Bilaga 6.
It- och informationssäkerhet (Konsultrapport Radar)

RiR 2016:8

Informationssäkerhetsarbete på nio myndigheter

En andra granskning av informationssäkerhet i staten

IT- OCH INFORMATIONSSÄKERHET

STATLIGA MYNDIGHETER OCH VERK, 2015–2016

radar. ECOSYSTEM SPECIALISTS

P 546 – Rrev. 1.0

OM RAPPORTEN

Denna rapport är producerad av Radar, på uppdrag av Riksrevisionen. Respondenturval, datainhämtning, djupintervjuer och analys har genomförts i Radars namn och Radar ansvarar självständigt för innehåll och slutsatser.
För mer information om Radars oberoende, dataintegritet eller konfidentialitet kontakta Hans Werner, CEO, Radar.
För frågor om metodik eller innehåll i detta whitepaper, kontakta ansvarig analytiker.

ANSVARIG ANALYTIKER:
Freddie Rinderud, analytiker/rådgivare
+46 707 830 490
freddie.rinderud@radareco.se

MODELLER OCH DJUPINTERVJUER:
Petter Wallin, senior rådgivare
+46 707 969 011
petter.wallin@radareco.se

RESEARCH OCH ANALYS:
Richard Werner, analytiker/rådgivare
+46 705 190 806
richard.werner@radareco.se

DATABEARBETNING:
Simon Fagerström, analytiker
+46 723 873 778
simon.fagerstrom@radareco.se

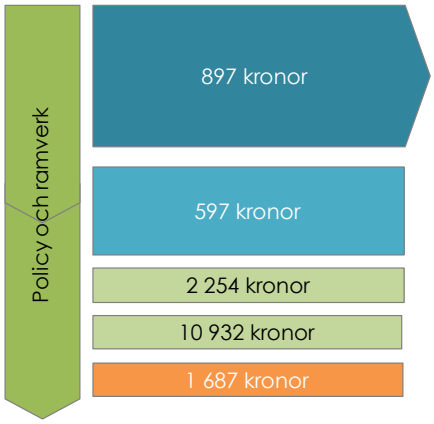
1. SAMMANFATTNING

I detta konsultuppdrag för Riksrevisionen har Radar undersökt totalkostnaderna för proaktivt informationssäkerhetsarbete inom statliga myndigheter och verk. Den reaktiva informationssäkerheten är exkluderad för att incidenter som rör informationssäkerhet varierar både i grad och komplexitet och därför inte går att beräkna på ett rättvisande sätt. För att beräkna totalkostnaden för proaktiv informationssäkerhet har en modell som tar hänsyn till tid, teknik och tjänster använts och respondenterna har estimerat kostnader inom respektive område (tid, teknik och tjänst) varpå Radar sedan lagt samman, anonymiserat och skapat de nyckeltal som ligger till grund för denna rapport.

Statliga myndigheter och verks genomsnittliga kostnad för proaktiv informationssäkerhet uppgår till 24 659 431 kronor per verksamhet och år vilket motsvarar 16 367 kronor per syselsatt och år. Skillnaderna mellan undersökta myndigheter och verk är dock stor. Detta beror på deras skilda uppdrag och storlekar, vilket innebär att de genomsnittliga kostnaderna för proaktiv informationssäkerhet bör snarare betraktas som en orientering än en exakt jämförelsebas. I Radars undersökande runt kostnader för proaktiv informationssäkerhet framkommer att myndigheter i genomsnitt spenderar från 13 809 kronor och upp till 29 159 kronor per sysselsatt och år.

De 16 367 kronor som statliga myndigheter och verk spenderar per sysselsatt och år på proaktiv informationssäkerhet fördelas enligt nedan:

- Verksamheten: 897 kronor
- Förvaltning och utveckling: 597 kronor
- IT-organisationen: 2 254 kronor
- IT-säkerhetsteknik: 10 932 kronor
- Externa IT-tjänster: 1 687 kronor



Undersökningen visar att teknik står för högst andel, relativt tid och tjänst, avseende totalkostnad för informationssäkerhet. Teknik står för 66,8 procent av totalkostnaden för informationssäkerhet, i genomsnitt 16 471 214 kronor per verksamhet och år. Tid står för den näst största delen med 22,9 procent av totalkostnaden med en genomsnittkostnad på 5 646 018 kronor per verksamhet och år medan tjänster står för 10,3 procent av totalkostnaden med en genomsnittskostnad om 2 542 200 kronor per verksamhet och år. Sammanlagt står teknik och tjänst för mer än tre fjärdedelar av kostnaderna för informationssäkerhet.

Undersökningen visar att verksamheten i större utsträckning än IT-organisationen spenderar tid på att ta fram policys/riktlinjer, ramverk och processer för informationssäkerhet. Verksamheterna spenderar i genomsnitt 613 692 kronor på att styra området informationssäkerhet medan IT-organisationen motsvarande del uppgår till 351 891 kronor vilket indikerar att styrningen av informationssäkerhet skapar styrning till IT-organisationen.

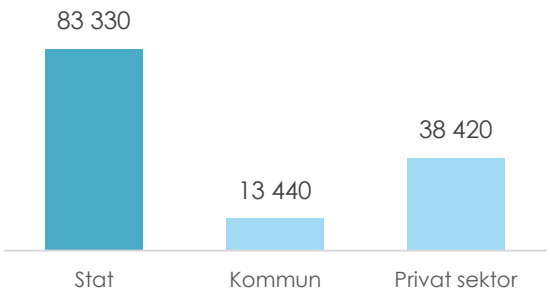
Det spenderas mest tid på informationssäkerhet i förvaltning och utveckling, i genomsnitt 898 786 kronor per verksamhet och år. Detta ska jämföras med verksamheten som spenderar 737 923 kronor per och år och IT-organisationens 318 583 kronor per år. IT-organisationens spenderade tid är antagligen lågt räknat då det är svårt för responderande myndigheters IT-organisationer att särskilja på tid de lagt specifikt på informationssäkerhet då detta allt som oftast är invävt i annat arbete. Inräknat heltidsekvivalenter (HTE) vilka arbetar med IT-säkerhetsteknik blir bilden annorlunda, då spenderar IT-organisationen mest ”tid” på att efterleva informationssäkerhet med en genomsnittlig kostnad på 3 043 725 kronor per verksamhet och år.

2. INNEHÅLLSFÖRTECKNING

3. IT-KOSTNADER OCH PRIORITERINGAR

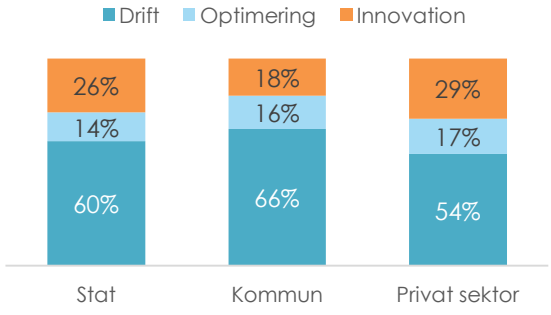
Den samlade IT-budgeten för svenska statliga myndigheter och verk uppgår 2015 till knappt 20,5 miljarder kronor, en ökning med 1,3 procent från föregående år. IT-budgetarna utgör dock bara en del av myndigheternas totala IT-kostnader (IT spend), som även finansieras av verksamhetsbudgetar. Hur stora de totala IT-kostnaderna är går inte att fastställa då myndigheternas redovisning vanligen inte sker på ett sådant sätt att det är möjligt att särskilja IT-kostnader från andra verksamhetskostnader med mindre än att studera varje enskild resultatenhet inom myndigheten verifikatsvis.
I Radars reguljära research under 2015 uppskattade IT-beslutsfattare (CIO, IT-direktör, IT-strateg, etc.) från 30 olika statliga myndigheter att verksamhetsfinansierad IT i genomsnitt utgör drygt 14 procent av de totala IT-kostnaderna. Ett antagande om att detta är ett representativt genomsnitt för samtliga statliga myndigheter och verk skulle i så fall innebära en total IT-kostnad om knappt 24 miljarder kronor. Baserat på de myndigheter där Radar har kartlagt IT-kostnader på uppdrag från den specifika myndigheten är 14 procent sannolikt en försiktig uppskattning.
Att de totala IT-kostnaderna uppgår till minst – och sannolikt mer än – 24 miljarder kronor stöds också av ett antal studier genomförda av andra aktörer. Som exempel kan nämnas ESV:s rapport ”IT-kostnadsmodell” (2014:50) som uppskattade de totala IT-kostnaderna 2014 till mellan 24 och 31 miljarder kronor.

IT-budget per sysselsatt 2015:



Källor: Radar 2015, Radar benchmarks, SCB

IT-budgetdistribution 2015:



Källor: Radar 2015, Radar benchmarks

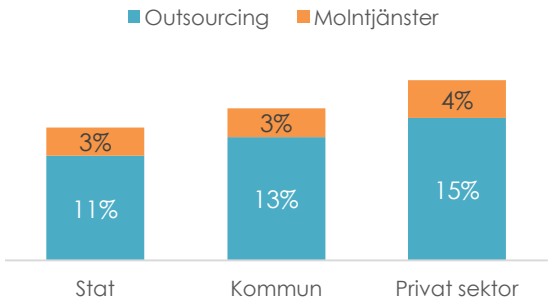
Statliga myndigheter och verks samlade IT-budget motsvarar ett genomsnitt om 83 330 kronor per sysselsatt. Skillnaderna mellan olika myndigheter är dock stor. I Radars research och benchmarkdata från 2015 finns myndigheter med IT-budgetar som motsvarar från 23 213 kronor till 307 692 kronor per sysselsatt. I dessa fall återspeglar skillnaderna i betydligt högre grad myndigheternas mycket skilda uppdrag och storlekar än eventuella skillnader i förmågan att producera/leverera IT kostnadseffektivt.
En jämförelse av genomsnittlig IT-budget per anställd mellan statliga myndigheter, kommuner och verksamheter i privat sektor ger slutsatsen att myndigheterna som helhet är jämförelsevis mycket IT-intensiva. Några vidare slutsatser än denna går enligt Radar inte att dra utifrån detta genomsnitt i sig, mot bakgrund av verksamheternas högst skilda uppdrag och storlekar. Nyckeltalet som sådant kan däremot vara relevant vid jämförelse av en enskild myndighets IT-budget, förutsatt att jämförelsetalet (benchmark) utgörs av andra verksamheter (i offentlig eller privat sektor) med liknande förutsättningar avseende storlek och verksamhet/uppdrag.

Ett annat vanligt nyckeltal vid jämförelser av verksamheters IT-budget är hur realiserade medel är distribuerade mellan löpande drift, optimering och innovation/transformation. Det får anses allmänt vedertaget att det i normalfallet är positivt med en högre andel innovation/tranformation jämfört med genomsnittet och att detta vanligen innebär en högre förmåga för IT-organisationen att stödja verksamhetsförändring/verksamhetsutveckling. För privat sektor har Radar även genomfört studier som bevisar ett samband mellan en högre innovationsandel av IT-budgeten och högre lönsamhet (vinst) för bolaget.
Den genomsnittliga andelen av statliga myndigheters IT-budget som används för innnovation/transformation uppgår till 26 procent. För att kunna möta ökade krav på IT-stöd från verksamheten och förväntningar från externa beslutsfattare och ”kunder” kommer de tillgängliga medlen för innovation/transformation att med all sannolikhet att behöva tillta över tid. Då ingen dramatisk tillväxt av den totala IT-budgeten är i sikte innebär detta att budget-distributionen gradvis måste förändras. Denna utmaning är gemensam för samtliga sektorer och branscher i Sverige.

3.1. PRIORITERINGAR OCH UTMANINGAR

Statliga myndigheter och verk har en större andel av sin IT-produktion i egen regi och en lägre andel standard-produkter i sin IT-portfölj jämfört med kommuner eller verksamheter i privat sektor. Det beror delvis på att myndigheternas individuella uppdrag och verksamhet till stor del är särpräglade eller unika, vilket kan göra det svårare att hitta lämpliga lösningar ”på marknaden”. Det gäller framför allt avseende systemstöd för kärnverksamheten. Myndigheterna producerar dock även infrastrukturdrift, applikationsdrift, systemutveckling och andra områden som helt eller i vissa fall lämpar sig väl för externa leveranser. Det senare beror sannolikt på en blandning en tradition att producera i egen regi och de särskilda (regulatoriska) krav som åläggs myndigheterna.

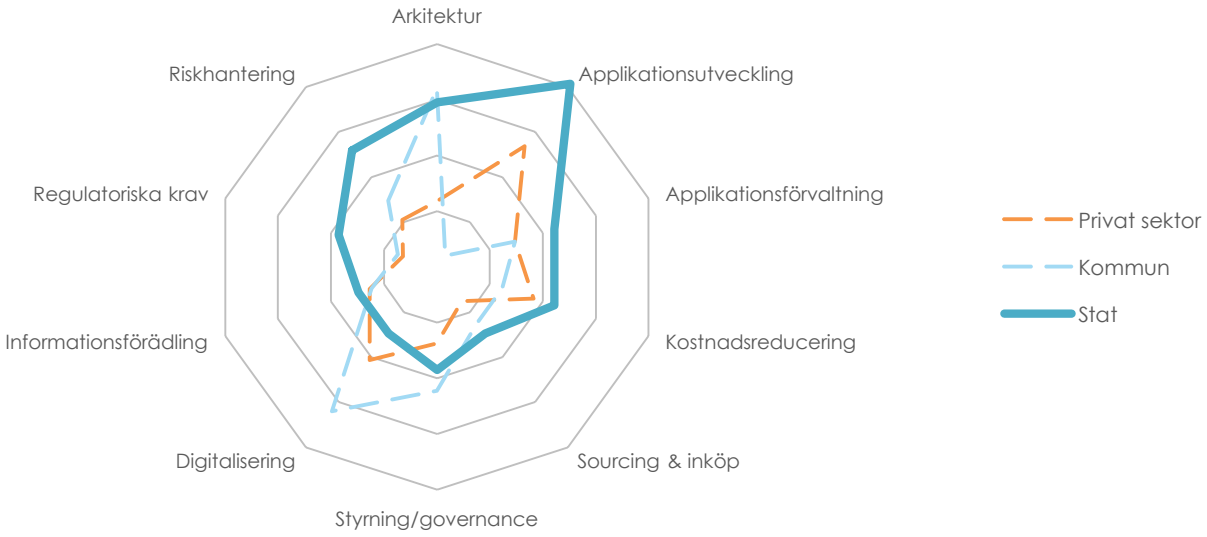
Andel externa leveransformer 2015:



Källor: Radar 2015, Radar benchmarks

Att myndigheterna producerar en större del av sin IT i egen regi påverkar också tydligt verksamheternas IT-prioriteringar jämför med privat sektor. Myndigheterna har under många av varandra efterföljande år haft tydligt fokus mot de tekniska områden som är sammankopplade till egen IT-produktion, samt krav- och säkerhetsrelaterade områden. Under 2015 är de enskilt viktigaste prioriteringarna applikationsutveckling och arkitektur. Det speglar väl hur IT-portföljen är uppbyggd. Detta följs av riskhantering och regulatoriska krav.
Mer förvånande är att de statliga verksamheterna i genomsnitt prioriterar informations- och verksamhetsorienterade områden som till exempel digitalisering och informationsförädling betydligt lägre (eller relativt till andra prioriteringar lägre) än genomsnittet för privat sektor och kommuner. Trots politisk vilja och initiativ avseende framför allt digitalisering är myndigheternas prioritering förhållandevis moderat.

Huvudsakliga IT-prioriteringar 2015 (urval baserat på statliga myndigheter och verk):

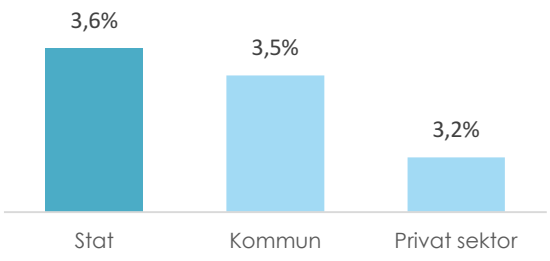


Källa: Radar 2015

4. IT-SÄKERHET

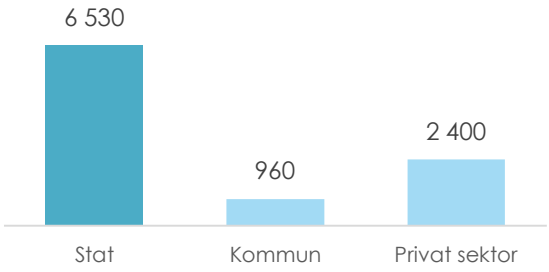
Statliga myndigheter och verk allokerade i genomsnitt 3,6 procent av sin IT-budget, totalt knappt 750 miljoner kronor, för planerade IT-säkerhetsinvesteringar och intern IT-säkerhetskompetens 2015. Sett som andel av IT-budget gör statliga myndigheter och verk därmed näst störst investeringar i IT-säkerhet jämfört med samtliga delar av offentlig och privat sektor. Bara verksamheter inom bank- och finansbranschen allokerar en större andel av sin IT-budget för planerade IT-säkerhetsinvesteringar och IT-säkerhetskompetens.
De proaktiva investeringarna utgör dock mindre än hälften av de totala investeringarna i IT-säkerhet hos statliga myndigheter. 2014 utgjorde de reaktiva investeringarna till 53 procent av de totala investeringarna, vilket med samma förhållande 2015 kommer att ge en total IT-säkerhetskostnad om 1,6 miljarder kronor. Det motsvarar 7,8 procent av IT-budgeten eller 6 530 kronor per sysselsatt och år – närmare tre gånger så mycket som genomsnittet för privat sektor och nästan sju gånger så mycket som genomsnittet för kommuner.

Planerade investeringar i IT-säkerhet som andel av IT-budget 2015:



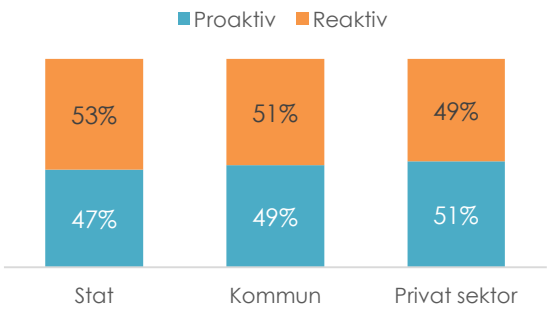
Källor: Radar 2015, Radar benchmarks

IT-säkerhetskostnader per sysselsatt 2015:



Källor: Radar 2015, Radar benchmarks, SCB

Fördelning av IT-säkerhetsinvesteringar:



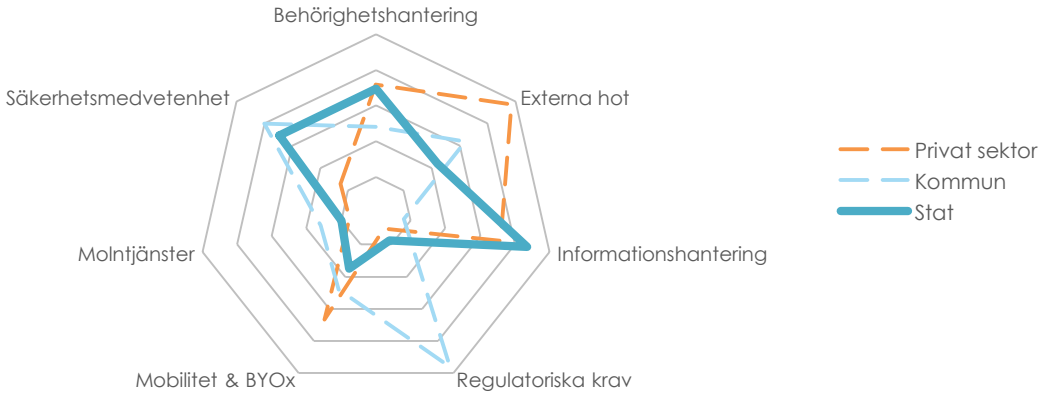
Källa: Radar 2015

Mot bakgrund av de skilda förutsättningarna för olika verksamheter, branscher eller delar av offentlig sektor bör de genomsnittliga IT-säkerhetskostnaderna snarare betraktas som en orientering än en relevant jämförelse.
Vad som däremot kan anses vara anmärkningsvärt är att statliga myndigheter trots mycket omfattande proaktiva investeringar inte lyckas värja sig mot uppkomna hot i högre grad än att en ännu större del, nästan 850 miljoner kronor, investeras reaktivt. En jämförelse av fördelningen mellan proaktiva och reaktiva IT-säkerhetsinvesteringar visar att statliga myndigheter, trots betydligt större IT-budget per anställd och större proaktiva IT-säkerhetsinvesteringar per anställd, har en större andel reaktiva investeringar jämfört med kommuner och privat sektor.
Detta kan möjligen till någon del förklaras av att myndigheterna – så vitt känt – är något mer utsatta för IT-säkerhetshot än den genomsnittliga verksamheten i privat sektor. Icke desto mindre finns det anledning att anta att berörda beslutsfattare inom statliga myndigheter och verk i högre grad än i privat sektor eller kommuner antingen saknar nödvändig insikt eller av något skäl hindras att genomföra nödvändiga investeringar i IT-säkerhet.

4.1. PRIORITERINGAR OCH UTMANINGAR

IT-säkerhetsarbetet inom statliga myndigheter och verk styrs och drivs till stor del av de externa (regulatoriska) krav som ställs på myndigheterna. Dessa krav tillhör också verksamheterna viktigaste IT-prioriteringar, vilket framgår av kapitel 3. Trots det är regulatoriska krav varken ett av de IT-säkerhetsområden som prioriteras högst eller ett av de säkerhetsområden som utgör de allra största utmaningarna för IT-organisationen. Detta bör ses som ett utslag av att myndigheterna både har lång erfarenhet av att hantera förändrade eller nya regulatoriska krav och att de är förvissade om sin egen förmåga att hantera dessa.
De viktigaste IT-säkerhetsprioriteringarna för statliga myndigheter och verk under 2015 är informationshantering, följt av säkerhetsmedvetenhet och behörighetshantering. Dessa tre är alla kopplade verksamhetsprocesser eller användare och visar tydligt den förändring som skett de senaste åren – från teknikorienterat säkerhetsarbete till verksamhetsorienterat säkerhetsarbete. Förflyttningen är ett utslag av en mognadsprocess. Det är i kontaktpunkterna mellan människa-människa eller människa-system som säkerhetskedjan är som svagast, vilket kräver att IT-säkerhetsarbetet och förståelsen för behovet av IT-säkerhet genomsyrar hela verksamheten.

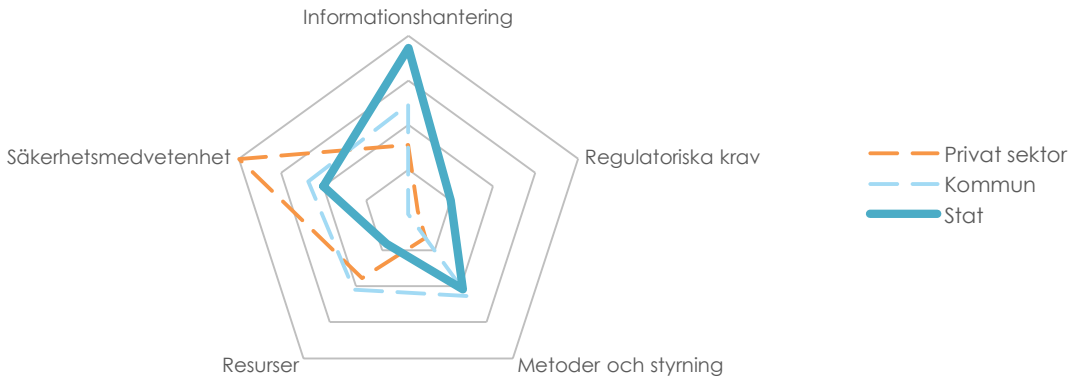
IT-säkerhetsprioriteringar 2015:



Källa: Radar 2015

Det är också verksamheternas förståelse för behovet av säkerhet (säkerhetsmedvetenhet) och behovet av att implementera säkerhetsarbete i de ordinarie verksamhetsprocesserna (informationshantering samt metoder och styrning) IT-beslutsfattarna uppfattar som den svåraste utmaningen. IT-beslutsfattarna upplever att verksamheterna har svårt att förstå behovet av IT-säkerhetsinvesteringar utan synbar nytta. Människor och teknik är det som skapar de svarta rubrikerna inom IT-säkerhet, vilket processer inte gör. Därför blir behovet av processer svårare att ta till sig för verksamheten, även om dessa är grunden för att styra säkerheten.

Största IT-säkerhetsutmaningar 2015:

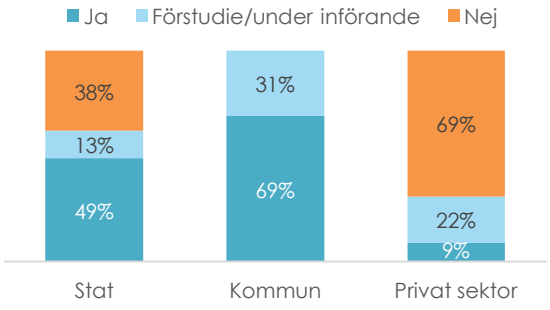


Källa: Radar 2015

4.2. INFORMATIONS- OCH BEHÖRIGHETSHANTERING

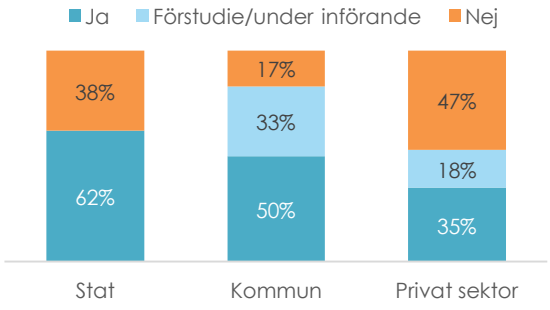
Grundförutsättningar för ett lyckat informationssäkerhetsarbete är att säkerhetsklassificera information (implementera och efterleva ramverk), kunna säkerställa individen vid varje tillfälle (autentisering) och följa individens användning av information (spårbarhet och loggning). Trots det uppfyller många myndigheter fortfarande inte dessa ”hygienfaktorer”. Pådrivna av de regulatoriska krav de lyder under har myndigheterna dock kommit längre inom dessa områden än verksamheter inom privat sektor.
I jämförelse med landets kommuner har däremot de statliga myndigheterna inte lika goda grundförutsättningar i dagsläget. Det gäller inte minst avseende autentisering, där samtliga kommuner använder flerfaktorautentisering i någon grad, medan bara varannan statlig myndighet har infört detsamma. Myndigheternas tillkortakommanden i jämförelsen är förvånande mot bakgrund av att de både har jämförelsevis större resurser inom området och att en enskild myndighets uppdrag och verksamhet vanligen är mindre diversifierad än en kommuns. Även om informationsmängderna hos vissa myndigheter är enorma borde det i vart fall inte vara svårare, generellt sett, för en myndighet att införa dessa principer eller lösningar.

Har ramverk för säkerhetsklassificering:



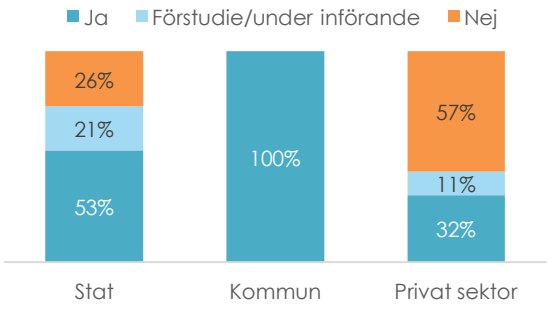
Källa: Radar 2015

Har spårbarhet och loggning:



Källa: Radar 2015

Använder flerfaktorautentisering:



Källa: Radar 2015

Nästan hälften av IT-beslutsfattarna anser att den största utmaningen i informationssäkerhetsarbetet är att säkerhetsmedvetenheten i verksamheten är för låg. Beslutsfattarna anger att de inte får ett aktivt stöd från verksamhetsledningen eller tillräckliga resurser och att det finns ett ointresse från verksamheten att ta ett aktivt ansvar för frågan. Detta visar att säkerhetsmedvetenhet fortfarande är det största bryderiet för IT-beslutsfattaren – det vill säga att skapa en kultur där verksamhetsledning och användare förstår riskerna kopplat till användningen av IT. Säkerhetsmedvetenheten styr med andra ord själva informationshanteringen som helhet.
Var fjärde IT-beslutsfattare anger också att informationshanteringen i sig är ett problem. Det är svårt att säkerhetsklassificera information på grund av den stora mängden och att det löpande tillförs ny information.

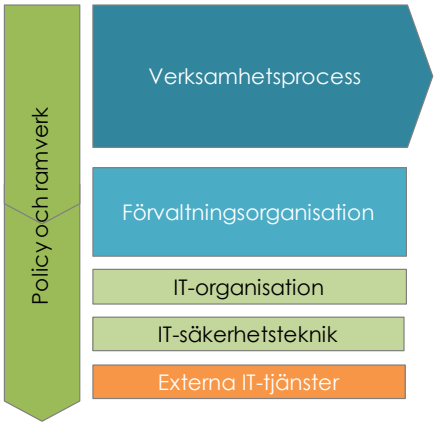
5. KOSTNADSBERÄKNINGMODELL INFORMATIONSSÄKERHET

För att beräkna totalkostnaden för informationssäkerhet i statliga myndigheter och verk har en modell som tar hänsyn till ”tid”, ”teknik” och ”tjänster” för proaktiv informationssäkerhet använts. ”Tid” i modellen är de timmar verksamheten, förvaltning och utveckling samt IT-organisationen spenderat på arbete med proaktiv informationssäkerhet. ”Tid” beräknas på de timmar olika befattningar och roller lägger ner på aktiviteter som; framtagning, efterlevnad och uppföljning av; policy/riktlinjer, ramverk och processer för informationssäkerhet. Kostnaden för ”tid” beräknas sedan på aktuell lönestatistik inom offentlig sektor. Till sist tar konstnadsberäkningsmodellen in kostnader för teknik och tjänster för att säkra verksamhetens information, detta är bland annat; antivirus, brandväggar, backup, penetrationstester etc. På detta sätt presenteras, genom kostnadsberäkningsmodellen, en helhetsbild för kostnaderna för proaktiv informationssäkerhet inom statliga myndigheter och verk. Det som inte ingår i kostnadsberäkningsmodellen är den reaktiva kostnaden för informationssäkerhet, det vill säga arbetet med att lösa olika typer av incidenter som relaterar till informationssäkerhet. Den reaktiva informationssäkerheten är exkluderad för att incidenter som rör informationssäkerhet varierar både i grad och komplexitet och därför inte går att beräkna på ett rättvisande sätt.

- **Tid** - de timmar olika befattningar och roller, vilka involverats i informationssäkerhetsarbete, spenderat på att ta fram, efterleva och utvärdera; policy, ramverk och processer. Verksamhetprocess, Förvaltning och utveckling samt IT-organisation beräknas på framförallt på ”tid”.

- **Teknik** (IT-säkerhetsteknik) - de löpande kostnader som kan härledas till system och applikationer som anskaffats i syfte att säkra verksamhetens information.

- **Tjänster** (Externa IT-tjänster) - de löpande kostnader som går att härleda till tjänster i syfte att säkra verksamhetens information.



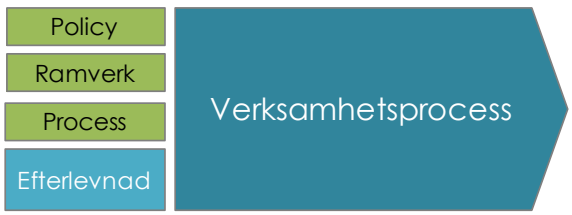
Kostnadsberäkningsmodell

5.1. VERKSAMHETSPROCESS

I kostnadsberäkningsmodellens ”verksamhetsdel” beräknas i den ”tid” verksamheten spenderat på framtagning, efterlevnad och uppföljning av; policy/riktlinjer, ramverk och processer för informationssäkerhet. Framtagning är de aktiviteter som verksamheten lägger ner på att ta fram policy/riktlinjer, ramverk, processer samt utbildningar för informationssäkerhet. I efterlevnadsdelen beräknas tid nedlagd på aktiviteter som; informationsinventering, riskanalyser och informationsklassning samt utbildningar av personal för att höja säkerhetsmedvetandet i verksamheten. Vidare har den tid som lagts i olika möten, beslutsunderlag samt beslutsfattande rörande verksamhetens information informationssäkerhet. Uppföljning är de kostnader (tid) som finns förknippade med uppföljning av det framtagna riktlinjerna och ledningssystemet. Utmaningen i denna del av kostnadsberäkningsmodellen består i att identifiera och separera timmar som också ligger parallellt i förvaltning och utveckling samt IT-organisation.

Tid (antal timmar) nedlagt på framtagande av;
- Policy/riktlinjer
- Ramverk
- Utbildningar (för personal)
- Verksamhetsprocesser (anpassning)

Tid (antal timmar) nedlagt på efterlevnad;
- Informationsinventering



Beräkningsmodell för verksamhet

- Riskanalys och klassning
- Möten, beslutsunderlag samt beslut
- Utbildningar (av personal)

Tid (antal timmar) nedlagt på uppföljning av;

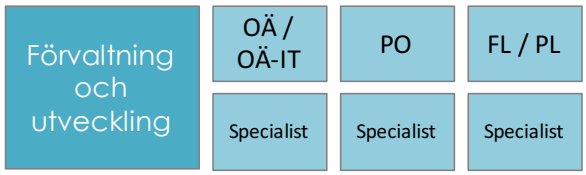
- Policy, ramverk, processer samt utbildning

5.2. FÖRVALTNING OCH UTVECKLING

Förvaltning och utveckling är ett område som i kostnadsberäkningsmodellen i huvudsak rör aktiviteter kopplade till efterlevnad av informationssäkerhet. Efterlevnaden är den ”tid” som förvaltnings- och utvecklingsroller som; informationsägare, objektsägare, produktägare, förvaltningsledare, projektledare eller specialister spenderar på aktiviteter som; informationsklassning, riskanalyser, möten, framtaganden av beslutsunderlag och beslut i sitt respektive förvaltningsobjekt, produkt, informationsobjekt eller motsvarande indelningsgrund. Det finns även en del som rör förvaltning och utvecklings deltagande i uppföljning av policy/riktlinjer, ramverk och processer.

Tid (antal timmar) nedlagt på efterlevnad;

- Informationsklassning
- Riskanalys
- Möten
- Beslutsunderlag samt beslut



Beräkningsmodell för förvaltning och utveckling

Tid (antal timmar) nedlagt på uppföljning av;

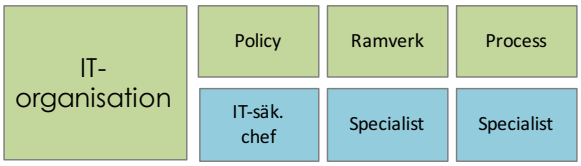
- Policy, ramverk, utbildning samt processer

5.3. IT-ORGANISATION

IT-organisationens arbete med framtagning av policy/riktlinjer, ramverk och processer är en rent konkret en förlängning av verksamhetens arbete, vilken skapar styrning till IT-organisationens eget arbete. Kostnadsberäkningsmodellen beräknad i IT-organisationen kostnaden för ”tid” spenderad på framtagning, efterlevnad och uppföljning av; policy/riktlinjer, ramverk och processer inom IT-verksamheten. ”Tid” och därmed kostnaden beräknas på befattningar och roller inom IT-organisationen vilka är involverade i arbetet med informationssäkerhet, dessa är; IT-chef, IT-säkerhetschef, arkiteketer, tjänsteägare etc. I IT-organisationens efterlevnadsdel beräknas, precis som i verksamhetens fall, ”tid” nedlagd på; inventering, riskanalys, klassning och utbildning dock med skillnaden att det i IT-organisationens fall handlar om de tekniska aspekterna av informationssäkerhet. Även deltaganden i möten, framtagande av beslutsunderlag samt beslutsfattande rörande informationssäkerhet tas med. IT-avdelningen har ett tillägg i form av heltidsekvivalenter (förkortat HTE), det vill säga heltidsanställda resurser som specifikt arbetar med IT-säkerhetsfrågor. Dessa resurser agerar både strategiskt och opertivt och utmaningen i kostnadsberäkningsmodellen är att hitta, kategorisera och beräkna de timmar dessa resurser specifikt lägger på informationssäkerhet, det vill säga deras proaktiva och strategiska bidrag till att säkra verksamhetens information.

Tid (antal timmar) nedlagt på framtagande av;

- Policy/riktlinjer
- Ramverk
- Processer (anpassning)
- Utbildningar (för personal)



Beräkningsmodell för IT-organisation

Tid (antal timmar) nedlagt på efterlevnad;

- Inventering (system)
- Riskanalys (system)
- Klassning (system)
- Möten, beslutsunderlag samt beslut
- Utbildningar (av personal)

Tid (antal timmar) nedlagt på uppföljning av;

- Policy, ramverk, utbildning samt processer

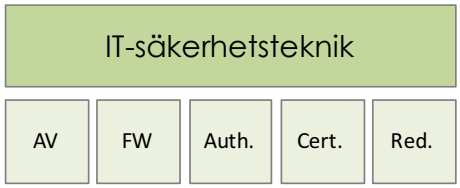
Antal HTE:er inom IT-säkerhetsavdelningen

5.4. IT-SÄKERHETSTEKNIK

Kostnadsberäkningsmodellen utgår i IT-säkerhetsteknik från de löpande kostnader som kan förknippas med ”teknik” som anskaffats i syfte att säkra verksamhetens information genom olika tekniska lösningar.

Kostnader för teknik relaterad till informationssäkerhet:

- Anti-virus
- Firewall
- Authentication
- Certificate
- Redundancy
- Etc.



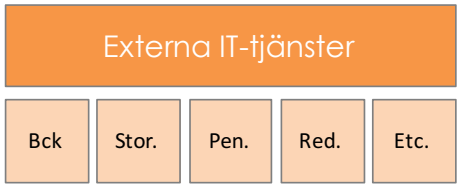
Beräkningsmodell för teknik

5.5. EXTERNA IT-TJÄNSTER

Externa IT-tjänster är de kostnader som kan härledas till tjänster anskaffade i syfte att säkra verksamhetens information. I kostnadsberäkningsmodellen beräknas löpnade kostnader för till exempel; back-up, storage, penetrationstester etc.

Kostnader för IT-tjänster relaterad till informationssäkerhet:

- Back-up
- Storage
- Penetrationstester
- Redundancy
- Etc.



Beräkningsmodell för tjänster

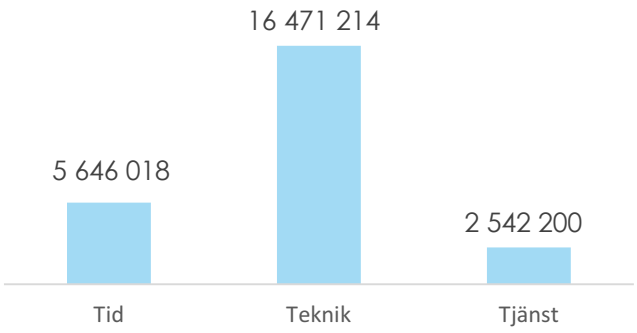
6. MYNDIGHETERS INFORMATIONSSÄKERHETSKOSTNADER

Statliga myndigheter och verks genomsnittliga kostnad för proaktiv informationssäkerhet uppgår till 24 659 431 kronor per verksamhet och år vilket motsvarar 16 367 kronor per syselsatt och år. Skillnaderna mellan undersökta myndigheter och verk är dock stor. Detta beror på deras skilda uppdrag och storlekar, vilket innebär att de genomsnittliga kostnaderna för proaktiv informationssäkerhet bör snarare betraktas som en orientering än en exakt jämförelsebas. I Radars undersökande runt kostnader för proaktiv informationssäkerhet framkommer att myndigheter i genomsnitt spenderar från 13 809 kronor och upp till 29 159 kronor per sysselsatt och år. Att hamna utanför, eller i närheten av, dessa ändpunkter på intervallet innebär sannolikt en stor risk. En risk att å ena sidan prioritera informationssäkerhet för lågt och å andra sidan antingen att verksamheten innebär en stor risk eller att informationssäkerhetsinvesteringarna är större än vad verksamheten kan ta till sig (ineffektivt).

6.1. TOTALKOSTNAD FÖR INFORMATIONSSÄKERHET

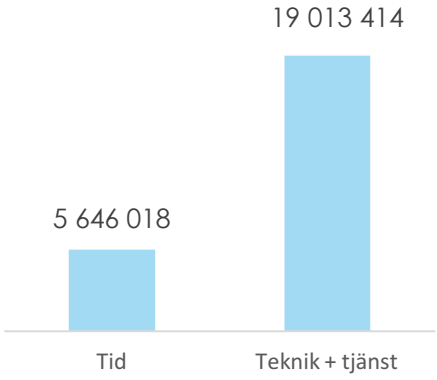
I genomsnitt kostar informationssäkerhet hos de undersökta myndigheterna och verken 24 659 431 kronor per verksamhet och år. Undersökningen visar att teknik står för högst andel, relativt tid och tjänst, avseende totalkostnad för informationssäkerhet. Teknik står för 66,8 procent av totalkostnaden för informationssäkerhet, i genomsnitt 16 471 214 kronor per verksamhet och år. Tid står för den näst största delen med 22,9 procent av totalkostnaden med en genomsnittkostnad på 5 646 018 kronor per verksamhet och år medan tjänster står för 10,3 procent av totalkostnaden med en genomsnittskostnad om 2 542 200 kronor per verksamhet och år. Sammanlagt står teknik och tjänst för mer än tre fjärdedelar av kostnaderna för informationssäkerhet.

Kostnader för informationssäkerhet 2015



Källa: Radar 2016

Tid vs teknik och tjänst



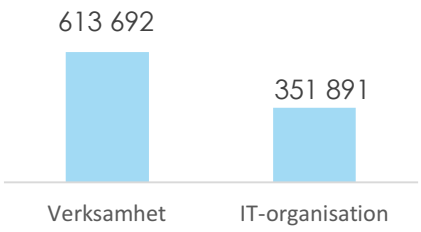
Källa: Radar 2016

De 16 367 kronor som statliga myndigheter och verk spenderar per sysselsatt och år på proaktiv informationssäkerhet fördelas enligt nedan:

- Verksamheten: 897 kronor
- Förvaltning och utveckling: 597 kronor
- IT-organisationen: 2 254 kronor
- IT-säkerhetsteknik: 10 932 kronor
- Externa IT-tjänster: 1 687 kronor

Strategisk tid (framtagande, uppföljning och utbildning) kostar i genomsnitt 965 583 kronor per år för statliga mydigheter och verk vilket motsvarar 214 kronor per sysselsatt och år. Vid en närmare granskning av kostnaderna för den strategiska tiden framgår det tydligt att verksamheten i större utsträckning än IT-organisationen spenderar tid på att ta fram policys/riktlinjer, ramverk och processer för informationssäkerhet. Verksamheterna spenderar i genomsnitt 613 692 kronor på att styra området informationssäkerhet medan IT-organisationen motsvarande del uppgår till 351 891 kronor vilket indikerar att styrningen av informationssäkerhet skapar styrning till IT-organisationen.

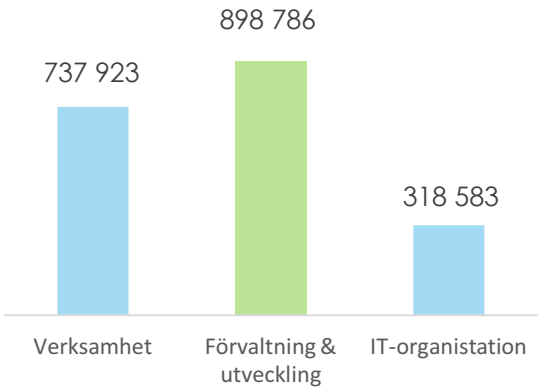
Strategiska kostnader 2015



Källa: Radar 2016

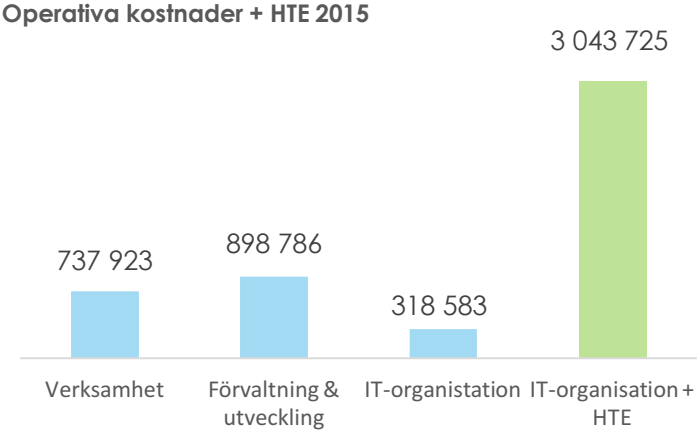
Operativ tid (inventering, riskbedömning, klassning, möten etc), det vill säga tid spenderad på efterlevnad, kostar i genomsnitt 1 955 293 kronor per år och verksamhet eller 433 kronor per sysselsatt och år. Vid en närmare granskning av *operativ tid*, det vill säga efterlevnad av informationssäkerhet, visar det sig att det spenderas mest tid på informationssäkerhet i förvaltning och utveckling, i genomsnitt 898 786 kronor per verksamhet och år. Detta ska jämföras med verksamheten som spenderar 737 923 kronor per och år och IT-organisationens 318 583 kronor per år. IT-organisationens spenderade tid är antagligen lågt räknat då det är svårt för responderande myndigheters IT-organisationer att särskilja på tid de lagt specifikt på informationssäkerhet då detta allt som oftast är invävt i annat arbete. Inräknat heltidsekvivalenter (HTE) vilka arbetar med IT-säkerhetsteknik blir bilden annorlunda, då spenderar IT-organisationen mest ”tid” på att efterleva informationssäkerhet med en genomsnittlig kostnad på 3 043 725 kronor per verksamhet och år. Räknar man in HTE i den operativa tiden spenderar statliga myndigheter och verk 4 680 434 kronor per år och verksamhet eller 1 035 kronor per sysselsatt och år på efterlevnad av informationssäkerhet.

Operativa kostnader 2015



Källa: Radar 2016

Operativa kostnader + HTE 2015



Källa: Radar 2016

6.2. KOSTNADER INOM VERKSAMHETEN

Kostnaderna för proaktiv informationssäkerhet inom verksamheterna mäts i tid spenderad på framtagning, efterlevnad och uppföljning av informationssäkerhet. Det skiljer sig, inte oväntat, mellan olika myndigheter och verk i hur mycket tid som spenderats på framtagning, efterlevnad och uppföljning av; policy/riktlinjer, ramverk samt processer för proaktiv informationssäkerhet. Detta kan förklaras med att de undersökta myndigheterna och verken befinner sig olika faser avseende införande och/eller revision av befintliga policys/riktlinjer, ramverk och processer samt i hur stor utsträckning man arbetar med efterlevnaden rörande informationssäkerhet i själva verksamheten. I genomsnitt spenderar verksamheterna 1 351 616 kronor per år och verksamhet på informationssäkerhet vilket motsvarar 897 kronor per sysselsatt och år.

De 897 kronor per sysselsatt och år som myndigheter och verks verksamhet spenderar på proaktiv informationssäkerhet fördelas enligt nedan:

407 kronor spenderas på ”strategisk tid”, det vill säga framtagning, uppföljning och utbildning:

- Policy/riktlinjer: 66 kronor
- Ramverk: 105 kronor
- Processer: 91 kronor
- Utbildningar: 146 kronor

490 kronor spenderas på ”operativ tid”, det vill säga efterlevnad:

- Inventering: 90 kronor
- Riskbedömning: 104 kronor
- Klassning: 105 kronor
- Möten, beslutsunderlag etcetera: 191 kronor

Efterlevnaden är den del som kostar mest i verksamheten med i snitt 490 kronor per sysselsatt och år och inkluderar informationssäkerhetsaktiviteter som: inventering, riskbedömning, klassning etc. Arbetet med efterlevnad är invävt i befintliga processer och respondenterna har svårt att redogöra för den tid som läggs specifikt på informationssäkerhet. Det som kostar mest i efterlevanden är möten och framtagning av beslutsunderlag. Det blir viktigt för verksamheterna att undersöka hur effektivt möten eller beslutsunderlag hanteras relativt styrningen, det vill säga: kostar möten och beslutsunderlag mest för att det finns oklarheter i hur involverade individer ser på informationssäkerhet? Vidare anges att det är svårt att involvera verksamhetsledningarna i att aktivt arbeta med informationssäkerhet både i framtagande och uppföljning (strategisk tid) samt i efterlevnad (operativ tid). Detta bekräftar den tidigare utmaningen IT-beslutsfattarna upplever, den att verksamheterna har svårt att förstå behovet av IT-säkerhetsinvesteringar utan synbar nytta. Nyttan av informationssäkerhet uppstår och konkretiseras om myndigheter och verk korrelerar arbetet med incidenter, då går det att jämställa informationssäkerhetarbete med försäkringar. Vid undersökning av den strategiska tiden visar det sig att utbildning är det som det spenderas mest tid på. Den genomsnittliga andelen för utbildning i verksamheten uppgår i dagsläget till 0,9 procent av totalkostnaden för informationssäkerhet. Intervjuerna visade att responderande myndigheter står i begrepp att satsa ytterligare på utbildning inför 2016 i syfte att höja kunskapen i verksamheten för att på så sätt och möta den av statliga myndigheter och verks näst viktigaste prioritering och utmaning, nämligen säkerhetsmedvetenhet. Det faktum att IT-organisationer som oftast mäts på driftsstabilitet (färre incidenter) innebär att tid lagd på incidenter behöver kopplas mot den tid som spenderas på utbildning och över tid bör utbildning resultera i färre antal incidenter[1]. Sammantaget visar intervjuerna att informationssäkerhet fortfarande är i en mognadsfas inom verksamheten men genom utbildningssatsningar finns en tydlig intention att ytterligare förbättra och utveckla området.

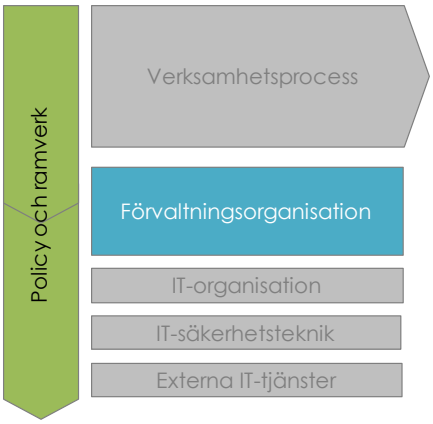
[1] Källa: IT Radar 2016

6.3. KOSTNADER INOM FÖRVALTNING OCH UTVECKLING

Statliga myndigheter och verk i genomsnitt spenderar i genomsnitt 898 786 kronor per verksamhet och år på proaktiv informationssäkerhet i förvaltning och utveckling vilket motsvarar 597 kronor per sysselsatt och år. Som tidigare nämnts är förvaltning och utveckling det område som sammanlagt spenderar mest tid på efterlevnad av informationssäkerhet och slår både verksamheten och IT-organisationen på alla områden; inventering, riskbedöming, klassning och möten. Säkerhetarbetet inom förvaltning och utveckling ser dock olika ut hos hos de undersökta myndigheterna och verken. Den myndighet som spenderade minst på informationssäkerhet i förvaltning och utveckling spenderade 50 kronor per sysselsatt och år och upp till 1 092 kronor per sysselsatt och år på informationssäkerhet.

De 597 kronor per sysselsatt och år som myndigheter och verks förvaltning och utveckling spenderar på proaktiv informationssäkerhet fördelas enligt nedan:

- Inventering: 104 kronor
- Riskbedömning: 149 kronor
- Klassning: 122 kronor
- Möten, beslutsunderlag etcetera: 221 kronor



Intervjuerna visar att finns det stora skillnader hur informationssäkerhet hanteras hos de responderande myndigheter. I en responderande myndighet hanteras i princip ingen efterlevnad av informationssäkerhet i förvaltning och utveckling bortsett från enstaka PEN-tester vid utveckling av system. En annan responderande myndighet har byggt upp ett kontinuerligt arbete med att inventera, riskbedöma och klassa information i sin förvaltning och utveckling. Att det skiljer sig så mycket mellan hur de undersökta myndigheterna och verken hanterar informationssäkerhet indikerar att förvaltning och utveckling befinner sig i en mognadsfas avseende proaktiv informationssäkerhet. Det som kostar mest i efterlevanden inom förvaltning och utveckling är möten och framtagning av beslutsunderlag som uppgår till 221 kronor per sysselsatt och år. Kostar möten och beslutsunderlag mest för att det finns oklarheter i hur involverade individer ser på informationssäkerhet eller att befintliga ramverk, modeller och metoder inte i tillräckligt hög grad tar hänsyn till informationssäkerhet? Förvaltning och utveckling som till största del är funktionsdrivet (fokus på att leverara modiferad och/eller ny funktionalitet) måste säkerställa att policys/riktlinjer efterlevs för att arbetet med informationssäkerhet i stort ska hanteras effektivt, det vill säga ta in ”garanti” i sin strävan att skapa värde. Informationssäkerhet faller in under ”garanti” i ramverket ITIL och nyttan med IT skall innehålla både ”funktion” och ”garanti”. Ramverk, förvaltningsmodeller och utvecklingsmetoder inom förvaltning och utveckling bör utvecklas och integreras, i de fall de inte redan är det, i arbetet med att återkoppla både till både verksamhet och IT-organisation hur policys/riktlinjer, ramverk och processer fungerar i det dagliga arbetet. Detta för att efterarbete med att korrigera eventuella brister eller uppkomna incidenter förmodligen blir både tidskrävande och därmed kostsamt.

6.4. KOSTNADER INOM IT-ORGANISATION

Kostnaderna för informationssäkerhet inom IT-organisationen, precis som för verksamheten, mäts i ”tid” spenderad på framtagning, efterlevnad och uppföljning av informationssäkerhet. I genomsnitt spenderar IT-organisationen 3 395 616 kronor per år och verksamhet på informationssäkerhet vilket motsvarar 2 254 kronor per sysselsatt och år. IT-organisationerna spenderar minst tid på strategiska och renodlade informationssäkerhetsaktiviter. Den genomsnittliga kostanden för strategiska aktiviteter uppgår till 234 kronor per sysselsatt och år och efterlevnaden uppgår till 211 kronor per sysselsatt och år. Det är först när man lägger till antal heltidsanställda resurser som den verkliga tiden framkommer, här spenderar statliga myndigheter och verk i genomsnitt 1 809 kronor per sysselsatt och år. Samtliga undersökta myndigheter och verk har svårt att särskilja och estimera tid som spenderas på informationssäkerhet. Den IT-organisation som spenderar mest på *strategisk tid* lägger motsvarande 354 kronor per sysselsatt och år och den som spenderar minst lägger 55 kronor per sysselsatt och år.

De 2 254 kronor per sysselsatt och år som myndigheter och verks IT-organisationer spenderar på proaktiv informationssäkerhet fördelas enligt nedan:

234 kronor spenderas på ”strategisk tid”, det vill säga framtagning och uppföljning:

- Policy/riktlinjer: 39 kronor
- Ramverk: 47 kronor
- Processer: 82 kronor
- Utbildningar: 66 kronor

211 kronor spenderas på ”operativ tid”, det vill säga efterlevnad:

- Inventering: 2 kronor
- Riskbedömning: 4 kronor
- Klassning: 93 kronor
- Möten, beslutsunderlag etcetera: 113 kronor

1 809 kronor spenderas på personal som arbetar i direkt anslutning till IT-säkerhetsteknik.

Djupintervjuerna bekräftar den tidigare indikationen att IT-organisationen styrs av verksamheten avseende informationssäkerhet. Det vill säga att intervjuade IT-beslutsfattare är direkt involverade i arbetet med framtagning av policys/riktlinjer, ramverk och processer för informationssäkerhet i samverkan med verksamheten. Dock anger två myndigheter att det idag inte pågår strukturerade initiativ för att integrera informationssäkerhet i befintliga processer för att producera och leverera IT men att detta ska ses över. Som tidigare nämnts faller informationssäkerhet in under ”garanti” i ramverket ITIL där det också anges att värdet med IT skall innehålla både ”funktion” och ”garanti”. IT-organisationerna behöver bättre konkretisera hur informationssäkerhetsprocesser kopplas samman med befintliga IT-ramverk och modeller, inte för att redogöra för spenderad ”tid”, utan för att säkra att hanteringen av teknik och tjänst uppfyller verksamhetens krav på informationssäkerhet i stort för att undvika ”styrningsglapp” och därmed ta onödiga verksamhetsrisker.

6.5. KOSTNADER FÖR TEKNIK

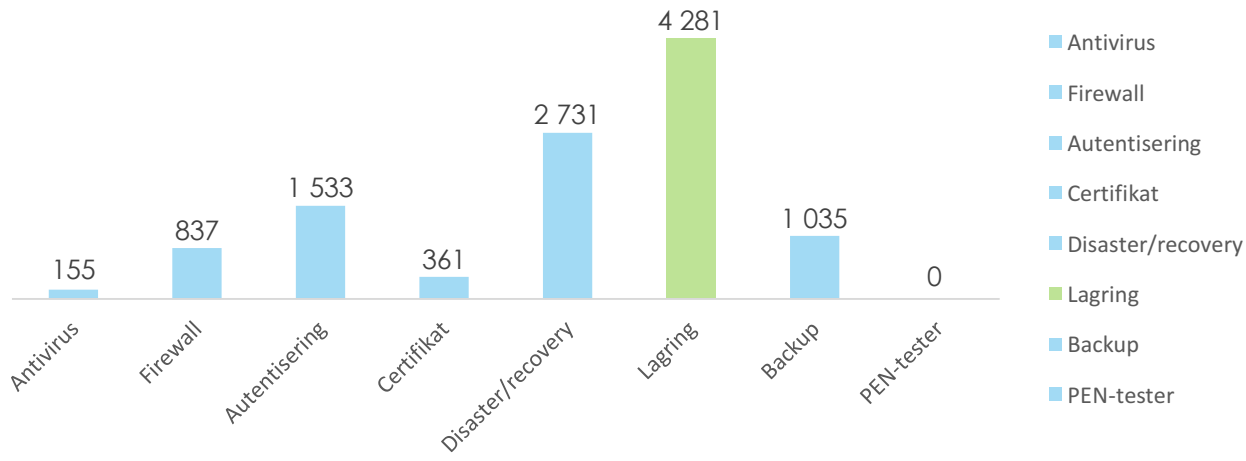
Som tidigare nämnts har statliga myndigheter och verk en större andel av sin IT-produktion i egen regi och en lägre andel standardprodukter i sin IT-portfölj jämfört med kommuner eller verksamheter i privat sektor. Det beror delvis på att myndigheternas individuella uppdrag och verksamhet till stor del är särpräglade eller unika, vilket kan göra det svårare att hitta lämpliga lösningar ”på marknaden”. Det återspeglas även inom teknik anskaffad för informationssäkerhet så tillvida att en större andel av infrastrukturen som; firewall, antivirus, lagring, backup etcetera produceras i egen regi. Den teknik som anskaffats för att skydda statliga myndigheter och verks information uppgår till i genomsnitt 10 932 kronor per verksamhet och år.

De 10 932 kronor per sysselsatt och år som statliga myndigheter och verk spenderar på IT-säkerhetsteknik fördelas enligt nedan:

- Antivirus: 155 kronor
- Firewall: 837 kronor
- Autentisering: 1 533 kronor
- Certifikat: 361 kronor
- Disaster/recovery: 2 731 kronor
- Lagring: 4 281 kronor
- Backup: 1 035 kronor

Undersökningen, av teknik anskaffad i syfte att understödja informationssäkerhet, visar att lagring är det område som myndigheter och verk spenderar mest pengar på med en kostnad på 4 281 kronor per sysselsatt och år.
I tidigare research[2] anges att IT-beslutsfattare anser att den ständigt ökande informationsmängden är en utmaning att hantera både kostnadsmässigt (för tekniken) men även med att de ska hinna med att klassificera nytillkommen information. Det näst kostsammaste området efter lagring är disaster recovery, vilket är det område som har störst osäkerhet då det uppleavs svårt att bryta och presentera kostnaderna för området, med en kostnad på 2 731 kronor per sysselsatt och år.

Kostnader för teknik 2015



Källa: Radar 2016

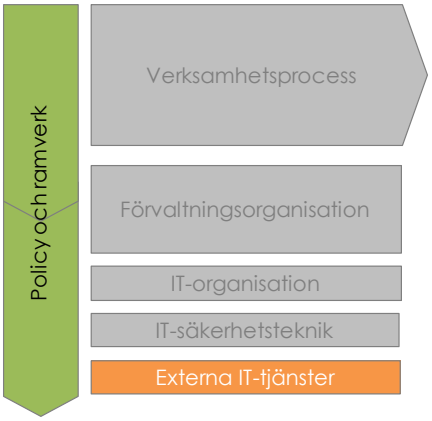
[2] Att säkerställa individen

6.6. KOSTNADER FÖR EXTERNA TJÄNSTER

Även om statliga myndigheter och verk i större utsträckning producerar IT i egen regi så outsourcas delar av infrastruktur för informationssäkerhet. Externa tjänster som anskaffats för att skydda statliga myndigheter och verks information uppgår till i genomsnitt 1 687 kronor per verksamhet och år. Den som spenderar mest på externa tjänster spenderar 3 318 kronor per sysselsatt och år och den som spenderar minst ligger på 400 kronor per sysselsatt och år.

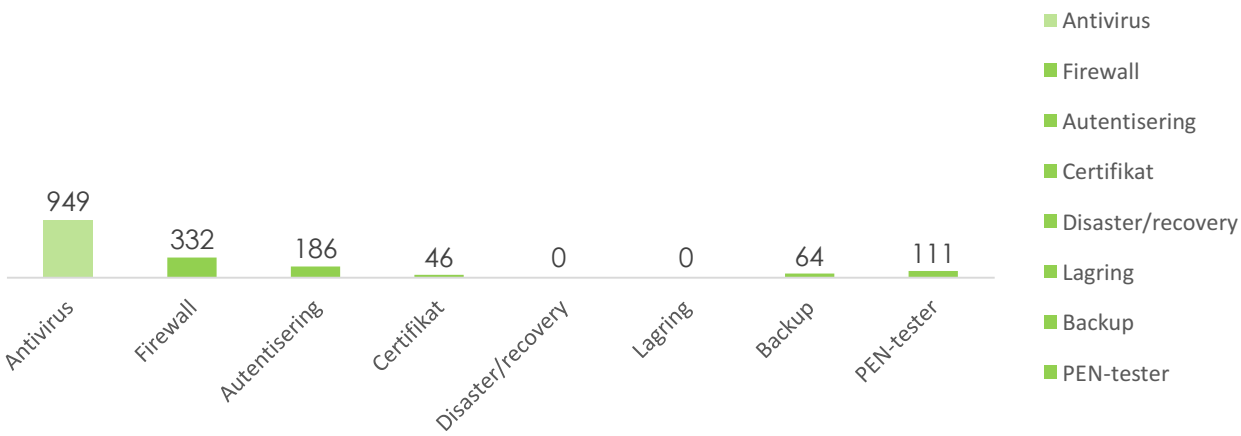
De 1 687 kronor per sysselsatt och år som statliga myndigheter och verk spenderar på externa IT-tjänster fördelas enligt nedan:

- Antivirus: 949 kronor
- Firewall: 332 kronor
- Autentisering: 186 kronor
- Certifikat: 46 kronor
- Disaster/recovery: -
- Lagring: -
- Backup: 64 kronor
- PEN-tester: 111 kronor



Undersökningen av visar att antivirus är det område som myndigheter och verk spenderar mest pengar på med en kostnad på 949 kronor per sysselsatt och år. Det näst dyraste området är Firewall med en kostnad på 332 kronor per sysselsatt och år. Det är inte ovanligt att det finns heltidsanställda resurser inom verksamheten som agerar både strategiskt och operativt med bland annat förvaltningen av bland annat Firewalls även om funktionen outsourcats. Detta kräver att ansvarsfrågan, när det kommer till efterlevnaden av informationssäkerhet, är utredd. Detta gäller framförallt hanteringen av incidenter.

Kostnader för externa tjänster 2015



Källa: Radar 2016

7. DATA OCH DEFINITIONER

Autentisering
Kontroll av uppgiven identitet, till exempel vid inloggning, vid kommunikation mellan två system eller vid utväxling av meddelande mellan användare.

Administrativ säkerhet
I den administrativa säkerheten inkluderas att upprätta styrdokument, utforma rutiner, övervaka efterlevnad samt genomföra uppföljningar, det vill säga arbete med framtagning, efterlevnad och uppföljning av; policy/riktlinjer, ramverk och processer.

Behörighet
Behörighet är i grunden samma sak som rättighet och avser den hierarki av rättigheter i ett datorsystem som är knutna till arbetsuppgifter och befattningar. Behörighet är knuten till autentisering.
IT-kostnader

IT-budget
Avser hela den summa pengar en verksamhet definierar som sin IT-budget och inbegriper således såväl interna- som externa kostnader. IT-budgeten omfattar dock bara en del av ”totala IT-kostnader”, då IT även kan finansieras via en annan budget.

IT-säkerhet
IT-relaterade tekniska säkerhetsåtgärder för att upprätthålla informationssäkerhet. IT-säkerhet omfattar områdena datasäkerhet och kommunikationssäkerhet såsom; skydd mot skadlig kod (antivirus etc.), brandväggar, autentiseringslösningar etc.

Informationssäkerhet
Informationssäkerhet ses som en uppsättning säkerhetsåtgärder för bevarande av egenskaper som hos information konfidentialitet, riktighet och tillgänglighet men även spårbarhet, autenticitet, ansvarsskyldighet, oavvislighet och auktorisation. Informationssäkerhet omfattar områdena administrativ säkerhet och teknisk säkerhet.

Proaktiv informationssäkerhet
Proaktiv informationssäkerhet avser kostnaderna för; *administrativ säkerhet* plus *IT-säkerhet* dock ej hanteringen av incidenter som katgoriseras som *reaktiv informationssäkerhet*.

Reaktiv informationssäkerhet
Reaktiv informationssäkerhet avser kostnaderna för hanteringen av incidenter.

Teknisk säkerhet
Tekniska säkerhetsåtgärder för att upprätthålla informationens konfidentialitet, riktighet och tillgänglighet.

Tillgänglighet
Åtkomst för behörig person vid rätt tillfälle.

Valuta
Samtliga monetära värden i denna rapport är angivna med svenska kronor (SEK) som valuta, i det fall inget annat särskilt anges.

Verksamhet	**5%**	**Strategisk tid**	**407 SEK**	**45%**
		Policy	66 SEK	16%
		Ramverk	105 SEK	26%
		Processer	91 SEK	22%
		Utbildning	146 SEK	36%
		Operativ (efterlevnad)	**490 SEK**	**55%**
		Inventering	90 SEK	18%
		Risk	104 SEK	21%
		Klassning	105 SEK	21%
		Möten	191 SEK	39%
Förvaltning och utveckling	**4%**	**Proaktiv informationssäkerhet**	**597 SEK**	**100%**
		Inventering	104 SEK	17%
		Risk	149 SEK	25%
		Klassning	122 SEK	20%
		Möten	221 SEK	37%
IT-organisation	**14%**	**Strategisk tid**	**234 SEK**	**10%**
		Policy	39 SEK	17%
		Ramverk	47 SEK	20%
		Processer	82 SEK	35%
		Utbildning	66 SEK	28%
		Operativ (efterlevnad)	**211 SEK**	**9%**
		Inventering	2 SEK	1%
		Risk	4 SEK	2%
		Klassning	93 SEK	44%
		Möten	113 SEK	53%
		Personal (HTE)	**1 809 SEK**	**80%**
Teknik	**67%**	Antivirus	155 SEK	1%
		Firewall	837 SEK	8%
		Autentisering	1 533 SEK	14%
		Certifikat	361 SEK	3%
		Disaster recovery	2 731 SEK	25%
		Lagring	4 281 SEK	39%
		Backup	1 035 SEK	9%
		Logg	0 SEK	0%
Externa tjänster	**10%**	Antivirus	949 SEK	56%
		Firewall	332 SEK	20%
		Autentisering	186 SEK	11%
		Certifikat	46 SEK	3%
		Disaster recovery	0 SEK	0%
		Lagring	0 SEK	0%
		Backup	64 SEK	4%
		Logg	0 SEK	0%
		PEN-tester	111 SEK	7%

OM RADAR

Radar Ecosystem Specialists är Nordens ledande leverantör av lokal faktabaserad insikt för aktörer i IT-branschens ekosystem. Genom att kunna följa en krona genom ekosystemet erbjuder Radar en unik detaljnivå för såväl IT-verksamhet som IT-leverantör på den lokala marknaden.
Med tusentals datapunkter i ekosystemet, samt närhet och kunskap om den lokala marknaden, levererar Radar ett värdeskapande som är ledande på såväl operativ som strategisk nivå. Våra insikter och tjänster skapar möjligheten att ständigt styra med aktuell information om nuläge, planer och prioriteringar.

Kontakta oss för mer information!

radar. ECOSYSTEM SPECIALISTS
Telefon: +46 8 12 20 80 00
Adress: Hammarby Allé 47, Stockholm
Hemsida: www.radareco.se