre trusler opptrer på *innsiden* og er representert ved de ansatte og (for UiB) studenter. Om trusselen for UiB er størst fra utsiden eller innsiden er vanskelig å dokumentere, men det vi med sikkerhet kan si er at begge eksisterer og må håndteres på en forsvarlig måte.

2.1.1 UiB og ytre trusselbilde

For UiB antar vi at den største ytre trusselen er økonomisk motivert, de kriminelle er ute etter raske økonomiske gevinster. Trusselen retter seg både mot den *enkelte ansatte/student* og UiB som *institusjon*. Vi har intet grunnlagsmateriale for å mene noe om trusselen er mest rettet mot UiBs forskning eller mot den enkelte ansatte/student.

Mange av dagens angrep er *web-basert*, og brukere blir *angrepet* ved at de besøker (populære) nettsteder som er kompromittert med skadelig software (såkalt *malware*[3]). Brukerens egen PC blir smittet ved besøket gjennom utnyttelse av svakheter og hull i egne systemer, som oftest uten at brukeren selv er klar over det. En annen og meget utbredt metode er *spam* og *phishing* teknikker. Spam og phishing misbruker tilliten hos brukeren til å få han/hun til f.eks å gi

[1] Identitetstyveri er f.eks et meget aktuelt mål for angrep. Personnummer (11 siffer) kan benyttes av kriminelle for å bestille både varer og kredittkort. Så kan en spørre hvor enkelt er det for en norsk statsborger å skifte personnummer?

[2] Denial of service or distributed denial of service

[3] Malicious software

fra seg sitt passord på email. Felles for de fleste angrep er å utnytte en sårbarhet eller tappet informasjon for å oppnå en økonomisk gevinst.

Et av de siste store angrepene (Conficker - som er en *orm/trojaner* [4]) demonstrerte hvor skadelig et datavirus kan være, og hvor krevende det kan være å nedkjempe videre spredning og redusere skadeomfanget.

UiB ble sommeren 2008 utsatt for et phishing angrep som hadde til hensikt å få en eller flere av våre egne ansatte eller studenter til å gi fra seg sin login id og passord. Angrepet var "vellykket" ved at de fikk oppgitt login id og passord til noen få UiB brukere og UiBs mailinfrastruktur ble utnyttet til å sende flere hundretusen spam mail. Dette er bare et eksempel på hvordan et angrep kan være. UiB blir hver dag bombardert med spam og i snitt blir 80% av innkommende mail stoppet av våre spamfiltre. Se seksjon 7 på side 12 for detaljer og tall om UiB og innkommende spam mail.

De kriminelle organisasjoner har en betydelig økonomi og de rekrutterer IT-folk med høy kompetanse. På internett i dag kan hvem som helst kjøpe software komponenter som kan benyttes til egne angrep. De kriminelle organisasjoner er spredt over hele verden og de bruker selv internett som redskap for sitt arbeid. De arbeider desentralisert og i det skjulte og har velutviklede planer for å reallokere nødvendige ressurser på nett når de selv blir angrepet av virusjegere. En klar trend er at de kriminelle blir mer og mer sofistikerte, målrettede og det blir vanskeligere å detektere at man er utsatt for et angrep.

Uautorisert bruk av UiBs IKT-infrastruktur En annen stor trussel som UiB har erfart er uautorisert bruk av universitetets IKT-ressurser. UiB har både mye båndbredde og serverkapasitet som er eksponert direkte på internett og som av noen er interessant å forsøke å utnytte for uærlige hensikter. Phishing angrep er allerede nevnt. En annen og kanskje like stor trussel er innbruddsforsøk på UiBs servere. Dersom uvedkommende har fått tilgang til en eller flere av våre servere vil disse igjen kunne misbrukes til f.eks DoS angrep eller som utsender av spammail. Uvedkommende kan få tilgang til universitetets ressurser enten gjennom svakt konfigurerte eller ikke tilstrekkelig patchede servere, eller via ukjente hull i server SW.

2.1.2 UiB og indre trusselbilde

UiB har mange administrative systemer både for ansatte og studenter som inneholder sensitive data. Med sensitive data menes f.eks data som er definert som dette i personopplysningsloven (POL). Det kan være karakterer og kursoversikter for studenter osv. Dette er data som skal være beskyttet og hvem som har innsyn og rett til å utføre endringer er regulert. UiB har en plikt til å beskytte denne informasjon og forhindre at verken ansatte eller studenter får urettmessig lese- eller skrive tilgang.

[4] En orm eller trojaner utnytter sårbarheter på maskiner/utstyr som er eksponert på internet uten at brukere er direkte involvert. Ormer og trojanere har og den egenskapen at de sprer seg selv på nettet.

Systemer som SEBRA, FS (Felles studentsystem) og økonomisystemer vil antakeligvis være systemer som er spesielt interessante for ansatte og studenter. Fler av disse systemer har vært gjennom egne revisjoner og det er ikke avdekket noen alvorlige sikkerhets hull i disse. Adgangen til disse systemene er regulert gjennom både passord og aksesslister. Teknisk sett er det ingen forskjell på ytre og indre trussel ift disse systemene. Dersom vi har en tilfredsstillende sikkerhet mot ytre trusler vil disse sikkerhetsmekanismene også gjelde fra "innsiden".

2.2 Overordnede IKT-sikkerhets tiltak

Det synes som om det er en evig kamp der utviklere av både åpen kildekode løsninger, fri programvare og software industrien kjemper mot den organiserte kriminalitet. Det forskes mye på IT-sikkerhetstema og det publiseres artikler og bøker i stort omfang. Det er ikke mulig for UiB sin sentrale IT-avdeling å ha en *forskers kunnskap* om dette. UiB IKT-infrastruktur er heterogen og favner et bredt spekter av teknologier. Men vi må ha tilstrekkelig kompetanse og forståelse av hva IT-sikkerhet betyr og hvordan vi skal administrere UiBs IKT-infrastruktur slik at den er mest mulig motstandsdyktig mot angrep.

Den sentrale IT-avdelingen kan IKKE utstede noen garanti for at UiBs IKT-infrastruktur aldri vil bli kompromittert. Vårt ansvar er å ha tilstrekkelige nok preventive tiltak og ha gode nok rutiner for å oppdage og håndtere en situasjon dersom vi blir smittet. Da er det viktig for UiB at vi har følgende:

1. forebyggende tiltak:
   (a) gode nok rutiner for å patche og oppgradere både operativsystemer og applikasjoner
   (b) herding av systemer mot angrep
   (c) utvikle *sikre* løsninger (sikker programmering)
   (d) holde oss selv (egenkompetanse) orientert og informert om sikkerhetstema
   (e) opplæring og kompetanse
   (f) informere UiBs brukere om trusler og farer
   (g) gode nok rutiner for å håndtere bærbart utstyr og håndholdte enheter
   (h) tilstrekkelig utstyrskontroll (både over hvilke PC/servere som IT-avdelingen har ansvaret for og utstyr som vi ikke har kontroll over)
2. å håndtere en situasjon når vi er blitt angrepet gjennom:
   (a) overvåking og oppdagelse av kompromitterte kilder
   (b) overvåking av logger
   (c) mail
   (d) nedstengning av smittede kilder i UiBs infrastruktur

Det er ikke mulig i et lite notat å formidle et annet budskap enn at det er store utfordringer og det krever både tid og ressurser for stå i mot trusselen fra internett. Det betyr og at UiB må ha spesialister som har fokus på sikkerhet innenfor sitt område (f.eks på Windows plattformen). En godt nok sikret UiB IKT-infrastruktur er avhengig av mange (desentralisert ansvar).

3 UiB IKT-infrastruktur (logisk)

UiB IKT-infrastruktur er meget kompleks og sammensatt. I *IT-sikkerhetskontekst* kan vi forenkle denne i logiske komponenter ift en IT-sikkerhets risiko.

Hovednettene i UiB IKT-infrastruktur er:

- ITA "driftede" nett (kontrollerte nett)
  - *servernett* (hvor alle sentralt driftede servere er installert)
  - *managementnett* (eget nett for management/administrasjon for servere og PC-er)
  - *administrativt nett* (129.177.8) beskyttet av dedikert brannmur (FW[5])
- Autentisert nett (bruker må logge seg på)
  - *privatnett* (alle tilkoblinger mot UiB via en VPN GW[6])
  - *eduroam* (maskiner koblet direkte på nett)
- *terminalnettet* (alle nettsegmenter som ikke inngår i noen av de ovennevnte)

ITA har ansvaret for den totale nettverksinfrastruktur på campus, men ITA kontrollerer ikke alt som blir koblet på nettverket.

3.1 Hva skiller UiB nett fra andre bedriftsnett?

I et normalt oppsett vil bedriften beskytte seg mot trusler fra internett ved å sette opp en brannmur mellom seg og internett. På den måten vil mye av sikkerheten bli ivaretatt av brannmursinstallasjonen. Det kan igjen bety at bedriften har noe mindre kontroll av sikkerheten på utstyret bak brannmuren og da med en viss fare for at dersom uønskede gjester slipper gjennom brannmuren kan skaden bli desto større. DnBNOR ble i februar/mars 2007 utsatt for en orm (viking.gt). Den rammet banken meget hardt, og ormen klarte å smitte store deler av det interne nettverket til banken. Banken ble tvunget til å stoppe all trafikk til/fra internett i flere uker. Det er lite sannsynlig at UiB hadde blitt rammet på samme måte.

Ved UiB er hovedtyngden av sikkerheten lagt på hver enhet (punktsikkerhet). UiB har og et enklere driftsopplegg (en standard konfigurasjon for både

[5] Firewall
[6] Virtual private network gateway

Figur 1: Logisk oppbygging av UiB IKT-infrastruktur

Windows og Linux), og det gjør det lettere å opprettholde et tilfredsstillende patchenivået. UiB har og en brannmur som beskytter de administrative systemer. Men hovedandelen av UiBs IKT ressurser står koblet direkte mot internett og må beskyttes deretter.

4 Tiltak for å opprettholde en *sikker nok* UiB IKT-infrastruktur

Hva er en sikker nok UiB IKT-infrastruktur? Spørsmålet er utfordrende, og det vil alltid være en balanse mellom sikkerhet og tilgjengelighet til tjenester. ITAs beste sikkerhetstiltak er kompetanse og anvendelse av den kunnskap vi har om sikkerhet i våre IKT-tjenester. God sikkerhet betyr tid, økonomiske midler og tilstrekkelig med ressurser. ITA medarbeidere må vedlikeholde og videreutvikle sin egenkompetanse om sikkerhet innenfor sine fagfelt. Det er f.eks stor forskjell på å sette opp en sikker servertjeneste og programmere en sikker web applikasjon. Men begge to er like viktige for den totale sikkerheten ved UiB.

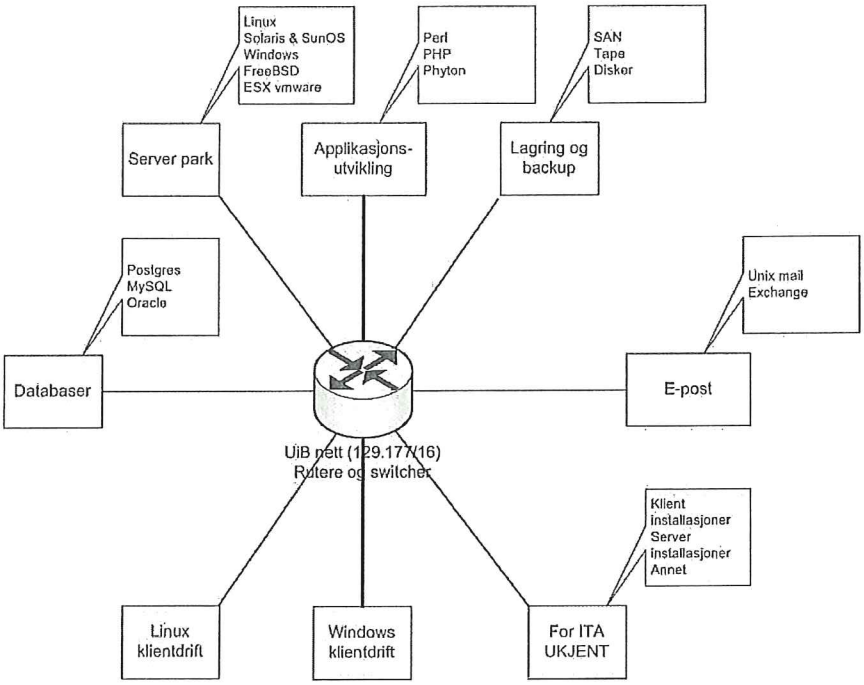
Organisasjonen SANS Institute (www.org.sans) har utarbeidet dokumentet "Twenty Critical Controls for Effective Cyber Defense". ITA har implementert flere av de tiltak som er anbefalt i nevnte dokument. Et universitetsnett er mer utfordrende å sikre enn et tradisjonelt bedriftsnett, både pga deler av UiB nettet er "utenfor" ITA sin kontroll (f.eks SiB studentbyer) og der er ingen ytre brannmur som sikrer UiB nettet. Et viktig sikkerhetsprinsipp er *punktsikkerhet*. Med punktsikkerhet menes at alt utstyr (PC klienter, servere, skrivere) skal være godt nok sikret i seg selv. Dersom en PC klient blir *hacket* skal den heller ikke klare å smitte resten av UiBs maskinpark. Det er kun det administrative nett som er beskyttet med en egen brannmursinstallasjon og det meste av UiBs utstyr er direkte eksponert for internett. Det er viktig å anmerke at fagnært og vitenskaplig utstyr er fakultetene sitt ansvar, men ITA bistår på forespørsel fakultetene/instituttene med å sikre dette. ITA forvalter og har ansvaret for sentrale og viktige komponenter som har stor betydning for sikkerheten. Dette gjelder spesielt *e-post* og *nettverksinfrastruktur*.

4.1 Organisatoriske tiltak

IT-direktøren har det operative ansvaret for sikkerhet ved UiB. ITA har ingen overordnet sikkerhetsansvarlig stilling. Det er seksjonene infrastruktur og applikasjoner som ivaretar sikkerheten innenfor sine områder. Seksjonene har delt ansvaret mellom seg som følger:

- seksjon applikasjoner - applikasjonsutvikling, databaser og e-post.
- seksjon infrastruktur - server park, lagring og backup, all klientdrift, nettverk og infrastruktur.

Det kan kanskje oppfattes som om organisering av IT-sikkerhet ved IT-avdelingen er noe defragmentert og da med fare for at noe glipper. Gruppene



Figur 2: Ansvarsområder IT-avdelingen

ved IT-avdelingen arbeider meget tett sammen, og vi opplever at sikkerheten pga det gode samarbeidet på tvers er godt nok ivaretatt. Vi ser foreløpig ikke behov for å etablere en IT-sikkerhets stilling som har et overordnet ansvar ved IT-avdelingen.

Spam og phishing mail UiBs ansatte og studenter blir (selv om sentralt mailsystem spamfilter filtrerer bort mye spam mail) til tider utsatt for phishing mail. IT-avdelingen har ved flere anledninger kringkastet at vi *aldri* vil spørre våre brukere etter informasjon som det etterspørres i phishing mail. I det sentrale mailsystem gjør det vi kan for å stoppe eventuelle utgående svar på phishing mail. Og dessverre så er det forsatt UiB brukere som svarer på phishing mail med å oppgi både brukerident og passord.

4.2 Tekniske tiltak

Det utføres mange tekniske tiltak for å opprettholde et tilstrekkelig sikkerhetsnivå. Det er ikke mulig i denne rapporten å dokumentere en uttømmende liste over tiltak, men felles for alle områder er at det er stort fokus på sikkerhet. Vi har på noen områder større utfordringer og de blir listet spesielt under seksjon 5 på neste side. Alle servere som driftes av IT-avdelingen har i utgangspunktet en sikker konfigurasjon (herdet), og de blir jevnlig oppdatert med sikkerhetspatcher etter hvert som de slippes. Det samme gjelder alle maskiner som IT-avdelingen klientdrifter. Alle rutere og switcher på UiB nettet har aksesslister, og det vanskeliggjør for utenforstående å få tilgang til UiB ressurser. I tillegg er det i UiB sin nettverksinfrastruktur implementert gode autentiseringsmekanismer som LDAP, AD (windows) og Kerberos. Gjennom det sentrale brukeradministrasjonssystemet SEBRA har alle enheter ved UiB god kontroll på hvem de har gitt adgang til UiB nettet.

4.3 Overvåking og oppdagelse av smittede kilder

IT-avdelingen har ifm POL[7]dokumentert hva som skal logges av data på servere og hvor lenge loggene skal lagres. Det er ingen sentralisert lagring og gjennomgang av logger, hver enkelt driftsansvarlig har som en del av sine rutinemessige oppgaver gjennomgang av logger på servere. Uninett har eget Cert team [8]som daglig sender UiB og de andre aktører på UH-nettet statusmeldinger om uønskede aktiviteter. IT-avdelingen lytter også etter unormal trafikk på alle grenserutere og alle vpn-servere (som står mellom UiB nettet og privatnettet - se figur 1 på side 7). Dersom det oppdages unormal trafikk blir det automatisk sendt mail til ansvarlige slik at smittekilden kan identifiseres og evt stenges ned.

[7]Person opplysningsloven
[8]Computer Emergency Response Team

5 Status sikkerhet UiB IKT-infrastruktur

Tabell 3 på side 14 er Avenir sin oppsummering av den tekniske sikkerheten ved UiB. Avenir sin oppsummering er lik IT-avdelingens egen oppfatning av den tekniske sikkerheten. Rapporten gir intet grunnlag for å iverksette noen strakstiltak, men det er flere tema som på sikt har betydning for IT-sikkerheten og som må adresseres og forbedres i løpet av 2009/2010. Disse kan inndeles i følgende hovedområder:

Maskinhaller og kapasitet Det er av Avenir også påpekt noen alvorlige og store svakheter ved maskinhaller i NG5 (Stein Rokkans hus). Dette omfatter kjøling, strøm og mangel på alternativ driftslokasjon. Alle anmerkninger som Avenir har påpekt er adressert og IT-avdelingen har i samarbeid med EIA enten utbedret flere av anmerkningene eller har planer om å utbedre. Den mest alvorlige svakhet nå er mangel på alternativ driftshall og en IT-messig etablert kontinuitetsløsning for å sikre drift av UiBs mest kritiske IKT-tjenester.

Avhengighet til enkeltpersoner UiB har en meget kompleks IT-infrastruktur. På enkelte av tjenestene er vi sårbare pga kunnskapen om hvordan enkelt tjenester er konstruert og fungerer på er på for få personer. Dette er et krevende punkt å utbedre pga ressurstilgangen.

Dokumentasjon Mangel på dokumentasjon er et gjennomgående tema. Her kreves det både en oppdatering av dokumentasjon og etablering av dokumentasjon der det mangler. I tillegg må det skapes rutiner/prosesser for å holde dokumentasjonen oppdatert ved endringer.

Passordregime UiB har et passordregime som har noen alvorlige sikkerhetsmessige svakheter ved seg. Pga tidligere tekniske løsninger (som nå er eliminert) er minimums lengde på passord og kvaliteten på passordene ikke god nok. En stor del av passordene inneholder samme mønster, lengden på passord er for liten og de fleste passord kan knekkes ved oppslag mot ordlister. IT-avdelingen er i ferd med å utarbeide et forslag til nytt regime for passord.

Eldre upatchede server OS Litt av utfordringen til IT-avdelingen er å rydde opp og sanere noen eldre servere. OSet på disse servere er gammelt og ikke lengre supportert, og det utgjør en sikkerhets risiko. På noen av disse servere kjører det en del udokumenterte rutiner, og det er både tidkrevende og utfordrende å rydde opp i dette. Vi vet hvilke servere dette gjelder, og migreringsplaner er innearbeidet i våre handlingsplaner.

Sikkerhet i web applikasjoner Sikkerhet i webapplikasjoner blir viktigere og viktigere. IT-avdelingen har ansvaret for flere applikasjoner som MiSide, SEBRA, EW osv som er mulige angrepsmål. Sikker programmering er et viktig

tema som IT-avdelingen vil bruke mer tid og kompetanseheving på. Dette er også et viktig område som vil bli mer belyst i en strategi for IT-avdelingen.

6 Forbedringstiltak

I all hovedsak har Avenir de samme konkusjoner som vi selv har. Det er ikke avdekket noen nye alvorlige sikkerhetshull, og IT-avdelingen har allerede addresert flere av de påpekte svakheter. For 2010 vil også opprettholdelse av samme sikkerhetsnivå og utbedring av svakheter være sentrale aktiviteter. Detaljert oversikt over sikkerhetstiltak er dokumentert i IT-avdelingens handlingsplaner for 2009, og dette vil også bli viderført i handlingsplaner for 2010.

7 Vedlegg 1 - oversikt over spam mail til UiB

Tabell 2 på neste side viser en oversikt i sentralt mail mottak ved UiB. Uken representerer et snitt av en normal uke, og antall forkastede mail i denne uken varierer fra 77 til over 90 prosent. En interessant observasjon er antallet ukjente mailadresser (se kolonne ukjent i tabellen). UiB bombarderes (antallet er økende) med mail til *ukjente* adressater ved UiB (ukjent@uib.no).

8 Vedlegg 2 - oppsummering teknisk sikkerhet

Tabellen oppsummerer Avenir sin vurdering av IT-sikkerheten ved UiB (innenfor den sentrale IT-avdelings ansvarsområde). Områder merket med OK er meget godt IT-sikkerhetsmessig ivareatt. Områder som er merket med må utvikles har potesiale for å bli bedre, men det er ingen umiddelbar risiko for eventuelle sikkerhetsbrudd. På *patching* er det anmerket sanere eldre OS under linux og unix. IT-avdelingen har noen få eldre servere som kjører utdatert og ikke lengre supportert OS. Disse servere er adressert og det arbeides med å migrerer disse over på en sikekr plattform.

Dato	Meld. lev OK	Mottagere	For-kastet	% kastet	Rbl	Greyl	Spam-assassin	Spam-adresser	Mail-filter	Annet.	Virus	Non_auth	Ukjent
1 mai 09	33870	97537	325978	90.59	72487	105387	1971	888	1411	11621	11	4766	993311
2 mai 09	20571	88419	298425	93.55	66606	97535	2060	1097	2331	11775	15	3571	778558
3 mai 09	25582	197399	321503	92.63	64458	113448	1810	1604	2545	10919	19	3457	1006146
4 mai 09	77627	292845	271066	77.74	66371	88379	2193	1140	2142	12901	63	5178	813215
5 mai 09	81737	282557	314363	79.36	78122	109500	2161	1493	1974	13337	35	5588	862469
6 mai 09	80819	277977	296165	78.56	72554	100042	2373	901	2211	12961	36	5416	749326
7 mai 09	81070	260048	308862	79.21	79163	102273	2141	1355	2115	12259	27	4988	822746

Tabell 2: Oversikt mail UiB første uke mai 2009

		Nettverk	MS Windows	Linux klient	Linux server	Unix server
Installasjon	Prosedyrer	OK	OK	OK	OK	OK
	Tilstand	OK	OK	OK		
Herding	Prosedyrer	OK	OK	OK	OK	OK
	Tilstand	OK	OK	OK	OK	OK
Patching	Prosedyrer	OK	OK	OK	Sanere eldre OS	Sanere eldre OS
	Tilstand	OK	OK	OK	Sanere eldre OS	Sanere eldre OS
Dokumentasjon	Tilstand	Må utvikles	Må utvikles	Må utvikles	Må utvikles	Må utvikles
Passord	Policy	Må utvikles	Må utvikles	Må utvikles	OK	Må utvikles
	Tilstand	Må utvikles	Må utvikles	Må utvikles	OK	Må utvikles

Tabell 3: Oppsummering IT-sikkerhet (Avenir)

UNIVERSITETET I BERGEN
Universitetsbiblioteket

VEDL. SAK NR.: 111 - 4
STYRE-MØTE 3 1/2 - 2009

Økonomiavdelingen

Referanse	Dato
2009/7019-BEB	14.07.2009

REVISJON AV IKT-REGLEMENT OG IKT-SIKKERHETSPOLICY - HØRING

Universitetsbiblioteket har sett på saken og har følgende kommentarer til forslaget til policy:

A - overordnet IKT-sikkerhetspolicy
På internett finnes en rekke gratis og nyttige tjenester man kan bruke i sitt arbeid/studium for eksempel Google DOCs til deling og felles skriving av dokumenter.

Vi savner at en overordnet IKT-sikkerhetspolicy for UiB gir retningslinjer/anbefalinger for hvordan UiBs ansatte og studenter skal forholde seg til gratis tjenester på internett i sitt arbeid/studium.

B - IKT-reglement for Universitetet i Bergen
I paragraf 3.8 foreslås det: "Ved opphør av ansettelsesforhold gis det varsel om sperring av brukerkonto 14 dager før sluttdato slik denne fremkommer i lønnssystemet eller er satt av godkjenner på den ansattes enhet. Konto sperres på sluttdato og ligger sperret i ett år for så å bli slettet."

Kommentar: Ansatte som går av med pensjon mister etter dette sin konto ved UiB og dermed bl.a. tilgang til bibliotekets elektroniske tjenester hjemmefra. UiBs pensjonister er en ressurssterk gruppe som fremdeles vil kunne bidra positivt til samfunnet og UiB bør derfor legge til rette for dette ved at de som er aktive bidragsytere også får nytte godt av UiBs IKT-tjenester etter at de er blitt pensjonister.

I paragraf 3.8 annet avsnitt foreslås det: "Ved opphør av studentforhold sendes varsel om sperring av brukerkonto en måned før konto sperres. Sperrevarsel sendes det 3. semesteret etter at en student sist var registrert som student (har betalt semesteravgift). Konto slettes automatisk ett år etter at sperring inntreffer."

Kommentar: Dette betyr bl.a. at tidligere studenter får tilgang til bibliotekets lisensierte e-ressurser via internett i over ett år etter at de har slutte som student. Dersom dette er ønskelig må dette bl.a. tas inn i lisensavtalene på e-ressurser, noe som kan medføre merkostnader. Dersom dette ikke er tilsiktet så må man finne en løsning slik at kun de som har betalt semesteravgift får adgang til bibliotekets lisensierte e-ressurser. Dette ble også påpekt av bibliotekdirektøren da saken ble håndtert i Systemeierforum.

Randi E. Taxt
bibliotekdirektør

Leif Magne Iversland
seniorrådgiver

Universitetsbiblioteket
Telefon 55582532
Telefaks 55584620
post@ub.uib.no

Postadresse
Postboks 7808
5020 Bergen

Besøksadresse
Nygårdsgt. 5
Bergen

Saksbehandler
Betty Britt Brattaule
55582532