Avdelningen för digitalisering
Jeanna Thorslund

Informationssäkerhet och outsourcing av IT-verksamhet med anledning av informationsläckage hos Transportstyrelsen

Denna pm utgår från de frågeställningar som har aktualiserats av det informationsläckage som har skett i samband med outsourcing av IT-verksamhet hos Transportstyrelsen och avser att lyfta aktuella förhållanden i motsvarande frågor för kommuner, landsting och regioner. Innehållet kan fungera som stöd vid diskussion om frågorna internt hos kommuner, landsting eller regioner.

Fem rekommendationer till SKLs medlemmar:

1. Alla kommuner, landsting och regioner samt kommunalägda bolag inom sektorn bör kartlägga vilka informationstillgångar (t.ex. information, IT-system) man har i sin verksamhet. Undersök särskilt ifall det finns informationstillgångar som kan vara kritisk för rikets säkerhet och omfattas av reglerna i Säkerhetsskyddslagen.
2. Säkerställ att rutiner för nödvändiga säkerhetsanalyser, riskanalyser och kontroll enligt dataskyddslagstiftning är införda och följs vid upphandling av IT-drift och liknande.
3. Se till att det finns aktuell information om vilka leverantörer och deras underleverantörer som anlitas och i vilka länder dessa finns. Säkerställ att nödvändiga säkerhetsanalyser av resurser, personal och rutiner finns på plats och efterföljs.
4. Arbeta för en god säkerhetskultur i hela organisationen där det finns ett fungerande samspel mellan olika kompetenser inom säkerhet, informationssäkerhet, juridik med projekt, styrgrupper och ledning.
5. Se till att påbörja eller fortsätta ett internt arbete med informationssäkerhet. Som minimum bör alla arbeta med dessa rekommendationer från MSB, som även SKL står bakom och har informerat om den 18 januari 2017: https://www.msb.se/Upload/Forebyggande/Informationssakerhet/MSBRekommendationer_kommuner_korthet_170113.pdf

Olika nivåer av känslig information

- Det finns flera nivåer av känslighet hos information och hur kritisk den är för verksamheten. Det finns en metodik för att göra den här indelningen – informationsklassificering. Den modell som rekommenderas finns presenterad i Metodstöd för informationssäkerhet, framtaget av Myndigheten för samhällsskydd och beredskap (MSB).
- SKL har tagit fram ett verktyg, KLASSA, för att stödja kommuner, landsting och regioner i detta arbete. Använd gärna det. https://skl.se/naringslivarbetedigitalisering/digitalisering/informationssakerhet/klassainformationsklassning.7558.html

Avdelningen för digitalisering
Jeanna Thorslund

- Kommuner, landsting och regioner har överlag inte alls lika mycket information av den mycket känsliga karaktär som varit aktuell hos Transportstyrelsen, inte heller i samma omfattning.
- Olika typer av känslig information behöver hanteras på lite olika sätt. Åtgärder skiljer sig åt för t.ex.:
    - Information som omfattas av vanlig sekretess (t.ex. personuppgifter inom social omsorg och hälso- och sjukvård) och som kräver riskanalyser och utvidgade säkerhetskrav vid IT-drift och upphandling. Denna typ av känslig information är vanligt förekommande hos kommuner, landsting och regioner och man arbetar också aktivt med skyddsåtgärder.
    - Information som kräver extra säker hantering eftersom den kan vara kritisk för verksamheten i samband med större kriser (t.ex. information inom infrastruktur, organisation inom hemsjukvård, läkemedelshantering, transporter, sophantering o.likn.). För denna typ av känslig information finns ofta behov av att arbeta med kontinuitetsplaner så att verksamhet kan upprätthållas även vid kriser och avbrott.
    - Dessutom finns information som är så känslig att den kan riskera rikets säkerhet om den kommer i orätta händer, som omfattas av reglerna i Säkerhetsskyddslagen. Sådan information kräver särskilda analyser och rutiner, skyddsklassad personal och upphandling som berör sådan information har en egen rutin, se information från Säkerhetspolisen: http://www.sakerhetspolisen.se/sakerhetsskydd/sakerhetsskyddad-upphandling.html
- Det åligger varje kommun, landsting, region, kommunalägt bolag att själva göra en bedömning av ifall man har denna senare typ av mest känslig information, identifiera den och därefter göra en säkerhetsanalys. Det finns regler om detta i säkerhetsskyddslagen, som gäller även vår sektor. Detta ansvarar normalt säkerhetschefen för. Vi vill gärna uppmana alla kommuner, landsting och regioner att säkerställa att detta är gjort.

God säkerhetskultur

- Som aktualiseras av informationsläckaget vid Transportstyrelsen är informationssäkerhet till stor del en fråga om förtroende. Dels ett förtroende från enskilda individer som ofta måste dela med sig av personliga, känsliga uppgifter till våra verksamheter, att vi har en förmåga att hantera dessa uppgifter på ett korrekt och säkert sätt. Men det gäller även ett förtroende myndigheter emellan eftersom uppgifter ska utbytas och kommunikationsvägar upprättas.
- När det gäller den här typen av händelser är det vanligt att det sker en ”smittoeffekt” med negativ påverkan på förtroendet från enskilda, som kan drabba även verksamheter inom vår sektor. Det kan därför vara extra viktigt att gentemot

Avdelningen för digitalisering
Jeanna Thorslund

sökande eller registrerade individer vara tydlig med vilka säkerhetsrutiner som finns införda och efterlevs inom verksamheten.
- För att undvika den här typen av händelser måste man givetvis följa de lagar och säkerhetsrutiner som finns. Men det behövs även ett kontinuerligt säkerhetsarbete som kan bidra till att skapa en god säkerhetskultur i hela organisationen. När man uppnår detta fungerar samspelet mellan olika kompetenser inom säkerhet, informationssäkerhet, juridik med projekt, styrgrupper och ledning. På så sätt kan man uppnå en balans mellan krav som ibland kan stå i konflikt med varann – tidspress, utvecklingsbehov och ekonomiska krav i förhållande till behov av tid för säkerhetsanalyser, riskanalyser, kartläggningar och ibland behov av att dra i handbroms och göra omtag och korrigeringar.

Informationssäkerhet och outsourcing

- Det är inte självklart att det blir bättre informationssäkerhet med IT-drift i egen regi. Med ökande komplexitet i regelverk, teknikutveckling, behov av investeringar i utrustning och resurser, ökande externa hot samt svårigheter att på alla orter rekrytera kompetent personal, kan outsourcing istället vara ett sätt att klara av ökande säkerhetskrav.
- Vi rekommenderar att alla kommuner, landsting och regioner genomför en kartläggning av alla sina informationstillgångar (t.ex. IT-system) för att först ha en aktuell bild över vilken information som kan vara extra känslig och som kan behöva granskas särskilt enligt Säkerhetsskyddslagen.
- I samband med upphandling av IT-drift och IT-kompetens är det nödvändigt att kunna ge korrekt underlag till leverantören om vilka behov verksamheten har och ifall man har sådan verksamhet som kräver särskild hantering enligt Säkerhetsskyddslagen och då leverantören kommer att behöva tillhandahålla personal som är säkerhetsklassade.
- I upphandlingen och i avtal med vald leverantör ska ställas relevanta säkerhetskrav som medför att leverantören upprätthåller en lämplig nivå av säkerhet i förhållande till verksamhetens behov och hur känslig information det är. Verktyget KLASSA ger underlag för att ställa säkerhetskrav vid upphandling, men vid upphandling som rör den alla mest känsliga informationen rekommenderas en anpassad och fördjupad analys.

Lagar och regler som ställer krav

- Offentlighets- och Sekretesslagen (OSL), reglerar vilken information som ska omfattas av sekretess. Det måste göras särskild sekretessprövning för att sådan information ska få lämnas ut från myndigheten. Detta måste göras även vid upphandling för att undvika sekretessbrott och att känslig information om enskilda eller affärsförhållanden blir tillgänglig för obehöriga.

Avdelningen för digitalisering
Jeanna Thorslund

- Personuppgiftslagen (PUL), reglerar dataskydd för individer då uppgifter om dem registreras och behandlas. Kommuner, landsting och regioner har stora mängder personuppgifter och även känsliga personuppgifter. Om man överlämnar åt t.ex. en leverantör att hantera sådana uppgifter måste man först säkerställa att de kommer att hanteras korrekt. Det finns även begränsningar när det gäller till vilka andra länder personuppgifter får överföras.
  PUL kommer under 2018 att ersättas av EU:s Dataskyddsförordning som kommer att medföra betydligt skärpta krav på bland annat konsekvensanalyser och informationssäkerhet.
- Säkerhetsskyddslagen innehåller bestämmelser om verksamheter och information som är så känslig att det kan riskera rikets säkerhet om den kommer i orätta händer. Detta förekommer mer sällan i vår sektor, men det finns.
  Det åligger varje myndighet, kommun, landsting och region att undersöka vilka uppgifter i verksamheten som ska hållas hemliga med hänsyn till rikets säkerhet. Resultatet ska dokumenteras i en säkerhetsanalys som ska ge stöd för vilka åtgärder som behöver vidtas, informationssäkerhet, fysisk säkerhet, personalsäkerhet eller annat. Exempel på sådan verksamhet inom vår sektor kan vara infrastruktur som elförsörjning, vattenförsörjning, hamn- och flygplatsverksamhet eller ritningar över vissa fastigheter och anläggningar. Sådan verksamhet finns ofta hos kommunala bolag, men ägaren bör undersöka att rätt åtgärder vidtas.
  Säkerhetsskyddslagen har nyligen utretts och 2015 lades betänkande fram med förslag till ny lag.
- Informationssäkerhet regleras inte genom en sammanhållande lag utan genom bestämmelser i flera olika regelverk, t.ex. i PUL. Det finns även i lagstiftning, föreskrifter och rekommendationer inom hälso- och sjukvård med flera områden. Sammantaget pekar dessa på att alla kommuner, landsting och regioner ska införa ett LIS (Ledningssystem för informationssäkerhet) som baseras på standarden inom området, ISO 27000-serien.

Sammanfattning av händelsen vid Transportstyrelsen

Transportstyrelsen har, såvitt framgår av uppgifter som finns tillgängliga nu, genomfört en upphandling av helhetsdrift av sin IT-verksamhet. Under upphandlingsprocessen, har myndighetens GD och styrelse beslutat om att frångå tre lagar, OSL, PUL och Säkerhetsskyddslagen samt ett antal interna säkerhetsföreskrifter. Beslut om avsteg från lagstiftning har varit föremål för granskning av SÄPO, internrevisor, intern säkerhetspersonal, har informerats till departement, m.fl. Avsteget har protokollförts och finns dokumenterat. GD har avskedats och har accepterat ett strafföreläggande. Styrelsens ordförande har avgått. Ärendet granskas även av KU osv på politisk nivå, denna senare del lämnas utanför i

Avdelningen för digitalisering
Jeanna Thorslund

denna pm. Se vidare information hos transportstyrelsen: https://www.transportstyrelsen.se/sv/Om-transportstyrelsen/fragor-och-svar/

De uppgifter som har lämnats ut från myndigheten förefaller vara uppgifter i körkortsregistret, med information om en stor del av befolkningen, uppgifter om sjukdomar, skyddade identiteter, militära fordonsregister med mera. En stor del av denna information är sådan för riket skyddsvärd information som endast får hanteras av skyddsklassad personal. Istället har personal hos en underleverantör som saknar sådan skyddsklassad personal haft tillgång. Dessa har varit baserade utomlands, i huvudsak i Tjeckien och Serbien. I vilken utsträckning dessa uppgifter har förmedlats vidare till aktörer som kan medföra hot mot rikets säkerhet verkar vara oklart, men kan inte uteslutas.

Läs mer om informationssäkerhet: https://skl.se/naringslivarbetedigitalisering/digitalisering/informationssakerhetdataskyddsforordningen.1238.html

Vid frågor kontakta:

Vecka 31

Björn Söderlund, bjorn.soderlund@lidingo.se

Lotta Nordström, lotta.nordstrom@skl.se

Vecka 32

Lotta Nordström, lotta.nordstrom@skl.se

Åsa Zetterberg, asa.zetterberg@skl.se

Vecka 33

Åsa Zetterberg, asa.zetterberg@skl.se

Jeanna Thorslund, jeanna.thorslund@skl.se (Semester till 16/8)