Kalle Wadin Eriksson, 880319

MITTUNIVERSITETET
Institutionen för informationsteknologi och medier

Informationssäkerhet och autenticitet i elektroniska arkiv

Magisterkurs i arkiv- och informationsvetenskap
Magisteruppsats 15 högskolepoäng
Handledare: Erik Borglund
VT 2013
Kalle Wadin Eriksson

Innehållsförteckning

Abstrakt

Uppsatsen studerar informationssäkerhet i de elektroniska arkiven. Denna står inför ett antal utmaningar som måste lösas för att minimera risken för informationsbortfall och obehörigt intrång i det digitala arkivbeståndet. I studien undersöks både vilka problem som den arkivvetenskapliga forskningen upplever och vilka som upplevs av representanter för den svenska arkivariekåren. Förslag på lösningar på dessa problem diskuteras likväl. De tillfrågade arkivarierna har fått besvara en enkät med elva olika frågeställningar och svaren på dessa utgör grunden för artikelns diskussion och sammanfattning.

I uppsatsen har formulerats följande tre frågeställningar:
– *Hur behandlas informationssäkerhet i den arkivvetenskapliga litteraturen?*
– *Hur ser svenska arkivarier på informationssäkerhet?*
– *Vilka problem och lösningar framhålls i informationssäkerhetsfrågorna?*
De tre frågeställningarna har besvarats dels genom en litteraturstudie inom den arkiv- och informationsvetenskapliga forskningen, dels genom en enkätundersökning bland svenska yrkesverksamma arkivarier.

Det som sammanfattningsvis framkommer är att den arkivvetenskapliga forskningen tycks uppleva situationen som mer problematisk än vad den svenska arkivariekåren gör. Flera av de tillfrågade arkivarierna upplever inte just några problem alls. Som framgår av uppsatsens enkät bedrivs dock på vissa håll ett mycket intensivt arbete för att stärka informationssäkerheten vid svenska arkiv, bland annat genom att representanter för den svenska arkivariekåren regelbundet håller möten där de diskuterar dessa frågor tillsammans med IT-personal, en viktig samarbetspartner.

Den arkivvetenskapliga forskningen hävdar att det är svårare att upprätthålla informationssäkerheten för elektroniskt arkivmaterial än för det analoga materialet. Att säkerhetsarbetet är svårare innebär också att riskerna är större. I studien tas dock en rad olika förslag på åtgärder upp och dessa diskuteras dessutom relativt ingående. Exempel på metoder för att lösa problemet är elektroniska signaturer, kryptering, säkerhetskopior, väl inarbetade rutiner och regelverk.

Inledning

Informationssäkerheten är central inom all form av arkivhantering, därför att arkiven har till uppgift att bland annat bevara material av känslig karaktär och handlingar som är belagda med sekretess. Fokus i denna uppsats ligger på informationssäkerhet inom elektroniska arkiv. Eftersom arkiven har till uppgift att bevara känsligt material blir det nödvändigt med ett informationssäkerhetsarbete inom den elektroniska arkivhanteringen. David Bearman har skrivit en artikel där han analyserar alla de hotsituationer där handlingar eller information riskerar att hamna i orätta händer, situationer som hotar arkivens informationssäkerhet.[1] Bearmans artikel är ett exempel på den medvetenhet som finns inom den arkivvetenskapliga forskningen kring hoten mot informationssäkerhet. Detta är inte bara ett abstrakt begrepp, utan någonting som konkret och praktiskt inverkar på arkivariens hantering av elektroniskt arkivmaterial.

Exempelvis när en elektronisk handling ska byta format eller förflyttas så är den enligt Bearman extra hotad för obehörig åtkomst.[2] Andra situationer när informationen är hotad är när handlingar ska föras in i hanteringssystem eller gallras.[3] Detta kräver att arkivarier som hanterar elektroniskt arkivmaterial behöver stora kunskaper om hur de ska gå till väga för att informationen i de olika risksituationerna ska kunna hanteras så informationssäkert som möjligt. Detta är någonting som påverkar arkivhanteringen, när IT-arkivarier måste ha kunskaper om och använda sig av olika krypteringssystem när de skickar handlingar mellan olika platser, exempelvis e-post. Det ställer också krav på väl inarbetade rutiner och att arkivarierna följer dessa, vilket inverkar i arkivariens arbete. De måste också utföra backuper och säkerhetskopieringar med jämna mellanrum.

Eftersom arbetet med informationssäkerhet inverkar så pass mycket på arkivariernas arbetsuppgifter vid hanteringen av elektroniskt material så är det ett område som måste studeras närmre och där det krävs mycket mer forskning. Framförallt är det viktigt att påminna om vikten av informationssäkerhetsarbete. En bristande informationssäkerhet hos arkiven kan leda till många negativa följder och en nedåtgående spiral där allmänheten förlorar förtroende för arkiven och därmed arkiven förlorar status och ställning i samhället.

[1] Bearman, David, ”Moments of risk: identifying threats to electronic records”, *Archivaria*, 2006:62.
[2] Ibid., s. 24.
[3] Ibid., s. 31, 39.

För att upprätthålla allmänhetens förtroende är det därför nödvändigt med ett omfattande och välfungerande informationssäkerhetsarbete och däri ligger mycket av forskningsrelevansen. Alltmer arkivmaterial digitaliseras idag och då blir arbetet med informationssäkerhetsarbete i de elektroniska arkiven ännu viktigare.[4]Detta betyder med största sannolikhet att arbetet med informationssäkerhet i de elektroniska arkiven blir viktigare, när allt större andel av arkivmaterialet blir elektroniskt.

Inom vissa arkiv förvaras material som är extremt känsligt och också mycket eftertraktat. Exempelvis skulle sekretessbelagda arkivhandlingar rörande forskning kring kemiska stridsvapen vara mycket eftertraktade hos olika terroristgrupper och därför går det inte att nog belysa hur viktigt de elektroniska arkivens informationssäkerhetsarbete kan vara. Det är viktigt att arkiv- och informationsvetenskapen studerar denna fråga och utarbetar modeller och metoder för att stärka informationssäkerheten så mycket det går samt sprider dessa kunskaper så mycket det går hos verksamma arkivarier. Under de senaste årens arkiv- och informationsvetenskapliga forskning har det skrivits en del artiklar om de elektroniska arkivens informationssäkerhet och olika metoder som kan användas för att stärka denna.[5]Detta visar att det finns en medvetenhet kring frågan inom forskningen och att det med tiden har börjat uppmärksammas alltmer.

Informationssäkerhet är ett mångsidigt begrepp och informationssäkerheten har många olika aspekter. Det finns exempelvis teknisk informationssäkerhet, mänsklig informationssäkerhet, IT-säkerhet, administrativ säkerhet, kommunikationssäkerhet och många fler.[6] Alla dessa är olika delar av samlingsbegreppet informationssäkerhet. Denna uppsats' syfte är inte att studera informationssäkerheten som helhet, därför att det skulle vara ett omöjligt stort projekt för en magisteruppsats. Fokus i uppsatsen ligger på framförallt den tekniska informationssäkerheten. Till att börja med behövs en definition av detta begrepp: vad är informationssäkerhet?

[4] SOU 2009:16, del 3, s. 39.
[5] Boudrez, Filip, "Digital signatures and electronic records", *Archival Science*, 2007:2; Duranti, Luciana, Eastwood, Terry & MacNeil, Heather, "Preservation of the integrity of electronic records", *Archivaria*, 2008:66, s. 135; Hansen, Lars-Erik, "Elektroniska signaturers omöjliga liv i ett långtidsarkiv", *Arkiv, samhälleoch forskning*, 2002:2; Meijer, Albert, "Accountability in an information age: opportunities and risks for records management", *Archival Science*, 2001:4; Meijer, Albert, "Trust this document! ICTs, authentic records and accountability", *Archival Science*, 2003:3; Speck, Jason, "Protecting public trust: an archival wake-up call", *Journal of archival organization*, 2010:8.
[6] *Ge din information rätt säkerhet – handbok i informationssäkerhetsarbete*, Teknisk rapport SIS/TK 318 N46, version 6.00, 2006-08-07, s. 4.

Projektet Ledningssystem för informationssäkerhet, LIS, har givit ut en rapport där de bland annat definierar begreppet. De definierar informationssäkerhet som en garanti för att användarna, i detta fall användarna av arkiv, alltid kan få tag på information när de behöver och att denna information är rätt och riktig.[7] För att upprätthålla informationssäkerheten krävs det därför, enligt LIS, att alla processer och rutiner fungerar på ett sådant sätt att ingen information riskerar att försvinna samt att informationen är skyddad mot att obehöriga personer på något sätt ändrar eller förvanskar dem.[8] Om viss information är belagd med sekretess eller liknande så är det bara vissa personer som har rätt att ta del av den, och skyddet mot att obehöriga personer får tillgång till känslig och sekretessbelagd information är också en del av definitionen av begreppet informationssäkerhet. Informationssäkerheten är i sin tur nära kopplad till begreppen sekretess, riktighet, tillgänglighet och spårbarhet.[9] Alla dessa är centrala delar som måste uppfyllas för att någonting ska kunna betraktas som informationssäkert.

Enligt den handbok som gavs ut för informationssäkerhetsarbete 2006 så kan informationssäkerhet även innefatta bland annat begreppen autenticitet och tillförlitlighet, vilka båda två diskuteras och behandlas i denna uppsats.[10] Enligt den amerikanska lagen så är autenticitet en av informationssäkerhetens beståndsdelar.[11] Enligt denna lag måste informationssäkerhet innebära att informationens autenticitet upprätthålls, alltså att obehöriga personer ej kan förändra eller förstöra informationen. Autenticitet innebär att någonting är äkta och om en handling är förvanskad kan den inte betraktas som äkta. Den amerikanske informationssäkerhetsforskaren Donn B. Parker har utvecklat en modell som kallas för Parkerian hexad.[12] I denna samlas sex olika element vilka tillsammans lägger grunden för informationssäkerhet. Ett av dessa element är autenticitet, en central beståndsdel i informationssäkerheten. Modellen återges i följande illustration:

[7] LIS, *Informationssäkerhet – Nyckeln till nya affärer*, 2001, s. 4.
[8] Ibid.
[9] *Ge din information rätt säkerhet – handbok i informationssäkerhetsarbete*, Teknisk rapport SIS/TK 318 N46, version 6.00, 2006-08-07, s. 4.
[10] Ibid., s. 6.
[11] http://www.law.cornell.edu/uscode/text/44/3542 (hämtad: 130406).
[12] Parker, Donn B., *Fighting computer crime*. New York 1998.

Confidentiality	Access to data is limited to those intended
Control	Data is only accessible or changeable by those intended
Integrity	Data can be relied upon to be accurate and unchanged
Authenticity	Veracity of data source and provenance can be assured
Availability	Timely access to data is always ensured
Utility	Security or insecurity does not inhibit the practical use of data

Källa: http://smartgridsecurity.blogspot.se/2010/06/hexad-dicted.html (hämtad: 130406).

En viktig beståndsdel i informationssäkerheten är att obehöriga personer inte får tillgång till och kan redigera och förvanska informationen. Det finns olika metoder för att förhindra detta, exempelvis användningen av elektroniska signaturer. Denna typ av metoder redovisas och diskuteras i uppsatsen. I uppsatsen diskuteras den viktiga roll som arkiven har i vårt samhälle och vikten av att det material som förvaras hos arkiven är tillförlitligt och behovet av att hindra förfalskningar från att tas in bland arkivmaterialet. Motiveringen till ämnesvalet är att försöka bidra till att föra arkivforskningen framåt på detta område. Det är viktigt att belysa de brister och problem som finns med arkivens informationssäkerhet, både för att arkivarier verksamma vid arkiven ska bli varse de risker och hot som finns och för att stärka deras arbete vad gäller att upprätthålla informationssäkerheten hos arkivmaterialet. Arkiven är en kedja i en lång process som omfattar all form vetenskaplig forskning. Forskare från alla möjliga forskningsfält måste kunna söka sig till arkivmaterialen och då veta att det arbetsmaterial de där hittar är informationssäkert, pålitligt och går att använda sig av.

Karl Wessbrandt har för Statskontorets räkning författat en rapport där han bland annat betonar behovet av nya metoder när det gäller att säkerställa informationssäkerheten för elektroniskt arkivmaterial.[13] Informationssäkerheten är viktig att studera och vidareutveckla för att från arkivens sida kunna garantera bästa möjliga service till sina användare. Det är nödvändigt att arkiven håller en hög nivå av informationssäkerhet, både när det gäller det analoga och det elektroniska arkivmaterialet. Forskare, myndigheter och privatpersoner använder sig av arkivhandlingarna och bör kunna lita på att materialet är informationssäkert och korrekt. Om informationssäkerheten brister så påverkar inte det bara arkiven negativt,

[13]Wessbrandt, Karl, *Förstudierapport om framtidens elektroniska arkiv*, Statskontoret, Dnr 2003/67, ändrad 2003-06-04, s. 34.

utan hela kedjan av användare. Därför är det ett mycket relevant forskningsområde som måste studeras ytterligare.

Syfte och frågeställningar

Syftet med uppsatsen är att studera hur informationssäkerheten har behandlats i den arkiv- och informationsvetenskapliga forskningen och hur detta påverkar det praktiska arkivarbetet. Som en direkt följd av detta studerar också uppsatsen vilka metoder och åtgärder som kan användas för att förbättra det elektroniska arkivmaterialets tekniska informationssäkerhet. Informationssäkerheten är nära kopplad till autenticiteten, vilket diskuterades mer utförligt i inledningen. Det har utarbetats två frågeställningar med nära koppling till varandra: först att ringa in och belysa de upplevda problemen, därefter komma fram med ett förslag till lösning.

Eun Park genomförde 1998 en enkätundersökning som bland annat kom fram till att 80 procent av hans respondenter hade haft bekymmer med de elektroniska handlingarnas autenticitet och 32 procent, motsvarande 33 personer, hade vid minst något tillfälle blivit tvungna att fastställa autenticiteten hos någon elektroniskt handling.[14] Detta fungerar som motivering för uppsatsens första frågeställning. Det har bland amerikanska arkivarier uppvisats upplevda problem med autenticitet för elektroniskt arkivmaterial. I denna uppsats studeras primärt frågor kring informationssäkerhet, och autenticiteten får ses som nära sammanbunden med informationssäkerheten. Parks undersökning har nu 15 år på nacken och det är därför nödvändigt att återigen 2013 undersöka den aktuella situationen, om någonting har förändrats sedan denna studie. Det finns en lucka i forskningen som måste fyllas igen. Det behövs en ny undersökning i stil med den som gjordes för 15 år sedan. Den föregående studien genomfördes bland amerikanska arkivarier och det finns därför ett behov att göra en liknande studie även inom den svenska arkivariekåren. Detta tycks aldrig tidigare ha gjorts på detta sätt.

För att konkretisera och ge ett verktyg för att uppfylla syftet så har dessa frågeställningar formulerats:
–Hur behandlas informationssäkerhet i den arkivvetenskapliga litteraturen?
– Hur ser svenska arkivarier på informationssäkerhet?
–Vilka problem och lösningar framhålls i informationssäkerhetsfrågorna?

[14]Park, Eun G., “Understanding ‘authenticity’ in records and information management: analyzing practitioner constructs”, *The American Archivist*, 2001:64, s. 276.

Metod, källor och källkritik

I uppsatsen kombineras två olika metoder med varandra. För att besvara den förstafrågeställningen har det dels genomförts en kvalitativ litteraturstudie, dels en enkätundersökning bland svenska arkivarier, specifikt sådana som hanterar e-arkiv. Ett första utkast till enkät skickades ut som provenkät till ett fåtal svenska arkivarier, för att kontrollera så att frågorna var begripliga och passande. Respondenterna för den första provenkäten var kommunarkivarierna i Nordanstig och Hudiksvall samt tidigare arkivchefen i Sundsvall. Därefter korrigerades enkäten något innan den slutliga enkäten skickades ut, 8 april. En påminnelse om enkäten skickades ut till de som ännu inte hade svarat 21 april. Svarsresultaten har sammanställts och satts i relation med resultatet från en litteraturstudie kring tidigare forskning, både svensk och internationell sådan. Det är en kvalitativ enkätundersökning som har genomförts och respondenterna har fått svara på öppna frågor.[15] Det beror på att syftet med enkäten var att respondenterna skulle få svara så fritt som möjligt och därmed ge så utförliga svar som möjligt. Denna typ av enkät med öppna frågor kategoriseras av Holme och Solvang som formell och ostrukturerad datainsamling.[16]Den kvalitativa metoden valdes för att ge mer djup i enkätsvaren, inte att samla stora mängder data till statistikbehandling.[17]

Anledningen till att just svenska arkivarier har valts som urvalsgrupp är flera. Bland annat tycks någon liknande studie tidigare aldrig ha genomförts bland svenska arkivarier. Den primära anledningen är dock att den bedömningen har gjorts att valet av svenska arkivarier kommer ge den högsta svarsfrekvensen. Denna bedömning är möjligen subjektiv och kanske till och med felaktig, men det går att anta att om en presentation av en svensk magisteruppsats av en svensk arkivstuderande och en skriftlig intervju med några frågor skickas ut till olika arkivarier, så kanske de svenska arkivarierna på något sätt känner större skyldighet eller intresse av att besvara frågorna än om den skulle skickas ut internationellt. Valet av svenska arkivarier som urvalsgrupp är alltså primärt ett försök att få svarsfrekvensen att bli så hög som möjligt.

[15] Ejvegård, Rolf, *Vetenskaplig metod*, Lund 2009, s. 51.
[16] Holme, Idar Magne & Solvang, Bernt Krohn, *Forskningsmetodik – Om kvalitativa och kvantitativa metoder*, Lund 2008, s. 85.
[17] Ibid., s. 78.

Till respondenter valdes Riksarkivet, de sju landsarkiven samt stadsarkivet i alla svenska kommuner med ett invånarantal på över 100 000 invånare, enligt siffror från årsskiftet 2012/2013. Detta rör sig om stads- och kommunarkiven i kommunerna: Stockholm, Göteborg, Malmö, Uppsala, Linköping, Västerås, Örebro, Norrköping, Helsingborg, Jönköping, Umeå, Lund, Borås och Huddinge, inalles 14 stycken. Efter tips utifrån valdes dessutom Hudiksvalls kommunarkiv samt Skatteverkets arkiv ut som ytterligare respondenter. Respondenternas totala antal är 24. Av dessa svarade 14, vilket ger en svarsfrekvens på 58 procent. Detta behandlas mer utförligt i den sammanfattande slutdiskussionen.

Anledningen till att de större arkiven valdes är för att de hanterar mest material och därför sannolikt bäst kan besvara frågeställningarna och sannolikt har bäst koll på problematiken kring teknisk informationssäkerhet, autenticitet och tillförlitlighet när det gäller elektroniskt arkivmaterial. Inom de större arkiven är det dessutom mer sannolikt att det finns särskilda enheter för just e-arkivering, vilket inte alltid finns vid de mindre kommunarkiven ute i landet. Vid den första provenkäten deltog bland annat Hudiksvalls kommunarkivarie och gav så pass utförliga svar på frågorna att även de redovisas i uppsatsens enkätundersökning och får därför utgöra ensam representant för mindre kommunarkiv.

Enkäten genomfördes rent praktiskt genom att ett e-brev skickades ut till respondenterna, ett brev som innehöll en presentation av uppsatsen samt en rad frågor för dem att besvara.[18] Tanken var att få in skriftliga svar och med denna typ av enkät har respondenterna fått mer betänketid än om muntliga intervjuer skulle ha genomförts. Med den skriftliga enkätundersökningen har det därför varit möjligt att få mer eftertänkta svar och sannolikt också en högre kvalitet på svaren.

Att två metoder kombineras med varandra motiveras med att vissa studier förutsätter en sådan kombination för att få fram så högkvalitativa resultat som möjligt.[19]De bägge metoderna kompletterar och bekräftar varandra. Resultaten blir då mer tillförlitliga, om de kan bekräftas genom två helt olika metoder.[20] På de punkter där resultaten från litteraturstudien och intervjuundersökningen skiljer sig åt kan det finnas anledning att bedriva fortsatt forskning.

[18] Trost, Jan, *Kvalitativa intervjuer*, Lund 2009, s. 22.
[19] Alvesson, Mats & Sköldberg, Kaj, *Tolkning och reflektion – vetenskapsfilosofi och kvalitativ metod*, Lund 2008, s. 18-19; Holme, Idar Magne & Solvang, Bernt Krohn, *Forskningsmetodik: Om kvalitativa och kvantitativa metoder*, Lund 2008, s. 85.
[20] Holme, Idar Magne & Solvang, Bernt Krohn, *Forskningsmetodik: Om kvalitativa och kvantitativa metoder*, Lund 2008, s. 86.

Genom denna kombination av metoder kan alltså uppsatsen bidra med att ringa in specifika områden som måste studeras ytterligare av den framtida arkivvetenskapliga forskningen. På så sätt kan metodkombinationen bidra med att ytterligare föra arkivvetenskapen framåt.

Genom kombinationen av metoder går det att studera frågan ur något olika angreppssätt och därmed ge en mer mångsidig bild av det studerade området. I denna uppsats utgör den kvalitativa litteraturstudien en form av förstudie som lägger grund för intervjuundersökningen. Litteraturstudien är nödvändig för att kunna ta reda på vilka frågor som behöver ställas i intervjuerna och på vilka områden som det finns luckor i forskningen som behöver analyseras ytterligare.Med hjälp av litteraturstudien går det dessutom att se trender och tendenser i den arkivvetenskapliga forskningen och hur denna har utvecklat sig när det gäller den tekniska informationssäkerheten under de senaste åren. Detta bidrar med viktig kunskap och hjälper till att uppfylla uppsatsens syfte. De bägge metoderna har i uppsatsen jämbördiga roller och ingen av dem bör betraktas som mer primär än den andra.

Avgränsning och urval

Sökning av arkivtidskrifterna har avgränsats till att gälla årgångarna från år 2000 och framåt. Detta är en rimlig avgränsning av ett par skäl. Eftersom det handlar om en magisteruppsats, ett 10 veckor långt arbete, så måste avgränsningen vara så pass snäv att arbetsmaterialet inte svämmar över till proportioner som är omöjliga att behandla under 10 veckors uppsatsarbete. En annan anledning till just avgränsningen år 2000 och framåt är att tanken med uppsatsen är att fokusera på informationssäkerheten kring elektroniskt arkivmaterial. Forskningen kring denna fråga har förstås varit som mest framskriden och avancerad under 2000-talet, eftersom den elektroniska utvecklingen ständigt går framåt i mycket snabb takt. Vetenskaplig forskning om elektronisk informationssäkerhet från 1900-talet är med andra ord ganska föråldrad idag och därför har denna valts bort.

Teoretiska utgångspunkter

I uppsatsens inledning redovisades en modell för informationssäkerhetsbegreppet med ett antal olika beståndsdelar som tillsammans utgör detta begrepp, vilken kallas för Parkerian hexad. Enligt denna modell utgörs informationssäkerheten av följande olika delar:

konfidentialitet, kontroll, integritet, autenticitet, tillgänglighet och användbarhet.[21]Det krävs en förklaring av vad som menas med de olika delarna. Att en handling är konfidentiell innebär att den är tillgänglig bara för de personer som har behörighet. Med kontroll menas att obehöriga personer inte har någon som helst möjlighet att ändra eller redigera handlingen. Integritet innebär att de elektroniska handlingarnas data är pålitligt och oförändrat. Ytterligare en del i begreppet är tillgänglighet, att användarna kan komma åt handlingen när de önskar, eller åtminstone med relativt kort varsel. Det är något oklart vad upphovsmannen Parker menar med begreppet användbarhet i informationssäkerheten, för enligt modellen innebär detta att säkerheten som sådan inte på något sätt ska inverka på handlingens praktiska användbarhet.[22]

Den sista återstående beståndsdelen inom Parkerian hexads beskrivning av informationssäkerheten är autenticitet, vilket ska förklaras och diskuteras närmre. InterPARES 1 beskriver begreppet autenticitet som att en handling är autentisk och att en handling i sin tur är autentisk om den bygger på fakta. De anger autentisk som en synonym med begreppet genuin, att en handling inte är förfalskad på något sätt, utan att den bygger på fakta från pålitliga källor.[23] En autentisk handling är alltså vad den utger sig för att vara och får inte vara ändrad på något sätt så att dess ursprungliga innehåll skadas. InterPARES 2 definierar autenticitet såsom att autenticiteten är en mätare för handlingarnas tillförlitlighet över tid.[24] Autenticitetsbegreppet beskrivs på samma sätt i ordlistorna för InterPARES 1, InterPARES 2 och InterPARES 3, nämligen att autenticitet garanterar handlingens tillförlitlighet och kvalitet, att den är vad den utger sig för att vara och inte har förvanskats eller förändrats på något sätt.[25]

Definitioner

Ett centralt begrepp i uppsatsen är digital eller elektronisk arkivhandling. En rapport från *Digital Preservation Testbed* definierar detta begrepp. Det går inte rakt av att säga att de digitala handlingarna enbart är en digital variant av de analoga handlingarna, utan de är skapade och måste utläsas under helt andra omständigheter. Detta därför att de är beroende av

[21]http://smartgridsecurity.blogspot.se/2010/06/hexad-dicted.html(hämtad: 130608).
[22]Ibid.
[23] MacNeil, Heather et. al., *Authenticity task force report*, 2001, s. 2.
[24]Roeder, John et. al., *Domain 2task force report*, 2008, s. 9.
[25]MacNeil, Heather et. al., *The InterPARES glossary*, 2001, s. 1; Duranti, Luciana et. al., *The InterPARES 2 project glossary*, 2008, s. 8; http://www.interpares.org/ip3/ip3_terminology_db.cfm?letter=a&term=13 (hämtad: 130608).

teknisk utrustning, både hårdvara och mjukvara.[26] De är därför mer komplexa och beroende av yttre omständigheter på ett annat sätt än de analoga handlingarna. Om de yttre omständigheterna inte är de rätta, om den tekniska utrustningen inte stämmer, så är de helt oläsbara. För att digitala handlingar ska kunna tolkas krävs det att hårdvara, mjukvara och datorfiler stämmer överens med varandra. Därför går det inte att använda begreppet handling som ett allmänt begrepp, utan i sina analoga respektive digitala varianter är de totalt skilda från varandra. Därför har handlingsbegreppet blivit mer komplext.

Ett annat centralt begrepp i uppsatsen är informationssäkerhet. Med informationssäkerhet menas att informationen är säker från olika angrepp eller informationsbortfall under hela sin livslängd. Begreppet informationssäkerhet har enligt en statusrapport från Riksarkivet ifrågasatts och vissa har föreslagit användning av begreppen ADB-säkerhet eller datasäkerhet istället, men här kommer informationssäkerheten att användas.[27]I denna uppsats rör det sig specifikt om information som finns i digitala arkivhandlingar. För att informationen ska vara säker måste den kunna klara sig oförändrad genom alla formatväxlingar och överföringar av olika slag, utan att någon information faller bort eller hamnar utanför sin kontext. Exempel på överföringar är dels när handlingen skickas från sitt upphov till sin mottagare eller när det skickas från sin användare till arkivet, men även migrering när den omvandlas från ett äldre utdaterat filformat till ett nyare och mer anpassat efter den nya tekniska utrustningen och mjukvaran. Informationen måste dessutom vara säker från olika former av obehöriga intrång, exempelvis hackare som vill förvanska handlingens innehåll eller att någon person av ren okunskap råkar förvanska handlingen så att information försvinner och informationssäkerheten därmed fallerar.

Uppsatsen studerar inte hela begreppet informationssäkerhet som sådant, utan primärt den tekniska informationssäkerheten, de rent tekniska detaljerna. Dessa är att skilja från mänskliga detaljer, såsom exempelvis att låsa arkivlokaler för att hindra obehöriga att ta sig in. Med den tekniska informationssäkerheten menas bland annat att den tekniska lagringen är säker, att informationen tar sig oskadad genom bland annat migreringsprocesser. Det handlar också om att information tar sig oskadad genom olika överföringar, exempelvis om de skickas från sin skapare till sin användare via e-post, att den inte i denna överföring riskerar att hamna i orätta

[26]Digital Preservation Testbed, *From digital volatility to digital permanence. Preserving text documents*, Haag 2003, s. 6.
[27] Riksarkivet, *Statusrapport informationssäkerhet – remissgenomgång*, Diarienummer RA 22-2007/3552, s. 1.

händer, förvanskas eller bortfall av information. Detta är ett klargörande av vad inom informationssäkerheten som uppsatsen syftar till att studera, respektive vad den inte studerar. Det är den tekniska informationssäkerheten som är det centrala och primära. Uppsatsen syftar inte till att närmare studera de rent mänskliga detaljerna och effekterna på informationssäkerheten.

Litteraturstudie

Inledning

När det gäller den arkiv- och informationsvetenskapliga forskningen kring teknisk informationssäkerhet samt de närliggande begreppen autenticitet och tillförlitlighet så går det att se vissa tendenser och trender, även under en så pass kort tid som 2000–2013, den period som studeras här. Som framgår i detta avsnitt så går det att se att det i början av 2000-talet skrevs mycket om framförallt elektroniska signaturer och övrig teknisk kryptering. Det går att förnimma en utveckling att det under senare år istället har skrivits mer allmänt om informationssäkerhetens koppling till begreppen tillförlitlighet och autenticitet samt dess betydelse för arkivens ställning och status i samhället. Utöver detta är det svårt att se några egentliga tendenser och trender i den arkivvetenskapliga forskningens utveckling på området informationssäkerhet.

Om elektroniska signaturer och övrig teknisk kryptering

En av de metoder som finns för att försöka skydda arkiven mot förfalskningar och stärka informationssäkerheten är elektroniska signaturer.[28]Som antyds av namnet är detta en metod som enbart används för elektroniskt arkivmaterial. Elektroniska signaturer baserar sig på kryptografi. Kryptografi innebär att det behövs en form av elektroniska nycklar för att kunna få tillgång till handlingen. Det innebär att enbart den som har tillgång till nyckeln kan ändra signaturen, vilket är tänkt att stärka de elektroniska handlingarnas informationssäkerhet och tillförlitlighet. Det har från Europaparlamentets sida utfärdats direktiv om de elektroniska signaturernas uppbyggnad och struktur. Detta system är baserat på i första hand PGP, vilket är ett elektroniskt chifferkodsystem, men även andra chiffersystem förekommer, så som PKI.[29] Enligt Boudrez har dock PKI-krypteringen en väldigt kort livslängd och handlingar krypterade med PKI kan bara lagras en kortare tid.[30]

[28] MacNeil, Heather, ”Providing grounds for trust II: the findings of the authenticity task force of InterPARES”, *Archivaria*, 2002:54, s. 26–27.
[29] Wessbrandt, Karl, *Förstudierapport om framtidens elektroniska arkiv*, Statskontoret, Dnr 2003/67, ändrad 2003-06-04, s. 33; MacNeil, Heather, “Providing grounds for trust: developing conceptual requirements for the long-term preservation of authentic electronic records”, *Archivaria*, 2000:50, s. 62.
[30]Boudrez, Filip, “Digital signatures and electronic records”, *Archival Science*, 2007:2, s 185.

Wessbrandt skriver att dagens elektroniska signaturer och krypteringssystem fortfarande bygger på teknik från 1970-talet.[31]Om tekniken är så pass gammal kan det kanske vara på sin plats att utveckla någon nyare teknik för att säkerställa äktheten hos elektroniskt arkivmaterial. Wessbrandt menar inte att exakt samma kryptografi har använts från 1970-talet och 40 år framåt, utan den uppdateras ständigt och med jämna mellanrum utvecklas starkare krypteringar. Själva tekniken har dock i 40 år i grunden varit densamma och det är möjligt att det skulle kunna skapas någon ännu säkrare metod för att säkerställa informationssäkerheten av elektroniskt arkivmaterial än kryptografin, även om vi inte har nått dit riktigt ännu. Kryptografin är inte helt bombsäker, utan denna typ av kryptering och chiffer går att knäcka och ta sig igenom. Det skulle behövas, om möjligt, en metod som helt enkelt inte går att ta sig igenom för den som vill komma åt känslig information utan att vara behörig. Den elektroniska signaturen är ganska säker, men eftersom den inte är perfekt och felfri så innebär det att en handling rent teoretiskt kan vara förvanskad trots att den har en giltig elektronisk signatur, om någon har lyckats knäcka krypteringen och på så vis kan ändra handlingen utan att skada signaturen.

I Eun Parks undersökning kring arkivens informationssäkerhet från 1998 har han bland annat frågat sina respondenter om vilka metoder de brukar använda för att verifiera äktheten hos olika dokument. När det gäller det elektroniska arkivmaterialet är det enbart 7 procent av respondenterna som har svarat att de primärt kontrollerar de elektroniska signaturerna, så enligt denna studie är signaturen en av de mindre viktiga faktorerna för äkthetskontroll.[32]När det gäller de elektroniska handlingarna har istället i första hand andra autenticitetssymboler eller tillförlitligheten av handlingens upphov granskats. 24 respektive 22 procent av respondenterna har uppgett att de i första hand kontrollerar dessa bägge faktorer. Detta visar att de elektroniska signaturerna 1998 var av mindre betydelse och att flera andra faktorer var betydligt viktigare. Nu är det 15 år sedan denna studie genomfördes och det är nödvändigt att kontrollera situationen idag och se om läget på något sätt har förändrats. Bland arkivarier 1998 var den mest betydelsefulla faktorn för pålitligheten av elektroniskt arkivmaterial att handlingens upphov eller källa var pålitlig.[33]

[31] Wessbrandt, Karl, *Förstudierapport om framtidens elektroniska arkiv*, Statskontoret, Dnr 2003/67, ändrad 2003-06-04, s. 32.
[32]Park, Eun G., "Understanding 'authenticity' in records and information management: analyzing practitioner constructs", *The American Archivist*, 2001:64, s. 282.
[33]Ibid., s. 283.

Ruusalepp har i en rapport skrivit att flera riksarkiv i världen har motsatt sig uppdateringen av de elektroniska signaturerna för sina elektroniska handlingar.[34]Han tar upp att det tyska riksarkivet låser upp och avkrypterar alla de krypterade elektroniska handlingar de får in, eftersom de vill ha sina handlingar läsbara utan att det ska krävas speciell utrustning eller nycklar. Han tar upp att flera andra riksarkiv har liknande förfaringssätt.[35]Om arkiven avkrypterar alla sina handlingar på detta sätt blir de elektroniska signaturerna i stort sett meningslösa och kan inte längre skydda handlingarnas informationssäkerhet.Ruusalepp förklarar detta agerande från arkivens sida med att det är svårt att långsiktigt bevara de elektroniska signaturerna och att de därför hellre väljer att avkryptera handlingarna och försöka säkra autenticiteten och informationssäkerheten med säker struktur och organisation istället.[36] Samtidigt som arkiven avkrypterar sina handlingar och därmed i stort sett gör de elektroniska signaturerna meningslösa så är det flera andra myndigheter som uppmuntrar till användningen av elektroniska signaturer för att stärka informationssäkerheten, såsom CSN, Posten och Telia.[37] Det har dessutom kommit förslag att arkiven ska underteckna alla sina mottagna handlingar med egna elektroniska signaturer för att komplettera eller eventuellt ersätta de ursprungliga signaturerna.[38]

Elektroniskt arkivmaterial måste med jämna mellanrum migreras från gamla föråldrade format till nya.[39] Detta eftersom den tekniska utvecklingen går framåt i väldigt snabb takt och handlingar i gamla format inte längre kan läsas eller få en försämrad läsbarhet i de nya programmen. Migreringen och den formatändring som denna innebär leder till vissa risker för informationsbortfall.[40] Wessbrandt anser att förekomsten av elektroniska signaturer förvärrar denna risk och problemen med migrering ytterligare.[41]Enkelt uttryckt så blir migreringen mer besvärlig ju fler olika element som en handling innehåller och om handlingarna är undertecknade med elektroniska signaturer så måste även dessa migreras oförändrade från ett format till ett annat. I vissa fall kanske till och med signaturerna utgör egna filer och då måste kopplingen mellan de olika filerna bevaras oskadad genom migreringsprocessen.

[34]Ruusalepp, Raivo, *Digital preservation in archives: An overview of current research and practices*, 2005, s. 11.
[35]Ibid., s. 11–12.
[36] Ibid., s. 12.
[37] Statskontoret 2000:5, *Intelligenta tjänster och elektroniska blanketter*, s. 25–26.
[38] Boudrez, Filip, "Digital signatures and electronic records", *Archival Science*, 2007:2, s 180.
[39] Hedstrom, Margaret, "'The Old Version Flickers More' – Digital Preservation from the User's Perspective", *The American Archivist*, 2006:69, s. 161.
[40] Ibid., s. 164–165.
[41] Wessbrandt, Karl, *Förstudierapport om framtidens elektroniska arkiv*, Statskontoret, Dnr 2003/67, ändrad 2003-06-04, s. 33.

Det elektroniska materialet utgör en allt större andel av det svenska arkivbeståndet i den nuvarande samhällsutvecklingen mot en alltmer papperslös arkivhantering. Lars-Erik Hansen har skrivit en artikel där han diskuterar de elektroniska signaturernas ohållbarhet på längre sikt. En riktigt skicklig hacker med rätt resurser kan, enligt Wessbrandts rapport, knäcka alla elektroniska krypteringssystem och då hjälper inte de elektroniska signaturerna för att bevara arkivhandlingarnas äkthet.[42] Om hela krypteringssystemet har blivit knäckt kan obehöriga personer ändra och göra redigeringar i elektroniskt arkivmaterial och då saknar signaturen betydelse. Det går med andra ord aldrig fullt ut att lita på de elektroniska signaturerna, även om många krypteringar kan vara väldigt starka och oerhört svåra att ta sig igenom.

I många fall finns det olika certifikat för de elektroniska signaturerna och krypteringssystemen som enbart gäller under en begränsad tid.[43] Certifikaten kräver vissa data för att kunna användas och utvecklarna av de olika certifikaten måste enligt lag kunna tillhandahålla dessa data i minst sju år efter att certifikaten slutar gälla.[44] De elektroniska signaturerna kan dock migreras eller regenereras precis som de elektroniska handlingarna i sin helhet.[45] I en sådan migrering ändras dock bitströmmarna i krypteringen och Boudrez anser att de elektroniska förlorar sin funktion i och med en migrering, att de inte längre kan garantera handlingens informationssäkerhet, eftersom dess bitströmmar är annorlunda och inte längre stämmer överens med originalet.[46] Ett förslag till lösning på detta som Boudrez tar upp är att återsignera de digitala handlingarna efter en migrering, även om detta rent praktiskt kan vara svårt i vissa sammanhang, om upphovspersonen bakom den ursprungliga signaturen är oförmögen eller ovillig att signera handlingen på nytt.[47] Vidare blir själva krypteringssystemen med tiden föråldrade allteftersom den teknologiska utvecklingen går framåt i mycket snabb takt.[48] Det är detta Hansen menar med att de elektroniska signaturerna inte är hållbara i längden.

---

[42] Hansen, Lars-Erik, "Elektroniska signaturers omöjliga liv i ett långtidsarkiv", *Arkiv, samhälle och forskning*, 2002:2, s. 72; Wessbrandt, Karl, *Förstudierapport om framtidens elektroniska arkiv*, Statskontoret, Dnr 2003/67, ändrad 2003-06-04, s. 33.
[43] Boudrez, Filip, "Digital signatures and electronic records", *Archival Science*, 2007:2, s 185.
[44] Digital Preservation Testbed, *From digital volatility to digital permanence. Preserving text documents*, Haag 2003, s. 20–21.
[45] Wessbrandt, Karl, *Förstudierapport om framtidens elektroniska arkiv*, Statskontoret, Dnr 2003/67, ändrad 2003-06-04, s. 34; Boudrez, Filip, "Digital signatures and electronic records", *Archival Science*, 2007:2, s 186.
[46] Boudrez, Filip, "Digital signatures and electronic records", *Archival Science*, 2007:2, s 187.
[47] Ibid., s 187–188.
[48] Hansen, Lars-Erik, "Elektroniska signaturers omöjliga liv i ett långtidsarkiv", *Arkiv, samhälle och forskning*, 2002:2, s. 74.

Det finns projekt som syftar till att skapa digitala signaturer som kan lagras långsiktigt. Det är bland annat ett EU-projekt vid namn EESSI. Victorian Electronic Records Strategy, VERS, är ett kanadensiskt initiativ med liknande syfte. Inom VERS försöker man lösa problematiken med långsiktigt bevarande av elektroniska signaturer genom att de ursprungliga elektroniska signaturerna och de nya migrerade signaturerna inkapslas tillsammans i samma filer och på så sätt är förhoppningen att den ursprungliga bitströmmen kan bevaras samtidigt som signaturen migreras till ett nytt och säkrare format.[49]

Filip Boudrez anser att elektroniska signaturer eller liknande former av krypteringssystem är en opassande metod för att garantera äktheten hos elektroniska arkivhandlingar. Detta därför att de enbart bevisar att personen som har skapat eller redigerat ett dokument har tillgång till en viss krypteringsnyckel. Den person som har skapat dokumentet behöver inte vara densamme som signaturen är registrerad på. Signaturen bevisar inte att en viss person har skapat handlingen, även om detta är sannolikt. Boudrez diskuterar möjligheten av stöld av krypteringsnycklarna. Om en någon har lyckats stjäla en nyckel kan denne skapa dokument och handlingar i någon annans namn.[50] Det går förvisso att invända mot Boudrez beskrivning att analoga signaturer i så fall har samma bristande funktion. Varken de analoga eller de elektroniska kan med hundra procents säkerhet garantera att en viss person har författat en handling, utan det bevisar enbart att någon har författat handlingen i denna persons namn. Ingen signatur är skyddad från urkundsförfalskning, utan alla former av signaturer kan förfalskas, vilket i Sverige är en brottslig handling.

I och med att den teknologiska utvecklingen går framåt så går det hela tiden att skapa nya mer säkra elektroniska krypteringssystem, men den teknologiska utvecklingen kommer även hackarna till del. Deras möjligheter att knäcka krypteringssystem är större om krypteringen är gammal och utdaterad. Detta är en problematik som måste lösas för att stärka den långsiktiga informationssäkerheten bland elektroniskt arkivmaterial. En typ av digitala arkivhandlingar som är extra känsliga för intrång och förfalskningar är de digitala personarkiven. De handlingar som finns i dessa arkiv är ofta lättare att manipulera och det är dessutom lättare att

[49]Boudrez, Filip, "Digital signatures and electronic records", *Archival Science*, 2007:2, s 189.
[50] Ibid., s. 184.

undvika upptäckt.[51] Upphovspersoner till personarkiv har sällan samma möjlighet att skapa en stark kryptering som olika myndigheter eller större organisationer har.

För att kunna ge handlingarna ett så starkt skydd som möjligt mot obehörigt intrång gäller det att konvertera äldre handlingars krypteringssystem och se till att det hela tiden är den senaste och säkraste krypteringen som används. Detta är kostsamt, både ekonomiskt och tidsmässigt.[52] Hansen föreslår att informationssäkerheten kan stärkas om alla elektroniskt signerade handlingar sparas i form av dubbletter som förvaras på olika platser.[53] På så vis är det lättare att upptäcka om någon har försökt ändra och förvanska handlingen, eftersom dubbletten förhoppningsvis klarar sig från denna ändring. Det blir svårare för hackare att göra exakt samma förvanskning av en arkivhandling som förvaras på två olika platser än om det skulle vara ett enda exemplar. Utöver elektroniska signaturer och säkerhetskopior kan informationssäkerheten kring digitalt arkivmaterial stärkas med vad Ruusalepp kallar för tidsstämplar, vilket verkar vara någon speciell variant av elektroniska signaturer som bevarar datum eller tidpunkter för olika handlingar.[54]

Olika metoder för att stärka den tekniska informationssäkerheten

De elektroniska signaturerna ensamma kan inte garantera informationssäkerheten, utan måste kombineras med tillit till avsändaren eller upphovspersonen.[55] En elektronisk signatur hjälper inte mycket om själva avsändaren är opålitlig och på samma sätt finns det anledning att vara tveksam kring informationssäkerhet och tillförlitlighet om en pålitlig avsändare skickar ett dokument utan elektronisk signatur. De bägge måste kombineras med varandra för att ge en stark informationssäkerhet och tillförlitlighet. Vidare diskuterar Ivarsson att de digitala handlingarna lätt kan påverkas av olika migreringar där elektroniska dokument omvandlas från gamla format till modernare, en vanligt förekommande åtgärd inom långtidshanteringen av digitala arkiv. Ju starkare kryptering som har använts för att skapa den digitala signaturen, desto bättre klarar den sig oskadad genom en migrering.[56]

[51] Hansen, Lars-Erik, ”Digital informationshantering för personarkiv”, *Arkiv, samhälle och forskning*, 2008:2, s. 114.
[52] Hansen, Lars-Erik, “Elektroniska signaturers omöjliga liv i ett långtidsarkiv”, *Arkiv, samhälle och forskning*, 2002:2, s. 74.
[53] Ibid., s. 74–75.
[54] Ruusalepp, Raivo, *Digital preservation in archives: An overview of current research and practices*, 2005, s. 11.
[55] Ivarsson, Elisabeth, ”Autenticitet och digitala dokument”, *Arkiv, samhälle och forskning*, 2007:2, s. 81.
[56] Ibid.

Hansen skriver om behovet av tydliga rutiner i den elektroniska informationshanteringen. Tydliga rutiner och användningen av signaturer kan komplettera varandra och stärka materialets tillförlitlighet. En ostrukturerad hantering utan rutiner ökar sannolikt risken att drabbas av olika former av obehöriga intrång där de elektroniska handlingarna riskerar att förvanskas.[57]Med ett tydligt regelverk och om de elektroniska handlingarna används i verksamhetsprocesserna så går det att spåra när personer på något vis ändrar handlingarna och vilka det är som gör dessa ändringar. Då går det lätt att upptäcka försök till förvanskning av handlingarna och detta stärker informationssäkerheten.[58]

Den tekniska informationssäkerhetens relation till tillförlitlighet och autenticitet

Price och Smith skriver att arkiven har ett trovärdighetsproblem i och med den bristande informationssäkerheten kring elektroniskt arkivmaterial. Användarna litar helt enkelt inte fullt ut på att det elektroniska arkivmaterialet i alla lägen är korrekt.[59] Anneli Sundqvist tar fram liknande forskning som pekar på att invånarnas förtroende just nu minskar inte bara för arkiven, utan också för samhälleliga institutioner och myndigheter generellt.[60] För att motverka detta är det nödvändigt att utveckla system och metoder som kan garantera informationssäkerheten och därefter att bevisa detta inför användarna. Om användarna misstänkliggör arkivmaterialet förlorar arkiven i sig både status och anseende, vilket kan få en rad olika negativa följdeffekter, såsom minskade anslag och en nedåtgående spiral där kompetensutvecklingen inom arkivvärlden stannar av eller går bakåt. Det är gynnsamt för arkiven om människor litar på dem, men denna tillförlitlighet måste förtjänas och den förtjänas enbart om arkiven kan tillhandahålla en mycket hög nivå av informationssäkerhet. Om detta inte kan tillhandahållas har användarna all rätt att misstänkliggöra arkivmaterialet.

Sundqvist skriver att arkivhandlingarna under den senare tiden har fått en allt viktigare roll inom framförallt affärsvärlden, att de fyller en viktig funktion i olika former av bevisföring för olika inträffade händelser.[61] Det är därför nödvändigt från arkivens sida att kunna garantera äkthet, handlingar som innehåller tillförlitliga och korrekta uppgifter. Felaktigheter i arkivmaterialet sprider sig vidare ut i samhället när handlingarna används i exempelvis

[57] Hansen, Lars-Erik, "Elektroniska signaturers omöjliga liv i ett långtidsarkiv", *Arkiv, samhälle och forskning*, 2002:2, s. 74
[58] Ivarsson, Elisabeth, "Autenticitet och digitala dokument", *Arkiv, samhälle och forskning*, 2007:2, s. 82.
[59] Price, Dara M., & Smith, Johanna J., "The trust continuum in the information age: a Canadian perspective", *Archival Science*, 2011:3–4, s. 262.
[60] Sundqvist, Anneli, "Documentation practices and recordkeeping: a matter of trust or distrust?", *Archival Science*, 2011:3–4, s. 284.
[61] Ibid., s. 277.

bevisföring. Om en arkivhandling med felaktig information används så etableras dessa felaktiga uppgifter. Samtidigt som arkivmaterialet och arkiven tycks viktigare än någonsin för samhället så befinner vi oss nu i en fas där vissa användare och medborgare ifrågasätter arkivens tillförlitlighet, enligt både Sundqvist, Price & Smith. I perioder av stora samhällsförändringar, däribland teknologiska förändringar, så ifrågasätts tillförlitligheten extra mycket och i en sådan fas befinner sig samhällsutvecklingen just nu.[62] Detta är en naturlig mänsklig reaktion på stora förändringar och samhällsomvandlingar, att visa viss osäkerhet.

Speck har skrivit en artikel om det elektroniska arkivmaterialets tillförlitlighet och påpekar att trots att tillförlitligheten är ett så centralt tema för arkivens roll, ställning och status i samhället så finns det förvånande lite forskning om detta.[63] Om användarna inte litar på arkiven har de ingen egentlig roll att fylla i samhället, så därför är det livsnödvändigt för arkiven att upprätthålla en god tillförlitlighet och därmed också en hög informationssäkerhet. Enligt Speck så förekommer viss diskussion bland dagens arkivarier och arkivvetare om tillförlitligheten, men många andra frågor diskuteras mycket mer. Tillförlitligheten måste vara ett ständigt arbetsområde för arkivarier, de måste ständigt verka aktivt för att upprätthålla tillförlitligheten så att användarna har tilltro till arkiven och de därmed kan ha en god ställning i samhället. Tillförlitligheten är inget permanent tillstånd, utan den kan raseras fort om det skulle inträffa någon dramatisk händelse som visar allvarliga missförhållanden i arkivens informationssäkerhetsmässiga arbetsrutiner inför allmänheten. Däremot kan sannolikt inte en förlorad tillförlitlighet byggas upp lika snabbt som den kan raseras.

Arkiven tillhör en förtroendebransch och arkivarier har en maktposition i och med att de hanterar betydande delar av samhällets information. Det ligger i arkivariens händer att fatta beslut om vilken information som ska lämnas ut och inte och till vilka som informationen ska lämnas ut.[64] Det finns riktlinjer för hur detta ska gå till, men i sista hand är det arkivarien själv som väljer eller inte väljer att lämna ut information. Arkivarien fattar vidare i sista hand beslut om vad som ska gallras och vad som ska sparas, även om det finns riktlinjer även för detta. Besluten ligger i sista hand hos arkivarien personligen. Därför måste inte bara arkiven i sig

[62]Sundqvist, Anneli, ”Documentation practices and recordkeeping: a matter of trust or distrust?”, *Archival Science*, 2011:3–4, s. 288.
[63] Speck, Jason, ”Protecting public trust: an archival wake-up call”, *Journal of archival organization*, 2010:8, s. 32.
[64]Ibid., s. 34–35.

vara tillförlitliga i samhällets ögon, utan även arkivarierna som individer. Det gäller att som arkivarier ha personer med gott omdöme och att allmänheten lägger märke till detta.

Arkivarien har ansvar gentemot flera olika parter på samma gång. En av parterna är allmänheten, en annan kan vara skaparen av olika handlingar och dokument och ytterligare en annan kan vara arbetsgivaren. Dessa olika parter kan ibland ha olika intressen och då blir det svårt att fatta beslut som gagnar alla, utan det kan bli nödvändigt att fatta beslut som leder till att den ena partens intressen väger över de andra.[65] Det kan exempelvis vara så inom ett kommunarkiv att delar av den kommunala redovisningen kan vara ofördelaktig för kommunledningens anseende, men arkivarien måste ändå lämna ut detta när allmänheten så begär. I ett sådant läge går allmänhetens intresse före arbetsgivarens intresse, om arkivarien väljer att följa arkivlagen. Att inte lämna ut sådan offentlig information vore tjänstefel. Allmänhetens rätt att ta del av denna typ av handlingar är dock olika i olika länder i världen och arkivlagstiftningen kan skilja sig åt markant. Därför har även arkivlagstiftningen en mycket viktig roll för arkivens tillförlitlighet bland allmänheten.

ISO-standarden 15489:1 kräver att alla arkivhandlingar måste vara tillförlitliga, vare sig de är analoga eller digitala handlingar.[66] För att vara tillförlitliga måste det finnas rutiner och eventuella krypteringssystem för att minimera riskerna för att obehörigt intrång och förvanskning inträffar. Handlingarna måste bevaras oförändrade i sitt ursprungliga skick för att inte riskera informationsbortfall. När det gäller offentliga handlingar ska alla användare kunna ta del av dem och de ska finnas fullt sökbara och tillgängliga, men samtidigt ska ingen på något sätt kunna förändra dem på något sätt.[67]

Ivarsson skriver att det är mycket lättare att kontrollera äktheten hos analoga dokument, genom att studera bland annat signatur, handstil, bläck, papperskvalitet m.m.[68]Detta är inte möjligt att kontrollera när det gäller elektroniskt material, även om det också för dessa finns en form av signaturer. Därför blir det svårare att fastställa äkthet hos elektroniskt arkivmaterial. Livia Iacovino är också inne på den linjen, att framväxten av de elektroniska

[65]Speck, Jason, ”Protecting public trust: an archival wake-up call”, *Journal of archival organization*, 2010:8, s. 37.
[66] ISO 15489:1, First edition, *Part 1 – general*, 2001, punkt 7.2.2–7.2.5.
[67] Ivarsson, Elisabeth, ”Autenticitet och digitala dokument”, *Arkiv, samhälle och forskning*, 2007:2, s. 80.
[68] Ivarsson, Elisabeth, ”Autenticitet och digitala dokument”, *Arkiv, samhälle och forskning*, 2007:2, s. 81; Wessbrandt, Karl, *Förstudierapport om framtidens elektroniska arkiv*, Statskontoret, Dnr 2003/67, ändrad 2003-06-04, s. 32.

arkivhandlingarna har ökat risken för obehörig manipulation.[69] Det tycks lättare att förfalska elektroniska handlingar utan spår och upptäckt än när det gäller analogt material.[70] I det analoga materialet går dessa förfalskningar lättare att upptäcka, som sagt genom att studera exempelvis bläck eller papper.

Ivarsson diskuterar kring begreppen autenticitet och tillförlitlighet och konstaterar att ett dokument eller en handling mycket väl kan vara autentisk även om den inte är tillförlitlig, autentisk även om den är förfalskad. Giles Constable har samma synsätt i frågan.[71]Rothenberg argumenterar dock emot detta när han skriver att autenticitet innebär att en handling bland annat har riktighet och ”trohet till originalet”.[72]Även *Digital Preservation Testbed*och andra skribentet belyser att en handling inte kan vara autentisk utan riktighet.[73]En förfalskad handling har inte denna riktighet. Den kan dock vara trogen till originalet om den redan som originalhandling var förfalskad. Hur som helst bör denna Rothenbergs definition innebära att Ivarssons och Constables påstående inte stämmer fullt, nämligen att förfalskningar kan vara autentiska. Detta helt enkelt därför att en förfalskning är oriktig i sin natur. En handling som har blivit förvanskad eller på något sätt förändrad så att dess ursprungliga information inte längre är densamma kan inte betraktas som en autentisk handling.[74] Ändringar av en handling i efterhand kan tillåtas om inte dess ursprungliga mening förändras av det.[75] Sett ur detta hänseende blir Ivarssons påstående obegripligt, att även förfalskningar eller icke-tillförlitliga handlingar kan vara autentiska.

Bonnie Mak har skrivit en artikel om autenticitetsbegreppet där tre olika varianter av autenticitet fastställs. Dessa är den diplomatiska autenticiteten, den juridiska och den historiska, alla tre med olika kriterier.[76] En handling kan vara diplomatiskt autentisk även om den är icke-autentisk både juridiskt och historiskt. En diplomatiskt autentisk handling skulle kunna vara både juridiskt icke-autentisk om den har uppkommit på ett oetiskt sätt och därför

[69] Iacovino, Livia, “Recordkeeping and juridical governance “, i McKemmish, Sue (red.) *Archives: Recordkeeping in Society*, Wagga Wagga 2005, s. 255–276.
[70]Meijer, Albert, “Trust this document! ICTs, authentic records and accountability”, *Archival Science*, 2003:3, s. 278.
[71]Constable, Giles, “Forgery and Plagiarism in the Middle Ages,” *Archiv für Diplomatik*, 1983: 2.
[72]http://www.clir.org/pubs/reports/pub92/rothenberg.html (hämtad: 130227); MacNeil, Heather, “Providing grounds for trust: developing conceptual requirements for the long-term preservation of authentic electronic records”, *Archivaria*, 2000:50, s. 53; MacNeil, Heather, ”Providing grounds for trust II: the findings of the authenticity task force of InterPARES”, *Archivaria*, 2002:54, s. 26.
[73]Digital Preservation Testbed, *From digital volatility to digital permanence. Preserving text documents*, Haag 2003, s. 8.
[74] Ibid.
[75] Boudrez, Filip, “Digital signatures and electronic records”, *Archival Science*, 2007:2, s. 180.
[76]Mak, Bonnie, ”On the uses of authenticity”, *Archivaria*, 2012:73, s. 5.

inte kan användas i domstolsprövning, men den kan även vara historiskt icke-autentisk om den framställer historien på ett väldigt subjektivt och vinklat sätt.[77] En sådan handling kan, enligt Mak, trots detta vara diplomatiskt autentisk. En handling är historiskt autentisk om den återger historien på ett korrekt sätt, oavsett vilken typ av handling det är och oavsett om den är diplomatiskt eller juridiskt autentisk.[78] Handlingar kan vara intressanta och användbara på helt olika sätt och av helt olika anledningar beroende på om de ska användas inom diplomatik, juridik och historia och därför går det inte att fastställa något klart autenticitetsbegrepp. Begreppet autenticitet kan variera beroende på vilket syfte handlingen ska användas till.

InterPARES är ett internationellt forskningsprojekt kring autenticitet för elektroniska handlingar, att försöka säkerställa deras autenticitet långsiktigt. Detta forskningsprojekt har genomförts i tre olika delmoment: InterPARES 1 under åren 1999–2001, InterPARES 2 under åren 2002–2006 och InterPARES 3 under åren 2007–2012.[79] I rapporten som utgavs av det första delprojektet så konstateras att de elektroniska handlingarna är mer känsliga än de analoga vad gäller förvanskningar, både omedvetna och medvetna sådana.[80] Det gäller också förändringar i vad som kan kallas miljö, det vill säga den hårdvara och mjukvara som handlingarna är beroende av för att kunna läsas. Författarna använder detta som argument för lanseringen av forskningsprojektet, att förutsättningarna för att stärka de elektroniska handlingarnas långsiktiga informationssäkerhet måste förbättras.

I rapporten från InterPARES 1 så beskriver man fyra olika kategorier av elektroniska handlingar och med tanke på att det finns olika autenticitetsbegrepp beroende på om en handling ska användas i juridiska, diplomatiska eller historiska sammanhang så är det möjligt att även de fyra olika kategorierna får olika autenticitetsbegrepp och att deras autenticitet därför måste hanteras på olika sätt. Två av de kategorier som InterPARES behandlar är bevisande handlingar, vilka kan användas juridiskt, och narrativa eller berättande handlingar, vilka kan användas bland annat av historieskrivningen som källmaterial.[81]

Under flera hundra års tid så var autenticitetsbegreppet ungefär detsamma, men under slutet av 1900-talet och 2000-talet har begreppet återigen börjat diskuteras flitigt eftersom

[77]Mak, Bonnie, ”On the uses of authenticity”, *Archivaria*, 2012:73, s. 6.
[78]Ibid., s. 7.
[79]Duranti, Luciana, Eastwood, Terry & MacNeil, Heather, “Preservation of the integrity of electronic records”, *Archivaria*, 2008:66, s. 137.
[80] MacNeil, Heather et. al., *Authenticity task force report*, 2001, s. 2.
[81]Ibid., s. 15.

framväxten av det digitala samhället sätter tidigare begrepp på prov.[82] Denna uppblossade diskussion beror på nödvändigheten att inordna de nya digitala handlingarna i autenticitetsbegreppet, som redan sen länge är etablerat när det gäller analogt material. Förutsättningarna och omständigheterna kring elektronisk autenticitet är dock annorlunda och därför blir det nödvändigt att utarbeta nya strategier för att säkerställa autenticiteten för detta material. De analoga metoderna fungerar inte för det elektroniska materialet. Det elektroniska samhället har beskrivits som nära på regellöst, där kontorsanställda runt om i världen kan skapa och radera elektroniska handlingar helt efter eget tycke, vilket är otänkbart för analoga handlingar.[83]

Framväxten av digitala handlingar har gjort den juridiska bevisföringen mer komplicerad och komplex än vad den var förut i det helt analoga samhället. Det beror bland annat på att det inte går att verifiera ett digitalt dokuments äkthet bara genom att studera själva dokumentet, utan när det gäller digitala dokument är det nödvändigt att spåra deras uppkomst och alla förändringar som har inträffat under deras livslängd, hur de har förändrats och av vilka.[84] I de analoga dokumenten går det relativt lätt att granska olika ändringar genom att studera bläck, papperskvalitet och liknande rent praktiska detaljer, men när det gäller de digitala dokumenten blir det nödvändigt att samla ihop all tänkbar metadata och alla relaterade filer. Hela granskningen och fastställandet av äktheten blir då mycket mer komplex. Därför blir också den juridiska bevisföringen mer besvärlig. Dessutom finns det en rad olika program, filformat, hårdvaror och mjukvaror som komplicerar det hela ytterligare, eftersom de digitala handlingarna är så heterogena.

För att fastställa autenticiteten hos en elektronisk handling måste både dess identitet och dess integritet fastställas. Integritet är en av de beståndsdelar för begreppet informationssäkerhet som listas i den teoretiska modellen Parkerian hexad som behandlats i uppsatsens inledningsavsnitt och dess teoriavsnitt. Identiteten fastställs genom att identifiera författare, ursprung, mottagare samt datum för uppkomst, mottagande, registrering och arkivläggning.[85] Integriteten innebär att handlingen är oförvanskad på så sätt att dess centrala information fortfarande går att utläsa. Handlingen kan förändras och ändå behålla sin integritet, under

[82]Mak, Bonnie, ”On the uses of authenticity”, *Archivaria*, 2012:73, s. 16.
[83]Duranti, Luciana, Eastwood, Terry & MacNeil, Heather, “Preservation of the integrity of electronic records”, *Archivaria*, 2008:66, s. 135.
[84]Duranti, Luciana, Rogers, Corinne & Sheppard, Anthony, “Electronic records and the law of evidence in Canada: the *uniform electronic evidence act* twelveyears later”, *Archivaria*, 2010:70, s. 98.
[85]Ibid., s. 20.

förutsättning att förändringarna är av sådan art att det blir svårare att utläsa information i handlingen.[86] Som ett exempel kan nämnas att en elektronisk handling kan byta format och ändå bibehålla sin integritet, om inte formatbytet leder till någon form av informationsbortfall.

Innan de elektroniska handlingarna arkivläggs är det nödvändigt att i så hög utsträckning som möjligt försöka ta reda på under vilka omständigheter handlingarna har förvarats innan arkivläggningen. Om handlingarna har förvarats på ett informationssäkert sätt och att sådan teknologi har använts som kan ge dem så hög informationssäkerhet som möjligt. Om handlingen har förvarats och hanterats på ett bristfälligt eller rent oansvarigt sätt så är risken större att den på något sätt har blivit förvanskad. Därför är det nödvändigt att fastställa detta.[87] Det är inte bara nödvändigt att handlingarna före de kommer till arkivet förvaras i en informationssäker miljö, utan också att det är pålitliga personer som har ansvar för denna hantering samt att dessa personer inte på något sätt har ett egenintresse av att redigera handlingarna. Detta måste säkerställas.[88]

För att sammanfatta slutsatserna av det första InterPARES-projektet har MacNeil skrivit en artikel. Hon tar upp att det finns en rad kriterier som kan användas för att analysera en handlings autenticitet. En handling kan antas vara autentisk om den uppfyller många av dessa kriterier, men för att vara riktigt säker kan det i vissa tveksamma fall vara nödvändigt att göra en fullständig verifikation av autenticiteten. Verifikationen utförs genom en detaljerad kontroll av alla kända fakta kring handlingen. Utöver detta är det nödvändigt att studera alla tänkbara källor som på något sätt har någon koppling till den studerade handlingen, för att se om där finns kompletterande information.[89] Det kan röra sig om eventuella kopior kopplade till handlingen eller andra handlingar som finns inom samma kontext.

De kriterier som går att använda sig av vid kontrollen av en handlings autenticitet är bland annat att fastställa författare, upphov, mottagare, datum för skapande, mottagande, arkivläggning, anteckningar om olika tekniska modifieringar samt en lång lista på olika kriterier som återfinns i sin fulla längd i MacNeils artikel.[90] Utöver de mest grundläggande

[86]Duranti, Luciana, Rogers, Corinne & Sheppard, Anthony, "Electronic records and the law of evidence in Canada: the *uniform electronic evidence act* twelveyears later", *Archivaria*, 2010:70,s. 20.
[87]Ibid., s. 20–21.
[88]MacNeil, Heather et. al., *Authenticity task force report*, 2001, s. 21–22.
[89] MacNeil, Heather, "Providing grounds for trust II: the findings of the authenticity task force of InterPARES", *Archivaria*, 2002:54, s. 46.
[90] Ibid., s. 48–52.

kriterierna kring inblandade personer, upphov och datum så gäller det att fastställa att handlingen har förvarats på ett informationssäkert sätt där risken för obehörigt intrång eller informationsbortfall har minimerats.[91]

Olika riskfaktorer och förslag på lösningar mot dem

2006 gav ett antal större svenska företag och organisationer ut en rapport kring informationssäkerhet, en rapport tänkt att fungera som handbok i dessa frågor. I sitt förord fastställer man att riskerna faktiskt är stora att elektronisk information förvanskas på olika sätt.[92]Detta gäller då rent allmänt och inte enbart arkivhandlingar, även om arkivhandlingar utgör en viktig roll av samhällets bestånd av elektronisk information. De fokuserar i rapporten kring en kravstandard som har utvecklats för informationssäkerhet, SS- ISO/IEC 27001, samt en standard med riktlinjer för informationssäkerhetsarbetet, SSISO/IEC 27002.[93]

Den sistnämnda standarden har ett antal olika huvudområden för att stärka informationssäkerheten, varav några centrala är att driftrutinerna kontrolleras av utomstående och säkerhetskopiering.[94] Det är viktigt att utomstående får göra denna typ av kontroll eftersom de som har utvecklat driftrutinerna kanske har missat något, vilket kan upptäckas av utomstående som inte varit involverade i utvecklingsarbetet och kan granska med nya infallsvinklar. Säkerhetskopieringen är viktig ifall någon form av obehörigt intrång skulle inträffa eller någon försöker förvanska information, därför att det är svårare att utföra samma förvanskning simultant på flera olika kopior än på en enda. Även Wessbrandt belyser detta som en metod för att stärka informationssäkerheten, att skapa flera olika kopior av handlingarna och förvara dessa på olika platser.[95] MacNeil skriver att ständiga backuper kan vara en användbar metod för att minska risken för informationsbortfall och stärka informationssäkerheten. Det är nödvändigt att inte bara göra backupkopior på själva handlingarna i sig, utan att försöka göra backup på hela systemet och handlingarnas kontext, med bland annat program och systemfiler. På så vis går det att försöka upprätthålla hela

[91]MacNeil, Heather, ”Providing grounds for trust II: the findings of the authenticity task force of InterPARES”, *Archivaria*, 2002:54, s. 50.
[92]*Ge din information rätt säkerhet – handbok i informationssäkerhetsarbete*, Teknisk rapport SIS/TK 318 N46, version 6.00, 2006-08-07, s. 3.
[93] Ibid., s. 4.
[94] Ibid., s. 9.
[95]Wessbrandt, Karl, *Förstudierapport om framtidens elektroniska arkiv*, Statskontoret, Dnr 2003/67, ändrad 2003-06-04, s. 34.

miljön kring handlingarna och bättre garantera deras fortsatta läsbarhet vid en eventuell systemkrasch.[96]

En central del i rapporten är riskanalyserna.[97] För att stärka informationssäkerheten inom en organisation eller hos ett arkiv underlättar det att ha en grundlig riskanalys i grunden. Att fastställa alla möjliga risker kring intrång eller förvanskning som skulle kunna inträffa och hur de kan inträffa. När detta är gjort gäller det att utarbeta strategier och metoder för att undvika eller åtminstone minimera riskerna. Om det inte går att utveckla fullständigt idiotsäkra metoder så kvarstår alltid en viss risk för angrepp mot informationen och då gäller det dessutom att utveckla metoder för att hantera dessa potentiella intrång om de väl inträffar.

När det gäller elektroniska arkiv är det nödvändigt att väga risk mot nytta. Arkiven har bland annat till uppgift att tillhandahålla offentliga uppgifter och information till sina användare och det är möjligt att detta ökar risken för intrång. Om elektroniska arkivhandlingar ligger tillgängliga för vem som helst på internet så kan det vara så att risken för intrång eller förvanskning är större än om arkiven skulle låsa in alla handlingar utan någon som helst insyn utifrån. Om arkivhandlingar läggs ut på nätet så finns risken att skickliga hackers knäcker olika säkerhetsnycklar och krypteringssystem och kan då förvanska arkivhandlingarna eller lyckas få tillgång till information som de är obehöriga att ta del av. Denna risk finns inte om arkivhandlingarna är helt inlåsta och undangömda, men detta skulle motverka arkivens syfte.

Risk måste vägas mot nytta och målsättningen bör vara att tillhandahålla så mycket information och vara så tillgängliga för sina användare som möjligt med en så hög informationssäkerhet som möjligt. Det blir en avvägning och det går inte att tillgängliggöra informationen i så hög utsträckning att informationssäkerheten kraftigt hotas, men heller inte att helt strypa tillgängligheten bara för att hålla en så stark informationssäkerhet som möjligt.En fråga som är kopplad till denna aspekt av informationssäkerheten är integritet. Arkiven förvarar information om enskilda personer, ibland känslig eller sekretessbelagd information. Deras integritet måste kunna upprätthållas, men samtidigt så ska arkiven vara så tillgängliga som möjligt för sina användare. Malcolm Todd har skrivit att tillgängliggörandet riskerar att öka hoten mot den personliga integriteten hos de personliga arkivhandlingarna, att

[96] MacNeil, Heather, ”Providing grounds for trust II: the findings of the authenticity task force of InterPARES”, *Archivaria*, 2002:54, s. 54.
[97] *Ge din information rätt säkerhet – handbok i informationssäkerhetsarbete*, Teknisk rapport SIS/TK 318 N46, version 6.00, 2006-08-07, s. 12.

tillgängliggörandet leder till en högre risk att den känsliga och sekretessbelagda informationen kommer obehöriga personer till del.[98]

I den tekniska rapporten diskuteras det om den mänskliga faktorn och dennas betydelse för informationssäkerheten. Informationssäkerhet handlar inte bara om metoder och regler. Det är människor som utvecklar och implementerar dessa metoder och människor kan många gånger fela, exempelvis av okunskap eller glömska. Dessa brister orsakade av den mänskliga faktorn kan leda till luckor i informationssäkerheten. Rent teoretiskt finns också en risk att exempelvis tidigare anställda med kunskaper kring kryptering och det informationssäkerhetsmässiga arbetssättet hos ett arkiv eller företag kan använda sig av detta för att göra intrång och förvanska material. Ofta är det så att olika tredjeparter har tillgång till krypteringsnycklar eller chifferkoder, kanske framförallt när det gäller elektroniskt arkivmaterial, eftersom arkivarier ibland måste förlita sig på it-personal när det gäller sådana frågor.[99] Speck tar upp några uppmärksammade händelser där detta har inträffat och utomstående har kunnat komma åt känsligt och hemligstämplat material.[100] Han tar också upp några omskrivna händelser där arkivarier själva har stulit eller medvetet förstört material som skulle ha sparats.[101]

I rapporten beskrivs människorna som en del av hotbilden mot informationssäkerheten och även om de flesta anställda är lojala så kan det rent teoretiskt vara så att vissa personer är ute efter att skada informationssäkerheten för egna syftens skull.[102] Sannolikt är det så att ju fler personer som får tillgång till krypteringssystemen och säkerhetsnycklarna, desto större blir risken för detta hot och ju mer värdefull informationen är, desto större blir risken. Det kan eventuellt vara positivt att göra vissa säkerhetskontroller av de anställda och givetvis från arkivens eller företagens sida vara försiktiga med vilka som ska få ta del av känsliga uppgifter. I rapporten tas upp att alla som på något sätt kommer i kontakt med aktuell myndighet och får ta del av den lagrade informationen ska kontrolleras på adekvat sätt och när

[98] Todd, Malcolm, "Power, identity, integrity, authenticity, and the archives: a comparative study of the application of archival methodologies to contemporary privacy", *Archivaria*, 2006:61, s. 183.
[99] Wessbrandt, Karl, *Förstudierapport om framtidens elektroniska arkiv*, Statskontoret, Dnr 2003/67, ändrad 2003-06-04, s. 33.
[100] Speck, Jason, "Protecting public trust: an archival wake-up call", *Journal of archival organization*, 2010:8, s. 40.
[101] Ibid., s. 42–43.
[102] *Ge din information rätt säkerhet – handbok i informationssäkerhetsarbete*, Teknisk rapport SIS/TK 318 N46, version 6.00, 2006-08-07, s. 32.

någon ska anställas så måste de klart och tydligt få veta vilket säkerhetsansvar som gäller för dem.[103]

Säkerhetskontroller kan hjälpa till att minska risken för medvetet obehörigt intrång och förvanskning av information, eftersom de personer som har sådana syften kanske inte passerar kontrollerna och därför inte ges tillgång till informationen. Risken för obehörigt intrång eller förvanskning som beror på ren okunskap eller oförsiktighet minimeras dock lämpligast med utbildningsinsatser bland de anställda, så att de är väl införstådda med de riktlinjer som finns och lär sig precis hur de ska hantera informationen för att den inte ska utsättas för någon form av hot.[104]När nya arkivarier ska anställas så är det viktigt att göra bakgrundskontroller för att säkerställa så att de inte tidigare har blivit dömda för exempelvis urkundsförfalskning, stöld av material eller liknande typer av brott.[105]Vidare måste själva arkivens förvaringslokaler för den elektroniska informationen vara säkra och skyddade mot både olika naturkatastrofer, olyckor eller mänskligt obehörigt intrång av olika slag.[106]Säkra lokaler med starka dörrlås och liknande är ett första steg för att skydda sig från mänskligt obehörigt intrång och ett nästa steg kan vara lösenord eller någon form av kryptering av de datorer och den information som förvaras i lokalen. Flera säkerhetssteg stärker den allmänna säkerhetsnivån och ju fler steg som en obehörig person måste forcera, desto svårare blir det.

David Bearman har skrivit en artikel där han försöker fastställa de största hoten mot elektroniskt arkivmaterial och konstaterar att handlingarna är som mest hotade när de på något sätt överförs eller förflyttas.[107] Det kan röra sig om exempelvis formatbyten eller att handlingen skickas via mail från skaparen till arkivet. I dessa situationer är handlingarna som mest hotade av informationsbortfall eller att obehöriga personer på något sätt får tillgång till dem och om de lyckas knäcka krypteringen även kan lyckas förvanska materialet. Detta innebär samtidigt att handlingarna är som mest säkra när deras situation är oförändrad och konstant, när de ligger i förvaring, även om de kan vara hotade då också. Exempelvis om

[103]*Ge din information rätt säkerhet – handbok i informationssäkerhetsarbete*, Teknisk rapport SIS/TK 318 N46, version 6.00, 2006-08-07, s. 32.
[104] Ibid., s. 33.
[105]Speck, Jason, ”Protecting public trust: an archival wake-up call”, *Journal of archival organization*, 2010:8, s. 46.
[106] Ibid., s. 38–43.
[107] Bearman, David, ”Moments of risk: identifying threats to electronic records”, *Archivaria*, 2006:62, s. 24.

någon inom den egna personalen medvetet är ute efter att förvanska materialet, vilket behandlas i en teknisk rapport utgiven av ett flertal svenska myndigheter.[108]

Bearman redovisar en kronologi över de elektroniska arkivhandlingarnas levnadsförlopp: först deras skapande, därefter perioden av aktiv användning inom verksamheten, arkivläggning och förvaring hos arkiven.[109] Inom dessa fyra olika levnadsfaser anser Bearman att det finns sex specifika tillfällen där handlingarna är extra utsatta för risker där både autenticitet, integritet och informationssäkerhet hotas. Samtliga dessa är olika former av förflyttningar eller förändringar. Den första risksituationen är när handlingen överförs från skapare till mottagare, den adressat som handlingen är skapad för. I och med denna överföring sparas data kring överföringen hos både avsändare och mottagare.[110] Om exempelvis handlingen skickas via e-post så sparas den i utkorgen hos avsändaren och inkorgen hos mottagaren. Överföringen är beroende av det e-postsystem som används och e-postsystemet ska garantera säkerheten. Olika e-postsystem har olika stark kryptering och olika stark informationssäkerhet, så valet av e-postsystem är en avgörande faktor för nivån av informationssäkerhet i denna överföring.

Överföringen av en handling från avsändare till mottagare är beroende av att e-postsystemet fungerar bra och är säkert samt att mottagaren ser till att spara det i någon form av hanteringssystem för handlingar. Det krävs att avsändare och mottagare har samma mjukvara så att de kan avläsa handlingen på samma sätt.[111] Överföringen förutsätter dessa saker och om förutsättningarna inte stämmer så är överföringen riskabel och kan leda till informationsbortfall.I överföringen är det inget original som skickas, utan mottagaren får en kopia på originalet, även om kopian är exakt. Det gäller att all metadata följer med i denna kopiering och överföring.Albert Meijer har skrivit att viss metadatakontext riskerar att försvinna när e-post skickas. Han tar dock upp att övergången från mänsklig kommunikation i telefon till e-post gör att mer information sparas. I ett telefonsamtal är det mycket information som enbart behandlas muntligt, aldrig antecknas och därmed försvinner, men detta informationsbortfall finns inte längre om istället e-post används för kommunikationen.[112] Det finns dock vissa svårigheter att långsiktigt lagra e-postmeddelanden som innehåller olika

[108] *Ge din information rätt säkerhet – handbok i informationssäkerhetsarbete*, Teknisk rapport SIS/TK 318 N46, version 6.00, 2006-08-07, s. 32.
[109] Bearman, David, ”Moments of risk: identifying threats to electronic records”, *Archivaria*, 2006:62, s. 25.
[110] Ibid., s. 27.
[111] Ibid., s. 28.
[112] Meijer, Albert, “Accountability in an information age: opportunities and risks for records management”, *Archival Science*, 2001:4, s. 366.

bilagor eller bifogade filer och därför är risken för informationsbortfall i dessa meddelanden större än när det gäller enkla textmeddelanden.[113]

En annan risksituation som behandlas av Bearman är när handlingarna ska föras in i ett hanteringssystem. Bland annat finns risken att handlingen i och med detta frikopplas från sina metadata och att information försvinner på så sätt.[114]För att undvika detta gäller det att upprätthålla en väl fungerande systemhantering med regelbundna backuper, kopieringar, databashantering. Detta för att garantera att kopplingen mellan handlingar och deras metadata inte försvinner. Om denna koppling på något sätt bryts så kan dessa åtgärder leda till att dessa metadata lätt kan återfinnas och problemet åtgärdas.[115]För att metadata när handlingarna förs in i hanteringssystemet ska vara aktuella och användbara är det dessutom nödvändigt att det hela tiden antecknas när metadata förändras på något sätt under den fas som handlingarna används ute i verksamheten.[116]

När det gäller databaser skriver Bearman att dessa förvisso kan hjälpa till att spåra förändringar hos olika handlingar samt när de har inträffat, men att databaserna inte kan visa effekterna av dessa förändringar eller varför förändringarna har genomförts.[117]Databaserna har sina brister, men kan ändå fungera som viktig del i arkivhanteringen av elektroniskt material, eftersom det med hjälp av databaserna lätt kan upptäckas när olika handlingar har förändrats och dessutom underlättar de arkivsökningen. Meijer tar upp exemplet om en databas som användes av det kanadensiska parlamentet som visade sig ha dubbla serienummer för vissa handlingar, medan andra handlingar inte hade några serienummer alls. Man misstänkte att databasen hade blivit utsatt för ett medvetet sabotage, men det kan också ha varit någon form av tekniskt fel.[118]Detta visar på en tänkbar effekt av bristande databashantering.

Ytterligare en process som Bearman beskriver som riskartad är gallringen. Gallringen bygger på en mänsklig bedömning att förstöra handlingar som anses inte längre behövas. När gallringen väl är genomförd finns det ingen återvändo, under förutsättning att inte handlingen

[113]Meijer, Albert, "Accountability in an information age: opportunities and risks for records management", *Archival Science*, 2001:4, s. 367.
[114]Bearman, David, "Moments of risk: identifying threats to electronic records", *Archivaria*, 2006:62, s. 31.
[115]Ibid., s. 32.
[116] Ibid., s. 33–34.
[117] Ibid., s. 37.
[118] Meijer, Albert, "Trust this document! ICTs, authentic records and accountability", *Archival Science*, 2003:3, s. 276.

finns sparad som kopia på annat håll. Eftersom gallringen leder till att handlingar förstörs permanent så innebär den ett informationsbortfall, även om det görs en bedömning att de handlingar som gallras enbart innehåller information som inte längre behövs. Gallringsbeslutet bygger på beslut fattade av människor och den mänskliga faktorn felar ibland. Om rutinerna är otydliga kan detta i värsta fall leda till att sådan information som egentligen är tänkt att bevaras kommer att gallras istället.[119]

Långtidslagringens effekt på teknisk informationssäkerhet, autenticitet och tillförlitlighet

Det möjligtvis allra största hotet mot informationssäkerheten för elektroniskt arkivmaterial är problematiken kring långsiktig lagring. Denna involverar ett flertal olika riskmoment. Bearman hävdar att det inte finns någon klara metod för att säkerställa denna långtidslagring, utan att det finns ett problem i att olika arkiv använder sina egna och olika metoder. Ingen av dessa är heller felfri, utan har allesammans olika brister.[120]Den tekniska utrustningen är avgörande för långtidslagringen av elektroniskt arkivmaterial. Denna långtidslagring är också beroende av olika migreringsmetoder, då de gamla filformaten med tiden blir föråldrade och måste förnyas.Enligt Bearman hotas informationssäkerheten av den elektroniska långtidslagringen. Detta eftersom långtidslagringen innebär ständiga formatändringar, vilka kan leda till informationsbortfall.

Det digitala arkivmaterialet har medfört nya möjligheter, men de har även medfört många nya problem.[121] Den elektroniska långtidslagringen involverar flera olika områden, exempelvis teknik, juridikoch ekonomi.Den elektroniska långtidslagringen hotas både av tekniska problem och av arbetsmetoder och rutiner. Det kan hända att vissa digitala arkivhandlingar lyckas bevaras, men ändå förlorar information om de faller ur sin kontext. Detta är ett möjligt resultat av en dåligt genomförd migrering.Migreringarna kan också innebära att delar av materialet blir omöjliga att tolka. Enligt Runardotter förekommer det dåligt fungerande arbetsmetoder och rutiner inom arbetet med långtidslagring. Detta i sig innebär ett hot mot

[119]Bearman, David, ”Moments of risk: identifying threats to electronic records”, *Archivaria*, 2006:62, s. 39.
[120] Ibid., s. 41.
[121] Runardotter, Mari,“Information Technology, Archives and Archivists – and Long-term Digital Preservation”, *Arkiv, samhälle och forskning*, 2007:2, s. 24.

långtidslagringen och den information man strävar efter att bevara intakt.[122] En faktor som förvärrar situationen är brist på resurser, både vad gäller ekonomi och utbildning.[123]

Både när det gäller analog och digital arkivering är arkivarier beroende av andra yrkesgrupper för att långtidslagringen ska fungera väl. Det finns vissa arkivarier som upplever att samarbetet fungerar dåligt med andra yrkesgrupper som har en roll vid bevaringen av digitala arkivhandlingar, såsom IT-tekniker och administratörer. Dessa har dessutom ofta långtidslagringen av arkiv långt ner på sin prioriteringslista.[124] Detta hotar långtidslagringen av digitala arkiv. Runardotter anser att det är inom den digitala långtidslagringen som de största bristerna finns och att denna är mycket svagare och mer hotad än den analoga lagringen.[125]

De digitala arkivhandlingarna lagras i datorer och är omöjliga att läsa utan tekniska hjälpmedel.[126]Det behövs både mjukvara och hårdvara som samarbetar för att materialet ska bli läsbart. Systemet är mycket komplext och involverar många olika komponenter.Detta är den digitala informationens säregenhet och därför är dess långtidslagring så besvärlig. Dessa problem med långtidslagringen av elektroniskt arkivmaterial leder till risk för informationsbortfall och därmed är långtidslagringen nära sammanbunden med informationssäkerheten. Det finns olika former av digitala lagringsmedia, men alla dessa har begränsade livslängder. Runardotter redovisar den förväntade livslängden för ett antalolika digitala lagringsmedia: en hårddisk håller i 3–6 år, magnetisk diskett i 1–5 år, magnetiskt band i 10–20 år, cd-skivor i 10–100 år och statiskt minne i 50–100 år.[127] De lagringsmedia som idag finns kan alltså lagra information i maximalt 100 år, men vissa lagringsmedia klarar bara av ett enda år.

Runardotter et al. listar ett antal problem med det elektroniska arkivmaterialet: det kan ibland saknas specifikationer för olika problem, det saknas lösningar för vissa problem, vissa av lösningarna kan inte levereras inom rimlig tid och det går inte att lita på hårdvaran. Risken finns att tekniska problem inträffar, både inom hårdvaran och mjukvaran. Ju mer komplex

[122]Runardotter, Mari,"Information Technology, Archives and Archivists – and Long-term Digital Preservation", *Arkiv, samhälle och forskning*, 2007:2, sida 25
[123] Ibid., sida 28
[124] Ibid., sida 29–30
[125] Ibid., s. 30.
[126] Runardotter, Mari et. al. "The Information Life Cycle – Issues in Long-term Digital Preservation", *Arkiv, samhälle och forskning*, 2006:1, s. 25.
[127] Ibid., sida 26

mjukvaran är, desto större är risken för att problem inträffar. Den mänskliga faktorn kan dessutom leda till problem och säkerheten kan ibland vara bristande, vilket kan leda till exempelvis virus och trojaner.[128]Under de digitala mediernas relativt korta livslängd har det redan hunnit inträffa en rad teknikskiften, vilka ibland har gjort elektroniskt arkivmaterial material mycket svårtillgängligt. Ett exempel på detta är att det nu är mycket svårt att hitta datorer som kan läsa disketter och att det numer bara finns läsare för USB-minnen på nya datorer. De paradigmskiften och tekniska förändringar som har inträffat har inte på något vis föregåtts av planering för den långsiktiga lagringen.

Cloonan och Sanett anser att dagensinformationär flyktig.[129] De är överrens med många andra arkivvetare om att livslängden för information har förkortats och att informationen dessutom är mer hotad idag än vad den tidigare har varit. De återger ett citat som hävdar att det primära när det gäller långtidslagring av digital information egentligen inte är tekniska frågor, utan i första hand ekonomiska och organisatoriska. Tekniska sammanbrott kan förebyggas och skadorna efter tekniska problem kan ersättas om det finns en välbyggd organisation och god ekonomi.[130] En undersökning pekar på att avsaknaden av kostnadsmodeller och bevarandestrategier är ett stort besvär för det långsiktiga bevarandet av digital information hos ett antal undersökta projekt i USA.[131] Denna fråga tycks vara lågt prioriterad hos många organisationer.

Sammanfattning

I litteraturen föreslås ett antal olika metoder för att stärka informationssäkerheten i elektroniska arkiv. Ett av dessa är elektroniska signaturer eller olika former av teknisk kryptering.[132]Elektroniska signaturer används i försök att garantera att handlingar är författade av de personer som står som undertecknare. Systemet bygger på kryptografi och det behövs en nyckel för att kunna göra signaturen, men om någon obehörig lyckas komma över denna nyckel kan denne förfalska eller ändra signaturer. Det betyder att systemet med nycklar är

[128]Runardotter, Mari et. al. ”The Information Life Cycle – Issues in Long-term Digital Preservation”, *Arkiv, samhälle och forskning*, 2006:1, s. 26.
[129] Cloonan, Michèle & Sanett, Shelby, “Preservation strategies for electronic records: Where we are now – obliquity and squint?”, *The American Archivist*, 2002:65, s. 70.
[130] Lynch, Clifford, ”Strategic Issues: Technology, Trends and Solutions”, i *Preserving Digital Information*, Vantage Point series, EBSCO Subscription Services, 2000, s. 3–4.
[131] Cloonan, Michèle & Sanett, Shelby, “Preservation strategies for electronic records: Where we are now – obliquity and squint?”, *The American Archivist*, 2002:65, s. 91.
[132]MacNeil, Heather, ”Providing grounds for trust II: the findings of the authenticity task force of InterPARES”, *Archivaria*, 2002:54, s. 26–27.

säkert så länge inte någon lyckas komma över nycklarna eller knäcka krypteringen. Detta gäller även annan form av kryptering, att den kan vara väldigt stark och säker, men ingen kryptering kan fullständigt garantera informationssäkerheten. All kryptering går att knäcka, även om det i många fall kan vara oerhört svårt. När krypteringen är knäckt så kan obehöriga personer komma åt känslig information, läsa eller kanske till och med förändra den.[133]

En problematik som finns med de elektroniska signaturera och den tekniska krypteringen, utöver att den faktiskt går att knäcka och att säkerhetsnycklar kan hamna i orätta händer, är att denna typ av handlingar kan vara svåra att konvertera från äldre format till nya och att information löper större risk att försvinna vid en formatkonvertering om handlingen är krypterad än om den inte är det.[134] Med tanke på de svagheter som finns med de elektroniska signaturerna eller de olika krypteringssystemen så har vissa arkivvetare utarbetat förslag på andra tänkbara metoder att stärka de elektroniska arkivens informationssäkerhet. Ett exempel är att använda sig av olika säkerhetskopior och dubbletter av handlingarna, som förvaras på olika platser, så att det ska bli så svårt som möjligt för obehöriga personer att förvanska handlingar.[135] Detta blir mycket svårare att göra en simultan förvanskning på flera olika kopior av samma handling som förvaras på olika platser än om det bara hade funnits ett enda exemplar.

För att väl kunna utforma informationssäkerhetsarbetet är det bra att ha en riskanalys i grunden, där alla risksituationer kartläggs och att arkiven genomför åtgärder för att stärka säkerheten extra mycket i just dessa känsliga lägen. Vid användningen av kryptering är det viktigt att hålla nere antalet personer som har tillgång till krypteringsnycklarna. Enbart de som verkligen behöver ha tillgång ska ha tillgång, för att minimera risken att de hamnar i orätta händer. [136] De största risksituationerna är när handlingarna på något sätt måste förflyttas eller förändras, bland annat skickas från en person till en annan via e-post. I sådana lägen används ibland kryptering som ett skydd och just då är det viktigt att så få personer som möjligt har

[133]Wessbrandt, Karl, *Förstudierapport om framtidens elektroniska arkiv*, Statskontoret, Dnr 2003/67, ändrad 2003-06-04, s. 33.
[134]Ruusalepp, Raivo, *Digital preservation in archives: An overview of current research and practices*, 2005, s. 12; Wessbrandt, Karl, *Förstudierapport om framtidens elektroniska arkiv*, Statskontoret, Dnr 2003/67, ändrad 2003-06-04, s. 33.
[135]Hansen, Lars-Erik, "Elektroniska signaturers omöjliga liv i ett långtidsarkiv", *Arkiv, samhälle och forskning*, 2002:2, s. 74–75.
[136]Wessbrandt, Karl, *Förstudierapport om framtidens elektroniska arkiv*, Statskontoret, Dnr 2003/67, ändrad 2003-06-04, s. 33.

tillgång till nycklarna, så att ingen obehörig lyckas få tillgång till materialet när det skickas och dessutom har en nyckel för att kunna läsa eller ändra i det.

Det tycks finnas en viss misstro från arkivanvändarnas sida gentemot det elektroniska arkivmaterialet. Användarna litar inte riktigt på att materialet är korrekt.[137] Vi befinner oss nu i en tid av stora samhällsomvandlingar och i sådana tider tenderar befolkningen att ifrågasätta olika institutioner och myndigheter.[138] Då är det extra viktigt att göra stora ansträngningar för att bevisa för användarna att de elektroniska arkivens informationssäkerhet är stark, så att arkiven kan upprätthålla ett högt anseende och en bra status. Att upprätthålla ett välfungerande informationssäkerhetsarbete är inte bara viktigt för arkivens status och ställning i samhället, utan för att garantera att informationen är korrekt. Om arkiven skulle förvara handlingar som är förvanskade och innehåller felaktig information skulle denna felaktiga information spridas till allmänheten när exempelvis forskare använder sig av arkivhandlingar som källmaterial som de sedan publicerar för offentligheten. Det är också viktigt att arkivens handlingar är korrekt när det gäller juridiska frågor, om det ska hållas en rättegång där bevismaterial behöver hämtas från arkiven. Då är det av yttersta vikt att materialet är korrekt så att också domen kan bli korrekt.

[137] Price, Dara M., & Smith, Johanna J., "The trust continuum in the information age: a Canadian perspective", *Archival Science*, 2011:3–4, s. 262.
[138] Sundqvist, Anneli, "Documentation practices and recordkeeping: a matter of trust or distrust?", *Archival Science*, 2011:3–4, s. 288.

Enkätundersökning

Inledning

Alla respondenter har inte besvarat alla frågor. Vissa av arkiven har istället valt att lämna ett samlat svar på hela enkäten, framförallt eftersom de säger sig inte hantera något elektroniskt arkivmaterial. Ett av kommunarkiven säger dock att de under 2014 ska börja ta in elektroniskt arkivmaterial och då arbeta med informationssäkerhet i form av systemmetadata och filformatbegränsningar. Samtliga landsarkiven i Sverige har funnits med i listan på respondenter för enkäten och vissa av dem har valt att svara. De har då svarat att de inte har någon form av elektronisk arkivhantering och hänvisar istället till Riksarkivet när det gäller sådana frågor.

Vilken funktion har du i ditt arkiv?

Av de som har svarat är det tre stycken som har svarat att de är IT-arkivarier. Utöver detta är det en vardera som har svarat att de är: arkivarie, biträdande stadsarkivarie, enhetschef, depåansvarig och landsarkivarie.

Har du deltagit i arbete eller överläggningar som handlar om organisationens informationssäkerhet?

På denna fråga är det nio respondenter som har svarat att de har deltagit på sådana möten. Några har specificerat sig ytterligare. En har deltagit i projekt som rör datasystem och haft möten med kommunens informations- och säkerhetsansvarige. En annan har deltagit i gallringsutredning kring Skatteverkets loggar, där informationssäkerhetsfrågor har diskuterats. En av respondenterna har varit med om att införa LIS, Ledningssystem för Informationssäkerhet.

Hur skulle du beskriva relationen mellan informationssäkerhet och det arbete du själv bedriver till skydd för organisationens arkivhandlingar?

Flera av respondenterna skriver att arkiven har en viktig roll i informationssäkerhetsarbetet. Arkiven sköter en stor del av informationshanteringen och har därför också ett stort ansvar för informationssäkerheten. De har till uppgift att skydda handlingarna och att se till så att användarna får tillgång till de handlingar som de är behöriga till, medan allt annat material skyddas från deras insyn. Informationssäkerheten har också en roll i arkivens gallring, där

arkiven har till uppgift att fatta beslut om vad som ska gallras och vad som ska bevaras, där en bedömning görs om vilken information som är värd att bevara för framtiden. De har också till uppgift att säkerhetsklassa olika handlingar och se till så att rätt personer får tillgång till rätt handlingar. Vid Riksarkivet har man möten varje vecka där frågor kring informationssäkerhet diskuteras, alltså ett ganska frekvent informationssäkerhetsarbete. En av respondenterna svarar dessutom uttryckligen att informationssäkerheten vid just det arkivet är hög.

Hur skulle du själv, rent principiellt, beskriva informationssäkerhetsproblemen ur en arkivsynpunkt?

En av respondenterna uttrycker att de har ett väl utvecklat säkerhetstänkande, men att det finns en risk för informationsbortfall i olika systembyten, någonting som måste åtgärdas så att denna risk minskar.Det finns utarbetade regelverk kring informationssäkerheten, så de olika arkiven har direktiv för hur de ska agera för att upprätthålla en så hög nivå av informationssäkerhet som möjligt. Det kan dock vara svårt att riktigt veta vilka som har ansvar för informationssäkerheten i elektronisk arkivhantering, om det är arkivarierna själva eller om det är någon form av IT-personal. Det beskrivs också som att det finns en ständig balansgång mellan att bevara sekretess och samtidigt upprätthålla en öppenhet. Arkiven ska helst vara så öppna och tillgängliga som möjligt samtidigt som sekretessen och säkerheten är så stark som möjligt, så att ingen information riskerar att nå ut till obehöriga. Det behövs mycket arbete för att kunna säkerställa detta. Det behövs åtgärder både för att garantera en öppenhet respektive åtgärder för att skydda information mot obehörig åtkomst.

Har du upplevt några brister i informationssäkerheten och i så fall vilka?

Flera av respondenterna har inte upplevt några brister inom informationssäkerheten. Från ett arkiv beskrivs att det ibland blir stopp i datasystemen och en överbelastning på servrarna. En tänkbar följd av detta kan bli brister i informationssäkerheten. Ett annat problem vid samma arkiv är att känsliga uppgifter ibland skickas via fax, som förvaras i ett kopieringsrum som ganska många personer har tillgång till. Detta är ett problem av tydlig rutinkaraktär. Vid ett arkiv beskrivs det som att viss information som egentligen ska gallras fortsätter att lagras, vilket kan vara ett problem. En annan av respondenterna skriver att det på vissa områden inom informationssäkerheten saknas etablerade rutiner samt ett par respondenter som skriver att personalen har bristande kunskaper om de rutiner som väl finns. I kontroll- och migreringsprocesserna är det en stor andel av arbetsmomenten som genomförs manuellt och

då är risken större för att det uppstår fel eller att tidigare uppstådda fel inte upptäcks än om datorer hade skött dessa uppgifter.

Vilka följder har dessa brister fått?
Det nämns viss förekomst av informationsbortfall vid olika migreringar eller formatbyten eller rentav att information har försvunnit genom gallring, där information som egentligen skulle ha sparats gallrades. Andra respondenter säger att inga problem har inträffat, men att det rent teoretiskt skulle kunna bli så att information kommer i orätta händer eller försvinner om informationssäkerhetsarbetet inte skulle fungera som det ska.

Hur har din arkivfunktion försökt lösa de olika bristerna inom informationssäkerheten?
Man håller bland annat möten med andra berörda yrkesgrupper och det har etablerats olika styrdokument. Andra svar från respondenter är att de gör tillsyn och bedriver undervisning bland olika anställda för att upplysa om informationssäkerhetsrelaterade frågor. Arkiven är också aktiva i olika projekt i samarbete med andra yrkesgrupper. Vid ett arkiv arbetar man med olika åtgärdslistor och har förbättrat sin dokumentation av rutiner och beslut. Det finns också ett samarbete med FRA och Riksrevisionen för att stärka arbetet kring informationssäkerhet. Dessa har hjälpt till att ringa in de brister som finns, så att dessa ska kunna åtgärdas.

Använder ni er av någon form av krypteringssystem eller elektroniska signaturer för de elektroniska handlingarna?
Flera av respondenterna svarar nej på denna fråga. Av de som svarar nej finns det däremot vissa som säger att detta kan vara tänkbart att börja använda i framtiden. Vissa av respondenterna använder olika former av krypteringar eller elektroniska signaturer. Ett av arkiven skriver att de använder checksummor till olika arkivpaket och att dessa arkivpaket långtidsbevaras. De tar emot handlingar med vissa typer av signaturer, men inte alla.

Om ni använder er av migrering, hur gör ni för att motverka informationsbortfall i migreringsprocessen?
En av de metoder som förekommer hos respondenterna är att jämföra mängden data före och efter migrering, för att se om något har försvunnit. En annan metod är användning av hash-funktionen SHA-256, medan en annan inför migreringen kontrollerar data och metadata, därefter paketerar detta i arkivpaket. Två exemplar av paketen bevaras på band och ett på

disk. När migrering ska genomföras så packas paketen upp. Efter migreringen så förändras metadata och en oberoende person får därefter kontrollera filerna för att säkerställa att ingenting har försvunnit. Filerna paketeras återigen och får nya checksummor och nya databärare.

Hur jobbar ni aktivt för att minimera risken för att felaktiga handlingar förs in i e-arkivet?

En av metoderna som nämns är kontroller vid leveransmottagande, en annan är gallringsutredningar, en tredje att använda sig av e-postsystemens spamfilter. Ett arkiv skriver att alla elektroniska handlingar förses med tekniska nycklar och att de överhuvudtaget inte tar emot handlingarna om de saknar tekniska nycklar. Vid ett av arkiven kontrolleras och valideras alla elektroniska handlingar innan de accepteras. De kontrollerar då struktur, teckenuppsättning och läsbarhet. De gör dessutom stickprov i informationsinnehållet och gör jämförelser. Ett av arkiven kräver att myndigheter ska lämna en leveransframställan innan de kan fatta beslut om att ta emot handlingarna. När de tar emot handlingar så kontrolleras att innehållet stämmer överens med leveransframställan. De kontrollerar dessutom förekomst av virus, godkända format och jämför handlingar mot metadata. Flera av arkiven kontrollerar metadata.

Sammanfattning

De respondenter som har svarat på frågorna finns på olika positioner inom arkivariekåren, men den vanligaste yrkestiteln bland respondenterna är IT-arkivarie. Alla respondenter skriver att de på ett eller annat sätt har deltagit i arbete eller överläggningar om informationssäkerhet. Respondenterna tycker att arkiven har en viktig roll i informationssäkerhetsarbetet, eftersom arkiven sköter en betydande del av samhällets informationshantering. Arkiven fattar beslut om vilka handlingar som ska säkerhetsklassas och vilka som ska vara öppna och allmänheten till del. De fattar också beslut om vilka handlingar som ska gallras respektive vilka som ska bevaras. Generellt sett tycks respondenterna tycka att informationssäkerheten vid arkiven är hög och att arbetet med dessa frågor fungerar bra, men vissa av dem har också upplevt vissa problem. Vid olika systembyten finns det risk för informationsbortfall. Det finns också en oklarhet i ansvarsfrågan, om det är arkivarierna som ansvarar för det elektroniska arkivmaterialets informationssäkerhet eller om det är IT-personalen som gör det. Ett par av respondenterna upplever ett problem med att på samma gång garantera så stor öppenhet som

möjligt samtidigt som de ska garantera sekretess och se till så att viss information hålls borta från användarna.

När det gäller informationssäkerhetens brister så nämns exempelvis från ett arkiv att känsliga uppgifter ibland skickas till faxen och att faxen finns i ett kopieringsrum som ganska många har tillgång till. Detta är ett klart rutinproblem. En annan respondent skriver att gallringsbesluten inte alltid genomförs som de ska, utan att viss information som ska gallras ibland istället bevaras. Detta är ett problem med informationssäkerheten. Det finns också vissa problem med bristande rutin och att personalen inte alltid har koll på vilka rutiner som gäller. För att undvika dessa problem brukar arkivarier ibland hålla möten med andra yrkesgrupper som också arbetar med frågor kring informationssäkerhet. En av respondenterna har dessutom samarbete med FRA, som har hjälpt till att ringa in olika brister som finns så att dessa ska kunna åtgärdas. Flera av respondenterna har svarat att de inte använder sig av elektroniska signaturer eller migreringar. De som väl har migreringar försöker undvika informationsbortfall genom att jämföra metadata och arbetar med checksummor och att paketera data i elektroniska arkivpaket. Metoder för att undvika att felaktigt elektroniskt material kommer in till arkivet är att genomföra olika former av kontroller, bland annat vad gäller metadata, struktur, teckenuppsättning.

Sammanfattande slutdiskussion

I den sammanfattande slutdiskussionen redovisas och diskuteras svaren på uppsatsens tre frågeställningar. Dess första frågeställning var formulerad på följande sätt: *Hur behandlas informationssäkerhet i den arkivvetenskapliga litteraturen?* Detta besvaras med en litteraturstudie. Uppsatsens andra fråga, *Hur ser svenska arkivarier på informationssäkerhet?*, besvaras med enkätsvar från olika respondenter som representerar svenska arkiv. När det gäller den tredje frågan, *Vilka problem och lösningar framhålls i informationssäkerhetsfrågorna?*, går det att finna svar både inom den studerade litteraturen och i enkätrespondenternas svar.

När det gäller svaret på frågorna ett och två finns det både likheter och skillnader vid en jämförelse av resultaten från litteraturstudien och resultaten från enkäten. Detta kan i hög grad bero på att materialet från litteraturstudien är mycket mer omfattande. Flera av enkätens respondenter har besvarat frågeställningarna kort, eller enbart besvarat vissa frågor eller inte svarat överhuvudtaget. Inom den arkivvetenskapliga forskningen har istället långa artiklar och rapporter skrivits om ämnen som gränsar till uppsatsens undersökningsområde.

Första frågeställningen

Detta är uppsatsens första frågeställning: *Hur behandlas informationssäkerhet i den arkivvetenskapliga litteraturen?* Från den arkivvetenskapliga forskningens sida har det påstått att arkivanvändarna av de elektroniska arkiven och själva allmänheten är skeptisk till hur tillförlitlig den elektroniska arkivhanteringen och det elektroniska arkivmaterialet egentligen är. Forskningen har visat att allmänhetens förtroende minskar både för arkiven och liknande typer av samhälleliga myndigheter.[139] Om användarna inte har tilltro till arkivmaterialet kan detta leda till en nedåtgående spiral, där mindre pengar satsas på arkiven från politikernas sida och att arkiven därmed förlorar sin ställning än mer, med försämrad kompetensutveckling och allt mindre resurser för att göra ett bra arbete. Därför är det mycket nödvändigt att bryta denna trend och visa för användarna att arkiven väl kan hantera dessa frågor och att arkivens arbete kring informationssäkerhet håller en mycket hög nivå. Det material som förvaras av arkiven används på så många olika håll i samhället och om

[139] Price, Dara M., & Smith, Johanna J., "The trust continuum in the information age: a Canadian perspective", *Archival Science*, 2011:3–4, s. 262; Sundqvist, Anneli, "Documentation practices and recordkeeping: a matter of trust or distrust?", *Archival Science*, 2011:3–4, s. 284.

informationssäkerheten brister hos arkiven och om deras handlingar förvanskas, så sprider sig denna förvanskning och felaktiga information ut i hela samhället. Därför vore det förödande.

Från forskningens sida beskrivs det som att informationssäkerhetsarbetet är mycket svårare och mer komplicerat när det gäller elektroniskt arkivmaterial än när det kommer till det analoga materialet. Detta beror på att det är lättare att upptäcka obehöriga förändringar eller förfalskningar inom det analoga materialet, bland annat genom att studera sådana rent praktiska detaljer såsom bläck, papperskvalitet, signaturer, stämplar och liknande detaljer.[140]

En central del i uppsatsen och i dess första frågeställning är autenticitet. Autenticitetsbegreppet har diskuterats en hel del i den tidigare forskningen och studerade litteraturen. Autenticitet är ett mångsidigt begrepp och det kan finnas flera olika former och betydelser av autenticitet. Enligt Bonnie Mak finns det bland annat tre olika former av autenticitet: den diplomatiska, den juridiska och den historiska, vilka har olika betydelser och innebörder.[141]Forskningsprojektet InterPARES har gett upphov till en rad rapporter och i vissa av dessa går det att finna definitioner av autenticitetsbegreppet. I InterPARES 1 beskrivs autenticitet som att någonting bygger på fakta och inte är förvanskat på något sätt.[142]Enligt InterPARES 2 är autenticitet en mätare på handlingarnas tillförlitlighet, en mätare som garanterar tillförlitlighet och kvalitet.[143]

Begreppet autenticitet var under mycket lång tid ungefär detsamma, men har under senaste tid börjat diskuteras mycket, eftersom framväxten av det elektroniska arkivmaterialet innebär en stor omställning i förutsättningarna för att upprätthålla autenticiteten.[144] Eftersom de elektroniska handlingarna är så mycket mer komplicerade med alla sina metadata och alla olika relaterade filer, mjukvaror och hårdvaror för att kunna läsa handlingarna så som de är tänkta, så blir också autenticitetsbegreppet mycket mer komplicerad för de elektroniska

[140]Ivarsson, Elisabeth, ”Autenticitet och digitala dokument”, *Arkiv, samhälle och forskning*, 2007:2, s. 81; Wessbrandt, Karl, *Förstudierapport om framtidens elektroniska arkiv*, Statskontoret, Dnr 2003/67, ändrad 2003-06-04, s. 32; Iacovino, Livia, “Recordkeeping and juridical governance “, i McKemmish, Sue (red.) *Archives: Recordkeeping in Society*, Wagga Wagga 2005, s. 255–276; Meijer, Albert, “Trust this document! ICTs, authentic records and accountability”, *Archival Science*, 2003:3, s. 278.
[141]Mak, Bonnie, ”On the uses of authenticity”, *Archivaria*, 2012:73, s. 5–7.
[142]MacNeil, Heather et. al., *Authenticity task force report*, 2001, s. 2.
[143]Roeder, John et. al., *Domain 2task force report*, 2008, s. 9.
[144]Ibid., s. 16.

handlingarna. I en artikel av Heather MacNeil finns en lång lista på kriterier som går att använda sig av i arbetet för att fastställa en elektronisk handlings autenticitet.[145]

Andra frågeställningen

Uppsatsens andra frågeställning lyder som följer: *Hur ser svenska arkivarier på informationssäkerhet?* De respondenter som har besvarat uppsatsens enkät svarar alla på ett eller annat sätt att informationssäkerheten är en viktig del i deras arbete. Riksarkivet har bland annat svarat att de varje vecka har diskussioner mellan IT-personal och arkivarier om informationssäkerhetsarbetet, så det tyder på att man arbetar mycket aktivt med dessa frågor och prioriterar dem högt. Stockholms stadsarkiv anser att deras informationssäkerhet är hög, men att det krävs ständiga ansträngningar för att upprätthålla denna. Örebros stadsarkiv har svarat att man har ett väl utvecklat system med backuper och säkerhetskopior, men att arbetet för att förhindra informationsbortfall vid exempelvis omorganisationer eller migreringar av olika slag ännu inte fungerar fullt ut som man önskar. Uppsalas stadsarkiv anser att det finns ett problem i att det är otydligt vem som egentligen har ansvar för informationssäkerheten och att detta är en brist. Enligt Riksarkivet är det hela tiden en utmaning att på samma gång garantera både sekretess och tillgänglighet, en utmaning nära kopplad till informationssäkerheten. Stockholms stadsarkiv har svarat på liknande sätt att man måste göra en ständig avvägning mellan sekretess och tillgänglighet, som i många fall står i motsats till varandra, men att man ändå måste kunna garantera båda två på samma gång.

Vissa av respondenterna har svarat att de inte har upplevt några brister i arbetet med informationssäkerhet, medan de flesta tycker att de har upplevt brister. Brister som nämns är bland annat att känslig information ibland skickas till faxen och att det på så sätt kan komma obehöriga personer till del. En annan brist som nämns är att den kryptering som vanligtvis används inte fungerar över smarta telefoner, det finns inte tillräckligt med etablerade rutiner och vissa kontroll- och migreringsprocesser utförs till stor del manuellt, vilket kan leda till vissa problem med den felande mänskliga faktorn. Flera av arkiven berättar att dessa brister i informationssäkerheten faktiskt har lett till ett visst informationsbortfall eller att spårbarheten ibland har försämrats.

[145]MacNeil, Heather, ”Providing grounds for trust II: the findings of the authenticity task force of InterPARES”, *Archivaria*, 2002:54, s. 48–52.

Respondenterna till enkätundersökningen har svarat att de metoder de använder för att stärka informationssäkerheten bland annat är etablering av olika styrdokument och riktlinjer. Flera av arkivrepresentanterna håller informationsmöten och för samtal med andra berörda yrkesgrupper, framförallt IT-personal, inom sina respektive kommuner. Riksarkivet skriver ständigt listor över åtgärder för att stärka informationssäkerheten, vilka de sedan arbetar intensivt med att leva upp till. De har också i sitt arbete tagit kontakt med andra statliga myndigheter specialiserade på dessa frågor och på så sätt fått många goda råd för att ytterligare stärka informationssäkerheten. Några av respondenterna använder sig av kryptering och elektroniska signaturer, men de flesta gör det inte.

När det gäller migrering så använder sig Västerås stadsarkiv av hash-funktionen SHA-256 för att se till så att det inte inträffar något informationsbortfall. Riksarkivet har en väl utarbetad metod för migreringsprocessen. De skapar arkivpaket som de förvarar i två exemplar på band och ett exemplar på disk. I migreringsprocessen packar de upp paketen och migrerar dem. Därefter gör de vissa förändringar i metadata som dokumenteras av en ansvarig och kontrolleras av en annan ansvarig, för att se så att allting har gått rätt till. När denna process är färdig gör de nya arkivpaket i de nya migrerade filformaten.

Respondenterna förhindrar att felaktig information förs in i det elektroniska arkivbeståndet genom en rad olika metoder. Det rör sig bland annat om att kontrollera materialet när det kommer in till arkivet. Arkiven brukar göra noggranna kontroller av materialet innan de väljer att ta in det i arkivbeståndet. När exempelvis Skatterverket beslutar om att ta in handlingar till sitt arkiv så får alla handlingar tekniska nycklar. Annars tas de inte emot. Man kontrollerar flera olika saker, bland annat handlingens struktur, teckenuppsättning och läsbarhet. Hudiksvalls kommunarkiv, ett mindre arkiv, skriver att den enda metod de använder är att de nyttjar e-postsystemens spamfilter för material som skickas via e-post.

Tredje frågeställningen

Uppsatsens tredje frågeställning är formulerad på följande vis: *Vilka problem och lösningar framhålls i informationssäkerhetsfrågorna?*Det finns vissa metoder som har behandlats mycket inom den arkivvetenskapliga forskningen när det kommer till att stärka det elektroniska arkivmaterialets informationssäkerhet och autenticitet. En metod som har diskuterats mycket är betydelsen av elektroniska signaturer eller olika former av kryptering.

Krypteringen och signaturerna har från vissa håll beskrivits som en viktig del i arbetet att stärka informationssäkerheten och autenticiteten, medan det från andra håll riktas stark kritik mot denna, som beskrivs som väldigt bristfällig och problematisk i ett längre perspektiv. Krypteringen och signaturerna innebär att personer behöver krypteringsnycklar för att kunna redigera en handling på olika sätt och i många fall krävs nycklar till och med för att ens kunna läsa handlingen. Eftersom nycklarna bara ges till ett fåtal betrodda personer, enbart de som verkligen behöver dem, så ska det hindra att obehöriga personer kan komma åt materialet.

När det gäller kryptering är det generellt så att ju äldre krypteringen är, desto svagare blir den. Allteftersom krypteringar föråldras behöver de alltså helst uppdateras till nya och starkare versioner, men detta är besvärligt. I sådana processer finns viss risk för informationsbortfall eller att själva handlingen förändras på något sätt, så att dess ursprungliga ordning skadas. Krypteringen är osäker ur ett längre perspektiv dels för att en kryptering relativt fort blir gammal och därmed försvagas, men också för att de företag som skapar olika krypteringssystem enbart ger krypteringarna och signaturerna certifikat som sträcker sig över en begränsad tid. Problemet finns också att även helt nya och riktigt starka krypteringar går att knäcka om någon hacker är riktigt skicklig och målmedveten. De olika säkerhetsnycklarna kan också komma på villovägar och nå orätta händer. Av bland annat dessa anledningar har krypteringen och signaturerna brister. En undersökning från 1998 visade att de elektroniska signaturerna var en av de mindre betydelsefulla faktorerna när arkivarier gör äkthetskontroll av olika handlingar.[146] Detta var dock 15 år sen, och hur situationen är idag kan förhoppningsvis visas genom uppsatsens enkätundersökning.

Utöver kryptering och elektroniska signaturer har det från forskningens sida föreslagits ett antal olika metoder för att stärka den elektroniska arkivhanteringens informationssäkerhet och autenticitet. Ett viktigt inslag i detta arbete är att ha tydliga rutiner och bra regelverk. Väl etablerade rutiner med god struktur innebär att det med lätthet kan upptäckas om någon person har redigerat en handling samt vem som har gjort det, så att den typen av händelser kan spåras och ingenting undgår upptäckt. En annan metod som har tagits upp i flera källor är behovet av säkerhetskopiering, förslagsvis att en originalhandling kopieras och att kopiorna förvaras på olika platser, så att det blir svårare för en eventuell hacker att simultant angripa alla olika kopiorna av en handling. Säkerhetskopior kan också vara ett skydd som hjälper till

[146]Park, Eun G., "Understanding 'authenticity' in records and information management: analyzing practitioner constructs", *The American Archivist*, 2001:64, s. 282.

att bevara information vid någon form av systemkrasch eller liknande, om de andra kopiorna förvaras på andra platser.[147]

För att så väl som möjligt stärka informationssäkerheten för elektroniska arkivhandlingar är det nödvändigt att utarbeta riskanalyser, ta reda på vilka situationer som är risksituationer och utarbeta strategier för att minska riskerna så mycket det går. Ett konkret exempel på detta kan vara när en handling överförs från avsändare till mottagare, sannolikt via e-post. Detta är en risksituation där handlingar riskerar att hamna i orätta händer, men en strategi för att stärka informationssäkerheten är att ha så stark kryptering som möjligt på handlingarna i denna överföringsprocess.

Diskussion

Sammanfattningsvis kan sägas att det finns mycket mer material att hämta i denna fråga från tidigare forskning än det finns att hämta från den egna enkätundersökningen och respondenternas svar. Det kan diskuteras vad detta beror på. Bara lite drygt hälften, 58 procent, av de tillfrågade myndigheterna har besvarat enkäten. En delförklaring till bortfallet kan vara det som några av landsarkiven har skrivit i sina svar: de landsarkiv som har svarat skriver att inga landsarkiv ägnar sig åt frågor om informationssäkerhet och att det är Riksarkivet som sköter detta för deras räkning. Vissa av landsarkiven har trots detta valt att ge korta samlade svar på enkäten, men detta bör rimligtvis också vara förklaringen till varför flera landsarkiv har valt att avstå. Flera av de tillfrågade stadsarkiven har också valt att avstå från enkäten. Detta kan bero på det som vissa av de svarande stadsarkiven har skrivit, att de inte upplever sig ha några problem med informationssäkerhet. De arkivmyndigheter som inte upplever några problem kanske inte har känt något större intresse av att delta i undersökningen för den sakens skull. Detta kan vara en förklaring.

I uppsatsens inledningsavsnitt och i dess teoriavsnitt diskuterades informationssäkerhetsmodellen Parkerian hexad och dess olika komponenter förklarades närmre. Enligt modellen behöver följande komponenter uppfyllas för att någonting ska betraktas som informationssäkert: konfidentialitet, kontroll, integritet, autenticitet,

[147] *Ge din information rätt säkerhet – handbok i informationssäkerhetsarbete*, Teknisk rapport SIS/TK 318 N46, version 6.00, 2006-08-07, s. 9; Wessbrandt, Karl, *Förstudierapport om framtidens elektroniska arkiv*, Statskontoret, Dnr 2003/67, ändrad 2003-06-04, s. 34; MacNeil, Heather, ”Providing grounds for trust II: the findings of the authenticity task force of InterPARES”, *Archivaria*, 2002:54, s. 54.

tillgänglighet och användbarhet. Denna hexad tycks inkludera alla väsentliga beståndsdelar för ett informationssäkerhetsbegrepp att använda inom arkiv- och informationsvetenskapen. Denna modell inkluderar väl den svåra balansgång som flera av enkätens respondenter har upplevt, nämligen att garantera både öppenhet och sekretess på samma gång. Konfidentialitet innebär att enbart behöriga personer ska kunna få tillgång till vissa handlingar, medan tillgänglighet ska garantera användarna snabb tillgång till de handlingar de önskar.

Alla kan inte få de handlingar de önskar, utan sekretess måste av olika skäl tillämpas på vissa handlingar, som dock kan lämnas ut till vissa behöriga personer. Det här innebär att alla informationssäkerhetens komponenter enligt Parkerian hexad inte kan användas på samma handlingar samtidigt. Vissa handlingar måste hanteras med konfidentialitet, medan andra måste hanteras med tillgänglighet. Det är detta som gör hexaden så användningsbar, att den har flera olika komponenter och är mångsidig. Olika handlingar måste hanteras med olika komponenter och alla kan inte hanteras med alla komponenter på samma gång, eftersom vissa av dem står i direkt motsats mot varandra. Dock kan ett helt arkivbestånd hanteras enligt alla hexadens olika komponenter. Inom ett arkivbestånd kan vissa handlingar hanteras konfidentiellt, andra tillgängligt. Vissa av komponenterna måste dock gälla för alla handlingar, såsom kontroll, integritet och autenticitet. En handling kan inte betraktas som informationssäker om någon av dessa fallerar. När det gäller komponenten användbarhet får det sägas att vissa handlingar ska vara användbara för alla, vissa handlingar användbara bara för ett väldigt litet fåtal. Alltså att när det gäller oerhört känsligt material ska det inte finnas någon möjlighet att använda materialet annat än för dem som verkligen måste.

Fortsatt forskning

Vid en jämförelse av uppsatsens litteraturstudie och resultatet av enkäten verkar det som att den arkivvetenskapliga forskningen upplever situationen som mer hotfull än vad de yrkesverksamma arkivarierna i undersökningen gör. Det kan finnas olika tänkbara förklaringar till detta. En förklaring kan vara att enkätundersökningen är genomförd 2013 och att många av de källor som används i litteraturstudien har några år på nacken, ofta 3–5 år gamla. Det kan alltså vara så att situationen var värre då och att den har förbättrats fram till dagens läge. Det kan också vara så att många av de yrkesverksamma arkivarierna är blinda för vissa av de problem som den arkivvetenskapliga forskningen har upptäckt, alternativt att den arkivvetenskapliga forskningen överdriver vissa risker och har bristande inblick i den praktiska arkivverksamheten och dess informationssäkerhetsarbete. Det är möjligt att de

svenska arkivmyndigheterna har ett egenintresse i att framställa sitt informationssäkerhetsarbete som starkare än vad det faktiskt är, för att på så vis hålla ett så högt anseende som möjligt. Allt detta är möjliga förklaringar. Detta är någonting som skulle kunna studeras vidare av den fortsatta forskningen i en framtida uppsats.

Käll- och litteraturförteckning

Litteratur

Alvesson, Mats & Sköldberg, Kaj, *Tolkning och reflektion – vetenskapsfilosofi och kvalitativ metod*, Lund 2008.

Bearman, David, ”Moments of risk: identifying threats to electronic records”, *Archivaria*, 2006:62.

Boudrez, Filip, “Digital signatures and electronic records”, *Archival Science*, 2007:2.

Burke, Peter, *New perspectives on historical writing*, Cambridge 2006.

Cloonan, Michèle & Sanett, Shelby, “Preservation strategies for electronic records: Where we are now – obliquity and squint?”, *The American Archivist*, 2002:65.

Digital Preservation Testbed, *From digital volatility to digital permanence. Preserving text documents*, Haag 2003.

Duranti, Luciana, Eastwood, Terry & MacNeil, Heather, “Preservation of the integrity of electronic records”, *Archivaria*, 2008:66, s. 135.

Duranti, Luciana, Rogers, Corinne & Sheppard, Anthony, “Electronic records and the law of evidence in Canada: the *uniform electronic evidence act* twelveyears later”, *Archivaria*, 2010:70.

Duranti, Luciana et. al., *The InterPARES 2 project glossary*, 2008.

Hansen, Lars-Erik, “Elektroniska signaturers omöjliga liv i ett långtidsarkiv”, *Arkiv, samhälle och forskning*, 2002:2.

Hansen, Lars-Erik, ”Digital informationshantering för personarkiv”, *Arkiv, samhälle och forskning*, 2008:2.

Hedstrom, Margaret, ”’The Old Version Flickers More’ – Digital Preservation from the User’s Perspective”, *The American Archivist*, 2006:69.

Holme, Idar Magne & Solvang, Bernt Krohn, *Forskningsmetodik: Om kvalitativa och kvantitativa metoder*, Lund 2008.

Iacovino, Livia, “Recordkeeping and juridical governance “, i McKemmish, Sue (red.) *Archives: Recordkeeping in Society*, Wagga Wagga 2005.

ISO 15489:1, First edition, *Part 1 – general*, 2001.

Ivarsson, Elisabeth, ”Autenticitet och digitala dokument”, *Arkiv, samhälle och forskning*, 2007:2.

Lynch, Clifford, ”Strategic Issues: Technology, Trends and Solutions”, i *Preserving Digital Information*, Vantage Point series, EBSCO Subscription Services, 2000.

MacNeil, Heather, ”Providing grounds for trust II: the findings of the authenticity task force of InterPARES”, *Archivaria*, 2002:54.

MacNeil, Heather, “Providing grounds for trust: developing conceptual requirements for the long-term preservation of authentic electronic records”, *Archivaria*, 2000:50.

MacNeil, Heather et. al., *Authenticity task force report*, 2001.

MacNeil, Heather et. al., *The InterPARES glossary*, 2001.

Mak, Bonnie, ”On the uses of authenticity”, *Archivaria*, 2012:73.

McKemmish, Sue (red.),*Archives: Recordkeeping in society*, Wagga Wagga 2005.

Meijer, Albert, “Accountability in an information age: opportunities and risks for records management”, *Archival Science*, 2001:4.

Meijer, Albert, “Trust this document! ICTs, authentic records and accountability”, *Archival Science*, 2003:3.

Moore, R. W.,“Building preservation environments with data grid technology”, *The American Archivist*, volym 69, nr. 1: 2006.

Park, Eun G., “Understanding ‘authenticity’ in records and information management: analyzing practitioner constructs”, *The American Archivist*, 2001:64.

Parker, Donn B., *Fighting computer crime*. New York 1998.

Price, Dara M., & Smith, Johanna J., “The trust continuum in the information age: a Canadian perspective”, *Archival Science*, 2011:3–4.

Riksarkivet, *Statusrapport informationssäkerhet – remissgenomgång*, Diarienummer RA 22-2007/3552.

Roeder, John et. al., *Domain 2task force report*, 2008.

Runardotter, Mari, “Information technology, archives and archivists – and long-term digital preservation”, *Arkiv, samhälle och forskning*, 2007:2.

Runardotter, Mari et. al. ”The information life cycle – issues in long-term digital preservation”, *Arkiv, samhälle och forskning*, 2006:1.

Ruusalepp, Raivo, *Digital preservation in archives: An overview of current research and practices*, 2005.

SOU 2009:16, del 3.

Speck, Jason, ”Protecting public trust: an archival wake-up call”, *Journal of archival organization*, 2010:8.

Statskontoret 2000:5, *Intelligenta tjänster och elektroniska blanketter*.

Sundqvist, Anneli, ”Documentation practices and recordkeeping: a matterof trust or distrust?”, *Archival Science*, 2011:3–4.

Thompson, Willie, *Postmodernism and history*, Basingstoke 2004.

Todd, Malcolm, “Power, identity, integrity, authenticity, and the archives: a comparative study of the application of archival methodologies to contemporary privacy”, *Archivaria*, 2006:61.

Wessbrandt, Karl,*Förstudierapport om framtidens elektroniska arkiv*, Statskontoret, Dnr 2003/67, ändrad 2003-06-04.

Ge din information rätt säkerhet – handbok i informationssäkerhetsarbete, Teknisk rapport SIS/TK 318 N46, version 6.00, 2006-08-07.

Webbaserade källor

http://www.clir.org/pubs/reports/pub92/rothenberg.html (hämtad: 130227)

http://www.law.cornell.edu/uscode/text/44/3542 (hämtad: 130406).

http://smartgridsecurity.blogspot.se/2010/06/hexad-dicted.html (hämtad: 130608).

http://www.interpares.org/ip3/ip3_terminology_db.cfm?letter=a&term=13 (hämtad: 130608).

E-post från Landsarkivet i Östersund (130408).

E-post från Norrköpings stadsarkiv (130408).

E-post från Örebros stadsarkiv (130409).

E-post från Landsarkivet i Vadstena (130410).

E-post från Malmös stadsarkiv (130411).

E-post från Hudiksvalls kommunarkiv (130412).

E-post från Uppsalas stadsarkiv (130418).

E-post från Skatteverkets arkiv (130421).

E-post från Västerås stadsarkiv (130422).

E-post från Riksarkivet (130422).

E-post från Stockholms stadsarkiv (130422).

E-post från Göteborgs landsarkiv (130423).

E-post från Landsarkivet i Visby (130424).

E-post från Landsarkivet i Lund (130429).

Bilaga 1

Enkät (presentation och frågor)

Hej!

Jag heter Kalle Wadin Eriksson och läser magisterkurs i Arkiv- och informationsvetenskap vid Mittuniversitetet i Härnösand och arbetar just nu med min magisteruppsats. Den handlar om informationssäkerhet hos elektroniskt arkivmaterial. Det jag vill göra är att ringa in de upplevda problem som finns bland svenska arkivarier när det gäller just det elektroniska arkivmaterialets informationssäkerhet och vilka eventuella lösningar som skulle kunna användas för att åtgärda problemen. Därför bifogar jag nu ett antal frågeställningar med detta brev, vilka jag hoppas att ni tar er tid att besvara och som kan hjälpa mig att försöka utveckla några förslag på lösningar på de problem som finns. Detta är mina frågor:

1. Inom vilket arkiv arbetar du?
2. Vilken funktion har du i detta arkiv?
3. Har du deltagit i arbete eller överläggningar som handlar om organisationens informationssäkerhet?
4. Hur skulle du beskriva relationen mellan informationssäkerheten och det arbete du själv bedriver till skydd för organisationens arkivhandlingar?
5. Hur skulle du själv, rent principiellt, beskriva informationssäkerhetsproblemen ur en arkivsynpunkt?
6. Har du upplevt några brister i informationssäkerheten och i så fall vilka?
7. Vilka följder har dessa brister fått?
8. Hur har din arkivfunktion försökt lösa de olika bristerna inom informationssäkerheten?
9. Använder ni er av någon form av krypteringssystem eller elektroniska signaturer för de elektroniska handlingarna?
10. Om ni använder er av migrering, hur gör ni för att motverka informationsbortfall i migreringsprocessen?
11. Hur jobbar ni aktivt för att minimera risken för att felaktiga handlingar förs in i e-arkivet?

Sista datum för svar är 30 april. Jag är tacksam över ert deltagande.

Kalle Wadin Eriksson, 880319

Hälsningar
Kalle Wadin Eriksson

Påminnelsebrev
Hej!

Jag har tidigare skickat ut ett meddelande till er om en enkätundersökning som jag vill att er arkivmyndighet är en del av, men har ännu inte fått in något svar, så därför skickar jag denna påminnelse. Det är viktigt för mig att få in svar, så att undersökningen blir så tillförlitlig som möjligt. Undersökningen omfattar bara elva frågor och tar inte alls många minuter att besvara. Detta var mitt tidigare meddelande:
Jag heter Kalle Wadin Eriksson och läser magisterkurs i Arkiv- och informationsvetenskap vid Mittuniversitetet i Härnösand och arbetar just nu med min magisteruppsats. Den handlar om informationssäkerhet hos elektroniskt arkivmaterial. Det jag vill göra är att ringa in de upplevda problem som finns bland svenska arkivarier när det gäller just det elektroniska arkivmaterialets informationssäkerhet och vilka eventuella lösningar som skulle kunna användas för att åtgärda problemen. Därför bifogar jag nu ett antal frågeställningar med detta brev, vilka jag hoppas att ni tar er tid att besvara och som kan hjälpa mig att försöka utveckla några förslag på lösningar på de problem som finns. Detta är mina frågor:

1. Inom vilket arkiv arbetar du?
2. Vilken funktion har du i detta arkiv?
3. Har du deltagit i arbete eller överläggningar som handlar om organisationens informationssäkerhet?
4. Hur skulle du beskriva relationen mellan informationssäkerheten och det arbete du själv bedriver till skydd för organisationens arkivhandlingar?
5. Hur skulle du själv, rent principiellt, beskriva informationssäkerhetsproblemen ur en arkivsynpunkt?
6. Har du upplevt några brister i informationssäkerheten och i så fall vilka?
7. Vilka följder har dessa brister fått?
8. Hur har din arkivfunktion försökt lösa de olika bristerna inom informationssäkerheten?
9. Använder ni er av någon form av krypteringssystem eller elektroniska signaturer för de elektroniska handlingarna?

10. Om ni använder er av migrering, hur gör ni för att motverka informationsbortfall i migreringsprocessen?
11. Hur jobbar ni aktivt för att minimera risken för att felaktiga handlingar förs in i e-arkivet?

Sista datum för svar är 30 april. Jag är tacksam över ert deltagande.

Hälsningar
Kalle Wadin Eriksson

Bilaga 2

Här redovisas enkätsvaren från de olika respondenterna. I vissa fall har respondenter gett ett samlat svar på hela enkäten och i dessa fall redovisas deras samlade svar under fråga ett.

Inom vilket arkiv arbetar du?

Norrköpings stadsarkiv:Vi har inget elektroniskt arkivmaterial, eftersom arkivmyndigheten inte disponerar något eget verksamhetssystem för elektronisk arkivering för bevarande, och jag därför har nekat alla verksamheter (= arkivbildare) att leverera bevarandematerial i elektronisk form.Under innevarande år har vi emellertid fått ett investeringsanslag för att inhandla ett sådant system, när SKL Upphandling/RA blir klar med sitt projekt.När systemet är på plats kommer många av informationssäkerhetsfrågorna att hanteras genom systemmetadata och filformatbegränsningar. Elektroniska signaturer blir dock inte en del av lösningen; de är snarare en del av problemet, eftersom de inte kan migreras/konverteras.

Landsarkivet i Östersund: Inom Riksarkivet sköts alla diskussioner kring elektronisk informationshantering från centralt håll. Landsarkivet i Östersund har heller ingen personal som arbetar med utvecklingsarbete inom det området. Jag förmodar att du skickat din förfrågan också till riksarkivet@riksarkivet.se, om inte rekommenderar jag att du gör det så vidarebefordrar de enkäten till ansvariga funktioner.

Landsarkivet i Vadstena: Eftersom vi lokalt på Landsarkivet i Vadstena inte varit direkt involverade i arbetet med den typen av frågor du vill få besvarade, avstår vi från att besvara enkäten.

Landsarkivet i Göteborg:Landsarkivet i Göteborg är en avdelning inom Riksarkivet. När det gäller elektronisk arkivhantering finns det inte någon på denna avdelning som arbetar med det utan den verksamheten är koncentrerad till andra delar av myndigheten. Eftersom din enkät gått till Riksarkivet centralt bör den ha nått de som arbetar med de aktuella frågorna.

Vilken funktion har du i detta arkiv?

Örebros stadsarkiv: Arkivarie med IT-ansvar (arbetar bl.a. med systemansvar för och förvaltning av arkivets databaser, tillgängliggörande av digitalt arkiverad information, arkivets webbsida).

Malmös stadsarkiv: IT-arkivarie.

Uppsalas stadsarkiv: IT-arkivarie.

Skatteverkets arkiv:Vi gör utredningar av vilken information som ska levereras till e-Arkiv och hur denna information ska hanteras, detta görs i form av anslutningar av verksamhetssystem till e-Arkiv.

Västerås stadsarkiv: Biträdande stadsarkivarie.

Riksarkivet: Arkivarie. Jag är också systemförvaltare för ett av systemen som ingår i RA:s digitala arkiv "RADAR" som implementerats för de digitala arkiv som levererats till RA. I RADAR hanteras inte bara s.k. "Born Digital-material" utan även analogt material som digitaliserats efter leverans såsom t.ex. skannade pappershandlingar eller digitaliserade audiovisuella handlingar.

Stockholms stadsarkiv:Enhetschef, tillsyn och rådgivning

Landsarkivet i Visby: Depåansvarig.

Landsarkivet i Lund: Landsarkivarie.

Har du deltagit i arbete eller överläggningar som handlar om organisationens informationssäkerhet?

Örebros stadsarkiv: I olika projekt rörande datasystem i kommunen har jag deltagit, samt även informations- och säkerhetsansvarig i kommunen. Då har vi diskuterat sådana frågor.

Malmös stadsarkiv:Ja, det förs en kontinuerligt pågående diskussion inom Malmö stad rörande frågan om informationssäkerhet.

Uppsalas stadsarkiv: Ja.

Skatteverkets arkiv:Delvis, frågan har bl.a. berörts när hanteringen av Skatteverkets loggar har utretts i en gallringsutredning.

Västerås stadsarkiv: Ja.

Riksarkivet: Ja, många gånger.

Stockholms stadsarkiv: Ja.

Landsarkivet i Visby: Ja.

Landsarkivet i Lund:I min tidigare roll som chef för Samordnings- och utvecklingsenheten deltog jag i Riksarkivets arbete med införande av LIS.

Hur skulle du beskriva relationen mellan informationssäkerheten och det arbete du själv bedriver till skydd för organisationens arkivhandlingar?
Örebros stadsarkiv: Gemensamma intressen av att informationen ska vara säker.

Malmös stadsarkiv: MSA är en del av stadens sammanhållna informationshantering. Kravställning sker utifrån verksamhetsbehov (t.ex. behörighetskontrollsystem, fysisk placering av serverrum etc.), dels utifrån samhälleliga behov som regleras i författning.

Uppsalas stadsarkiv: Skydd av arkivhandlingar är en del av arbetet med informationssäkerhet.

Skatteverkets arkiv:För vår del handlar det i första hand om åtkomsten till handlingarna och detta styrs genom en central behörighetshantering.

Västerås stadsarkiv:Informationssäkerhet hänger tätt ihop med de frågor som Stadsarkivet driver och även har tillsyn över. Att rätt information bevaras och gallras (även utifrån PUL-aspekten), att rätt information visas för rätt användare, att medvetandegöra att informationen ska säkerhetsklassas (vad är viktigast att börja med åtkomstmässigt efter ett ev. totalhaveri).

Även lagringsproblematiken kan vara ett problem i stort samt att organisationen inte gallrar trots att gallringsbeslut finns. Det är en säkerhetsrisk i sig.

Riksarkivet: Som hårt knutna till varandra. Min sektion arbetar inom flertalet av RA:S huvudprocesser som t.ex. "Att hantera statliga arkivleveranser" "Att bevara arkiv" och "Att tillhandahålla arkiv". "Informationssäkerhets-tänket" måste ständigt vara närvarande för att vi ska kunna bibehålla och förbättra vår informationssäkerhet. Det måste finnas en implementerad säkerhetsorganisation som arbetar i enlighet med LIS. Själv deltar jag i RADAR:s förvaltningsråd samt i IT-avdelningens Förändringsadministrations-möten en gång i veckan. I båda dessa grupper diskuteras och beslutas i informationssäkerhetsfrågor. Grupperna består av både IT-personal och arkivarier. Jag har också varit delaktig i framtagande av underlag till Försvarets radioanstalt (FRA) och Riksrevisionen när de granskat vår IT-verksamhet.

Stockholms stadsarkiv:Jag bedömer att informationssäkerheten är hög, det måste säkerställas genom kontinuerligt arbete.

Landsarkivet i Visby:Landsarkivet i Visby har inte tagit emot några leveranser av elektroniska handlingar. Vi har enbart tagit emot analogt material.

Landsarkivet i Lund:Det centrala är informationsklassificeringen, ett säkert handhavande av de digitala arkivhandlingarna och skalskyddet.

Hur skulle du själv, rent principiellt, beskriva informationssäkerhetsproblemen ur en arkivsynpunkt?

Örebros stadsarkiv: Det finns ett utvecklat säkerhetstänk när det gäller drift och backup av information servrar etc. Där det finns mer att göra är när det gäller säkerställande av att det inte blir informationsförluster i samband med t.ex. systembyten, när verksamheter upphör, vid omorganisationer, när projekt avslutas och när personal slutar. Det är inte alltid man då på ett strukturerat sätt tar hand om informationen och ser till att den blir arkiverad. Brister i systemdokumentation gör att information kan bli svår att förstå.

Malmös stadsarkiv: Informationssäkerhet är en av flera aspekter som omgärdas av ett regelverk som myndigheter ska följa. Området skiljer sig på det viset inte från andra verksamhetsdelar ur arkivsynpunkt.

Uppsalas stadsarkiv: En allomfattande och svår fråga. Jag tror att några av de största problemen med informationssäkerhet är otydligt eller obefintligt ansvar för frågan samt okunskap. Ytterligare ett problem är att man enbart ser informationssäkerhet som en IT-fråga.

Västerås stadsarkiv:Det är ungefär samma frågor inom hela organisationen oavsett vem som ansvarar för informationen: att rätt person får ta del av den information man har rätt till och inget annat, att de som har skyddad identitet är skyddade även när information överlämnas till Stadsarkivet. Att ingen information ”försvinner” på sikt är också en informationssäkerhetsutmaning med en inbyggd lagringsproblematik.

Riksarkivet: Kravet att bevara sekretess och riktighet hos informationen samtidigt som vi har krav på oss om öppenhet/tillgänglighet är hela tiden en balansgång. Mycket arbete måste läggas ner på åtgärder för att säkra drift och funktionalitet, spårbarhet och skydd mot obehörig åtkomst, arbete med kvalitetssäkring av information, autentisering och tillförlitlighet m.m. I informationssäkerhetsarbetet ingår viktiga arkivfrågor kring dokumenthantering, metadata, långtidsbevarande, arkivering, konvertering, riskhantering och ansvarsfördelning.

Stockholms stadsarkiv:Informationssäkerhet i vårt e-arkiv handlar främst om avvägningar kring de två intressena att göra informationen tillgänglig till så många som möjligt utan överträdelser av sekretess och PUL-bestämmelser, samt andra inskränkningar som upphovsrättsliga. Informationssäkerheten i vårt e-arkiv handlar dessutom att säkerställa informationens autenticitet och integritet över tid.

Landsarkivet i Visby: Det är viktigt att autenticiteten bevaras.

Landsarkivet i Lund:Att personalen är medveten om de säkerhetsregler och rutiner som gäller inom organisationen och följer dem.

Har du upplevt några brister i informationssäkerheten och i så fall vilka?
Malmös stadsarkiv: Nej, inte som har kommit till min/MSA:s kännedom.

Hudiksvalls kommunarkiv: I Hudiksvall har det vad jag kan erinra mig aldrig varit några problem vad gäller säkerheten. I Ljusdal händer det att det blir stopp i de olika datasystemen. Oftast är det mailen. Och det beror endast på överbelastning i servrarna. MEN detta skulle säkert kunna leda till ett större fel. En sak som jag kan uppleva som ett integritetsproblem är dock att det i Hudiksvall ibland kommer mycket känsliga uppgifter till vår fax som finns i vårt kopieringsrum, alltså rätt öppet. Men det problemet är ju inte av teknisk art utan mer ett informations- och rutinproblem.

Västerås stadsarkiv: För staden eller för Stadsarkivet? Inom staden finns kryptering när information skickas. Den fungerar dock inte för s.k. smarta telefoner, vilket allt fler använder. Det sker en lagring av information trots att gallringsbeslut finns. Inom vår förvaltning Stadsarkivet kan jag i dagsläget inte se några större problem eller brister i dagsläget för information som vi tagit emot.

Riksarkivet: Självklart. T.ex. att det saknas dokumenterade rutiner och beslut som också är kommunicerade i organisationen, att behörighetssystemet inte är tillräckligt finfördelat för att kraven på spårbarhet uppnås, hög andel manuella moment i kontroll- och migreringsprocesserna vilket ökar risken för att fel inte upptäcks eller att fel görs.

Stockholms stadsarkiv: Nej.

Landsarkivet i Lund:Brister i personalens kunskaper om regelverket.

Vilka följder har dessa brister fått?

Örebros stadsarkiv: Information som borde arkiverats och bevarats finns inte kvar p.g.a. skäl som nämnts i punkt 5. Delar av information har tappats i samband med konvertering vid systembyten.

Hudiksvalls kommunarkiv: Ja, det har som tur är inte givit upphov till några större problem, annat än att man inte kan arbeta så länge datorerna inte fungerar.

Uppsalas stadsarkiv: Information saknas eller går inte att hitta eller är inte komplett.

Västerås stadsarkiv:Om brister skulle finnas så kan det innebära att information riskerar att komma orätta händer, försvinna eller förvanskas.

Riksarkivet: Att arbetssätten inte kunnat standardiseras, svårt att spåra händelser på individnivå, risk att brister i leveranser inte upptäcks vilket kan leda till informationsförluster.

Landsarkivet i Lund:Inga incidenter har inträffat än så länge men en följd skulle kunna bli att information kommer i orätta händer eller förstörs.

Hur har din arkivfunktion försökt lösa de olika bristerna inom informationssäkerheten?
Örebros stadsarkiv: Genom styrdokument för kommunens verksamheter, som riktlinjer och instruktioner för digital arkivering (hemsidan). Information till och möten med ansvariga.

Hudiksvalls kommunarkiv: Har inte aktivt deltagit i några lösningar av liknande problem. Möjligen blivit tillfrågad ibland vid byte av program och vad det kan få för konsekvenser ur konverteringssynpunkt.

Uppsalas stadsarkiv: Jobbat med tillsyn, undervisning, verksamhetsutveckling, lobba för frågan i olika forum inom kommunen.

Västerås stadsarkiv:Vi deltar i strategiska projekt inom olika områden.

Riksarkivet: Vi arbetar aktivt med åtgärdslistor. Vi har vid implementationen av RADAR förbättrat behörighetsadministration, virushantering och loggning. Även det fysiska skalskyddet har stärkts. Dokumentation av rutiner och beslut är också delar som styrts upp. Automatiserade kontroller av leveranser har införts i många moment i RADAR. Vi har också tagit hjälp av FRA för att få en bedömning av vår IT-verksamhet. Detta har hjälpt oss att hitta viktiga brister som vi kunnat åtgärda eller foga till åtgärdsplan på längre sikt. Även Riksrevisionens granskning har gett oss liknande hjälp.

Landsarkivet i Lund:Genom införande av LIS, utarbetande av checklistor och internutbildning.

Använder ni er av någon form av krypteringssystem eller elektroniska signaturer för de elektroniska handlingarna?
Örebros stadsarkiv: Inte inom arkivet.

Hudiksvalls kommunarkiv: Nej, det förekommer inte idag men det är en fråga som i likhet med frågan om e-arkivering finns på agendan.

Uppsalas stadsarkiv: Vi har inga arkiverade e-handlingar på stadsarkivet.

Västerås stadsarkiv:Elektroniska signaturer förekommer i vissa e-tjänster. Vi bevarar inte den elektroniska signaturen, däremot dokumentationen om att kontroll är gjord. Kryptering sker och finns inom staden.

Riksarkivet: Vi använder checksummor för arkivpaketen som långtidsbevaras i RADAR. Enligt våra leveranskrav kan vi ta leveranser med elektroniska signatureren enligt IETF RFC 2315 PKCS #7: Cryptographic Message Syntax Version 1.5, eller XML-signatures för strukturerade dokument i XML (Extensible Markup Language). Detta är dock i nuläget bara tänkt att tas emot och bevaras oförändrat och en framtida användare får bedöma användningsbarheten av signaturen.

Stockholms stadsarkiv: Nej.

Landsarkivet i Lund: Nej.

Om ni använder er av migrering, hur gör ni för att motverka informationsbortfall i migreringsprocessen?
Örebros stadsarkiv: Vid varje kopiering kollar vi och jämför mängden data.

Malmös stadsarkiv: MSA utför inte migreringar. Malmö stad migrerar dock inte sällan information från ett IT-stöd till ett annat. Då ansvarar ofta en extern leverantör för själva migreringen som i sin tur har kravställts av Malmö stad. Från MSA:s perspektiv trycker vi på vikten av att gallringsutreda informationen inför migrering.

Hudiksvalls kommunarkiv: Migrering förekommer inte så frekvent. Vid exempel byte av programvara sker en ständig dialog med gamla och nya leverantörer.

Västerås stadsarkiv:När migrering av elektroniska handlingar sker hos Stadsarkivet, exempelvis till nya databärare, används hash-funktionen SHA-256 för att säkerställa att informationen överförts korrekt.

Riksarkivet: De arkivformat som vi tar emot för arkivering från myndigheter framgår av RA-FS 2009:2. Efter kontroll av data och metadata paketeras arkivpaket i RADAR som är uppbyggt i enlighet med OAIS-modellen. Vi har två exemplar på band och ett på disk av paketen, med checksummor. När det är dags för migrering till nya databärare och eventuell konvertering till andra format så packas paket upp och migreras/konverteras. Tanken är det ska finnas teknik så att konvertering till nya filformat i princip ska kunna ske utan informationsförlust. Efter migrering görs förändringar i metadata och hela processen dokumenteras av den person som utför konverteringen/migreringen. De nya filerna kontrolleras sedan av annan person som också kör RA:s s.k. Kontrollramverk (KRAM) för automatiserad kontroll av data mot metadata. Filerna paketeras sedan igen, får nya checksummor och läggs på nya databärare.

Stockholms stadsarkiv:Vi har ännu inte kommit i behov av migrering.

Landsarkivet i Lund:Dokumentation av arbetet, validering efter migrering och kontroll av checksummor.

Hur jobbar ni aktivt för att minimera risken för att felaktiga handlingar förs in i e-arkivet?

Örebros stadsarkiv: Genom kontroller vid leveransmottagande.

Malmös stadsarkiv: Gallringsutredningar samt informera kring godkända format och metoder vid överföringar.

Hudiksvalls kommunarkiv: Det enda kända säkerhetsaspekten vi här i dessa småkommuner har att åberopa är mailsystemets Spamfilter. E-arkiv har vi inte ännu men det ligger ett förslag att Regionen ska titta på denna fråga så vi får en gemensam satsning.

Skatteverkets arkiv:Detta hanteras i anslutningsutredningarna som resulterar i tekniska nycklar som måste användas för att e-Arkiv ska ta emot handlingarna.

Västerås stadsarkiv: Stadsarkivet har inget e-arkiv, däremot en stor mängd elektroniska handlingar från olika kommunala verksamheter. Alla elektroniska handlingar som inkommer till Stadsarkivet kontrolleras och valideras innan de godkänns av oss. Bl.a. sker kontroller av struktur/syntax, teckenuppsättning och läsbarhet. Rör det sig om information i XML-format sker därutöver validering mot XML-schema. Vad gäller informationsinnehåll, så brukar vi dessutom göra stickprov och jämföra informationen med den i det ursprungliga verksamhetssystemet. Stadsarkivet arbetar även förebyggande genom att kravställa arkiveringsfunktionalitet vid upphandling av IT-system och sedan testa denna vid respektive systems införande.

Riksarkivet: Först efter att myndigheter lämnat in en "Leveransframställan" till RA och Leveransfunktionen vid RA beslutat om leverans ska ske så undertecknas en överenskommelse där det anges vilka arkiv det handlar om och vilken ersättning RA ska ha för detta. Vi kontrollerar sen, vid leverans av e-arkiven, att innehållet är det som står i överenskommelsen. Gäller frågan handlingarnas kvalité så kontrolleras dessa både angående virus, godkända format och jämförs mot metadata.

Stockholms stadsarkiv:Genom en kvalitetssäkrad process för anslutningar till e-arkivet som ska säkerställa bl.a. den frågan i anslutningsarbetet.

Landsarkivet i Lund: Använder en etablerad leveransprocess med kontroll av leveranser och metadata.