BYOD-utredningen
Peter Möller och Richard Johansson

BYOD vid Lunds universitet – en inledande orientering

Innehållsförteckning:

Postadress Box 118, 221 00 LUND Telefon 046-222 41 56 E-post peter.moller@cs.lth.se, richard.johansson@ht.lu.se

Abstract

Peter Möller (Computer Science) took on the task to gather the material needed to more deeply understand the problems and possibilities surrounding BYOD ("Bring Your Own Device") at Lund University.

Along with Richard Johansson (Humanities and Theology) and a group of four additional project members, an investigational project was formed. By summoning expertise from the areas of law, IT security, staff health and IT support, a broad basis was formed on which the different areas for further investigation became clear.

BYOD is a multi-faceted phenomenon and many institutions are unsure how to are unsure about how to react to it. The project identified problems in the following areas:

- Legal (who owns what on both private and University devices, how to make sure that laws are being followed regarding public access, archiving)
- Human resources (managing work with weak boundaries, separating work and non-work life – both from the point of view of the employee and the employer)
- Policy (recommendations for use)
- Information overload (how not to drown in information)

On the upside, the report found that BYOD increases possibilities for employees to move across and outside the physical boundaries of the workplace. By eliminating the need of physically being at the workplace, the freedom of the information owner increases. Along with this freedom comes the implicit responsibility of not overworking and a second emphasis in the report is that of possibilities for recuperation.

Presented as a roadmap, the aim of this initial report was to present an overview of the different areas where problematic situations may arise. Even though some answers are presented along with the questions, this report has no ambitions to be "the answer" to BYOD but rather to serve as an inventory of the area and input for future, more focused, projects. At least six areas are needed to be looked into more deeply by future interdisciplinary projects.

1. Inledning

BYOD, "Bring Your Own Device", är ett samhällsfenomen som har kommit som en stormby och ställt de flesta invanda begrepp och föreställningar om IT-miljö på huvudet.

Mycket har sagts och kommer att sägas om det. I en ringhörna har vi de som menar att det är tokigt och att BYOD tillhör en curlad generation som prompt vill ha det de vill ha, när de vill ha det. I en annan ringhörna har vi de som ser fram emot att befria arbetet från arbetsredskapen och arbetsplatsen. Andra skyller på den s.k. konsumentariseringen av it-landskapet.

Projektet tar avstamp i en definition av att BYOD är ett fenomen som vilar på en ekonomisk/teknisk grund: Moores lag. Denna "lag" från 1960-talet som säger att antalet transistorer på en given yta fördubblas var 18:e månad (och därmed halveras kostnaden), har nu lett till att man för en låg kostnad kan ha en mycket kapabel elektronisk enhet[1] i bröstfickan eller handväskan. Denna enhet har i dag prestanda som överstiger en kraftfull dator för ett antal år sedan. Man kan alltså ha, och många har redan, en hel dator i fickan med alla möjligheter och risker som följer med en sådan. I takt med att tekniken fortsätter att bli billigare och mer kompetent, kommer människor att ha med sig fler enheter, varav de flesta ägs av dem själva.

Den långsiktiga trenden är att informationen håller på att frigöras från formen (d.v.s. dator och programvara). I framtidens digitala miljö kommer själva datorn att ha allt mindre betydelse: antingen är alla enheter tillräckligt kraftfulla eller så körs systemet, eller en del av det, på en dator som *är* tillräckligt kraftfull (t.ex. i molnet). Informationen, och inte hårdvaran, är navet i det digitala livet.

Samtidigt med detta ökar trenden att tjänster och funktioner personifieras. Bakgrunden är en omstrukturering av sättet att ta betalt: användarna vill ha tjänster men inte betala för dem i direkta pengar och företagen, som måste få in pengar, tar då betalt via reklam. Handelsvaran är kunskap om användaren och dennes intressen, vanor etc.

En aspekt som är ny och unik är att i och med att man har enheten fysiskt nära sig så upplevs den som mer personlig och mer som en del av en själv än vad desktopdatorn på kontoret gör. Detta förväntas öka när tekniken dyker upp på fler ställen nära vår kropp (glasögon, armband, pulsmätare etc.) och samtidigt integreras alltmer på ett sätt som gör det svårt att bryta loss dem. Denna integration centreras runt den enskilde människan just som människa och tar dåligt hänsyn till de olika roller som individen har. Ett sätt att se hur viktig t.ex. telefonen är att om man åker hemifrån utan plånbok lånar man pengar av någon men en glömd mobil åker man hem och hämtar.

Denna enhet ägs i nästan alla aspekter av den enskilde, d.v.s. både hårdvaran och de program som finns på den (en del program kan vara köpta av arbetsgivaren). Tillsammans med enheten finns en elektronisk identitet som ofta är kopplat till ett privat kreditkort.

Tillsammans med denna mognad av hårdvarusidan, har det skett en motsvarande utveckling av mjukvaran och då inte enbart den programvara som körs på enheten i

[1] Med enhet menas både handhållna enheter (telefoner och plattor) och bärbara datorer samt andra typer av elektronisk utrustning som kan lagra och/eller bearbeta information

fickan utan även tjänster mellan maskiner och framförallt i molnet, d.v.s. servrar som någon annan har ansvar för, ofta i ett annat land (med annan lagstiftning, eller med oklart rättsförhållande).

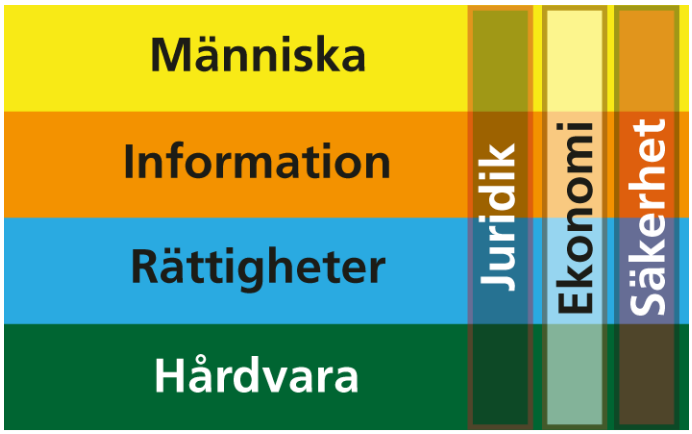
Datainspektionen rekommenderar i ”Samrådsyttrande om användning av anställdas egen utrustning i tjänsten, s.k. bring your own device-lösningar, BYOD” (se referenslista) starkt att man särskiljer tjänste- och privat information. Man poängterar att ”Ju bättre åtskillnad mellan privat- och tjänsterelaterad information desto större möjlighet att möta de konflikter som kan uppstå mellan säkerhetskraven å ena sidan och den anställdes, och andras, personliga integritet å den andra.”[2]. De anser vidare att det är av stor vikt att arbetsgivaren fredar den anställdes privatliv och information angående detta och lyfter fram arbetsgivarens stora ansvar i denna fråga. För att underlätta detta rekommenderar projektet att LU implementerar en tydlig hållning avseende tjänstemobiltelefon.

I och med att man har en hel dator i fickan, en dator som man själv äger och administrerar och som hela tiden får mer och mer funktionalitet, så sker ett antal saker:

- mängden information som presenteras för en människa ökar.
- antalet enheter man arbetar med ökar och då gäller det att man kan nå sin information från alla dessa enheter.
- möjligheten att jobba var som helst och när som helst ökar.
- den anställde kan följa med i jobbet fastän man är hemma. Sjukdom kan vara rent fysisk (som t.ex. en bruten fot) och BYOD vidgar gränserna för när den anställde potentiellt kan arbeta.
- när det gäller kompetensutveckling blir det möjligt att nätverka och omvärldsbevaka fastän man inte är på jobbet. Den anställde kan genomgå webbkurser oavsett tid och plats. Globalt sett gör BYOD det möjligt att delta i en utbildning eller webbinar även på annan tid än svensk arbetstid.
- vikten av att användaren har ett kunskapsöverläge i denna flora av möjligheter accentueras.
- gränserna mellan arbete och privatliv luckras upp.
- förmågan att kunna hantera denna gränslöshet blir allt viktigare.

[2] ”Samrådsyttrande om användning av anställdas egen utrustning i tjänsten, s.k. bring your own device-lösningar, BYOD”, sida 1-2 (se referenslista)

Projektet lägger fram följande skiktmodell för att enklare se de olika delarna av BYOD-kakan:



Förklaring av de olika nivåerna, uppifrån och ner:

1. Människan
   Här är de saker som har med den mänskliga sidan av BYOD: att alltid kunna bli nådd, att alltid kunna arbeta o.s.v.
2. Information
   Här hanteras den information som bearbetas.
3. Rättigheter
   Programlicenser och tjänsteavtal hör hemma här (dock inte enhetens medlevererade dito). Exempel: AppleID och hur man hanterar det.
4. Hårdvara
   Själva enheten och allt kring den: inköp, underhåll, reparationer, medlevererad programvara etc.

Vertikalt genom dessa skikt löper de tre aspekterna juridik, ekonomi och säkerhet.

I behandlingen (punkt 9) kommer vi i huvudsak att använda oss av skiktmodellen för att redovisa vår syn på området.

2. Bakgrund till projektet

Projektet kom till genom att Peter Möller på Datavetenskapliga institutionen tog kontakt med John Westerlund på Rektorskansliet och frågade om LU hade någon hållning kring BYOD. Det hade man inte, men ville gärna ha hjälp att komma fram till en sådan och därmed var bollen i rullning.

2.1. Projektgruppens sammansättning

Projektet gavs till Peter Möller, Datavetenskap (Peter.Moller@cs.lth.se). Richard Johansson, HT (Richard.Johansson@ht.lu.se), uttryckte tidigt ett starkt intresse av att vara med och dela projektledarskapet. Övriga medlemmar i projektgruppen är:

- Anne Link, Företagshälsovården
  Företagshälsovården möter anställda i olika roller och tedde sig en naturlig part för

projektet. Man var dessutom från Företagshälsan mycket intresserade av projektets mjuka sidor som man ser som ett potentiellt stort framtida bekymmer.

- Magnus Persson, LDC
  Säkerhet är Magnus område i hans vanliga tjänst och det tedde sig naturligt att ta del av hans omfattande kunskaper och erfarenhet på området.
- Fredrik Edman, LU Innovation System
  Frånsett personnummer och outgivna tentor är patent det som är känsligast för LU. På LU Innovation System hjälper man forskare att navigera på detta fält och man har dessutom i det området en stor mängd legala frågor att känna till/ta ställning till.
- Jens Nockert och Vanja Tufvesson, studenter
  Studenter är inte bara "konsumenter" av universitetets tjänster utan även i en hel del fall blivande anställda. Eftersom deras sinnen inte är lika grumlade av gamla föreställningar som vi äldre, och de dessutom ofta ligger närmre den tekniska framkanten, är det en stor tillgång att ha dessa båda studenter som bollplank. Jens Nockert är kåraktiv med stort kunnande och tillika kontaktnät. Vanja Tufvesson har förutom flera års studier vid LTH dessutom tillbringat två år vid ett universitet i Australien och kan alltså tillföra ett utifrånperspektiv som är mycket nyttigt.

Härutöver har kontakt tagits med Sektion Personal (Mona Hansson) och sedan vidare med Juridiska sektionen. Möte har hållits med Carl Pettersson för att få klarhet i de juridiska frågorna.

3. Målgruppsdefinition

Målgrupperna för denna slutrapport är indelade i tre nivåer, främst med utgångspunkt i projektets uppdragsgivare och dess leveransmål med utredningsprojektet. Då vi från projektgruppen tidigt identifierat andra potentiella målgrupper inom ämnet, har vi även valt att ta med en andra och tredje ordningens målgrupp.

3.1. Första ordningens målgrupp

I första hand vänder sig denna rekommendationsskrift till personer som har mycket stort inflytande på organisationens IT-policyer (främst John Westerlund, Andreas Wikfeldt, Karl Ageberg) och från vilka dokument och rekommendationer som flödar ut från organisationscentralt håll. Dessa personer förutsätts ha mer än enbart grundläggande kunskaper om de på marknaden tillgängliga plattformarna på vilka BYOD florerar.

3.2. Andra ordningens målgrupp

De som skall driva nästa leds projekt vari man verkligen kommer att arbeta mot konkretion av våra rekommendationer alternativt studera problemområden på ett större djup. Detta kan och eventuellt bör vara personer som även de har en mer än grundläggande kunskapsnivå på respektive område där de sätts till att arbeta vidare. Dock bör poängteras att även dessa personer förutsätts ha åtminstone grundläggande kunskaper kring de tekniska fenomen på vilka BYOD-fenomenet uppkommit.

3.3. Tredje ordningens målgrupp

IT-personal på andra universitet i Sverige. Dessa befinner sig i flertalet fall i fasen "klia sig i huvudet" och kommer med intresse ta del av vad man kommer fram till, och hur man tänker bland dem som "gått före". Här har arbetsgruppen inte valt att ta hänsyn till vilka

bakomliggande kompetenser som finns hos denna målgrupp. Snarare är innehållet att betrakta såsom en grundläggande utredning vid Lunds Universitet, på vilken man sedan kan välja att bygga vidare utifrån respektive delämnesområde.

4. Termen BYOD

Termen BYOD kan tyckas vara klar och tydlig men det täcker endast delar av *fenomenet* BYOD. Projektets referensgrupp (SamIT-gruppen vid LU) kritiserade projektet för att man trodde att det handlade om just B-Y-O-D (alltså hantera smarta telefoner) medan projektgruppen/ledningen hade valt att tolka det betydligt bredare:

- tekniska aspekter av enheterna
- programvarulicenser på dessa
- tjänster som springer ur BYOD (molnlagring etc.)
- arbetsrelaterade aspekter

Även om man kan sträva efter att hitta en bättre benämning, tror vi att det bästa är att hålla fast vid BYOD men förklara att det handlar om mer än smarta telefoner.

5. Om BYOD vid LU

Vi saknar mätvärden för att säga något definitivt om hur utbrett BYOD är vid LU i nuläget (2013). Projektet har heller inte någon ambition att kvantifiera BYOD-situationen vid LU utöver att översiktligt konstatera att det (bland personal):

- är mycket vanligt med privata smarta telefoner
- är ovanligt med LU-ägda smarta telefoner
- är mycket vanligt med omvänd BYOD (privatbruk av jobbdatorn)
- börjar bli vanligt med surfplattor

För studenter är det ännu vanligare med smarta telefoner och plattor.

Projektet kan dock se att det inte handlar om att ”införa” BYOD vid LU, det är redan här, utan att hos LUs ledning skapa en tydlig förståelse för vad BYOD innebär. Detta bör sedan ligga till grund för rekommendationer från LU:s ledning till de anställda.

6. Uppdraget

Uppdraget från John Westerlund är detta:

Hur skall ett arbete läggas upp för att komma fram till en LU-gemensam rekommendation kring fenomenet BYOD?

- Identifiera och dokumentera fördelar med BYOD och vad vi kan göra för att maximera dessa fördelar
- Identifiera och dokumentera nackdelar med BYOD och vad vi kan göra för att hantera/minimera dessa nackdelar
- Vilka grupperingar är relevanta målgrupper
- Hur kan en tidplan för ett sådant arbete se ut

Det långsiktiga resultatet är dels en rekommendation och dels ngn form av handlingsplan för genomförande.

7. Avgränsning

En nödvändig avgränsning på detta stadium är att det inte kommer bli någon djupare behandling inom något specifikt problemområde samt att bi-områden, t.ex. skattemässiga problem, inte avhandlas annat än ytligt.

Utredningen kring BYOD-fenomenet är primärt tänkt som ett inspel till fortsatta utredningsprojekt, som i sin tur har som leveransmål att producera konkreta riktlinjer och rekommendationer för organisationen. Den primära orienteringen skall vara att peka på områden som behöver utredas vidare. Vidare även att inom ramen för dessa områden, visa på förslag på underområden där vidare utredning är mer eller mindre viktiga. Eftersom projektet funnit fler relevanta områden än förmodat, blir en handlingsplan en fråga för respektive kommande underprojekt (se de sammanfattande rutorna i slutet av varje avsnitt).

Projektet behandlar inte mätning av BYOD vid LU, främst med hänvisning till att det i dagsläget inte finns någon gemensam lösning för att mäta den totala användningen. Dock är en sekundär orsak till att vi valt att inte inkludera en sådan mätning, just att mätsiffrorna väntas bli inaktuella innan utredningen är färdig eller dess efterföljande underprojekt kommit till någon färdig slutsats.

8. BYOD i omvärlden, specifikt universitetsmiljö

Universitet har en särställning jämfört med industri/näringsliv i BYOD-hänseende eftersom:

- studenterna till mycket stor del är BYOD; de har i allt högre grad med sig sina egna enheter och arbetar på dem, parallellt med att använda skolans utrustning.
- många anställda började sina universitetsliv som just studenter och har därigenom med sig det gränslösa förhållningssättet från studietiden.
- mycket av det universitetet producerar är genom lag offentligt.
- olika typer av känsligt/hemligt material förekommer.
- forskaren äger själv rätten till sina resultat genom lärarundantaget.

Många universitet är medvetna om att BYOD finns, men få har hittills tagit tag i frågan på allvar. Några undantag finns dock.

University of Oregon har publicerat en litteraturstudie med titeln: "Factors for Consideration when Developing a Bring Your Own Device (BYOD) Strategy in Higher Education"[3]. Denna är väl värd att läsa för att söka inspiration för kommande projekt.

KTH i Stockholm har en klar policy för hur man hanterar egenadministrerade datorer, men inget om egentlig BYOD. De har även ett antal publika skrifter som är väl värda att studera, t.ex. "Ansvar, befogenheter och skyldigheter för systemadministratör" (se referenslista).

[3] Samtliga webblänkar finns utskrivna i referenslistan sist i dokumentet

9. Rapport från de undersökta områdena

9.1. Människa – ”Hälsomässig gränsdragning”

Alla individer är olika, vill ha olika gränser och har dessutom olika förmåga att sätta gränser. Många arbeten innebär att man har kollegor och kontakter i olika länder och tidszoner. Det gäller att skapa förutsättningar för att jobba gränslöst och samtidigt ha möjlighet att styra över sin egen tid och för att på sikt behålla hälsan.

Det är av vikt att diskutera tillgänglighet och gränslöshet på arbetsplatser och skapa gemensamma överenskommelser, riktlinjer och rekommendationer. Primärt handlar det inte om att få skarpare gränser utan hitta bra sätt att hantera gränslösheten.

Frågor som ett efterprojekt bör utreda vidare:
- Vilka krav på flexibilitet och tillgänglighet kräver verksamheten?
- Hur kan LU underlätta den anställdes möjligheter till återhämtning?
- Vilka IT-behov har de anställda?
- Ska vi ha ambitionen att inte ringa eller mejla på kvällstid?
- Man bör även titta på hur den informella kulturen ser ut. Vilka normer och värdegrunder finns det idag?
- Hur upptäcker man personal som är i riskzonen för stressjukdomar?
- Hur hanterar man de upptäckter man gör?
- Vem ansvarar för handlingsplaner gällande dessa upptäckter?

Den moderna IT-miljön (inte endast fenomenet BYOD) är en miljö som alltmer karakteriseras av ökat informationsflöde från ett ökat antal källor och att människor samtidigt är både mer sammankopplade elektroniskt men, paradoxalt nog, mer isolerade från varandra (vi sitter bredvid varandra och tittar i varsin telefon/surfplatta). Det tar 3-5 minuter för en människa att byta fokus i sitt arbete och oansad riskerar den moderna IT-miljön att innebära fler uppmärksamhetskrävande avbrott. Projektet anser att det är av stor vikt att LU aktivt arbetar med prevention av stressrelaterade arbetsskador[4].

Det finns anledning att överväga en mänsklig kontaktpunkt för anställda för BYOD-relaterade uppgifter/frågor.

I det personliga mötet kan ett antal goda saker ske:
- den anställde upplever att arbetsgivaren bryr sig.
- LU får en god möjlighet att få ut viktig information (t.ex. policy).
- det blir en naturlig kanal att få information, synpunkter, kritik etc. *tillbaka* till LU.

Det finns också en risk att de som inte följer med (eller följer med för mycket) i den tekniska utvecklingen kommer att drabbas av ”informationsångest” och både blir mindre produktiva och hamnar i riskzon för ohälsa.

[4] Teorell, Thöres,professor emeritus, Karolinska Institutet. *Det moderna livet stressen och hälsan*. Statens Folkhälsoinstitut.

9.1.1. Gränslöst arbete

Det finns ett relativt nytt forskningsområde benämnt ”gränslöst arbete” och som utforskar detta nya sätt att arbeta.

Gränslöst arbete KRÄVER:

- Hög grad av planering och strukturering av arbetet, egen gränsdragning mellan olika roller.
- Skapandet av egna sociala kontaktytor.
- Ständig anpassning till nya förhållanden.

Gränslöst arbete ger MINSKAD stressbelastning genom:

- Hög grad av kontroll och inflytande över eget arbete.
- Hög grad av variation, omväxling, flexibilitet.
- Ökade möjligheter att kombinera olika roller.

Gränslöst arbete ger ÖKAD stressbelastning genom:

- Obegränsade arbetsuppgifter, höga krav.
- Svårigheter att hålla isär olika roller.
- Lågt socialt stöd.
- Förändringsstress.

Gränslöst arbete påverkar sannolikt kvinnors arbetssituation mer än mäns genom att kvinnor fortfarande har huvudansvaret för de flesta obetalda sysslorna i hemmet.

Gränslöst arbete innebär en frihet som i sin tur förutsätter en förmåga att ta ansvar, för sitt arbete men också för sin fritid. Återhämtning[5] liksom flexibilitet och frihet är en kritisk förutsättning för att kunna vara kreativ vilket är en viktig del av LU:s kärnverksamhet. För att ha koll på att balansen arbete/fritid inte blir sned blir ledarskap och personalvård viktigare än tidigare och det är viktigt att de olika nivåerna av ledning har klart för sig hur det faktiskt går för medarbetarna. Det bedrivs aktiv forskning inom området, t.ex. forskar Fil Dr Christin Mellner, Institutionen för Psykologi, Stockholms universitet, om ”gränser mellan arbets- och privatliv” och det finns all anledning att hålla sig à jour med den pågående forskningen på detta område.

Med syfte att både hjälpa personalen att värna fritid och återhämtning och att samtidigt lösa potentiella försäkringsproblem, rekommenderar projektet LU att föreslå institutioner/enheter att de överväger att skaffa kassaskåp för personalbruk. I ett sådant kan anställda själva låsa in och hämta ut känslig utrustning. Problem som kan lösas med detta är:

- Den anställdes återhämtningsmöjligheter fredas då utrustningen befinner sig på jobbet
- Anställda behöver inte fundera över försäkringsaspekten när de är på semester
- Mobil utrustning är säkert förvarad och därmed mindre stöldutsatt

Det systematiska arbetsmiljöarbetet (SAM) är viktigt att lyfta fram för att uppmärksamma och hantera det gränslösa arbetet. Detta bör tas i beaktande vid utvecklingssamtal och i kompetensutvecklingsplanering. Enligt SAM skall det regelbundet ske arbetsplatsträffar (APT), utvecklingssamtal och psykosociala skyddsronder på arbetsplatsen. Detta är ett

[5] Forskningen kring återhämtning är i sin linda; man vet att det är mycket viktigt, men inte mycket mer (Docent Petra Lindfors, Institutionen för psykologi, Stockholms Universitet)

forum som stimulerar dialog och fysiska mötet på både organisations-, grupp- och individnivå.

Sammanfattning av "9.1 Människa":
Det gränslösa arbetet ger oss en möjlighet att själv styra över vårt arbete och att arbeta med människor över hela världen.
Vårt sätt att kommunicera har förändrats och utvecklats i samband med teknikens snabba utveckling. Detta leder till att gränsen mellan fritid och arbete blir otydlig, vilket i sin tur kan leda till ohälsa.
Organisationen och individen bör därför förhålla sig till detta genom ökad kunskap och tydliga strategier hur vi ska hantera det gränslösa arbetet. Projektet rekommenderar att LU implementerar en tydlig hållning avseende tjänstemobiltelefon.

Rekommendation om efterkommande projekt/arbete:
LU bör ägna ökat fokus åt det systematiska arbetsmiljöarbetet, avseende både implementation och uppföljning. Vidare bör LU öka sin kompetens och avsätta resurser för utbildning inom det gränslösa arbetet.

9.2. Information

Lunds Universitet har på sig en statlig myndighets krav på arkivering och hantering av information. I den moderna informationsmiljön kommer informationen att dels hanteras mer som dussinvara och dels flyta alltmer fritt mellan hårdvaruplattformar och mjukvarutjänster. Det är då en viktig uppgift för Universitetet att göra klart för sina anställda att arkivplikten fortfarande gäller (alltså även för BYOD-lagrad information), för vilket slags material det gäller samt att visa på användbara vägar för att kunna göra detta.

LU bör ha rutiner för den information som skall vara hemlig.

Ökad informationsmängd är en av konsekvenserna av BYOD. Därför bör en av åtgärderna vara en god ”informationshygien”, inte endast information om BYOD utan egentligen all information LU hanterar. Det innebär:

- tydlighet: avsändare, målgrupp, giltighetstid bör framgå klart.
- tydliga strukturer för att hitta information:
  - webbsidors visuella navigation.
  - papperskopior bör ha någon form av ”hemvist”.
  - url-uppbyggnad (används av få, men är en vinnande flirt med mera avancerade användare).
- det går inte att nog understryka vikten av att rätt och relevant information går att hitta i sökmotorer.
- utdaterad information skall antingen märkas med tydlig information om att den är utdaterad eller helt enkelt städas bort.

Vad gäller regelverk kring BYOD (och reverse-BYOD) vid LU kan det inte nog understrykas vikten av en tydlig information från myndighetens ledning från dag 1! Det måste stå klart att ledningen förstår vad BYOD är och har en policy som man står bakom. Det bör också vara tydligt hur information strömmar tillbaka till arbetsgivaren (vem kontaktar man om för förbättringar, synpunkter o.s.v. – inte nödvändigtvis rektor)! Om informationen från arbetsgivaren är tydlig och användningen reglerad (så att det är tydliga gränser mellan tjänste- och privatbruk) är BYOD-utrustning att betrakta som LU-ägd utrustning[6]. Datainspektioner menar vidare att ”Som generell utgångspunkt gäller att arbetsgivare som har personuppgiftsansvar måste ha tekniska förutsättningar att på lämpligt sätt ha möjlighet att följa upp att den anställde lever upp till den personuppgiftsansvariges krav på personuppgiftsbehandlingen och verkligen följer de riktlinjer och krav som finns.”

Exempelvis måste det vara klart:

- vad som är tillåtet bruk, d.v.s. vad som täcks av försäkringar och kommer att vinna stöd hos arbetsgivaren.
- vad som är otillåtet bruk – det omvända mot ovan.
- vilken utrustning som kommer i fråga.
- vad gäller den personliga integriteten på både BYOD- och LU-utrustning.
- vilka säkerhetsregler som gäller och de viktigaste sakerna att tänka på för plattform X, Y och Z.

[6] ”Samrådsyttrande om användning av anställdas egen utrustning i tjänsten, s.k. bring your own device-lösningar, BYOD”, sida 3 (se referenslista)

Projektet bedömer att ett antal frågeställningar måste kommuniceras klart till de anställda, följande är exempel på sådana (denna lista behöver dock bearbetas/kompletteras av kommande underprojekt):

Frågeställning	LU-ägd utrustning	Privat utrustning
Gäller arkivplikten	Ja	Ja, om arbetsrelaterat
Får installera programvara från LU	Ja	Se tabell under 9.3
Får installera privat anskaffad programvara	*LU bestämmer själva om detta är godtagbart*	Ja
Gäller försäkring	Ja men självrisken är ett basbelopp	Kontrollera privat försäkring
Kan jag få support på enhet / programvara	Ja	Ingen utöver befintliga guider
Kan jag få backup	Ja	Nej
Kan jag använda eduroam (vid LU & utanför)	Ja	Ja
Får jag lagra / bearbeta personuppgifter	Ja	Nej
Får jag lagra sekretessbelagd information	Ja, krypterad	Nej
Får jag arbeta med personuppgifter mot ett VDI-system vid LU	Ja	*Detta är en fråga för LU att besluta om*
Får jag arbeta med sekretessbelagd information mot ett VDI-system vid LU	Ja	*Detta är en fråga för LU att besluta om*
Får jag använda synktjänst X, Y, Z	Ja, box.net[7]	Inte för arbetsrelaterat material
Får LU spåra mig (GPS / foto etc.)	Nej	Nej
Gäller offentlighetsprincipen (d.v.s. kan information komma att lämnas ut)	Ja, dock ej information som är av privat natur, har kommersiellt värde, etc.	Om det är material som har samband med arbetet inom myndigheten, ja

Sammanfattning av ”9.2 Information”:
LU behöver tydligt och kortfattat kommunicera de regler som gäller för information och informationshantering, på arbetsplatsen och utanför. Det är en utmaning att se till att relevant information inte drunknar. LU behöver arbeta fram policy-dokument för att styra upp användningen av BYOD.

Rekommendation om efterkommande projekt/arbete:
LU bör tillsätta ett projekt med uppdrag att ta fram policy för BYOD och reverse-BYOD.

[7] För överföring av personuppgifter till tredje land, ett land utanför EU och EES, finns restriktiva bestämmelser i 33-35 §§ personuppgiftslagen (PUL, se referenslistan)

9.3. Rättigheter

För att inte bryta mot licensregler kan man göra på ett antal olika sätt:

- Komplettera asset management och mjukvarudistribution med BYOD-verktyg. Företag behöver verktyg som kan spåra och hantera en bred mix av användarenheter, för vilket man behöver en formell policy. En sådan måste stipulera att om en användare vill använda en egen enhet så måste IT-personal få komma åt enheten för att kunna säkerställa att mjukvaruavtal hålls.
- Skaffa en företags-App Store 60% av IT organisationerna i USA planerar att sjösätta en egen App Store till 2014.
- Tillhandahålla access till program via VDI[8], vilket kraftigt förenklar licenshanteringen.
- Flytta till en moln-modell. Många använder SaaS (Software as a Service) för e-post, men även andra tjänster. Även detta förenklar licenshanteringen.
- Uppmana anställda att skaffa ett privat betalkort (Eurocard) för vilket LU betalar årsavgiften. Den anställde kopplar detta kort till en elektronisk identitet knuten till sin LU e-post. Därefter ansöker den anställde om kostnadsersättning från LU i form av ett normalt reseutlägg.

Problemet med App store-identiteter gentemot Apple, Google, Microsoft m.fl. är problematiskt. I fallet att den anställde får en tjänstetelefon (exempelvis) är det enkelt: då rekommenderar projektet att den anställde skaffar a) en identitet hos leverantören (t.ex. Apple) kopplad till sin LU-mail och b) ett LU-privatkort. Projektet rekommenderar att denna identitet skall avslutas[9] då anställningen upphör. Om det däremot är en privat enhet kan det bli problematiskt. Denna har med allra största sannolikhet redan en elektronisk identitet, kopplad till den anställdes privata e-postadress och dito kreditkort. Om den inte har en identitet med giltig betalningsinformation kan LU:s privatkort komma ifråga. Detta behöver dock utredas vidare av LU. I båda fallen sker den ekonomiska ersättningen via reseutlägg i Primula res. Mer om rättigheter och ekonomi står under 9.7.3.

Lösningar är sakta på väg vilka kan hantera flera identiteter i en enhet – Apple har t.ex. ”VPP” (Volume Purchase Program), men det går mycket sakta för dessa lösningar att komma ut utanför USA.

Android kan hantera multipla konton. Google har en möjlighet att knyta flera konton till samma enhet och på så sätt få tillgång till de appar som är knutna till respektive konto. På så sätt kan en enda enhet hanteras via flera konton, även om ett av dem är s.k.primärt konto. Detta öppnar en möjlighet för LU att hantera appar som betalts med LU-medel via ett LU-knutet Google-konto.

Microsoft Phone kan inte hantera flera konton. I Microsoft Store är endast ett konto möjligt att använda per Store, medan man kan ha ett enstaka Store-konto till flera inloggade användarkonton i en dator. I telefoner är det dock endast ett konto per telefon i nuläget, men i takt med en ökad BYOD-användning ser projektet det som troligt att även detta kan komma att ändras

---

[8] VDI = Virtual Desktop Infrastructure, en programvara med vilken man kan komma åt en full skrivbordssession på en dator som står någon annanstans. Man kan t.ex. komma åt en centralt driven Windows-miljö från en iPad eller en enkelt utrustad PC.

[9] I fallet Apple: manuell procedur genom att kontakta Apple: http://www.apple.com/se/contact/ I fallet Google loggar man in på sitt konto för att där stänga sitt konto. Samma sak gäller fallet Microsoft.

iOS och OS X (Apple) kan med viss möda hantera flera konton (man får logga ut och in mellan de olika kontona). Apple har en lösning, ”VPP” (Volume Purchase program), som löser dessa problem, men det finns inte i Sverige ännu. Det finns två sätt att lösa betalningen av program för iOS och OS X (se även 9.7.3):

1. Huvudlösning: skaffa ett LU-sponsrat Eurocard och ange det som betalning i App Store. Gör sedan en traditionell reseutläggsersättning i Primula.
2. Köp presentkort (detta är dock förmånsbeskattningsbart). Man kan ha ett befintligt AppleID utan angiven betalningsinformation och i efterhand lägga till betalningssättet ”Inget”. Institutionen/enheten köper sedan GiftCard (mot faktura) för att handla program som kostar något.

Det är värt att notera att man kan ha *olika* AppleID för att hantera programvara, kalender, kontakter etc.

Följande är en tabell över programvara som LU har licensavtal på och hur den kan installeras på olika datorer:

Företag / program	Kan installera på privat utrustning	Student kan installera
Adobe	Ja	Nej
Alfasoft (EndNote)	Ja	Ja
Apple	Nej	Nej
FileMaker	Ja	Nej
Matlab	Ja	Ja
Microsoft Office	Ja	Nej
SAS	Nej	Nej
SPSS	Ja	Nej
Symantec	Nej (kan fås billigt)	Nej
VMware	Nej	Nej
Wolfram (Mathematica)	Ja	Nej
WordFinder	Nej	Nej

Sammanfattning av ”9.3 Rättigheter”:
Det finns i dagsläget inte något enhetligt och enkelt sätt att knyta en anställds programvaruköp till LU utan de knyts praktiskt taget alltid till den enskildes konto hos respektive leverantör.

Rekommendation om efterkommande projekt/arbete:
LU bör tillsätta ett projekt för att utreda hur programvaror som köps in till privatägda enheter ska hanteras.

9.4. Hårdvara

MDM-lösning

Med utgångspunkt i att det kommer fler och fler enheter som kan räknas in under BYOD-termen så ställer detta krav på arbetsgivaren att kunna veta vad dess anställdas enheter har för sig (dock utan att kränka integriteten). För att kunna göra detta behövs någon form av hanteringsprogramvara, Mobile Device Management system (MDM). Från projektet kan vi se att det primärt finns tre syften som alla kan uppfyllas med ett MDM-system:

- installera programvara på enheten.
- säkerställa att en viss grundnivå på säkerhet uppfylls i enheten.
- säkerställa att en stulen enhet snabbt kan sättas ur funktion eller fjärrtömmas (främst för enkel radering eller otillgängliggörande av sekretessbelagd information).

Då det finns ett större antal MDM-lösningar på marknaden så behöver det sättas upp någon slags kravbild över vad man från LUs sida vill kunna göra med sina anställdas enheter respektive vad man vill förhindra sina anställda att göra med dessa enheter. Båda aspekterna är något som ställer krav på MDM-lösningar och därför något som bör bli föremål för någon slags utredning eller upphandling.

Facket bör bjudas in för att förankra lösningen.

Oaktat att LU centralt kan sätta upp eller rekommendera någon MDM-programvara så bör det likväl vara varje institution/fakultet fritt att välja lösning, så länge den svarar mot en lägstanivå som rimligen bör sättas i samråd med IT-säkerhetspersonal på LDC. En sådan lösning bör då också vara framtidssäkrad så att nuvarande och framtida operativsystem för respektive plattformar säkert kan hanteras och så att en infrastrukturell satsning kan ge avkastning även under längre tid, oberoende av plattformsbyten på de olika enheterna.

En infallsvinkel som kan vara intressant för LU att ta ställning till, är huruvida man bör styra hanteringen av MDM-lösningar och huruvida det skall utses en enda MDM-lösning som sedan driftas centralt. Om LU fattar ett sådant beslut, kan sedan varje fakultet/institution få delegerat ansvar för respektive underavdelning, medan man centralt kan säkerställa en överblick över hela beståndet.

Sammanfattning av ”9.4 Hårdvara”:
För att säkerställa att anställdas information inte sprids till obehöriga behövs någon form av system för att säkra upp framförallt mobila enheter. Ett sådant skulle kunna hanteras centralt på LU.

Rekommendation om efterkommande projekt/arbete:
LU bör tillsätta ett projekt för att utreda och eventuellt upphandla ett system för att kunna styra och göra information på mobila enheter otillgänglig vid stöld eller förlust.

9.5. App-utveckling: ömsesidigt samspel

Både för att förankra BYOD i organisationen och för att (faktiskt) möta ett reellt behov, rekommenderar projektet att LU allvarligt överväger att ta fram en eller par Appar för tillämpliga plattformar riktat mot personal och mot studenter (ev. en för varje målgrupp).

Denna/dessa App(ar) bör karakteriseras av:
- relevans.
- uppdaterad såväl till information som funktion.
- att både ge och ta, för att på så sätt göra den attraktiv för användarna.

Funktionalitet man kan tänka sig att ha med är:
- hantera sin semester/sjukfrånvaro, kontrollera lön (läs: Primula).
- hantera sin fasta telefonanknytning.
- hantera reseräkningar för forskare på resande fot (eller åtminstone stöd för detta).
- visa en personlig agenda.
- nyhetsinformation (kalendarium).
- söka information inom LU, t.ex. leta reda på vem som har ett visst telefonnummer, vilket hämtställenummer en viss anställd har etc.
- hitta både till Lund och inom LU.

Från studenthåll har vi fått tips om labbanmälning där man skulle kunna få information om kötider i olika salar och ställa sig i kö för labbar eller övningsassistans. Relevanta plattformar för en sådan är såväl dator som telefon/platta med den skillnaden att datorn kan antas vara nätansluten medan telefonen/plattan inte kan antas vara nätansluten och alltså måste ha en del av informationen på enheten.

Sammanfattning av ”9.5 App-utveckling: ömsesidigt samspel”:
Att erbjuda anställda en ”morot” kan vara ett fungerande sätt att sälja in en BYOD-policy. Det finns reella behov som skulle fyllas av en sådan strategi.

Rekommendation om efterkommande projekt/arbete:
LU bör vidare utreda såväl de tekniska aspekter av egna appar som de ekonomiska möjligheterna att bedriva sådan utveckling.

9.6. Juridik

De juridiska aspekterna av BYOD är svåra att definiera. Detta främst eftersom området i sig är mycket brett och kan omfatta många aspekter. Några viktiga frågor som identifierats är:

- Vem äger utrustningen?
- Vem ansvarar för utrustningen och dess säkerhet?
- Vem sköter utrustningen?
- Sekretess (vad för information hanteras på anställdas enheter)
- Övervakning – när får man göra vad?

Det är viktigt att tillfråga jurister, HR och anställda vid framtagande av rekommendationer och policys som rör dessa utmaningar.

Vid kontakt med Juridiska enheten (Carl Petersson) vid Lunds universitet har följande lagar bedömts ha direkt påverkan gällande BYOD:

- tryckfrihetsförordningens (1949:105) kapitel 2 om offentlighetsprincipen
- offentlighets- och sekretesslagen (2009:400) i sin helhet
- personuppgiftslagen i sin helhet (1998:204)
- lagen om ansvar för elektroniska anslagstavlor (1998:112)
- arkivlagen (1990:782)
- för Medicinska Fakulteten även patientdatalagen (2008:355)

Även lagar som är kopplade till det immaterialrättsliga området är viktiga att beakta, speciellt när det gäller material som har och göra med kommersialisering och forskningsmedelsansökningar.

9.6.1. Juridik – Människan

Det är viktigt att anställda förstår innebörden av offentlighetsprincipen och effekten på det arbete man utför i tjänsten på privat elektronisk utrustning. De gällande regelverken kring offentlighet, sekretess och personuppgifter påverkar material som anställda lagrar på privat utrustning och myndigheten har ett ansvar enligt gällande lagstiftning för att t.ex. allmänna handlingar lämnas ut eller att den personliga integriteten inte kränks. Detta ansvar måste givetvis utövas efter noggrann prövning i det enskilda fallet. Dock finns det en viss okunskap om detta, varför projektet rekommenderar att LU har en tydlig kommunikation till den anställde om vad som gäller. Rekommendationen från Datainspektionen[10] gällande att skilja mellan privat- och tjänsterelaterad information bör på ett tydligt sätt kommuniceras ut till den anställde.

Projektet har varit i kontakt med Sektion personal (Mona Hansson) och följande har framkommit som viktiga punkter:

- Försäkringsområdet.
- Tydlig kommunikation till den anställde.
- Frågan om skatteförmån bör utredas (se 9.7.3).

[10] "Samrådsyttrande om användning av anställdas egna utrustning i tjänsten, s.k. bring your own device-lösningar, BYOD" (se referenslista)

Arbetsrätt

Fackets inblandning i BYOD anser projektet vara tydlig och de fackliga organisationerna skall hållas informerade och efterhand beredas möjlighet till synpunkter kring arbetets fortgång i de olika leden. Därför rekommenderar projektet, i enlighet med MBL, att alla underprojekt aktivt bjuder in fackliga organisationer till diskussion och interaktion vid framtagandet av handlingsplaner och rekommendationer.

9.6.2. Juridik – Information

All elektroniskt sänd information kan läcka till andra än den tänkta mottagaren och därför bör inte sekretessbelagd information sändas som e-post. Om sekretessbelagd information av någon anledning måste sändas via e-post så rekommenderar projektet att den bör vara krypterad. Sekretessbelagd information ska hanteras säkert, oavsett hur eller var den hanteras. Projektet rekommenderar att sekretessbelagd information lagras krypterat med krypterat filsystem som lägstanivå och krypterad fil som rekommenderad nivå. Immaterialrättsligt material bör skickas i krypterad form över nätet.

Molntjänster

Med molntjänster menas i denna skrift en teknik där stora skalbara resurser, exempelvis processorkraft, lagring och funktioner, tillhandahålls som tjänster på Internet.

I dagsläget bör man inte lagra vare sig immaterialrättsligt material eller sekretessbelagd information i ”molnet”. Om man av någon anledning temporärt behöver lagra sådan information i molnet, t ex. vid överföring av material mellan två datorer, skall detta vara i krypterad form. Även bearbetning av sådant material i en molntjänst bör i dagsläget undvikas så långt som möjligt.
Vidare rekommenderas att affärsmässigt material såsom immaterialrättsligt material (t ex patent, mönster, företagshemligheter etc) bör lagras i krypterad form oavsett om den ligger lagrad på en privat enhet (t ex. hemdatorn, privat mobiltelefon, privat läsplatta, etc.) eller på en av universitetets datorer/server.

Man bör även iaktta försiktighet när det gäller att lagra och sprida upphovsrättsskyddat material via olika molntjänster. I vissa länder är det fritt att göra kopior av upphovsrättsskyddat material för enskilt bruk och i vissa fall även lagligt att sprida dessa inom en nära krets, medan det i andra länder är förbjudet. Problem kan då uppstå t.ex. när användaren delar material mellan olika länder via molntjänsten. Molntjänsten kan omfattas av ett lands lag medan avsändaren och mottagaren av t.ex. en upphovsrättsskyddad fil är lokaliserade i vars ett annat land med olika upphovsrättsregler.

Att i en molntjänst behandla uppgifter som är skyddade enligt Personuppgiftslagen kan projektet se som potentiellt problematiskt (se t.ex. bestämmelser i 33-35 §§ Personuppgiftslagen gällande förbudet mot överföring av personuppgifter till tredje land). I dagsläget har projektet tolkat de svenska universitetsnätverkens avtal med lagringsleverantören Box som att det dock ger användare möjlighet att kunna lagra och behandla uppgifter skyddade av Personuppgiftslagen.

Sekretessbelagd information

Sekretessbelagd information bör lagras på en av universitetet avsedd och kontrollerad enhet och inte i privata enheter. Därför rekommenderar projektet att synktjänster såsom Dropbox och Box, bör undvikas för sådan information.

Angående arkivering

Myndigheters handlingar är i allmänhet offentliga och skall behandlas i enlighet med arkivlagen. Regler kring arkivering och gallring finner man i LU-dokumentet Bevarande- och gallringsplan för forskningsmaterial. Ett problem som kan uppkomma i samband med arkivering och BYOD är att material och korrespondens som finns lagrad på privata enheter inte arkiveras i enlighet med arkivlagen eller att informationen inte gallras i enlighet med gallringsreglerna.

9.6.3. Juridik – Rättigheter

Projektet ser att det finns en problematik i ägandeskapet av programlicenser. Detta gäller såväl BYOD[11] som Reverse-BYOD[12]. Då licensrättigheterna i de moderna AppStor-arna oftast är knutna till den enskilde och hennes privatekonomi, behöver detta tittas djupare på:

- hur säkerställer man att LU-betald programvara endast utnyttjas i tjänsten samt
- hur säkerställer man att köpt programvara återlämnas vid tjänstens upphörande?

9.6.4. Juridik – Hårdvara

Försäkringar

Vad gäller den försäkringsmässiga aspekten av fenomenet BYOD så har utredningen kommit fram till att det i princip inte finns några vedertagna praxis inom försäkringsbranschen kring hur privata enheter i jobbet hanteras, samt skadefall relaterade till dessa. Kort sammanfattat är dock grundregeln att man som arbetstagare inte kan räkna med att ha någon som helst skydd i termer av sakförsäkringar från arbetsgivarens sida. Allt försäkringsskydd som den enskilde förväntar sig, är denne ansvarig för att ordna med själv när det gäller själva enheten. Eftersom det är den anställde som äger enheten så är det också dennes eget försäkringsskydd som gäller.

[11] Enheter som den anställde äger och som tas med till arbetsplatsen och nyttjas i tjänsten.
[12] Enheter som universitetet äger och som tas med hem och nyttjas utanför tjänsten.

Sammanfattning av ”9.6 Juridik”:
BOYD spänner över en mängd olika juridiska områden och tyvärr finns det väldigt lite domar, beslut eller praxis att luta sig mot. Det finns dock några återkommande enkla regler som man kan ta fasta på och dessa är bl.a. att tydligt separera privat- och tjänsterelaterat material samt att inte hantera personuppgifter eller sekretessbelagd information i annat än av universitetet godkända enheter. Det är av vikt att säkerställa att hanteringen av myndighetens information sker enligt lag.

Rekommendation om efterkommande projekt/arbete:
Projektet rekommenderar att LU tillsätter en arbetsgrupp med personer med juridisk expertis och olika kompetensområden för att jobba vidare med de olika juridiska spörsmål som identifierats i detta dokument. Några juridiska rättsområden som bör vara representerade i en sådan grupp är förvaltningsrätt (offentlighet och sekretess), immaterialrätt, IT-rätt och arbetsrätt.

9.7. Ekonomi

De ekonomiska aspekterna av BYOD vid LU är dels svårbedömda och dels utanför projektgruppens kompetensområde. Av denna anledning ser vi endast översiktligt på detta område. En djupare studie föreslås ske i ett efterkommande projekt.

Projektet upplever att de internationella erfarenheter som finns att ta del av inte är särskilt relevanta att använda eftersom de ofta innehåller grepp som:

- den anställde betalar sin arbetsutrustning (arbetsgivaren slipper helt enkelt att köpa arbetsredskap till de anställda).
- ingen som helst support ges för BYOD-utrustning.

Sannolikt gäller det dock även vid LU att anställda är:

- mer rädda om egen utrustning än arbetets dito.
- mer nöjda med egen utrustning.
- mer produktiva med egen utrustning.

9.7.1. Ekonomi – Människa

Anställda är som sagt mer produktiva med egen utrustning. Dock ställer de nya krav på organisationen vilka inte hade behövt lösas om LU kunde ignorera BYOD – både support och förändrat nätverk räknas hit. Anställda som *inte* kan hantera den nya gränslösheten riskerar att gå i väggen och bränna ut sig. Det har visat sig svårt att få en kostnad på detta, men försiktigtvis kan man säga att det snabbt blir sjusiffriga belopp om året. Projektet rekommenderar att LU noga sätter sig in i denna problematik och söker finna sätt att arbeta proaktivt då detta enligt all forskning är betydligt billigare än att ta kostnaderna som uppstår i efterhand.

9.7.2. Ekonomi – Information

LU har inte, som företag, värde kopplat till att hålla sin information hemlig – i de flesta fall är det tvärtom. LU lider vanligen inte heller ekonomisk skada om information läcker. Tvärtom är det av stor vikt att LU i denna ökade ström av information kan formera sin information så att den effektivt bidrar till:

- att locka studenter.
- förbättra LU:s ranking internationellt.
- förbättra möjligheterna att erhålla forskningsanslag.

Alla dessa saker bidrar till att förbättra den ekonomiska situationen, dock först på sikt.

Dock finns det några ”kostnadshål” att vara vaksam på:

- skydda immaterialrättslig information.
- intrång på privat- såväl som LU-ägda enheter som kan smitta LU:s nätverk och andra enheter.

9.7.3. Ekonomi – Rättigheter

Programlicenser för anställda får vid det här skedet betraktas med viss frikostighet. ”Riktiga” lösningar förväntas komma, men det kommer sannolikt ta ytterligare tid innan detta segment mognar. Med ”riktig lösning” menas antingen

traditionell IT-drift vad gäller hantering av licenser och enheter (mer eller mindre oavsett vem som juridiskt äger enheten) eller en LU-AppStore i någon form.

Det finns en problematik kring förmånsbeskattning vad gäller köp av programvara. Projektet har varit i kontakt med Skatteverket (diarienummer LTHCS2013/3) och följande har framkommit:

- Verksamhetsutlägg = inte förmånsbeskattningsbart.
- Utan kvitto = förmånsbeskattningsbart.
- Presentkort kan inte nöjaktigt redovisas varför de är förmånsbeskattningsbara.
- Programvaran skall vara köpt för att användas i tjänsten och då är även ringa privat användning godkänd.

En fungerande mellanlösning kan vara att uppmana anställda att ansöka om de privatkort för vilka LU bekostar årsavgiften och sedan göra traditionella reseutläggsersättningar för inköpen. Projektet uppmanar dock LU att se över möjligheten att förenkla hanteringen av dessa köp; att om möjligt göra det till en egen utläggskategori i Primula.

9.7.4. Ekonomi – Hårdvara

Ett antal hårdvarurelaterade kostnader är att vänta:

- En mer heterogen miljö innebär att det kommer att finnas fler enheter med fler operativsystemsmiljöer som skall kunna använda samma tjänster och läsa samma information. Det kräver att man testar igenom fler miljöer och inte bara anpassar applikationer till t.ex. Internet Explorer på en stationär dator med Windows 7 och 19” skärm. Från projektet anser vi att LU bör vara medvetet om dessa nya kostnader.
- BYOD är vanligen bärbart (ofta WiFi), vilket kräver andra lösningar
  Stationära datorer kommer att bli färre och därmed kommer krav på molntjänster och liknande portabla lösningar. Bärbar utrustning kräver annan infrastruktur och detta är en extra kostnad.
- Skärmarna blir mindre, vilket innebär att om man skall läsa information på en netbook, platta eller telefon så krävs det att informationen anpassats till mindre skärmar. LU kanske måste börja programmera appar för telefoner och plattor, vilket kommer innebära ytterligare kostnader.

9.7.5. Ekonomi – övrigt

Dolda kostnader för BYOD

Om man slår ihop alla kostnader för att hantera BYOD kan totalkostnaden bli upp till 33%[13] högre än för vanlig. Man tjänar pengar på inköp men förlorar på service, support och säkerhet.

Följande bidrar till ökade kostnader:

- Alla dessa enheter kommer att äta upp WiFi-resurser.
- Nya säkerhetsproblem; varje incident kostar mycket pengar.
- Fler falsklarm i säkerhetsövervakningen med mindre standardiserad miljö.
- Större krav på Servicedesk att hantera incidenter på ett antal nya plattformar.
- Krav på ökad trafikövervakning och arkivering av trafikdata.
- ”Kontoret” kommer nu att finnas på andra platser, t.ex. via osäkra WiFi-nät. Vi måste bättre kunna identifiera vem som är vem.
- Utrustning kommer inte att finnas på samma plats längre. Uppdatering av OS och program kommer inte att kunna göras nattetid längre.
- Även om man segmenterar nätverk och gör liknande säkerhetsåtgärder måste man till slut kunna spåra individuella användare.
- BYOD finns redan på nätet. Man kan inte förbjuda det, snarare bör man hitta ett sätt att hantera det som fungerar för de flesta och som ändå håller sig inom regelverket.

Sammanfattning av ”9.7 Ekonomi”:
De ekonomiska konsekvenserna av BYOD för LU är svåröverskådade. Kostnaderna kan öka och LU måste vara både ”med” i utvecklingen och proaktiva för att stävja kostnadsökningar.

Rekommendation om efterkommande projekt/arbete:
LU bör ta reda på kostnader för sjukskrivningar av arbetsrelaterad ohälsa samt följa upp kostnadsutvecklingen avseende BYOD för support, nätverksinfrastruktur, säkerhetsarbete och programlicenser.

[13] Aberdeen Group ”BYOD in the SoMoClo™ Era: Hidden Costs, Unseen Value”

9.8. Säkerhet

Säkerhet är det normalt viktigaste i ”vanlig” BYOD, d.v.s. i företag. Som universitet har vi en annorlunda situation: vår verksamhet kännetecknas av öppenhet och endast en mindre del information är ”hemlig”.

Projektet rekommenderar att LU överväger något slags ”hotline” dit anställda kan ringa för att få akut hjälp att både spärra konton och spåra eller spärra/radera borttappade enheter. Denna hotline bör dessutom ha en webbplats dit anställda kan ta sig om de endast förlorat enheten och inte lösenord. Där bör den anställde själv kunna:

- ändra relevanta lösenord och PIN-koder.
- lokalisera borttappad utrustning.
- fjärrtömma borttappad utrustning.

Detta bör ses både som en service till de anställda och ett sätt för LU att skydda sig självt mot säkerhetsincidenter. Detta kan kanske lösas av nuvarande ServiceDesk men borde utsträckas i tid för att kunna möta behov från forskare på resande fot. Kanske kan man ha ett större samarbete mellan flera högskolor i Sverige?

Förutom att varmt stödja det pågående arbetet att genomföra LUCAT-autentisering av alla LU-system, rekommenderar projektet LU att ge användarna ett bra redskap att hantera de säkerhetsproblem som den stora mängden konton och lösenord innebär. Projektet har tittat på två sådana system:

- 1Password Pro (https://agilebits.com/onepassword)
- LastPass (https://lastpass.com)

Båda dessa stödjer alla tillämpliga plattformar (Windows, Mac, Linux, iOS, Android, Windows Phone) och är därför intressanta.

I korthet

- BYOD innebär inte bara besparingar – det finns också kostnader.
- Ökad service och support på flera OS och plattformar.
- Applikationer måste anpassas.
- Trådlösa nät och VPN måste kanske uppgraderas.
- Backuplösningar för mobila enheter.
- Fler OS och enheter ger ökade säkerhetsrisker och vi har mindre kontroll.
- Ökad övervakning och nya management-verktyg.

Största hoten

- Stulna och borttappade enheter som innehåller information och lösenord.
- Malware (d.v.s. skadlig kod).
- Legitima applikationer som inte hanterar information enligt vår policy.
- Intrång på enheter.
- Informationen är inte under vår kontroll längre.
- Ingen/sämre central kontroll på utrustningen.

Vad måste vi göra

- Se över regler och policy och skapa de som behövs.
- Se över vilka skydd mot stöld vi kan erbjuda från centralt håll.
- Se över vilka skydd mot malware vi kan erbjuda från centralt håll.
- Inventera och erbjuda tjänster för att locka in enheter under vår kontroll.
- Utbilda användare.
- Se till att vår infrastruktur fungerar och har tillräcklig kapacitet.
- Se till att Servicedesk kan lämna support på det som LU anser skall innefattas.
- Se över vår identitetshantering och hur den kan utnyttjas för att segmentera nätverk såväl som åtkomst till olika resurser inom LU.
- Undersöka om NAC[14]-lösningar kan hjälpa oss att öka säkerheten.
- Titta på olika MDM-lösningar.
- Se över skydd av servrar som måste öka när klientskyddet minskar.

Nödvändiga funktioner och minimikrav

- Starka lösenord och låskoder.
- Kryptering av känslig information.
- Raderingsfunktioner på distans.
- Antimalwareprogram.

Detta är svårt att uppnå utan att installera program på utrustningen.

Tips för att starta med BYOD

- Ha lagom nivå på regelverket så att produktiviteten inte förhindras.
- Känn din fiende; var uppdaterad med var hoten finns.
- Minska attackytan. Skydd på telefonen – fungerar överallt. Nätbaserat skydd – fungerar inte hemma.
- Skriv inte regler för exakt den utrusning som finns idag. Den kommer att förändras.
- Installera MDM för att kontrollera efterlevnad.
- Installera raderingsfunktioner.
- Installera antimalwareprogram.
- Använd VPN för att nå lokala tjänster och nät om det inte gäller öppen information.
- Fokusera på autentisering och identitetshantering.
- Utbilda, följ upp, uppdatera regler löpande, arbeta med användarna – inte mot.

De största problemen

Stulna eller borttappade telefoner och plattor kommer att vara ett större problem än virus och skadlig kod, åtminstone i det korta perspektivet. Eftersom dessa enheter snabbt blir en databas över inloggningsuppgifter och lösenord är detta nog det viktigaste problemet vi måste tackla. Någon form av MDM (Mobile Device Management) system bör användas för att kunna radera enheter på distans. Det är inte enkelt att få alla användare att inse att det är nödvändigt att de skall installera program som tillåter arbetsplatsen att radera och låsa deras privata utrustning. Men de kommer ändå att

[14] Network Access Control. NAC kräver att användare/datorer autentiserar sig innan de kan använda nätverk. NAC möjliggör också i vissa fall kontroll av att datorer är uppdaterade, har uppdaterat antivirusprogram, etc innan de ges nätaccess.

använda sina enheter i jobbet och på Lunet och det finns ingenting vi kan göra åt den saken.

9.8.1. Säkerhet – Människa

Enligt rapporten "Kontorsrevolutionen" från Kairos Future är lojalitet från de anställda minst lika viktig som tekniken när det gäller IT-säkerhet. Man konstaterar att säkerhetsfrågan måste lyftas från IT till företagsledning och HR.

Blanda jobb och privatliv

- Privata säkerhetsbrister kan äventyra jobbets säkerhetsåtgärder
- Säkerhetsbrister på jobbet kan exponera privata uppgifter och information

Man måste skydda sig åt båda hållen. Säkerhetsåtgärder för att skydda information och utrustning får inte påverka rätten till personlig integritet.
Den policy man använder för fasta PC och bärbara datorer kan troligen inte användas rakt av för BYOD. Den är helt enkelt oftast för rigid och kan hindra produktiviteten. Dessutom är användare mer benägna att bryta mot reglerna vad gäller BYOD, då det är deras egen utrustning och den är fysiskt mindre och känns mindre "farlig". LU har dock redan en ganska hög acceptansnivå i sitt regelverk och har sedan länge haft en sammanblandning av jobb och fritid. Det är nog ett mindre steg för att införa BYOD inom LU än för ett företag av samma storlek.

9.8.2. Säkerhet – Information

I och med att den privata enheten har smält samman mer och mer i arbetsrollen så sätts ett antal saker på sin spets vad gäller den information som finns i de aktuella enheterna. Bland annat blir den klassificering av information som återfinns i ISO 27002 (SS-ISO/IEC 27002:2005) väsentlig när arbetsgivaren ska bedöma om och hur den anställde kan och får komma åt information. Statliga myndigheter skall uppfylla ISO 27000. ISO-standarden klassificerar hur stor skada som informationsläckage skulle göra. Med utgångspunkt i detta så anser vi från projektet att det ligger på arbetsgivarens bord att göra bedömningen och klassificeringar av olika generella typer av information. Dessa klassificeringar är det sedan av största vikt att de kommuniceras till de enskilda anställda, så att man skapar en förståelse för de många andra säkerhetsrisker som en privatägd enhet innebär.

Med en ökad spridning av informationen så ökas också riskytan genom vilken informationen kan spridas.

Kontrollen över informationen minskar

I och med att det blir en blandning av personlig och LU-ägd utrustning minskar den centrala kontrollen över utrustningen. Backup kommer att vara svårare eftersom det finns privat- och tjänsteinformation blandad i olika enheter. Relevant information kommer att finnas i många olika enheter där vi inte har kontroll över den. Exempel: knäpp en bild med telefonen och den är uppladdad i Dropbox och Google+ direkt, skriv ett dokument på plattan och den synkas iväg till en server vi inte har kontroll över.

Centrala backuplösningar för arbetsrelaterad data är ytterligare en kostnad som måste budgeteras för att få ett samlat grepp om BYOD.

Backup av handhållna enheter

Följande gäller för backup av de i nuläget vanliga operativsystemen för handhållna enheter:

- iOS
  iPhone/iPad synkroniseras antingen med sladd mot iTunes på en dator eller trådlöst mot Apples iCloud-tjänst. Det som lagras i iCloud skyddas av "Safe Harbor"[15] och detta utgör (enligt EU) tillräckligt skydd för myndighetsmaterial[16]. Det som synkroniseras/säkerhetskopieras är: Köpta appar och böcker, bilder och video i kamerarullen, enhetsinställningar, data i appar, hemskärmarna, meddelanden (iMessage, sms och mms), ringsignaler.
- Android
  Android-telefoner kan delvis säkerhetskopieras mot Googles servrar genom att användaren själv väljer att ha denna säkerhetskopiering aktiv. Det som säkerhetskopieras är inställningar knutna till Google-identiteten såsom trådlösa nätverk, vilka appar som installerats osv. Bilder och musik på enheten säkerhetskopieras inte automatiskt till Google.
- Windows Phone 8
  Windows-telefoner med version 8 av operativsystemet har inbyggd säkerhetskopiering mot Microsofts SkyDrive av installerade applikationer, samtalshistorik, favoriter i Internet Explorer, foton, SMS, mail, plats, röstdata med mera. Dock sker denna säkerhetskopiering primärt över trådlöst nätverk. Om användaren inte anslutit till ett trådlöst nätverk inom en vecka, skickas endast historiken av installerade appar till säkerhetskopiering.

Hur skall vi ställa denna kontrollförlust mot offentlighetsprincipen? Information rörande ett ärende kan kanske inte plockas fram "skyndsamt" som lagen kräver. Vi kan kanske inte komma åt den alls! Vi förlorar kontrollen över hur sekretessklassad information hanteras om den bärs runt okrypterad i privata enheter. Om sådan information lagras i en utrustning som automatiskt backas upp via en molntjänst kan personen göra sig skyldig till ett regelbrott och ett lagbrott.

Andra hot gäller applikationer som i princip inte är skadliga men som genom sin ToS (Terms of Service) gör att andra får tillgång till information som kanske borde hållas hemlig eller inte får exporteras. Applikationer som installeras för privat bruk gör ingen skillnad på om den data som användaren accepterade att dela med sig av egentligen tillhör jobbet. Ofta vill applikationer ha tillgång till fler resurser i telefonen än vad som de rimligen borde behöva och användare klickar normalt OK på frågor om ToS. Man vet inte heller om applikationen som tillverkades av ett "snällt" bolag blir uppköpt och får andra skadliga funktioner senare.

---

[15] Safe Harbor är en samling frivilliga regler om personlig integritet och dataskydd som har tagits fram och beslutats av USA:s handelsdepartement (Department of Commerce - DoC), se även Datainspektionens frågor och svar om Safe Harbor

[16] Förutsatt att lagring, support, service, backup och samtliga underleverantörer av tjänsten befinner sig i ett land som är godkänt av EU/EES eller, om det gäller USA, är anslutet till Safe Harbor

BYOS – Bring your own software

Att man använder egen utrustning i jobbet betyder också att man använder egen mjukvara. Denna kan vara möjlig att missbruka och man vet inte hur informationen skyddas. Man måste fundera på sådant som

- Hur krypteras data
- Används samma krypteringsnyckel, alt. finns en huvudnyckel
- Vem har access till nycklarna
- Kan de komma att lämna ut nycklar till myndigheter
- I vilka länder finns servrarna

9.8.3. Säkerhet – Rättigheter

Malware

Malware är fortfarande inte så spritt men enheter som kör "Lookout Mobile Security's" mjukvara identifierade 30.000 unika program med skadlig kod i juni 2012 mot 3.000 bara sex månader tidigare. Skadlig kod för mobila OS ökar mycket snabbt. Efterhand som man mer och mer kommer att hantera pengar eller andra saker av värde via sina handhållna enheter, kommer vi att se att tillverkning av skadlig kod kommer att ändra fokus till OS för handhållen utrustning. Skall du hitta buset, följ pengarna!

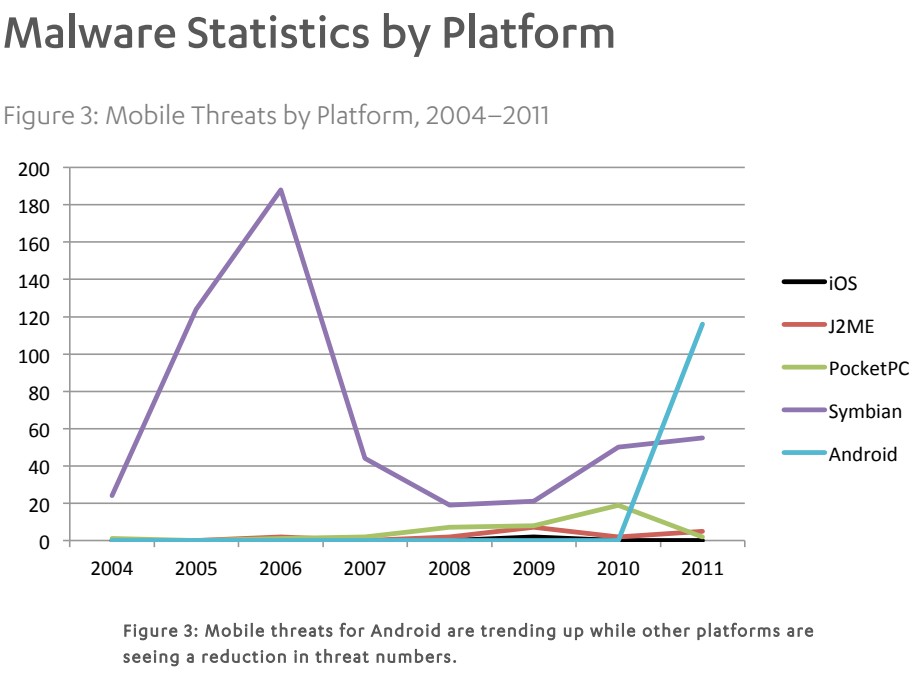


Diagram över ökningen av malware för handhållna operativsystem[17]

[17] F-Secure. Mobile Threat Report Q4 2011

FIGURE 5: MOBILE THREATS MOTIVATED BY PROFIT PER YEAR, 2006-2012

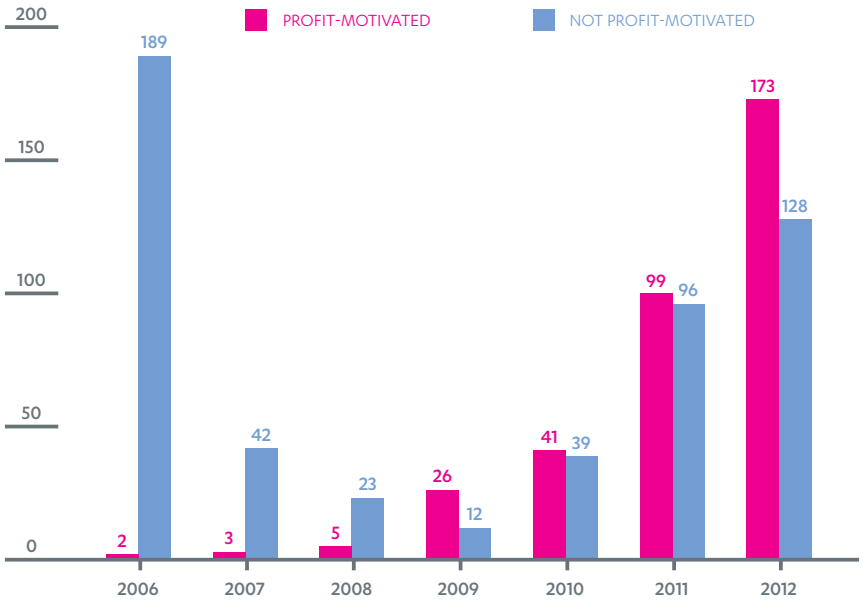


Diagram över drivkrafterna bakom malware för handhållna operativsystem[18]

IBM stoppade sina 400 000 anställda från att använda två populära applikationer på enheter som de använde i arbetet. De förbjöd även Dropbox och Apples Siri (som skickar frågorna till Apples servrar för analysen). Det är lätt att förbjuda sådant men hur skall man följa upp att reglerna följs?

9.8.4. Säkerhet – Hårdvara

En jailbroken iPhone eller rootad Android är inget annat än en Unix-dator med nästan alla de resurser som en sådan dator har, inklusive möjlighet att logga in. Detta är information som är svår att få fram till användare. Utbildning och information är grundläggande och ytterst viktigt för att BYOD skall fungera smärtfritt eftersom vi har BYOD varken vi vill det eller ej. Här gäller att vara proaktiv om man skall överleva.

9.8.5. Säkerhet – Övrigt

Klientsäkerheten minskar

Man kommer att ha ännu mindre kontroll över säkerheten i de enheter som används. Det är inte troligt att det någonsin kommer en universell lösning för nätinloggning för samtliga plattformar som gör att man kan kräva en miniminivå på säkerhet. Troligen kommer någon form av nätinloggning att användas på Lunet. Klientkontroll kommer troligen att vara någorlunda effektiv endast på Windows och OS X. Alla andra operativsystem kommer nog bara att få en rudimentär kontroll. Övervakning måste öka och anpassas för att kunna identifiera fler smittade och hackade datorer. Även en säkerhetskontroll via nätinloggning är inte ett på långa vägar ett fullgott skydd. Trojaner och liknande malware förblir ofta oupptäckta idag och det kommer nog inte att bli

[18] F-Secure. Mobile Threat Report Q4 2012

bättre inom överskådlig framtid. Med fler antal och typer av klienter kommer problemen att öka.

Hårdare skydd för servrar och system

Servrar kommer att behöva skyddas hårdare för att möta problemen med den minskade klientsäkerheten. Tyvärr går det lite emot tanken med BYOD där man vill kunna nå sin information och sina applikationer från alla enheter och överallt. Kanske måste man kunna verifiera sin utrustning på något sätt och möjligen bör man bara acceptera kontrollerad och autentiserad utrustning till känsliga system. Hårdare skal runt servrar och system och hårdare accesskontroll till känsliga system. Att kräva VPN-inloggning löser andra problem men inte BYOD. NAC löser vissa problem men inte alla. Autentiserade utrustningar är inte heller den heliga gralen. Projektet anser att det krävs ett antal olika insatser som tillsammans ger en tillräcklig säkerhet. Dock riskerar man att det blir krångligt att både administrera och använda systemen.

Sammanfattning av "9.8 Säkerhet":
BYOD skapar en betydligt mer heterogen och svårkontrollerad miljö vilket ökar och förändrar behoven och metoderna för övervakning. Service och support får nya utmaningar i den nya miljön. En borttappad eller stulen enhet innehåller en mängd lösenord och känslig data tillsammans med blandad personlig och arbetsrelaterad information. Informationen kommer till högre grad att finnas utanför arbetsgivarens kontroll i framtiden vilket gör att man har svårt att uppnå kraven i ISO2700. Autentisering och identitetshantering kommer att bli ännu viktigare än idag.

Rekommendation om efterkommande projekt/arbete:
LU bör tillsätta ett projekt som belyser följande frågor:

- Hur kan vi införa MDM-system och hur lockar vi användare att medverka?
- Hur kan vi införa NAC, stöd för kryptering och för lösenordshantering och antivirus/antimalware?
- Hur skall vi utbilda och informera användare?
- Hur inför vi stöd för att backup av myndighetsdata från enheter?
- Hur ökar vi serversäkerheten för att möta minskad klientsäkerhet?

9.9. Support

Vid kontakter med Marcus Tanninen på LDC har framkommit att support av BYOD-utrustning för närvarande inte är ett problem för LDC. Man menar sig ha effektiva guider som man hänvisar de som ringer till och man finner även stöd för detta i webbtrafikloggar. Eftersom det inkommer en viss mängd ärenden till LDC avseende ett visst problem, skapas ofta guider för att den uppringande själv ska kunna lösa problemet.

Erfarenheter från undersökningar av BYOD servicenivå

75% av servicedesk har support för telefoner och plattor
Bara 47%[19] har en policy,
De flesta är dåliga på att meddela till användarna att support finns

Vad används telefoner och plattor till?[20]

- E-post 94%
- Anteckningar 38%
- Nå interna applikationer på lokala servrar 14%
- Lagra information 12%
- Nå interna applikationer i molnet 12%

Vilken support ges?

- Komma igång hjälp, E-post + kalender 84%
- Policy för användarna 54%
- Support om SIM-kort 52%
- Ersättningstelefon 47%

Säkerhet

- Radera information på distans 45%
- Har inga säkerhetsåtgärder 40%
- Kräver låskod 38%
- Blockera oönskade funktioner 9%
- Virusskydd 8%

Sammanfattning av "9.9 Support":
Serviceorganisationen måste kunna hantera fenomenet BYOD på ett kostnadseffektivt sätt eftersom fler tjänster och enheter kommer komma i framtiden. Det måste finnas tydliga gränser för vad en anställd kan och inte kan få support på.

Rekommendation om efterkommande projekt/arbete:
Projektet rekommenderar LU att tillsätta ett projekt för att klargöra vad serviceorganisationen ska respektive inte ska ge support för.

[19] SURVEY: Mobile Threats are Real and Costly, Webroot.
[20] Support, säkerhetspolicys och synk – så hanterar Sveriges it-avdelningar smarta telefoner och surfplattor. Techworld och Dustin

9.10. Studentsynpunkter

För många studenter är redan idag BYOD en viktig möjlighet. De utnyttjar den genom att ta med laptop, tablet eller telefon för att förbättra sin studiemiljö på universitetsområdet, eller för att undvika att behöva hitta en datorsal eller studieplats med dator.

Projektet har tänkt på de grundläggande behov som finns för studenter som använder sig av BYOD idag eller den nära framtiden och de problem som redan finns. Vissa av de belysta problemen påverkar även studenter som till stor del inte utnyttjar BYOD, men använder datorer hemma, på universitetet eller har särskilda behov.

9.10.1. Fysisk infrastruktur

De grundläggande problemen med BYOD för studenter idag är ofta relaterade till bristande fysisk infrastruktur, eftersom den är det som möjliggör hela fenomenet.

- Kapaciteten och täckningen på WiFi-nätverken är idag ofta låg, speciellt vid de tidpunkter många studenter rör sig på universitetets olika campus. Det bör finnas nog med kapacitet, ip-addresser och andra resurser för att alla studenter ska kunna ha möjlighet att ta med sig flera enheter utan att det leder till problem.
- Idag är antalet eluttag på många studieplatser och undervisningslokaler begränsade och man bör vid renovering och ombyggnad se till att framtida behov tillgodoses. Även laddning av t.ex. telefoner via USB kan vara av intresse, men man bör undersöka säkerhetsaspekten först.
- Idag är det svårt att hitta en skrivare som går att skriva ut från på vissa platser på universitetet och försöker man skriva ut från en privat enhet så är det i princip omöjligt. Problematiken för scanners är i princip samma.
- Det måste vara klart med hur en student får hjälp med krånglande utrustning som ägs av universitetet, t.ex. en krånglande skrivare.

9.10.2. Informationsinfrastruktur

Mycket av den informationsinfrastruktur som önskas finns redan, vi behöver bara bli bättre på att använda den. TimeEdit är ett exempel på ett system som om det skulle användas fullt ut av schemaläggare och lärare, skulle vara ett mycket bra sätt att kommunicera med studenterna vid t.ex. akuta schemaändringar.

- Korrekta scheman med kursnamn, plats och med stöd för synkronisering med egen kalender (iCal etc.)
- En väl uppdaterad programportal med licenser för program som krävs i skolarbetet för egna datorer uppskattas, gärna med information om vilka kurser som använder vilka program. Även guider för att installera open-source program skulle kunna finnas här.
- Kurslitteratur som e-bok (om möjligt PDF eller epub) uppskattas mycket, speciellt när litteraturen kostar mycket.
- Inspelade föreläsningar i kurser och introduktioner till program (och övrigt) man förväntas kunna men inte nödvändigtvis fått undervisning i som t.ex. Matlab.

- Egenvald push-notifiering. Som student vill man kunna prenumerera på notifieringar från olika LU-gemensamma system om det är så att det är relevant för en själv. Därför är det också viktigt att få välja *vilka* notifieringar man önskar

9.10.3. Kurswebb och Lärplattformar

Kurswebbsidor är navet i studierna (eller borde vara det) och är idag mycket inriktade på nya/blivande studenter. Vissa grundläggande krav

- Den senaste versionen av kurshemsidan måste gå att hitta lätt via Google, tidigare versioner skall vara markerade med en länk till den senaste.
- Kurssidorna måste vara i responsiv design så att de fungerar på surfplattor och telefoner.
- Viktig kurskommunikation sker via kurswebbsidorna, t.ex. scheman, tentamenstider, kursplaner och litteraturlistor.
- Om det är möjligt, så bör kursflödes-scheman och info om liknande och fördjupande kurser finnas tillgängligt.

9.10.4. App

- Applikation för övnings- samt. tentamensanmälning och labbsalstillgång, vilket även kan ge användbar statistik till institutionerna.

9.10.5. Övrigt

- Om externa tjänster erbjuds måste de vara och hållas moderna, det räcker inte med att de är bra när de köps in.
- Det kan behövas hjälp att installera program som används i undervisningen på den egna datorn. Det är inte säkert att dessa program krävs för lektioner eller föreläsningar, men studenterna vill ha tillgång till dem i alla fall.
- Det räcker inte med att saker fungerar väl på vissa delar av LU, tillräckligt många studenter rör sig ”över gränserna” för att ett dåligt rykte ska sprida sig.

Sammanfattning av ”9.10 Studentsynpunkter”:
Studenternas behov är i delade i två delar: basal fysisk infrastruktur (ström, nätverk, skrivare) och en välunderhållen informationsinfrastruktur i vilken det viktigaste är att LU spelar väl med Googles sökmotor.

Rekommendation om efterkommande projekt/arbete:
Etablera en tydlig lägsta-nivå och rekommenderad nivå för nybyggnation/ombyggnad avseende fysisk infrastruktur för elever samt lägga tungt fokus på informationsinfrastrukturen med tonvikt på sökning, navigation och plattformsoberoende.

9.11. Referenser

1Password. Tillgänglig *https://agilebits.com/onepassword*

Aberdeen Group "BYOD in the SoMoClo™ Era: Hidden Costs, Unseen Value", *http://www.aberdeen.com/Aberdeen-Library/8099/RA-bring-your-own-device.aspx* [2013-05-15]

Betalkort vid Lunds universitet. Tillgänglig: *http://www5.lu.se/anstaelld/foer-mitt-arbete/tjaensteresor/betalkort*

Bevarande- och gallringsplan för forskningsmaterial. *http://www5.lu.se/upload/Juridiskaenheten/GallringsplanForskningsmaterial.pdf*. [2013-06-04]

Bohman, Murphy (2012) Bring Your Own Device: Analys av trenden, dess möjligheter och problem.Tillgänglig: *http://uu.diva-portal.org/smash/record.jsf?pid=diva2:533649* [2013-04-04]

Datainspektionen, Samrådsyttrande om användning av anställdas egna utrustning i tjänsten, s.k. bring your own device- lösningar, BYOD, Diarienummer 1260-2012

Datainspektionen. Mobila enheter Checklista för behandling av personuppgifter. *http://www.datainspektionen.se/Documents/faktablad-mobila-enheter.pdf* [2013-05-16]

Dr Christine Mellner (2013). Forskning om gränser mellan arbets- och privatliv. Tillgänglig: *http://www.psychology.su.se/om-oss/nyheter/2-miljoner-till-forskning-om-granser-mellan-arbets-och-privatliv-1.94310*

Enterprise iOS Lista över MDM-lösningar. Tillgänglig: *http://www.enterpriseios.com/mdm/*

F-Secure (2011). *Mobile Threat Report.* Tillgänglig: *http://www.f-secure.com/weblog/archives/Mobile_Threat_Report_Q4_2011.pdf* [2013-05-15]

F-Secure. Mobile Threat Report Q4 2012. *http://www.f-secure.com/static/doc/labs_global/Research/Mobile Threat Report Q4 2012.pdf* [2013-05-16]

Gränslöst arbete / *"Boundary Theory"*. Tillgänglig: http://www.psykologifabriken.se/tag/granslost-arbete/

ISO/IEC 27002:2005 Information technology -- Security techniques -- Code of practice for information security management. Tillgänglig: *http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=50297*

KTH (2009) *Ansvar, befogenheter och skyldigheter för systemadministratör.* Tillgänglig: *http://intra.kth.se/regelverk/overgripande-styrning/informations-it-sakerhet/ansvar-befogenheter-och-skyldigheter-for-systemadministrator-1.27163*

LastPass, Password Service. Tillgänglig: *https://lastpass.com*

Patrizio, Andy (2012) *When Employees Become IT Hardware Providers.* Tillgänglig *http://h30565.www3.hp.com/t5/UK-Articles/When-Employees-Become-IT-Hardware-Providers/ba-p/1310*

Professor emeritus Thöres Teorell, Karolinska Institutet – *Det moderna livet, Stressen och hälsan.* *http://www.fhi.se/Documents/Aktuellt/konferensdokumentation/2007/halsoframjande-sjukvard/thores-teorell-det-moderna-livet-stressen-och-halsan.pdf* [2013-05-02]

Safe Harbor. Department of Commerce – DoC. Tillgänglig: *https://safeharbor.export.gov/list.aspx* samt *http://www.datainspektionen.se/fragor-och-svar/personuppgiftslagen/vad-ar-safe-harbor-principerna/*

Support, säkerhetspolicys och synk – så hanterar Sveriges it-avdelningar smarta telefoner och surfplattor. Techworld och Dustin. Tillgänglig: *http://www.dustin.se/page/6176/tw-undersokning*

SURVEY: Mobile Threats are Real and Costly, Webroot. *http://www.webroot.com/shared/pdf/byod-mobile-security-study.pdf* [2013-05-15]

TDC Labb. *Kontorsrevolutionen.* Tillgänglig: *http://www.kontorsrevolutionen.se/*

Ulf Lundberg. Det gränslösa arbetet. Tillgänglig: *http://www.arbejdsmiljoforskning.dk/upload/Ulf_Lundberg.pdf* [2013-05-08]

University of Oregon (2012) *Factors for Consideration when Developing a Bring Your Own Device (BYOD) Strategy in Higher Education.* *https://scholarsbank.uoregon.edu/xmlui/bitstream/handle/1794/12254/Emery2012.pdf?sequence=1* [2013-01-30]

Scot Finnie, Computerworld The Real Consumerization of IT. Tillgänglig: *http://www.computerworld.com/s/article/9230148/Scot_Finnie_The_real_CoIT*

U.S.-EU Safe Harbor List. Tillgänglig: *https://safeharbor.export.gov/list.aspx*

Skatteverket. *Klargörande angående förmånsbeskattning av programvara för privata, mobila enheter*. Diarienummer LTHCS2013/3. Tillgänglig: *https://dfs.adm.lu.se/Asp/W3D3urllogin.asp?DIARYREF=116&CASEREF=547603&WORKDOCUMENTREF=821317*

Personuppgiftslagen (1998:204) Tillgänglig: *http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Personuppgiftslag-1998204_sfs-1998-204/*

University of Oregon, *Applied Information Management.* Tillgänglig: *https://scholarsbank.uoregon.edu/xmlui/bitstream/handle/1794/12254/Emery2012.pdf* [2013-01-30]