Bilaga 5.
Enkät till Affärsverket svenska kraftnät, Bolagsverket, Lantmäteriet, Post- och telestyrelsen, Sjöfartsverket samt Statens tjänstepensionsverk

RiR 2016:8

Informationssäker-hetsarbete på nio myndigheter

En andra granskning av informationssäkerhet i staten

Enkätundersökning

Denna enkätundersökning är ställd till sex myndigheter som var föremål för Riksrevisionens granskningar av informationssäkerhet åren 2005–2007: Bolagsverket, Lantmäteriet, Post- och telestyrelsen, Sjöfartsverket, Statens tjänstepensionsverk samt Svenska kraftnät. Rapporterna från granskningarna framgår av avdelning D nedan.

Enkätundersökningen består av en allmän del, avdelning A, där samtliga sex myndigheter ska besvara frågorna. I avdelning B och C återfinns särskilda frågor till Sjöfartsverket och Statens tjänstepensionsverk. Avdelning D innehåller korta sammanfattningar av respektive granskning.

Vänligen svara på dessa frågor i en Word-fil, skriv ut på papper och skicka till oss med vanlig postgång. Vi ser fram emot era svar senast den ***27 november 2015***. Adressera svaret till:

Riksrevisionen
Att. Johan Ågren
114 90 Stockholm

Observera: innan ni skickar svaren till Riksrevisionen, vänligen bedöm om det finns uppgifter i svaren som innehåller sekretess eller är känsligt på annat sätt. Kontakta oss i så fall, så att vi kan lösa detta på bästa praktiska sätt.
Vid frågor, hör gärna av er till Johan Ågren (0734-45 20 53, johan.agren@riksrevisionen.se) eller Per Dackenberg (0734-45 22 72, per.dackenberg@riksrevisionen.se).

A. Frågor som ska besvaras av samtliga sex myndigheter

Allmänt om ert ledningssystem för informationssäkerhet.

1. Finns en aktuell policy för informationssäkerhet som omfattar hur säkerhetskrav och säkerhetsåtgärder bidrar till att målen för verksamheten uppfylls
2. Om ni har upprättat en policy för informationssäkerhet som beskrivs ovan, bedömer ni att den efterlevs i praktiken?
3. Om ni bedömer att efterlevnaden av ovanstående policy är god, vilket underlag finns då för den bedömningen?
4. Har ni även upprättat andra styrande dokument som behövs för er myndighets informationssäkerhet?

5. Om ni har upprättat andra styrande dokument, som i frågan ovan, ange i så fall vilka?
6. Finns det en dokumenterad process för att förvalta och utveckla ledningssystemet?
7. Har ni utsett en eller flera personer som leder och samordnar arbetet med informationssäkerheten?
8. Följs ledningssystemet upp systematiskt och regelbundet (alltså inte ad hoc), så att det säkerställs att beslutade åtgärder har genomförts?
9. Dokumenterar ni granskningar och säkerhetsåtgärder av större betydelse som har vidtagits när det gäller informationssäkerhet.
10. Tillämpar ni fullt ut följande standarder i ert informationssäkerhetsarbete?
    a. Krav på ledningssystem för informationssäkerhet enligt SS-ISO/IEC 27001
    b. Riktlinjer för styrning av informationssäkerhet enligt SS-ISO/IEC 27002
11. Om ni inte tillämpar ovanstående standarder fullt ut, vilka begränsningar har ni gjort och av vilken orsak?

Ansvar, roller och kompetens

12. Har myndighetsledningen utsett en eller flera personer att leda och samordna arbetet med informationssäkerhet (roller)?
13. Är respektive roll likalydande beskriven oberoende av var i organisationen den finns?
14. Finns det en tydligt utpekad person eller befattning som ansvarar för att följa upp säkerhetsåtgärder?
15. Har ni säkerställt att nyckelpersoner för informationssäkerheten får tillräcklig och återkommande utbildning inom området?
16. Utbildas övrig personal i frågor som rör informationssäkerhet?
    a. Omfattas all personal av denna utbildning?
    b. Om inte, vilka omfattas?
    c. När och hur ofta äger denna utbildning rum?

Riskanalys

17. Genomförs en systematisk riskanalys inom informationssäkerhetsområdet?
18. Om det genomförs en sådan systematisk riskanalys:
    a. Hur ofta äger denna analys rum?

b. Omfattar analysen hela myndighetens verksamhet?

c. Tar analysen hänsyn till:

   i. Konfidentialitet?

   ii. Riktighet?

   iii. Tillgänglighet?

   iv. Spårbarhet

d. Vilket regelverk ligger till grund för analysen?

   i. LIS, det vill säga MSB:s föreskrifter (2009:10) om ledningssystem för informationssäkerhet.

   ii. FISK, det vill säga förordningen (2007:603) om intern styrning och kontroll.

   iii. 9 § förordningen (2006:942) om krisberedskap och höjd beredskap, det vill säga risk- och sårbarhetsanalyser (RSA).

   iv. Förordningen (1995:1300) om statliga myndigheters riskhantering.

   v. Annat regelverk eller inget regelverk.

e. Beskriv processen och hur den följs upp eller utvärderas.

19. Har er myndighetsledning, ur ett informationssäkerhetsperspektiv, tagit ställning till:

    a. vilka risker ni är beredda att ta?

    b. vilka risker som ska minskas?

    c. vilka risker som kan undvikas?

    d. vilka risker som ska få kvarstå?

20. Finns ovanstående ställningstaganden dokumenterade?

Informationsklassning

21. Har ni en metod eller modell för att klassificera myndighetens information?

22. Finns det en samlad förteckning över myndighetens samtliga skyddsvärda informationstillgångar?

23. Om det finns en samlad förteckning över myndighetens samtliga skyddsvärda informationstillgångar, som i frågan ovan:

a. Är samtliga informationstillgångar klassificerade efter en bedömning av vilken skyddsnivå som är lämpligt sett till värdet av informationen och de hot som omger den?

b. Framgår av förteckningen av informationstillgångar:

i. Skyddskrav?

ii. Vidtagna skyddsåtgärder?

iii. Vem som ansvarar för (äger) respektive informationstillgång?

iv. Beroendeförhållanden mellan informationstillgångarna?

Incidentrapportering

24. Finns det en incidentrapportering som bedrivs systematiskt?
25. Sammanställs erfarenheter från incidenter?
26. Återförs erfarenheter från incidenter till dem som är berörda?
27. Beskriv incidentorganisationen och rutinerna för att hantera incidenter.

Planer m.m.

28. Finns det en övergripande plan för informationssäkerheten?
29. Om det finns en sådan plan som i frågan ovan, omfattar den följande:
    a. Alla beslutade nya skyddsåtgärder?
    b. Vilka som ansvarar för att genomföra skyddsåtgärderna, att de fungerar korrekt och när de ska vara genomförda?
30. Finns det en kontinuitetsplan?

Om det finns en kontinuitetsplan,

a. hur ofta brukar den övas?

b. när övades den senast?

31. Om det finns en kontinuitetsplan som i frågan ovan, täcker den samtlig verksamhet?
32. Om en kontinuitetsplan inte täcker samtlig verksamhet, uppskatta på ett ungefär hur stor del den täcker av verksamheten?
33. Finns en samlad och uppföljningsbar plan över nya säkerhetsåtgärder (åtgärdsplan), som gör det möjligt för myndighetsledningen informeras om vilka beslutade åtgärder som genomförts och kontrollerats.

Lägesbild

34. Finns det på er myndighet en samlad lägesbild över informationssäkerheten som omfattar risker, skyddsåtgärder och händelser?
35. Om det finns en sådan samlad lägesbild, som i frågan ovan, är den kommunicerad med myndighetens högsta ledning?

IT-säkerhet

36. Finns det dokumenterade regler för hantering av fjärranslutning till myndighetens IT-miljö?
37. Finns det dokumenterade regler för behörigheter?

B. Specifika frågor till Sjöfartsverket

1. Finns det i dag någon dokumenterad rutin för att rapportera problem, möjligheter och åtgärdsbehov till verksledning, IT-råd och avdelningschefer när det gäller informationssäkerheten?
2. Om det finns en rutin enligt ovan: följs den, eller finns det brister i dess efterlevnad?

C. Specifik fråga till Statens tjänstepensionsverk

Finns det i dag en etablerad samverkan när det gäller informationssäkerhetsarbetet mellan enhetschefer, säkerhetschef, säkerhetsskyddschef (om sådan finns separerad från föregående befattning), IT-chef, chefsjurist, systemägare, informationsägare och informationssäkerhetssamordnare? När vi säger etablerad samverkan menar vi att den både ska vara dokumenterad och fungera väl.

D. Riksrevisionens granskning av de sex myndigheterna

Bolagsverket

Bolagsverkets informationssäkerhet (RiR revisionsrapport 2005-08-19, dnr 32-2005-0717)

Sammanfattning av granskningen[1]

Avsaknaden av en övergripande styrande policy, såsom en informationssäkerhetspolicy, innebär att ledningen inte kommunicerat sin helhetssyn avseende vikten av informationssäkerhet. Detta innebär bland annat att det inte finns några krav avseende

[1] Citat från revisionsrapporten, s. 7.

kontinuitetsplan, incidentrapportering, virusskydd etc. Det saknas också en fördelning av roll- och ansvar avseende informationssäkerheten.

Bolagsverket har inte genomfört någon riskanalys, vilket är en viktig förutsättning för myndighetens riskhantering. Avsaknaden av en metodisk process för analys av informationssäkerhetsrisker medför svårigheter med att skapa ett fullgott underlag för beslut som avser hanteringen av riskerna.

Vi har även noterat brister i ledningens uppföljnings- och kontrollrutiner, information och utbildning samt förvaltningen av LIS. Detta bedömer vi som en följd av det inte genomförts någon övergripande riskanalys samt avsaknaden av en informationssäkerhetspolicy.

Lantmäteriet

Granskning av Lantmäteriverkets interna styrning och kontroll av informationssäkerheten (RiR 2006:26)

Sammanfattning av granskningen[2]

Har Lantmäteriet ett fungerande system för informationssäkerhet?

Vid Lantmäteriverket finns flera fungerande delar av ett ledningssystem för informationssäkerhet. Vissa delar av ledningssystemet är dock inte tillräckligt väl utvecklade. Granskningen visar att ledningens informationssäkerhetsarbete har tre huvudsakliga brister: ansvarsfördelning är oklar, riskanalysarbetet har inte fullföljts och uppföljningen är inte systematisk. Det saknas t.ex. en tydligt utpekad ansvarig för uppföljning av att beslutade säkerhetsåtgärder införts. Lantmäteriverket har dock under 2006 påbörjat ett arbete som bl.a. syftar till en bättre riskanalys.

Bristerna innebär bl.a. att Lantmäteriverkets ledning inte har tillräckligt stöd eller tillräckliga hjälpmedel för att skapa överblick över, leda och följa upp informationssäkerheten. Bristerna medför att det finns en risk för att informationssäkerheten inte ligger på den nivå som är ledningens avsikt.

Sammantaget innebär bristerna att Lantmäteriverket inte fullt ut arbetar systematiskt med sin informationssäkerhet utifrån gängse normer.

Post- och telestyrelsen

Post- och telestyrelsens informationssäkerhet (RiR revisionsrapport 2006-02-09, dnr 32-2005-0738)

[2] Citat från granskningsrapporten, s. 8.

Sammanfattning av granskningen[3]

Den osäkerhet som tycks råda om status på nuvarande informationssäkerhetspolicy, innebär att ledningen inte till fullo kommunicerat sin helhetssyn avseende vikten av informationssäkerhet. Detta återspeglas även genom att det inte finns några formellt fastställda krav avseende kontinuitetsplanering, rutiner för incidentrapportering, e-postanvändning m.m. vid myndigheten. Det har också saknats en fördelning av roll- och ansvar avseende informationssäkerhetsarbetet. Denna fråga adresseras delvis i en förvaltningsmodell som beslutats i oktober 2005, men denna kan behöva vidareutvecklas ytterligare, beroende på utfallet av nu pågående utredning av myndighetens informationssäkerhet.

PTS har först under hösten och vintern 2005 genomfört en riskanalys och heltäckande informationsklassificering av myndighetens informationstillgångar, vilket är en grundläggande förutsättning för en effektiv riskhantering vid myndigheten. Det är viktigt att nivån och omfattningen av såväl organisatoriska och tekniska kontroller rörande verksamhetens informationstillgångar baseras, dels på ovan nämnda ställningstagande och inriktningsbeslut från ledningen, dels på utfallet av en strukturerad process för riskanalys och informationsklassificering. Detta innebär i praktiken att verksamhetsföreträdare och myndighetsledningen måste ta ansvar för att bedöma vilken nivå av kontroller och informationsskydd som krävs.

Vi har även noterat att ledningens uppföljnings- och kontrollrutiner inte varit tillfredsställande avseende LIS. Vi vill poängtera vikten av att informationssäkerhetsarbetet ses som en kontinuerlig process. Detta innebär bl.a. att det bör finnas en modell för (och resurser avsatta till) kontinuerlig prövning och värdering av myndighetens informationssäkerhetsarbete. Detta dels genom regelbunden omprövning av tidigare riskanalyser, dels genom uppföljande åtgärder för att bedöma om införda kontroller fungerat på avsett sätt. Det bör även finnas en plan för att säkerställa att all personal på lämpligt sätt får tillgång till uppdaterad information om myndighetens övergripande ställningstaganden i informationssäkerhetsfrågor, och inte minst det ansvar som åvilar den enskilde.

Sjöfartsverket

Granskning av Sjöfartsverkets interna styrning och kontroll av informationssäkerheten (RiR 2005:27)

Sammanfattning av granskningen[4]

Har Sjöfartsverket ett fungerande system för informationssäkerhet?

[3] Citat från revisionsrapporten, s. 8–9.
[4] Citat från granskningsrapporten, s. 8.

Både ja och nej. SjöV har flera av de delar som enligt standarden tillsammans utgör ett LIS. Vissa delar av LIS är dock mindre väl utvecklade – funktioner som skapar överblick, rapportering, riskanalys, utbildning samt uppföljning och förvaltning av LIS. Dessa länkar i den kedja som ledningssystemets delar bör bilda saknas eller är för svaga. Dessa brister medför att SjöV:s LIS inte utgör en fullt ut lämpligt utformad och fungerande helhet. Praktiskt innebär bristerna bl.a. att SjöV:s möjligheter att systematiskt upptäcka och lära sig av erfarenheter i informationssäkerhetsarbetet och i användningen av LIS minskar. Det i sin tur minskar möjligheterna att driva ett effektivt förbättringsarbete som syftar till att stegvis förbättra LIS.

Bristerna i LIS påverkar i sin tur möjligheterna att uppnå och vidmakthålla eftersträvad informationssäkerhet. Svaret på den fråga som granskningen syftat till att besvara är därmed att SjöV inte fullt ut arbetar systematiskt med sin informationssäkerhet utifrån gängse normer.

Statens tjänstepensionsverk

Granskning av Statens pensionsverks interna styrning och kontroll av informationssäkerheten (RiR promemoria 31-2004-1295)

Sammanfattning av granskningen[5]

Har Statens tjänstepensionsverk ett fungerande system för informationssäkerhet?

Både ja och nej. Vår bedömning är att de områden som SPV behöver arbeta med och utveckla är sådana som ofta är problematiska i säkerhetsarbete. Det finns styrdokument, men i kombination med omfattande delegering och högt produktionstryck prioriteras inte områden som samverkan, uppföljning och fortlöpande utbildning inom informationssäkerhetsområdet. Det starka förtroende för sina medarbetare som präglar SPV innebär också att riskanalysen, och därmed även skyddsåtgärderna, fokuserar på yttre hot. Även sekretessfrågorna fokuseras. Skyddet gentemot exempelvis interna hot blir då naturligt lägre prioriterat.

De delar av LIS (ledningssystemet för informationssäkerhet) som utgörs av styrdokument och i hög grad även tekniska skyddsåtgärder finns alltså till största delen på plats. Men, de delar av LIS som handlar om säkerhetsbeteende och samverkan mellan personer behöver utvecklas. Det senare är avgörande för att LIS ska göra avsedd nytta. Slutsatsen är att SPV inte fullt ut har lyckats åstadkomma de förutsättningar för god informationssäkerhet som de insatser och investeringar som gjorts i myndighetens LIS varit avsedda att åstadkomma.

[5] Citat från granskningsrapporten, s. 8.

Bristerna i LIS påverkar i sin tur möjligheterna att uppnå och vidmakthålla eftersträvad informationssäkerhet. Svaret på den fråga som granskningen syftat till att besvara är därmed att SPV inte fullt ut arbetar systematiskt med sin informationssäkerhet utifrån gängse normer.

Svenska kraftnät

Löpande granskning av Affärsverket Svenska kraftnät (RiR revisionsrapporter 2006-02-13, dnr 32-2005-0714 samt 2007-02-15, dnr 32-2006-0700)

Sammanfattning av granskningen

Avsaknad av dokumenterad riskanalys på aggregerad nivå gör att det för Riksrevisionen är oklart hur SvK kontinuerligt bedömer och tar om hand de risker och hot som finns i verksamheten. Sannolikt påverkar detta SvK:s möjlighet att göra en realistisk bedömning om systemen i dagsläget har ett relevant skydd. Detta intryck förstärks ytterligare av att resultaten av faktiskt genomförd granskning i enstaka system inte dokumenteras i systemsäkerhetsplaner. SvK har heller inte i kontinuitetsplaner visat att verksamhetskritiska system skyddas på ett sådant sätt att man kan försäkra sig om god säkerhet och tillgänglighet.[6]

Vid en uppföljande granskning av ledningssystemet för informationssäkerheten under 2006 kunde Riksrevisionen konstatera att SVK hade påbörjat att förbättra styrningen och kontrollen av informationssäkerheten. Ett antal av de iakttagelser som avrapporterades året innan kvarstod fortfarande.[7]

[6] Citat från Riksrevisionens revisionsrapport 2006-02-13, dnr 32-2005-0714, s. 1.
[7] Riksrevisionens revisionsrapport 2007-02-15, dnr 32-2006-0700, s.1.