Intervju KTH1

Uppstartsmöte med KTH 10 januari 2023

Avdelningschef/bitr. universitetsdirektör, koordinator för forskningsdata, it-säkerhetschef tillika Chief Information Security Officer, systemspecialist, dataskyddsombud

Närvarande RiR: Sara Monaco, Ludvig Stendahl, Jens Pettersson, Josefine Olsson

Inleds med presentation av samtliga.

Mötet inleds med översikt av forskningsverksamhet

KTH är Sveriges största tekniska universitet, och rankas högt i världen. Forskningsverksamhet kännetecknas av en hög grad av internationell samverkan. Visar bild på sampublicering, dvs med vilka andra organisationer i världen som KTH publicerar forskningsresultat. Nästan hela världen. Har nationellt ansvar för 5 strategiska forskningsområden. Och partner inom fem programområden i information och technology (EU) har även nästan 50 centrumbildningar. Detta är miljön vi verkar i på forskningssidan. Samverkan och öppenhet mot omvärlden. En standardfråga i revisionssammanhang, har ni tredjelandsöverföring, svaret är ja, det går inte att undvika i denna verksamhet.

Det finns centrala stödfunktioner som ska hjälpa verksamheten i de här frågorna, när det gäller forskningsdata och informationssäkerhet har vi plockat ut följande funktioner:

Security management center (SMC) – CISO, dataskyddsombud och utredare.

Forskningsdatastödverksamheten som RIR:s kontaktperson samordnar.

Research support office – där sitter affärsjuridik och exportkontroll och etikprövningsfunktionerna.

Förvaltningsjuridik under ledningskansliet (management office).

Arkiv och registratur under IT.

Sen finns det ett övergripande myndighetsansvar, och ansvar för skolans verksamhet som ligger under skolchefernas och skolornas delegationsordning. Sen finns det ett ansvar för den operativa datahanteringen och det tydliggörs i riktlinjer för hantering av forskningsdata inom forskningsverksamheten.

Vi använder MSB:s nomenklatur, strategisk, taktisk och organisatorisk. Vi verkar på alla nivåerna. Sedan ett år eller ett halvår träffas vi regelbundet, säkerhet och forskningsdata och tar specifika ärenden, för att kalibrera oss och sen reda ut saker, i stället för att skicka runt saker i organisation.

På informationssäkerhetsområdet har det varit ett par *interna revisioner* de senaste åren som är relevanta. Det har tagits fram åtgärdsplaner efter revisionerna, vilket har tagits upp i VP och i en reviderad delegationsordning. Det har trätt i kraft en hel del i januari.

Parallellt pågår en utredning om totalsäkerhet, även den fysiska säkerheten och säkerhetsskydd. Vi har haft en vakans på säkerhetschef och säkerhetsskyddschef. Av den anledningen har vi inte flyttar fram positionerna så mkt. Denna chef är inte på plats än.

I ett första steg i ett två-årigt projekt inrättades en stödfunktion för hantering av forskningsdata, jag är forskningsdatakoordinator sedan 2019. Sen sammankallades en supportgrupp som tog fram olika stöd, webbinformation, stöd för att skapa datahanteringsplaner då det är ett krav från många finansiärer. KTH har även gått med i SND. Fick ett uppdrag av vicerektor att ta fram en digital utbildning i hantering av forskningsdata och öppen vetenskap som är ett ytterligare yttre krav.

Utbildningen finns tillgänglig i vårt lärsystem, learning management system. Sen tog vi också fram en ny riktlinje för forskningsdata för att göra det tydligare. Det var väldigt spritt tidigare, så det var svårt för forskare att veta vad som gällde. Det var de två första åren, sen inrättades en mer löpande verksamhet. Vi började också samarbete mer med SMC i och med att det är ganska mycket informationssäkerhet och gemensamma ärenden. Ärenden som vi får in har oftast många komponenter. Det kan vara skydd, avtaljuridisk. Det handlar om att samordna kontakter internt i stödverksamheten.

Vad kan det vara för ärenden?

Ett projekt som har tränat en machine learning-modell på upphovsrättsskyddat material, får vi tillgängliggöra modellen?

Sen fick vi (oklart vilka men tror forskningsstödverksamhet) ett formellt uppdrag i VP att främja god hantering av forskningsdata. 2022 bedrev vi tre projekt för att vidareutveckla stödet. Sen har det blivit mer tydligare styrning av IT och utvecklingsprojekt, som etablerats 2022. Det håller på att beredas ett förslag som ligger under chefen för RSO För tvärfunktionell grupp för efterlevnad på digitaliseringsområdet. Sen har vi fått en digitaliseringsstrategi, några mål i den har vi jobbat mot.

Det finns många typer av efterlevnad. Nu pratar vi it-infosäk. Sen finns det juridik och it-rätt. Anskaffning och IT-arkitektur och historiskt har det varit utspritt, som forskare blir det många instanser att få ok i. Vi har en idé vilja att samla efterlevnad i en service för att få hjälp med alla typer av efterlevnad samlat. Det finns ett stort värde att se på efterlevnad som en helhet.

2020–21 gjorde vi ett antal intervjuer och enkäter och identifierade områden där vi såg att det fanns ett extra stort behov av ökat stöd. Och det låg till grund för de åtgärder som föreslogs inför projekten 2022, det kommer jag gå in på imorgon med min kollega i forskningsdatastödgruppen. Vi har sett i informationslivscykeln vissa pinpoints där vi skulle behöva utveckla stödet för att förbättra verksamheten. Vi ser att det är väldigt mkt blanketter och formulär som forskare måste fylla i vid uppstart av projekt som vi vill förenkla på sikt. Sen är det väldigt många frågor kring datadelning i samverkan. Sen är det vad som händer vid projektavslut. Vi har gjort en hel del kartläggningsarbete som ligger till grund för det här. Sen är det skönt att vi har en övergripande och tydlig strategi i och med digitaliseringsstrategin som kom i november -22.

Biträdande universitetsdirektör

Man kan skruva upp och skruva ner krav, det gäller att hitta en balans i ett kvalitetssystem, och det är svårt i praktiken. Jobbar man bara med regelefterlevnad generellt, kan man ju skruva upp den, men det kan få konsekvenser för verksamheten och inte nödvändigtvis till det bättre. Det är därför viktigt att hitta en balans. Nu har vi haft ett fokuserat arbete under flera års tid i dessa frågor. Och det gäller att hitta en balans där det blir tillräckligt mycket men som inte motverkar det som vi är här för att göra. Forskarna måste känna att kraven vi ställer på dem är rimliga i förhållande till den forskningsverksamhet de ska bedriva. Det är inte lätt att hitta den balansen.

Det är svårt att prioritera. Vi satt och började räkna på hur många intresseområden det fanns i verksamheten, och vi tappade räkningen vid 200 olika aspekter, ska man gå ut till verksamheterna då så är deras dagar på året slut, så är deras tid slut, alla de här fokusområdena måste samverkas, vi måste samverka med riskhanteringen, arkiv, it, infosäk, vi kan inte landa i varje särintresse. Vi har givetvis myndighetskrav på oss som våra konkurrenter i USA inte har. Skatteverket är ETT skatteverk, den aspekten finns inte där. Nästan alla projekt har även avtal med externa partners, så oavsett hur mkt vi vill...

Varför sker detta arbete som ni pratar om just nu?

VI har en hög grad av externfinansiering – och det här är ökade krav på forskningsfinansiärer, det handlar om införandet av datahanteringsplaner vid uppstart och kraven på FAIR. Sen har vi GDPR 2018, det blev en wake-up. I forskningspropositionen lyfts att all forskningsdata ska vara FAIR 2026.

Jag uppfattar också att det är en mognadsfråga över hela sektorn. IT-användandet är ju lika gammalt hos oss som på Uppsala universitet. Och tittar man på olika lärosäten, gör man inte saker tillsammans så gör människor saker i ungefär samma takt. Det gäller allt från decentralisering med forskargrupper som har it lokalt till mer centralisering. Det kommer mer krav på efterlevnad, GDPR var en sådan sak. Vi tycker om att prata om data här idag, eftersom det blev en så otrolig tyngdpunkt på personuppgifter. Sen är det omvärlden. Privacy shield. Det har lagts mycket energi på hur mkt vi ska lita på USA, och om vi kan ha persondata där. Sen kom Ukrainakrisen. Det är flera saker som samverkan mao. Och pandemin och ökad digitalisering av den anledningen. Och kommunikationsmönster som kanske mer kommer från livet, men som flyter in i det professionella. Molntjänster är ett sådant exempel och annan typ av social kommunikation som förekommer inom vissa kanaler.

Det finns en massa tuffa frågor att lösa, OSL och molntjänster, är man skatteverk är det lättare att hålla sig till det, är man en myndighet som ska vara forskningssamarbetspartner över hela världen då är inte alla aspekter av OSL inte riktigt... skulle vi följa den till punkt och pricka skulle vi det vara svårt att vara konkurrenskraftiga, det handlar om att förstå vad vi kan jobba med i publika molntjänster och vad vi inte kan jobba, och hitta balans. Och balansen att vi inte kan använda publika molntjänster så fungerar vi inte som det lärosäte som vi vill vara, som forskningshubb.

Att vara lärosäte – jmf med myndigheter – så bedriver vi verksamhet som är av en helt annan natur, och själva grundsyftet med vad vi håller på är ju att vara öppna. Och i världen bygga kunskap tillsammans. Då hamnar man i olika svåra frågor. Hela vetenskapsvärlden handlar ju om det. Dessutom den här tydliga riktningen mot öppen vetenskap.

Så vill forskare ha snabba svar på var de kan ha sin data, och så är man inte överens mellan USA och EU. Det är en del intressanta slitningar i gränslandet.

Sen har vi det här med dubbel användning och säkerhetsperspektivet är ju också nytt för högskolesektorn sedan ett antal år. Och det är ju högaktuellt för tekniska lärosäten.

Tillbaka till universitetsdirektör, biträdande.

Började min tjänst här i mars (2022), så mkt av det som pågått här har jag inte varit med om själv.

Delegationsordning – är ett löpande arbete att se över, men i det här fallet har det funnits särskilda skäl att göra det utifrån temat för det här mötet. Det finns en ny delegationsordning för KTH och för verksamhetsstödet, där vi har försökt att tydliggöra ansvaret kring dessa frågor. Där framgår ex att universitetsdirektören har ett övergripande ansvar för informationssäkerhet. Och vi har försökt skriva fram vad skolcheferna ska ansvara för. Vi kommer att göra ytterligare omtag i vår.

KTH har en arbetsordning, och sen delegationsordning där rektor delegerar ansvar till universitetsdirektör och skolchefer. Sen har direktören en delegationsordning och arbetsordning där hon delegerar ansvar till mig som avdelningschef, till exempel. Och skolcheferna har sin delegationsordning per skola. I vår kommer ett arbete att göras för att se över skolornas delegationsordningar. Och få lite mer centralt stöd i det arbetet. På ledningskansliet har vi en *styrdokumentsfunktion* som är involverad i så mkt styrdokumentsarbete som vi kan.

Universitet och KTH, det är stora organisationer, där kärnverksamhet bedrivs på skolor och i praktiken institutioner. Det är där studenter, lärare och forskare är anställda, det är där projekt och externa pengar finns, det är där centrumbildningarna ligger. Då måste ansvaret ner, det går inte på ett enkelt sätt att från centralt håll uttrycka vem som ska ansvara för vad, du är lämnad till en skolchef att ytterst bestämma vem som ska ansvara för vad inom skolan, och det innebär att det kan blir skillnader mellan skolor. Ex vad prefekt får besluta om och vad skolchef vill besluta om. Tar du det lokala ansvaret blir det svårt för skolan eller institutionen att ta ansvar. Det blir ingen kvalitet i verksamhet, beslut måste fattas långt ner. Vi utmärker oss inte att vi har delegerat ut ansvar långt ut, jämförelsevis.

Det är skillnad på hur man bedriver verksamhet om det är partikelfysik, eller kemi eller industriell ekonomi.

Historiskt muskelmassan hos dem därute var beroende på hur mkt externfinansierade de var, kemi var ex rätt starka, runt 50–70 procent externfinansierat.

När det gäller IT så är trenden tydlig, lärosätena vill centralisera stödet. Så är det på KTH och de flesta universitet. Man vill inte ha 100 system för epost, utan ett.

Sen finns det ju specifik mjukvara för masspektrometer så kan du inte använda samma mjukvara som om du har ett rymdteleskop.

Vi har varit 150 institutioner, nu 50, vi har varit 10 skolor nu är vi 5. Vi hade olika fläktar på olika ställen. Nu har vi fört ihop det på gott och ont, med skolreformen. Det har blivit mindre av dubbelforskningen.

Jmf med SU har KTH en starkare linje, rektor har en tydligare roll, och skolcheferna också.

Som ett exempel, vi fyller 25 år vår delegation att vi kan gå ut och på it-säksidan och stänga av apparatur som är hackad, det är inte självklart frtf på alla lärosäten att man får göra det, utan det kan vara enskild forskare ska bestämma. Det är en stark central funktion. Det beror lite på att vi hade bekymmer på 90-talet. Nu har vi ganska hög grad av centralisering av IT. Mätutrustning och annat är en helt annan bransch. Där har vi bekymmer med MSB 2020, testa system referenssystem och driftssystem, vilket skulle tredubbla vår forskningsbudget.

Samgående av verksamhetsstöd. Kanske inte helt relevant för arbetet med forskningsdata men det är en generell organisationsfråga, speglar lite det här med centralisering eller inte. Från 1 jan 2023 gäller en stor reform som arbetats med under fler års tid, all teknisk-administrativ personal, all stödpersonal på KTH, då hade man den personalen inom den centrala förvaltningen. Ex en IT-avdelning, ett ledningskansli, ett bibliotek. Sen finns det också stödpersonal ute på skolorna, men dessa (all stödpersonal) ska samlas under verksamhetsstöd. De ungefär 100 stödpersonal per skola, som tillhör skola, tillhör nu förvaltning och har UD som chef. Det är för att kunna jobba mer enhetligt kring stödet. Det kommer se olika ut och man behöver stötta efter skolors specifika behov. Egentligen är uppgifterna desamma, men skolornas stödorganisation har ”bara” behöv förhålla sig till skolornas specifika behov och de val man gjort där, på sikt innebär omorganisationen att det blir lättare att ensa i de processer som finns anledning att ensa i. Vi tror det blir mer effektivt och högre kvalitet. Arbetet ska pågå till 2027, så det kommer att innebära fortsatta omorganisationer. Alla är kvar på sin plats, mest en förändring på papper än så länge med det finns ett arbete att se över processer vilket kan innebära att personal kan flyttas fysiskt.

Vi har fler campus, Vallhallavägen, Kista, Södertälje, Flemingsberg och Solna. Och där är miljöerna kan ha sina specifika infrastrukturer som kräver sina IT-system.

Hör dessa campus till en skola?

Det ser lite olika ut. Kista tillhör ec-skolan. Södertälje då är det ITM. Flemingsberg är det CBH. Men på scilifelab är det cbh, skiva spiva (ohörbart). I Södertälje är det en institution, och likadant i Flemingsberg. I Kista är det flera institutioner och avdelningar som är involverade.

Ny säkerhetsfunktion. UD har sett ett behov att se över säkerhetsorganisation av KTH, bland annat av anledning av granskningar, interna och externa. Vi har haft en säkerhetschef, som inte längre är här. Man har identifierat att man behöver rekrytera en ny, med delvis annat uppdrag. Det har harvats under en längre tid, utlysning gjordes för mer än ett halvår sedan. Men det finns ingen rekryterad. Svårrekryterad grupp. Tanken är att skapa en säkerhetsavdelning, en ny avdelning inom verksamhetsstöd, avdelningschef som är säkerhetschef.

Vad är det nya i funktionen?

Det kan jag inte riktigt svara på.

Tanken är att samordna säkerhetsskydd och säkerhet i samma. Nu är det lite öppet, tanken är att ta in en person som ska vara säkerhetschef och jobba förslag till organisation, det har hämmat oss.. den här avdelningen finns inte, det vore lättare att om man tillsatte en chef till en avdelning. Man vill att denna person ska bygga upp avdelningen, så därför har man inte inrättat en avdelning. Det har funnits säkerhetschef tidigare på KTH då var det här en tydlig roll som var knuten till henne, när hon slutade så ersattes hon av fem eller sju personer, en roll som var tydlig centraliserad spreds ut och det bar inte riktigt. Hon höll ju såklart en position som var viktig för oss, den insikten kom i efterhand, att det här nog behövde finnas, från vårt perspektiv handlar det om att skulle vi vilja ngt i vårt säkerhetsarbete över hela KTH och hitta ett sätt att enas och bygger en sådan organisation, nu ligger ansvar för säkerhet ligger på verksamheterna, men man kan ju inte lämna vc med svåra avvägningar.

Komplext ämbete, vi har jobbat med fysisk säkerhet, vi har personalfrågor, han kanske inte är en person utan en gruppering. Det är alltid ngt som händer här, någon avlider etc, anhöriga som behöver hjälp och stöd. Sen har vi det med säkerhetsskydd, som har aktualiserats på senare tid. Även om vi alltid haft,

Under mina 30 år här har alltid varit samma problematik. Då var det mer tydligt vilka det var. Nu har vi jag vet inte hur många från X. Jmf med Linköping, skickar medel till oss och säger att XX har överträtt ngn regel, men vi har fem XX. Enorm yta. Där har vi sökt hjälp SÄPO, militär och andra, kalibrering vad vi ska ha för förmåga. MSB skrev att vi skulle öka vår förmåga att motstå väpnade hot, vilket känns helt orimligt. Det är ett komplext ämbete.

Det återkommande mönstret är att det finns många svåra överväganden att göra, det behövs kvalificerad personal, och ha höjd och pondus att sätta dem, det behöver vi göra tillsammans i organisationen, för att sen stödja dem som finns i verksamheten där verksamheten ska pågå. Det som har varit historiskt är att alla de svåra övervägandena ska göras i linjen, och alla olika lärosäten och myndigheter ska tolka OSL och privacy shield och sådana saker. Här borde myndigheter och MSB hjälpas åt och tolka så att vi kan återanvända dem. Det görs inte. Varje skola och skolchef har unika verksamheter som de behöver sköta, unik it, unika avvägningar att göra avsteg. Då är det specialare man gör ute i löven, men då ska man göra rätt saker lokalt och själv, men det mesta kan vi göra tillsammans, i synnerhet de svåra och tuffa avvägningar, då är det bra med den här typen av funktioner (de som är på mötet). KTH måste ju ta sitt ställningstagande, oavsett vad SU eller någon annan gör, utan att bryta mot lagen.

Ett av våra mantra är att vi ska hjälpa varandra att ta fram underlag, sen är det verksamhetsansvarig, kanske skola, personalchef som får ta beslutet, jag tar riskerna i det här, men vi hjälps åt att ta fram tillsammans ett underlag att besluta på. Låt inte den ensamma chefen att besluta allting själv och utreda.

Det handlar om att förtydliga den strategiska dimensionen, att samordna, få en strategisk kompetens som samlar olika delar av säkerhetsarbetet, säkerhetsskydd, personsäkerhet, krisorganisation, informationssäkerhet, allt det där hänger ihop. Det finns stora förväntningar på den här rollen och den här avdelningen. Det kommer vara en resa att bygga upp den här avdelningen. Informationssäkerhet där har vi en bra bemanning och ett arbete på IT-avdelningen, men kring vissa andra delar är det en utvecklingsresa. Det är på gång, det är försenat. Nu är målsättning att det finns en ny avdelning inrättad i juni 2023.

Arbetsuppgifterna är delegerade?

Ja, de befintliga finns.

Åtgärder efter internrevisionsarbete

Det har gjorts flera granskningar och styrelsen har fattat beslut om åtgärdsplaner. Och det har man arbetat med och vissa saker är åtgärdade, vissa saker har skrivits in i åtgärder i förra årets VP, vissa av dem är frtf inte åtgärdade, därför finns det nu nya åtgärder för vp 2023, bland annat kring it och infosäk. Det handlar om att åtgärda de saker som har identifierats.

Ett uppdrag till IT-avdelningen är att säkerställa att det finns en LIS.

PAUS ca 01.03.30

För 20-25 år sedan freebasade forskarna helt. Då kunde man sätta upp en egen server och köra. Det går inte idag, då är den crackad efter en vecka. Det är väsensskild miljö idag, med yttre krav. Centrala stödet kostar mycket mer än vad det gjorde för 20 år sedan. Den digitala miljön har ökat i vikt och den kostar ju också.

CISO

Det finns ett årshjul för ska vi kalla det KTH centralt, jag har det här men vi kan titta på det sen. Där är vår ambition att ligga i synk med det här, vi har t.ex. internrevisionen samlar upp sina göromål, de tar fram på kommande granskningar osv och då vill vi ligga lite i takt med det, så vi kommer med lite inspel vad som kan vara lämpligt att ta upp under året. Sen så vill försöka komma med våra inspel till förändringar till budgetarbetet annars kan det komma två år tiden. Vi börjar ju nu med 2024, nästan. När det gäller vp så har de under de här pandemiåren har det blivit så att de här granskningarna som internrevisionen gjort – det har varit ett antal – då fungerar det numera så att det kommer en granskning och vi får ta del av den, ibland är det internrevisionen, ibland är det externa konsulter. T.ex. i samband med granskning av IT-säkerhet där man tittat på tre system, ekonomisystem, canvas och sen ärendehanteringen. Vi tittar på resultatet och skriver förslag till direktören och rektor. Rektor har med sig upp på nästa styrelsemöte och ger förslag till åtgärdsplan som klubbas om inte styrelse har andra synpunkter, eftersom vi har haft så många granskningar så blir, gdpr, avyttringar etc, det vår vp. Som nämndes här har vi vissa saker som vi har bockat av och några hänger kvar. En del hänger ihop med vår ambition att hålla ihop det, ta gemensamma steg med juridik, arkiv och så vidare. Så vi har inväntat den här utredningen, och att det ska sätta sig på det övergripande säkerhetsområdet. och det här med verksamhetsstöd har vi också inväntat för att det ska komma ett mer KTh-ledningssystem. Vi har ju ett miljöledningssystem, det är wag the dog, det leder verksamheten

nästan, man måste samverka och ta hänsyn till varandras krav. I år så kommer vi gå tillbaka till det traditionella. Verksamhetsberättelsen är vi ju egentligen en sammanställning och där går vi tillbaka från och med nu, det här årsskiftet, det normala, då är det den här tunga punkten är den här ledningens rapport som vi har försökt att synka in lägga samtidigt som miljöledningen, nu har ni gjort entré på banan och tagit några timmar av oss men vi har ambitionen att hinna med. Och som input till dem här. Dels ingår det som ni vet omvärldsbevakning, interna krav osv så samlar man upp året dels på infosäk, itsäk men också skolbesök då vi har kvartssamtal som vi kallar det. Vi brukar försöka få det runt årsskiftet så att vi kan får det som input till ledningens rapport om det flyter upp ngt, om man vill ha mer kurser eller information, eller mer stöd att sköta sin forskningsinfrastruktur så får vi med oss det. kommer det med i ledningsrapport så kan det komma upp på styrelsemötet i början av februari. Det kan även komma in som input som internrevisionens granskningar om det är ngn oegentligheter som kommer upp.

Vilka är det ni pratar med på skolorna?

Det är framför allt skolledningen. Man vill ju få fast skolchefen. Sen har vi sedan skolorganisationen började har vi haft god relation med de administrativ chef, som är spindel i nätet, skolchefen är mycket ansiktet utåt. Den administrativa chefen är en stark person. De är de nya avdelningscheferna (i den nya organisationen). Vissa har du haft parallellt någon annan person vi pratat om. Vi hade en hybrid igår med en av skolorna, då hade vi med prefekt, från fysik och teknisk mekanik.

Vi har varit här ganska länge, så vi har god personkännedom. Vi kan söka upp dem som är extra intressanta. Igår hade vi med oss en person under sitt paraply kärnkraftsäkerhet, där man verkligen har externa krav på sig, med väldiga rutiner och säkerhet. Kan vara ett bra exempel för er att titta på. Sen förmedlar vi våra synpunkter dels på it-säkerhetsidan, om de har apparatur som är dåligt säkrad och det finns förbättringspotential. Löpande vid behov ex under corona hade vi veckomöten med skolcheferna, vi ingår även i krisgruppen. Vid behov så träffas vi, det är en av våra styrkor att vi har haft ganska bra – mina kollegor i landet vet ju knappt hur rektor och UD ser ut, men vi har alltid haft en tradition att när det behövs har vi haft en kanal till ledningen och kunnat komma upp med våra frågor, inte bara övergripande årliga utan även vid viktiga händelser, sen har vi våra rutiner så fort vi har tyngre ... tyngre händelser, attacker, ddos eller att vi riskerar att hamna i pressen, direktinformation så att ledningen ska... det är även kopplat till de här rapporterna till IMY och MSB och även it-säkerhet sitter borta vid rektor och så vidare, och direktören får direkt veta att ngt är på gång.

VEM ÄR DIN CHEF?

Det är egentligen it-chef linjemässigt, sen rapporterar jag till rektor och UD i olika frågor. Det är lite parallellt med säkerhetschefen... normala arbetet till direktören, men säkerhetsskyddet ska gå till rektor. På samma sätt har jag rapporterat till rektor, när det handlar om disciplinärenden. Till styrelsen vid behov.

Vi har en tillförordnad säkerhetschef, det är en tf konsult. Fokus hittills har varit på fysisk säkerhet från hans sida, det är inte informationssäkerhet.

Den tidigare som vi sa var det en person hängde det ihop på ett annat sätt, men det var problematiskt med att det var bara en person, men pendeln ska slå tillbaka.

Årsrapport hänger ihop med ledningens rapport. Granskningar görs vid behov, det är framförallt vid nya anskaffningar som det görs. Vi har en slide för det.

Det här med IT-säkerhet är lite beroende på verksamhet, vi har kanske 2-3 maskiner per capita, vilket inte en normal myndighet har. Datorer alltså, sen är det mätutrustning, surfplattor. Det är en helt annan värld. Historiskt har professorer kört sina egna mejlservrar, det är nedtonat, alltmer är centraliserat. Traditionellt har vi haft ganska öppet nätverk, fria forskningen osv. Vi har fyllt på, vi har haft en ganska stor grupp med incidentrapport och övervakning tidigare, för tjugo år sedan var det väldigt mycket hackande, det har bytt skepnad, nu är det mer pengar man är ute efter, inte kapacitet, bredband är inte exklusivt, tidigare var vi ensamma om kraftiga internetförbindelser, då var det attraktivt att skaffa sig kapacitet.

Sen har MSB skrivit förordningar där man pratar mkt om nätsegmentering, vi har en tuffare framtid vi också, vi kommer strypa... hur mycket vet vi inte men det ingår i den här rundan med skolor och verksamhet att vi ska strypa ganska ... sen har vi alltid omgärdat ekonomisystem och sådant, men om vi nu pratar forskningsdata varit mer .... förutom vissa miljöer som varit extra känsliga. Min gamla institution, vi mätte på pansarvagnselektronik då är man nere i källaren och följer med militär och drar ur alla kablar. Det styrs mycket av externa krav.

Vi är lite stolta över att vi har morgonmöten och gör upp om dagens ärenden. Säkerhet, utveckling, kl 09 på morgonen och ser vad som hänt under natten ... sen har vi alltid så att säga en TIB. Vi har en koordinator som alltid sitter och har koll på övervakningsskärmar och koordinerar om det skulle hända ngt. Om vi får en it-incident som är rent driftmässigt, är det säk kan det eskaleras, beroende på allvar så kommer det ända upp till mig. Det har vi rutin för. Pratar mycket med andra lärosäten och det har de svårt att få till det här, det har vi kämpat hårt för och fått fast så att de verkligen görs. Sen finns det i ngn mening beredskap för det här så att vi kan göra saker även off hours, det är inte önskvärt, men skulle det behövas så finns det möjligheter.

Vilka är med på morgonmötet?

Operations, de sitter på ett speciellt rum. Det sitter en person i beredskap schemalagt varje dag kontorstid som håller ihop det, sen sitter vår support i en annan byggnad, men vi har heta linjen emellan så att man kan hålla....

Om du är förvaltare eller ansvarig för ett system, när du har byggt upp så lämnar du till förvaltning, till driftteam eller operations, då har de pulsen på ditt system, och kan ha koll på om det behöver startas om eller slut på disk eller minne eller vad som kan hända i vardagen, och blir det större problem så vet de hur man kan eskalera, de hjälper dig och kan avlasta experter.

Vår önskan är att driftstopp ska ligga i servicefönster, men det färdiga rutiner för att rapportera när man ska patcha ngt eller uppgradera ngt eller testa nya saker, eller referensmiljöer, eller gå över ngn sömn.

SMC har en utredande förmåga, en SOC som är en förmåga som jobbar med nätövervakning och liknande, men att det också är operationsteamet, men också serverdrift som är med på morgonmöten. Det är de som driver och vidmakthåller infrastrukturen som är med på morgonmöten.

Operations ronderar datorhallar, kontrollerar fysiskt så att lås är på plats och miljöfaktorer, som fukt och värme och kyla fungerar så att det inte är ngt som är trasigt, larmar fysiskt i hallen, att det ser bra ut och är stadigt.

Vi i SMC är mer seniora och tar de långa frågorna, som kan ta lite längre tid. Sen har vi SOC:en som är andra personer, då är det några få personer som ska ha tillgång till loggar och utreder personer, vi har pekat ut några personer som får titta i loggar och utreda och sådana saker. Disciplinära frågor, avstängning av frågor så är det bara jag som får göra det så att supportpersonal inte ska bli utsatt ...

man kan bli hotad ändå... sen är det två i förening, det är jag och universitetsdirektör eller jag och personalchef (exempelvis) som beslutar. Alla får inte göra allt, men vi måste givetvis ha redundans vid sjukdom. Det är samma i e-postfrågor, vi behöver initiera ett ärende och sen kan vi titta.

När man är student så är man privatperson och då är det inte självklart att man kan stövla in i hemkatalogen.

Abuse-funktionen som är inkommande då, vi har ju ett antal olika huvudtyper, en huvudtyp är ju personuppgiftsincidenter, vi har haft några men inte översköljts. Vi har rutiner för det. Sen har vi MSB och det är sex timmar så det ska gå undan. Sen har vi interna incidenter där vi involverar ledningen eller vilka som behövs, ledning på skola, enskilda forskare osv. Där är det viktigt att i fredstid ha byggt upp, man behöver kontaktinformation till vem som sköter vilket system och vem som kan det här. Täckning under semestertid osv.

Det stora spelarna är ju MSB och IMY som vi ska anmäla till sen har vi internt att vi ska reda ut det så att säga.

Tycker ni det är tydligt vad som ska anmälas?

Jag har ju tyvärr suttit med i referensgruppen, så jag får ta på mig en del av otydligheten. Bakgrunden till, ett stort vägande skäl är att vi alltid har haft det akademiska, vi talar glatt om oss att vi gjort bort oss. Det är inte standard hos andra myndigheter och företag. Vi har snarare haft det som en merit att berätta att vi haft ngt. VI har inte i sektorn varit hemliga, utan varit öppna. Knappast någonsin har MSB rapporterat vidare, de har ju inte den... vi provkörde system för ett antal år sedan, där man loggar in och gör anmälningar, men det är fortfarande inte i sjön, det är frtf pdf-mallar. Och jag som kör på en låst dator kan knappast använda den pdf-mallen för den är anpassad till ngn speciell word-verison. Nu har de ändrat att man ska ringa in, först och så fort man kan. Det är sällan den här typen av incidenter. De vi använt är tillgänglighets... om vi haft nätavbrott. Där Canvas haft ngn störning. Där kan man väl diskutera. MSB är inte ngn action-myndighet, de är mer kontaktskapande. De har lagt allt i knät på SUNET.

Är det svårt att hålla tiderna, de här 6 timmarna?

tystnad

Sen är det en annan sak med MSB är att de byter folk hela tiden. Det finns mycket att säga men det är en separat utläggning.

Vi har länge haft ambitionen att ta många små krusningar på ytan istället för att vänta på ett jätteintrång, och än så länge har vi klarat oss. Så att där är det kalibrering av system skulle vi uppskatta om vi fick av MSB; SÄPO, militär vilka det nu kan tänkas vara. Och att man kan komma igång i myndighetssfären och samarbeta bättre i de här frågorna.

Apropå IMY och MSB, det är ibland mkt fluffigt, man beskriver i gråskalor, det ska vara ökad grad av känslighet osv, men med det här dokumentet vad är det som verkligen gäller, och vilket krav gäller på systemet som det ska ligga i.

Vi kämpar mkt när forskarna kommer och säger att vi har krav att vi ska vidta tillräckliga tekniska och organisatoriska säkerhetsåtgärder, vad innebär det?

Den konkretiseringen, jag kan förstå att den uteblir, det är svårt att konkretisera för alla myndigheter, men man kan ju komma med säg tre exempel på vad som är fullgott för olika typer av uppdrag. Om man lusläser utlåtande från IMY och gissar sig till vad de kanske rekommenderar, eller

tittar på vad som händer andra lärosäten, Umeå universitet åkte på en granskning, man mejlade straffregisterutdrag för väldigt känsliga brottstyper, ur det kunde man läsa vad kritiken var, då kan man indirekt förstå vad de kräver, men det kanske inte är den bästa ordningen. KTH behöver ju göra ngn form av konkretisering, KTH behöver tillsammans bestämma vad den blir. Man behöver gå med samtliga discipliner och komma lagom långt för att det ska vara praktiskt för alla.

Ett exempel, vi lyckas på ngt sätt. Under pandemin under Zoom-möten, då tog vi ställning och satte ner foten. Vi gör så här, det här är ok. Sen är det föräldrar som mejlar tidigare rektor, men ska min son verkligen behöva köra det här hemska Zoom, men vi har en verksamhet som måste komma vidare, och man måste ta några risker, det är inte 100 procent men vi vet det. Där lyckades sektorn, vi måste göra så här. Ibland när nöden kräver det, men det måste vara ganska mycket nöd...

Verksamheten skulle ju inte fungera utan ett system för kommunikation.

Angående din fråga om rapportering till MSB, vi har en slide om dataskydd som tangerar... när vi väl har gjort en bedömning, och det är svårt initialt, så gör vi en rapportering till IMY så får man inte en feedback från IMY, utan det är mer vi lägger ner ärendet, eller vi kan komma att granska det. jag som dataskyddsombud får inte feedback som jag kan ge tillbaka till SMC. Vi vet inte hur IMY som tillsynsmyndighet har resonerat i det här ärendet. Hur ska vi då vid nästa gång som det dyker upp en incident med samma karaktärsdrag... vi kan ju inte se hur IMY har reflekterat, det finns olika typer av incidenter, men vi har ju haft några med känsliga personuppgifter, där jag personligen hade förväntat mig ngt mer än två tre rader som är standardmall. Speciellt när det är forskning, speciellt för att kunna då ... det blir ju alltid en dialog med forskare, och det här med incidenter skrämmer upp folk. Det kan ju bli konsekvenser, dels finns det ett rykte inom vissa forskargrupper, sker en incident så rör det upp mkt damm. Och då vill iaf jag kunna känna, att få ngn ... det är intern kompetensutveckling likväl, få ngt konkret från IMY. Det tycker jag är allvarligt att man inte får den feedbacken. Förväntar mig inte ngn lång rapport men ngn form att de kan lyfta på luren och berätta hur de resonerat, men avsaknaden av konkreta ... känner jag då ... nu kan vi lära oss av det här. Man vill ju inte återupprepa samma utan få kompetensutveckling. Nu vet jag inte om MSB är bättre. Det borde ligga på IMY ansvarsområden.

Det är en svaghet att det ska vara personberoende. Tanken att få in det här, dels statistik, dels koppla så att det kommer alla till gagn. Jag förstår om de har drunknat i tokiga frågor...

Men de borde ju ha ett beslutsunderlag.

Det tycker man.

Vi var med i den här forskningsdatautredningen för en tio år sedan. De som var med där var ju mer eller mindre dekorerade professorer från forsknings-Sverige och de var ju otroligt medveten om personuppgifter, hela deras heder och forskning bygger på att man ska ha koll på personuppgifter, för annars är man rökt och blev av med finansiering. Så att de är ju, just det här, de som jobbar med vad det kan vara, gendata, sekvenser och allt det, blodprover, de är väldigt medvetna om att det måste skötas, så de blir väldigt skakiga när ngt händer. Sen har de inte riktigt kunskaperna hela vägen ut men där måste vi ju hjälpa dem.

Ca 01.43. Prat om krisledning. Och att CISO har många järn i elden.

Sårbarhetsanalys. Det är ett spektrum. Dels har vi sådana här rena tekniska som går, scannrar som går på alla våra apparater periodiskt. Försöker leta efter kända sårbarheter som kan finnas. Till en viss grad. Generellt på alla apparater som vi har anslutna till våra nät. Sen gör vi då, vid morgonmöte eller om ngn har hittat ngn speciell sårbarhet som extra känslig, den värsta senaste var wannacry

2017 ngt sådant där när det var virus över hela världen. Typiskt en sådan så måste man scanna en per minut. Mot kanske en gång i veckan normalt. Sen har vi en del andra saker som går som är mera bra för statistikinsamling. Sen har några av oss erfarenhet att granska system, 1 och 1. Nu har vi då provat den här modellen så att internrevisionen tog in ett företag, sen har vi haft en dialog med vår styrelse om det är så att vi.... Vi har ju då haft ambitionen att titta på systemen så att man inte ska kunna ta sig in utifrån, men nu har vi haft dialog med styrelsen, att vi ska titta på inloggade, det finns en del tunga behörigheter i ekonomisystem. Då är vår fråga till styrelsen om vi ska hålla den kompetens som är nivå med den bästa firman i norden då måste vi ha mer i budget och är det rimligt överhuvudtaget. Sen har vi i sektorn drivit – it-chefer har ett nätverk, itcf, där har man undergrupperingar, det finns en undergruppering om it-säkerhet, där är det MSB förordningar och sen rena it-säk-grejer, men i varje fall, den grupperingen är tänkt att vara kravställare in på SUNET. Just hantering av cert osv. Man har börjat rekrytera där så att de ska få kompetens där, så att det går att avropa eller fylla på med folk och samarbeta så att vi inom sektorn tittar på ett system var, det är fånigt att vi alla tittar på alla system, som Agresso. Sen gör vi när vi får förfrågan om system som ngn ska starta upp, ngt forskningsstöd av ngt slag. Är det externt system så tittar vi på om det finns avtal, kryptering och alla de här sakerna, är det bra ställt med avtal. Och det handlar oftast om att köpa en begagnad bil, det är också intressant att titta på försäljaren, är det en förtroendeingivande verksamhet. Är det de stora drakarna så kanske vi har större förtroende. Är det en mindre firma får man titta på lite andra saker. Då gör vi en enklare teknisk genomgång, där kan vi, vi håller på att jobba upp det, men vi har en ganska stor utvecklingsgruppering som vi kan ta hjälp av, det är ju allt mer webbtjänster och molntjänster som de kan förstå sig på. Så att det finns en hel del sådant.

Utredare:

Väldigt ofta granskar vi system. Vi diskuterar ställningstaganden. Antingen får vi in det genom att forskargrupper vill köpa licenser, det går in genom vår licensfunktion, eller via RiRs kontaktperson, när forskare frågar hur de ska hantera deras data, vi dataskyddsombud när frågor kommer om GDPR; vi vill använda det härs systemet för att hantera dessa uppgifter, kan vi göra det?

Tar vi in alla underlag från alla avtal, tjänsteavtal, gruppavtal, it-infosäk, white papers, pappersperspektivet på en produkt, gärna arkitekturell beskrivning, hur ser systemkomponenterna ut att hänga ihop, hur ser flöden ut, hur ska de använda det, vilken data ska hanteras, vilka ska arbeta i systemet, hur ser rollerna ut, hur ska ni använda det, alla personuppgiftsbiträden som finns. Sen bygger man liksom 360 runt produkten ur ett systemuppläggsperspektiv och avtalsperspektiv, för att se om det är en sunt upplagad produkt och vad man uppfattar att den lever upp till. Då går vi igenom och gör sådana bedömningar. Och det gäller också anskaffning, finns det avtal, om ni avropa, vad som ingår i det som man vill köpa, det finns olika typer av stöd, om man tar gdpr, många gånger köper du den billigaste versionen av produkt, då kan du inte välja var data ska bo, ex i USA; köper du ngn enterprise så kan du välja residence, europa eller till och med i Sverige. De flesta forskare tycker att gratis är gott, man vill således köra gratis. Men det finns ju inte gratis utan man betalar på ngt sätt. Då driver den affärsfrågan och visar för dem vilken risk de utsätter sig för genom att vara för snåla eller välja fel. Vi hjälper dem ur ett helhetsperspektiv, i samband med anskaffning eller upphandling eller om det kommer en uppgraderingsprodukt eller det görs ändringar i pub-avtal eller de byter länder för driftsättning, alla de här perspektiven tittar vi på. Jag uppfattar att vi har en bra och djup förmåga att göra det, det luriga är att komma till i alla sammanhang. Förr var det bring your own device, idag är det bring your own service man köper en hel IT-avdelning på burk, google compute cloud eller vad det kan vara. Det är oerhört lätt att skaffa sig tillgång till en gigantisk IT-infrastruktur utan ngn egentlig broms. Därför är det så viktigt att få efterlevnad på KTH-nivå och inte till varje forskargrupp.

Har ni ngn uppfattning om hur många ni når?

I de stora systemen har vi ganska stor träffsäkerhet, ex HR-system, det går vi igenom och granskar. Det har varit alltifrån chattbotar som man vill ha som stöd för antagning, då kommer vi typiskt med. Det finns alltid en gråzon, vi kan ju inte veta vad en forskare ute på en forskningsgrupp gör, det vi vet är att de gör saker som de inte alltid borde, men det är svårt att komma åt och polisa dem.

Lagringslösningar som är specifika för forskningsdata, hur efterlevnaden ser ut?

Vi har gått ut en del under här åren och gjort djupintervjuer och enkäter. Det kommer mer i det här avsnittet om utmaningar, hur man arbetar som forskare, det är ju en rätt grad av akademisk frihet, vi har externfinansiering där krav kommer in. Vi har väldigt mkt som regleras i samverkansavtal som ni kommer prata mer om vid intervjun med jurister. Där regleras väldigt mycket på avtalsvägen. Där är ju en fördel att det hr förbättrats på senare år så att det sker med koordinerat (avtalshantering) och enhetligt på alla skolor. Då får man på den vägen en bättre insyn och kontroll över hanteringen.

Det finns ett antal större intressenter som levererar lagringslösningar, SND har vi touchat tidigare. Vi har parallelldatacentrum på KTH som också är en storskalig driftställare, vi har SUNET som levererar lagringslösningar. Vid KTH använder vi onedrive, för viss typ av forskningshanering är det fullgott, tittar vi på Sci life lab så tar man fram separat lokalt hostad lagring i ngt som kallas (ohörbart) där man arbetar för att man ska ha data inhouse för att det ska vara skalbart, i paritet med molntjänster, de är så skalbara (molntjänster) så det är svårt att konkurrera med dem som IT-avdelning. Det är en bred flora av lösningar. Många av samarbeten vi har är ju internationella. Ofta är samarbeten i inom ngn it-infrastruktur som ngn kick (ohörbart) som ett forskningssamarbete har satt upp och då jobbar i de ex office 365 men då är det europeiska eller internationella samarbeten, som en av intressenterna i ett projekt kör. Det kan vara samarbetsytor som andra lärosäten tillhandahåller.

Har ni koll de olika vägarna och kanalerna som data hamnar i?

I den här SNC-funktionen har vi inte en förteckning över all forskning och vad de gör, jag uppfattar inte att det har varit möjligt att kartlägga på det viset.

Nej de resurserna har inte funnits. Det som finns nu i riktlinjerna för hantering av forskningsdata är ju att man ska ha en datahanteringsplan, och där beskriver man var data sk lagras och det är ju ett sätt att få ren tydligare bild, och möjlighet att bygga på stöd kring regelefterlevnad vid projektstart innan det är för sent.

Där är ansatsen att vi ska kroka in i planerna och se till att man kan matcha det med, om ngn säger att jag ska ha min data i en krypterad databas eller lösenordskyddad databas, vad menar man, det kan betyda vad som helst, det kräver att det är en väl vald projekt med kryptering som är trovärdig (ohörbart). Det är en verksamhet som sakta blir växer fram och blir alltmer strukturerad.

Ser ni att man skulle kunna få kontroll eller har bättre koll på de externa dataflöden som finns, är det en möjlig uppgift eller är den en...

Det uppfattar jag. Det är en ändlig uppsättning av projekt. Det är mkt jobb att ta sig dit, det kräver mkt mer resurser än vad vi har idag.

Sen är ju dataflöden inte bara lagring. Det är ju hela processen. Du kan ha en överföring mellan ngn projektlagringsyta och en mjukvara för analys. Det är ju lagring i anslutning till analys, sen kan du ha överföring till ngn mer avancerad beräkningskapacitet, och i nästa steg i kedjan vad händer då och långtidslagring, det är ju inte bara ett ställe, en hårddisk, så ser det inte ut. Det är processningen som är det intressanta egentligen.

Fyrtioåtta centrumbildningar, det är centrumbildningarna, om man tar hur många forskargrupper det är, det är en lång lista. På ngt sätt så är det så här, man jobbar med att få på plats. Är man HR-chef här då är man informationsägare för HR:s infotillgångar. Då har du koll på alla uppgifter i HR-system. Ägaren har till sitt stöd folk som är förvaltare. En term som – idag är det att vara data steward, det är de som faktiskt sköter och hanterar informationsmängden i praktiken. Vi är på väg att etablera sådana, och forskningsområdet är första steget, väl?

Ja vi håller på att titta på olika modeller för data stewards, aalto i finland har en modell, och vi för diskussion med Chalmers, Örebro och SU hur man skulle kunna göra det i praktiken för att få till den operativa datahanteringen på ett bättre sätt för att både få det tekniska att fungera men också det här med efterlevnad att man hanterar det på ett korrekt sätt, genom hela livscykeln.

Det kommer att finnas ett fåtal ett informationsägare, forskningsdata, hr-data, eller forskningsdata inom några större sjok, och under dem kommer det finnas många data stewards, och det innebär att det kommer att finnas en möjlighet för att samla och kartlägga, men det finns väl alltid ngt rand-fall som vi inte kommer att fånga, men vi kommer över tid att ha mkt bättre katalogisering än vad det har varit förr. Historiskt har det varit skolornas och institutionernas eget ansvar att sköta det, och det viktiga var artefakterna, forskningsrapporter och resultat som har varit fokus på historiskt och idag har det förändrats, idag är större fokus på att tillhandahålla datamängder. Det byggs ett nytt behov och en ny verksamhet som växer fram.

Data steward – var de under informationsägare eller systemägare?

Det är det vi tittar på lite olika modeller vad som faktiskt skulle kunna fungera i verksamheten.

Informationsägare, är det forskarna själva?

Det regleras ofta i samverkansavtal, och det kan var komplext, du som forskare kan vara inblandat i 3-4 projekt, ett av projekten är KTH huvudman och du är huvudansvarig forskare, och du kan vara med i ett annat projekt och ett annat uni är huvudman och därmed huvudansvarig för datahanteringen, men du bedriver forskning där, sen har du ett tredje projekt vilket är KTH internet, men ligger med huvudman på annan institution, det finns en stor mängd variationer på möjliga konstellationer. Och det är också det här forskningsprojekt, det är lätt att definiera när det finns externfinansiering, men har du enbart basanslag då finns det inget sådant väldefinierat projekt som löper över en viss tidsenhet, nu KTH:s forskning är till 60-70 procent externfinansierat, så att en ganska stor andel bedrivs som projekt, med en viss projektlängd där finansiering är definierad över en viss tidsenhet. Men det är ju 60 -70 procent. Det som är basanslag enbart kanske är lite mer samlat inom en institution, det finns de här jätte-EU-projekten, då kan det vara 30 olika parter. Det är avtalsjuristens gebit. Det kan bli komplext.

När man pratar i digitala möten, har forskarna koll på vad de får säga och vad de inte får säga i olika lösningar?

Vi har en liten anvisning där vi poängterar att om man hanterar känsliga data att det ju oavsett fysiskt eller digital form att informationsöverföring muntligt är ju också informationsöverföring, eller digitalt möte. Att man tänker på hur man sprider information. Det finns en sådan rekommendation när man hanterar mer känsliga data. Men väldigt mycket ska jag ju säga, och det är ju offentlig handling, offentlig allmän handling där konfidentialitetsgraden är noll.

Den zoom-lösning vi kör idag, det finns ingen i ett ordinarie-möte finns ingen tredjelandsverföring, det har funnits det om man har kört externa kopplingar, ringt in till möten har det tidigare funnits tillfällen när data har varit i tredjeland. Det heter att zoom förde över data till fb, men det var om

man körde gratisvarianterna. Sedan dag ett har kryptering, inte en till en, men det finns också i zoom, men det var samma upplägg för kryptering i zoom som i teams, det var krypterad överföring på de som var på möten. Det är få samtal på myndigheten som är av sådan karaktär som inte skulle ha gått att köra i zoom likväl som på telefon.

De forskningsprojekt som faktiskt omfattas av säkerhetskyddsklassade uppgifter, där gäller det andra spelregler. Då är det som ciso sa tidigare, då finns det en extern tillsynsmyndighet som redan har varit med ett jobbigt projekt och sagt att ni som ingår i det här projektet med FMV eller FOI... då skriver ni på att det här gäller, då har ni inte era möten i Zoom osv, då har man fått förhållningsorder om vad som gäller för er verksamhet. Jag uppfattar att vår bild har varit att de videokonferenslösningar som vi kör 1 inte innefattar tredjelandsöverföring för dem som ingår och att de ska vara tillräckligt säkra för . . .

Vi har ju kärnkraftsäkerhet, Då har vi strikta regler med kassaskåp och passersystem. Vi har inte anläggningen, vi har rivit vår reaktor, men just när det gäller dokumentation, då har vi kalibrerat så att vi ska ha samma nivå, när vi pratade som sagt igår med en av skolorna, då hade nästan svårt att hitta projekt där det inte fanns extern part där man ställer krav på varandra och kalibrerar. Vi hade tidigare när vi hade militärsamarbeten vi hade tunnelbanevagnen, en bit av volvo-tak, alla sådana saker regleras med liksom strikta avtal. Det är inte sällan så att det följer med personal som levererar sakerna som kanske medverkar i testerna.

Det här är väl en stor orsak till att mkt av ansvaret är vidaredelegerat ut i verksamheten för att det kan se så enormt olika ut. Kärnkraftteknik eller om man är ren forskare i matematik. Det som du har som arbetsredskap kan vara en whiteboard, penna och papper. Du har inte några känsliga data. Inga externa samarbeten. Då är det kanske orimligt att ha samma säkerhetskrav på matematikerna som på kärnkraftteknik.

På tal om det – förlåt – så står det i er anvisning i för informations- och IT-säkerhet står det att det ska finnas ngn ansvarig för infosäk på varje skola?

Vi har rent praktiskt använt den administrativa chefen som är ordningsmänniska, sen har det förekommit nu har det varit personer som gått runt i organisationen, det kan vara så att man anmält en annan person. Just nu är det inte så, nu går vi hårt på... den formuleringen skulle möjligen justeras i anvisningen.

Sen är det en utmaning för det är ganska stora verksamheter. När man pratar om det här med skyddet, till ex inom läkemedelsindustrin är det formidabla skadestånd där finns det verkligen. Sen har vi då där vi stött på ... det här som jag kallar för övermolnifiering eller onödig... vi hade till exempel en forskare som höll på att detektera tidigt hjärtfel i ngt blodkärl. Det finns inget skäl, han kunde lätt simulera det, han behövde inte plocka data från enskilda personer, han kunde göra sitt matematikprogram och testa. Det är så lätt att det åker med information, inte bara att hantera utan låt bli att hantera det som du inte behöver. Vi säger också lagra hos dem, plocka inte hem det till oss.

På zoom och på andra plattformar, den här rådgivningen, försöker vi hjälpa till med helhetsbedömningar, juridiskt, tekniskt, avtalsmässigt, affärsperspektiv alla perspektiv. Det är en löpande fråga, ofta vill man ha ngn ny plug-in, för att koppla ihop ex zoom med en ny plattform. Där håller vi emot. Det är en sak att granska och få ett upplägg för som säger att inom det fungerar så här på den här plattformen som den ser just nu. Sen får du nya komponenter, då är det svårt att veta var data tar vägen nu. Då tycker folk att vi är trista och hindrande, för att de inte kan slå på alla features. Vår linje är att det ska vara ordning och reda. Vi håller inte på 15 videokonferenslösningar, vi puffar för en på KTH, för personal och studenter.

Sen är det olyckligt att andra myndigheter kör teams som har bedömts har andra risker, men eftersom vi har samverkan måste vi ha licenser för teams för de som har sådana externa samverkansprojekt, men alla har inte tillgång till teams.

Med teams ser vi ju att Microsofts grejer håller sakta men säkert på att flytta från EU till Sverige. Men det är bara en revisionsteknisk förbättring för man har frtf problem med jurisdiktion, de utmaningarna kvarstår.

Det finns andra risker med teams, det blir lätt att datahantering hamnar i teams.

Det en fördel att köpa en sak av varje leverantör, det finns en fördel att köpa av samma för att det sitter ihop. Men Microsoft vill ju att man ska komma in, man ska skaffa konto. En annan sak är ju att vi kan granska Zoom och Canvas. Jättefint och det är perfekt. Sen kommer ngn på att vi ska ha plug-ins; mötesbokningar, transkribering, det finns ingen ände, du ska laga bilder på ett speciellt sätt. Då visar det sig att integrationsplattformen minsann ska logga in och liksom ha admin-rättigheter, vi försöker ju vägra om vi får veta, man kan ha jättefin lösning men det finns nästan alltid ngn bakväg.

Från FAIR-dataperspektiv kan man vara integrationsförespråkare, men då måste man ju skala upp resursmässigt kring informations... och det har vi inte idag.

Att rådge på det här sättet och göra bedömningar, det är ständigt pågående, vid anskaffning och sen vid morphningen, den förändrar sig över tid. Över fem år avtalad tid så hinner den byta skepnad.

Och sen varenda app har en funktion, på papper enkelt vi har ordnat och avtalat, men den lilla appen den har molnlagringar och kopplingar.

Upphandling. Vi har en upphandlingsavdelning, omsättning på personal men vi tror nu att det ska bli bättre. Det är inte bara för att man upphandlar och betalar, utan vi får, vi har ett exempel, med IA-system. Man är medlem i förening, arbetsgivarverket, då får man gratis ett system, få in studenter i arbetslivet. Det ska ju också granskas. Men det här nålsögat skaffa pengar, det är inte säkert att man lyckas ta sig runt eller passera, det här är en utmaning, alla de här olika möjligheter att skaffa mjukvara. De tittar på oss och säger att det är gratis. Men det spelar ingen roll det måste ändå granskas. Sen finns det när man inte kan/har råd/vill eller vi är besvärliga, då utvecklar man själva. Men det ska också kravställas. Det finns ju en tradition att man är snällare mot sina egna utvecklare och sin egen drift. Vi försöker ju då ... vi har etablerat på utvecklingssidan det finns en utvecklingsgrupp på IT-avdelningen. Dels har vi månadsmöten med dem där vi tar upp de stora frågorna, loggning, spårbarhet, autentisering, molnfrågor. Där har vi möten där vi försöker skola dem i det här, vi kan inte vara med varje sekund, och i transformationen det går direkt från utveckling rakt in i drift, men det passerar inte under ngn jobbig driftperson som kravställer, och det är inte heller där ngt stopp i form av att du ska köpa hårddiskar, minnen och datorer. Det är mer att man trycker på en knapp så sätter det igång. Men i korthet det finns ett antal fasetter på den stenen också. Och det försöker vi fånga så att det inte bara går via upphandlingsavdelningen, det finns ju en gång en lista förteckning, upphandlingsplan. Den har gått årligen eller vartannat år, det är skolorna, nya mätinstrument, större investeringar ligger där. Det är ju en utmaning för oss att veta när det döljer sig ITC informationssystem i bakgrunden, det är inte bara den fotospektrometern, vi anar ju att om ngt kostar 30 miljoner så är det nog IT för 15 som döljer sig bakom. Inte sällan är det så att det går att fixa det ändå med ordinarie utrustning, det kan vara så att flera kan utnyttja det här. Det är ngt som vi ...

Ofta är det ngn dålig mjukvara som inkluderas. Och ibland låst proprietärt. Och sen har vi trenden att man säljer en produkt, men att man vill sälja en plattform. De stora klassiska hårdvaruleverantörerna

har ju mer gått till att man säljer hårdvara plus mjukvara. Och de allra största vill ju att du ska koppla upp dig till deras plattform. Det är ju en utmaning.

Sen får vi baksidan, om vi ska samutnyttja med dual use och annat, det har förekommit uppdrag granskning för ett antal år sedan när vi hade de här kineser som fick använda saker som jag tror inte... skolan Science, flödes... så att det ...

Men huvudbudskapet är att det kommer saker antingen gratis, eller via utveckling, inte bara via upphandling. Sen där vi har svårt och det är ju det här som Skatteverket håller på med leveranskedjan. Om det då finns en leverantör, av det här, och leta leveranskedja bakom det här är nästan omöjligt för oss. Om det ens går. Vi håller ju på att EU och USA inte ska handla från Kina, jag vet inte om det gäller i forskningssvängen.

Öppen källkod är också en utmaning. Man inkluderar paket som är utvecklas av frivilliga utvecklare runt om i världen, det är många steg. Vilka sitter längst bort i näringskedjan. Det vet man ganska lite om.

Om det smyger sig in ngn kod i ngn komponent. Där har vi ju varit open source-tillvända historiskt och open source-leverantörer, men det finns en extra utmaning där. Just nu, i tidens tempo, många sneglar på open source-lösningar för att köra sin egen synk, nextcloud – öppen källkod är ofta ett av svaren för de som tycker det är jobbigt med amerikanska ägare. SUNET anlitar en norsk underleverantör som har en open source-produkt i stället för onedrive eller box, som har en liknande molntjänst med svenska datorhallar, men det är ju inte så transparent hur säkerhetsarbetet ser ut. Det är inte okomplicerat att granska det. lärdomen, vi har ju granskat borde hårdvara och mjukvara, det har ju aldrig hänt att vi inte har hittat fel, oavsett om det är ett avtal eller en produkt, det här mantrat om open source..

Vad kan det finnas för fel då, går det att vara konkret?

dels kan det ju mkt väl vara, om man ska vara konspiratorisk, vara medvetna fel. Det var ett uni eller studenter som skickat medvetna fel till Linux och blev bannade. Men det var ju inte svårare än så, man litar ju i hög grad på folk.

Behörighetshantering.

Vi omborrade folk i huvudsak historiskt, det började 3000 nya och då fick man in 3000 nya. Och då fanns det en ide att ha kvar dem i systemen för att ha kontakt med dem över åren. Vi är på väg bort från det. enligt gdpr så får vi inte det, vi har inte en aktiv relation med dem. Där har vi gjort ett stort arbete, det pågår en centralisering av verksamhetsstöd, i stället för att ha en HR-avdelning per tio skolor utan kanske ha en HR-avdelning och kanske ha en gemensam rutin för hur onboardar och crossboardar personal. Historiskt har varje skola varit fria att sköta det själva i deras system, och se till att de individerna hamnar i centrala system för HR och ekonomi. GDPR var såklart en sådan startklocka för det här. En annan handlar om att vi historiskt köpte programvara och installerade den lokalt ofta är det nu en service istället, nu vill Microsoft ha betalt för hur många FTE och hur många personer du har i dina AD hur många du kan autentisera. Har vi 250 000 personer fast vi inte behöver så blir det såklart dyrare för oss, istället för säg 75 000 som vi borde ha. Vi jobbar mkt med livscykelhantering, att se till att om man är borta från KTH i fem år och kommer tillbaka kan man inte få tillbaka sitt gamla utan man får ett nytt. Så var det inte historiskt.

Historiskt var det en feature och vicerektorsbeslut att så här ska det fungera. Det är ett sätt att hantera att man har alumner. Vi städar frtf efter det. saker är byggda på ett sätt under 20 år så har an en liten teknisk skuld att lösa upp det.

Detta är såklart autentiseringsfrågor, det pågår ett projekt kring flerfaktor, först till anställda sen till studenter. Analogt med det pågår ett idogt arbete med att kunna dela ut identiteter, historiskt stod folk i kö. Så kollade man leg och så fick man anvnamn och lösenord. Idag med e-leg vill vi ju såklart att du ska kunna göra det distans, att kunna aktivera konto med e-legitimation.

Hur gör ni med internationella forskare och studenter?

De får vi göra on-prem för de har inga e-legitimationer. Men nu har vi skaffat oss mer tid att hantera dem. Det finns europeiska legitimationer, så sådana som kommer från EU-program ska vi kunna ta hand om. Men vi har många som kommer utanför EU.

Passersystem har vi tack vare ett idogt arbete har vi ett system för KTH och alla campus. Som sköts centralt på vår fastighetsavdelning.

Internrevisionskritiken har handlat om att folk har haft kvar passerkort längre än vad de har behövt. Det städar vi manuellt både inför automatiseringsinförandet, och när det är på plats så faller lejonparten av den kritiken. Om jag börjar på en ny avdelning får jag automatisk de rättigheterna, och byter jag eller slutar så försvinner jag ur systemen och så plockas rättigheterna bort från korten.

GDPR och dataskydd (oerhört svårt att hänga med i vad som sades, halva ord, halva meningar, avbrutna ord, avbrutna meningar, anteckningarna är därför väldigt bristfälliga, ca 02.36.20).

Dataskyddsombud ingår i SMC, har en arbetsordning, ska vara oberoende men fruktsamt att arbeta med SMC. Den rollen ... jag granskar en del avtal inom ramen för SMC, stödjer förvaltningsjuridik och även affärsjuridik, det behöver inte bara vara personuppgiftsbiträdesavtal det kan vara data transfer agreements och ngt annat agreement ca 02.37. forskningsdataavtal. Om vi har en komplex samverkan har vi också personuppgiftsavtal, personuppgiftsbiträden, etc som också reglerar hur vi får då skicka information med personuppgifter sinsemellan inom samverkansavtal eller partner. Det är ju då tittar på själva avtalet i sig själv, nu pratar vi om tekniska... själva avtalet kan vara ett av de här organisatoriska skyddsåtgärder, att vi då får granska, är det projekt är det standardavtal, det kan också vara olika partners, det är sällan som KTH använder sina avtalsmallar vi får granska avtal, jurist kommer berätta mer om detta. Vi styr upp så att förhandlingsposition, regelverk, vi försöker få igenom det vi har, är det internationell reglering, svensk reglering, kontra nationella eller regionala lagstiftningar som ska samsynkas. Det är här jag ger stöd till affärsjuridik framförallt, men även förvaltningsjuridik.

Dataskyddsområdet – det är specifikt om forskningsdata – personuppgifter i forskningsprojekt, vi har en generell utbildning som gäller för alla anställda. Det är en webbutbildning. Samarbete med LU som har tagit fram en webbutbildning för personuppgifter för personuppgifter inom forskning. Vissa delar kan vi direkt plocka in, en del behöver vi skriva om. Jag har flaggat för det här inom SMC, men fått ok från LU att vi kan använda det här, lansering under våren. Med kopplat till ngn form av informationsinsats. Det har vi inte haft tidigare. Incidenthantering personuppgifter, den incidenthanteringen i stort skiljer sig inte från incidenthantering till MSB. Vi har ju då de här mer specifika delarna som kopplad till... personuppgifter, bedömning av hur allvarlig incidenten är. Det här gäller även i forskningsprojekt. Än så länge mig veterligen sådant. Vi har haft några enstaka. Konsekvensbedömningar gäller inte bara forskningsprojekt utan vi har även på hemsida mall svenska och engelska och mallen är tänkt som vi har ett nationellt nätverk för dataskyddsombud som arbetar inom universitet och högskolesektorn. Vi har gjort en samsynkning, vissa delar skiljer sig men i övrigt mycket lika, samma till 95 procent.

På vilken nivå görs dessa bedömningar?

Det mesta jag har haft är forskningsprojekt. Vi försöker jobba... ett ärende kan initieras, de kan kontakta RiRs kontaktperson eller ngn annan. Konsekvensbedömningen är en del av ett pågående forskningsprojekt, dmp är parallellt med det, parallellt med avtalsprocesser. Det kan komma in genom etikprövning där man behandlar känsliga personuppgifter. Vid konsekvensbedömningar, då är det hur man hanterar konkreta risker, en av de där är ju också hur man hanterar – om man nu har en molntjänst – vad är det för risker. Kan vara kameraövervakningslagen om den är applicerbar, då är det ytterligare en miniriskbedömning utifrån det, eventuellt en anmälan till IMY om det kommer vara... vi har några sådana projekt som har kameraövervakning i allmän miljö då kan vi komma till etikprövning, lite kontakt där men inte mycket. Små bedömningar, IT-säkerhet, riskbedömningar, angränsande lagstiftningar. Vi får se med den nya AI-förordning hur det får beröring på konsekvensbedömningar. Vi har haft en del catbot vi har också haft konsekvensbedömningar av AI.... Vi har mkt ai-forskning där då konsekvensbedömning kan bli aktuellt. Även också etikprövning.

Vi har FAQ rent generellt, som är ganska täckande. Införandet av rutiner och rutiner i praktiken. Vi har ju det här med dataskydd, till skillnad från ... nu pratar vi om infosäk, ser man då på dataskydd vad det är, det är personuppgifter, vi har även registrerande skyldigheter, om det är registrerande som är involverade i forskningsprojekt, deltagande i projekt, aktivt, vi har ju en del laborationer här där de gör kopplat till AI-forskning, interagerar med olika sociala robotar, men även då information från andra myndigheter där de registrerande ingår. Vi har de enskildas rättigheter, vi har rutiner för hur vi hanterar det, vi har en så att säga, single point of contact, enskild kontaktyta, för alltså generell kontaktyta för dataskyddsfrågor, det är på supportgruppen KTH dataskydd, det är i princip, jag och utredare och ciso, men jag hanterar det i princip. Det är ärenderelaterat.

Det som kommer nu är, vi har, nu ligger det lite i träda, vi har som andra rekommendationer som jag måste ta fram... vi har redan nu en också ngt som vi tagit fram, sektorgemensamt, hantering av examen, studenternas examensarbete hur man hanterar personuppgifter i dessa stöd till handledare. Det är ngt jag kommer kika på, sådant finns. Dock inte förankrat i KTH men sektorsövergripande. Det var en väldigt snabb utflygning så.

Vi kanske får boka in fler möten ifall vi har behov.

Säg till bara. Vi träffas ju en gång i veckan även utan revision.

Det blir ju så på KTH och det kanske skiljer sig från andra, det blir operationellt arbete för min del som dataskyddsombud, det här med tillsyn som ändå är en sak som ... i GDPR är ngt som har, jag har ju en årsrapport och årscykel så, men är just nu så har det här operationella har tagit över, det har jag lyft upp i årsrapporten och ledningen är medveten, det har blivit av naturliga orsaker att mer operationellt ändå mer än tillsyn.

Det var väl uppe med Ernst & Young, vi upphandlar ju system tydligt, allt är en cykel, om vi är med när det blir nya anskaffningar, även om dataskyddsombud inte hinner med att göra en aktiv tillsyn på ett system som jag anskaffat, men inom en avgränsad period är det nyanskaffning och då gör vi automatiskt en ny granskning då finns det implicit tillsyn även kopplat till anskaffning.

Upphandlingsavdelning har också skaffat ett system för uppföljning av upphandlingar så att vi ska få...

Väldigt sammanfattande kring utmaningar inom forskningsverksamheten.

Det är ju det här att informationshantering sker mer som regel än undantag i samverkan med flera olika aktörer. Det regleras ofta i avtal. Som regel i avtal och då beror det på vem som är huvudman vem som är personuppgifter, vem är huvudman vem är personuppgiftsbiträde, så blir det ... det är

rättsinforamtiskt område som gav ett seminarium och det var väldigt oklart för experten om vi föll in under den lagstiftningen eller inte. Och det ska ju finnas en nationell myndighet som ansvarar för det här. Då frågade vi DIGG om de hade fått det, och det hade inte hört ngt. Och då trädde lagstiftningen i kraft, men vi har ingen ansvarig myndighet i Sverige.

Vilket departement, det var ju inte utbildning, det var ju antagligen infrastruktur...?

Ja, och det sa ju DIGG... vad de nu faller under.

De har ju stöpt om en del efter valet. Och på hälsodataområdet kommer jättemycket lagstiftning och där är regionerna jättefrustrerade och där ska det vara en myndighet och de vet inte vilken...

Då kan man ju tänka sig att regionerna har en huvudlagstiftning, det är hälsodata, det är en sak. Vi har trafikdata, transportdata, miljödata, hälsodata. Alla typer. Hela paletten av lagstiftning, NIS2, ai-akten. Det är en lång solfjäder. Astra Zeneca som har en legal department som har 100 anställda det är för ett av de områden som vi verkar inom.

inte så enhetliga processer helt enkelt för att det inte är möjligt. Varje forskningsprojekt är ganska unikt därför har vi riktlinjer där man i datahanteringsplaner ser en forskningsdatahanteringsansvarig inom projekt eller verksamhetsområde inom forskningen. Så har vi det här att verksamhetsnytta uppstår i och med publicering av forskningsresultat och nu kommer det mer externa krav från finansiärer att man ska publicera data som ligger till grund för resultat, och då kommer svårigheterna för forskaren att avgöra är det här offentlig och allmänt och kan tillgängliggöras eller kan vi tillgängliggöra viss beskrivning med viss åtkomst. Och det är inte helt lätt att sitta själv med den bedömningen. Det här med externa krav hänger ju också ihop med ökad externfinansiering de senaste 15 20 åren, nu är nästan 70 procent som är externfinansierat. Väldigt lite kommer som statliga basanslag, och en stor del av de pengar är uppbundna som in kind bidrag, de externa kravbilderna. Vi har en ökad kravbild men inte ökad statliga anslag för att ge stöd till verksamheten, det är en grundutmaning. Sen var vi ju inne på det här som exempelvis föreskrifter från MSB, de är ju lite skrivna efter tänket man har, att vi har Skatteverket, vi har en intern informationshantering, universitet och lärosäten ser ut så här. Vilket gör hur vi ska tolka det här är en utmaning. Och det finns då en komplex digital infrastruktur, det finns väletablerade forskningsinfrastrukturer som går på andra ledder än internt. Och sen har vi en bristande samordning nationellt med olika bitar fragmenterat på olika myndigheter. Det finns en VR-rapport om det här som pekar på de här problemen. Det är en sektor i högt förändringstryck och hög grad av internationell konkurrens. Sen ser vi ju det även efterlevnadsfrågorna inom digitalisering kräver stöd av flera kompetenser, vi har ju här dataskydd och it- och infosäk, vi har ju god kommunikation med juristerna och vi hoppas kunna samla det här ännu mer för att det här svaret, hur var när och med vem får jag dela forskningsdata ligger ju i mitten. Och sen det här som man pratar om på tunnelbanan, med vem, hanteringsregler, hur tar jag med data och i vilken form. Det är ju lite så... och det här då det gör det inte lättare för oss att vi har då en sektor där vi har den svenska nationell datatjänst, som är nationell forskningsinfrastruktur och de har i uppdrag att hjälpa sektorn att hitta beskriva och dela forskningsdata men de erbjuder ingen lagring. Det är lärosätenas ansvar att anskaffa det på ngt sätt. Sen har vi en annan nationell forskningsinfrastruktur för beräkningsresurser, och det är stordatamiljöer som har processorkraft men också det i anslutning med lagringskapacitet, då måste man ha data i anslutning till beräkning. Och då har man kallat för hot storage, aktiv snabb lagring. Men de har inget nationellt ansvar eller uppdrag för lagring. Och sen har vi andra mer ämnesspecifika infrastrukturer och där kan det finnas resurser för lagring och delning och också mjukvara för analys och visualisering. Som då kan erbjuda på nationell nivå till lärosäten. Sen har vi SUNET som är en tjänsteleverantör samtidigt som man har en underavdelning på vetenskarpsrådet som är en finansiär. Det är lite olyckligt förhållande, och det ju VR själv påpekat, de här rapporten om e-infrastruktur. Sen har vi ytterligare kockar i den här soppan med DIGG och Riksarkivet, och KB och Vetenskapsrådet som har olika bitar det här ansvaret. Vilket inte gör vårt jobb lättare kan jag säga. Så det här är en sådan man får förhålla sig till på ngt sätt. Men det är en komplexitet i det här. Sen om man ska skala upp det på europeisk eller internationell nivå så går det inte ens att se alla aktörer i den här soppan. Det är många aktörer, det är ett ökande komplext regelverk, vi har digital singel market, som ska reglera den inre digitala marknaden, det kommer enormt mycket pengar från european science cloud med lite oklar kravbild kan man sammanfatta det.

På EU-nivå är det fem-sex olika direktiv som är på gång på hur man ska jobba med informationshantering och krav på det. Regleringstrycket är stort.

Om man ska nu rikta en känga uppåt – jag pratade med om representant för DIGG, det har ju kommit nu dels data-akten om öppna data, myndighetsdata, DIGG har ju antagit att det myndighetsuppdraget faller på dem, men det har inte fått det formellt det från departementet. Och sen så trädde ju data förvaltningsakten i kraft den 23 december, vi hade en expert på