

Öhrlings

PRICEWATERHOUSECOOPERS 

K O M R E V

Revisionsrapport



2005-04-11

Granskning av
IT-säkerheten
Landstinget i Jönköpings län

Göran Persson Lingman
Louise Cedemar

Innehållsförteckning

<u>1.</u>	<u>Inledning</u>	2
<u>1.1</u>	<u>Bakgrund</u>	2
<u>1.2</u>	<u>Syfte</u>	2
<u>1.3</u>	<u>Metod</u>	2
<u>1.4</u>	<u>Avgränsning</u>	2
<u>2.</u>	<u>Övergripande beskrivning av organisation och systemstruktur</u>	3
<u>3.</u>	<u>Granskningsresultat</u>	4
<u>3.1</u>	<u>Finns det en aktuell och fastställd IT-säkerhetspolicy samt andra styrande riktlinjer inom landstinget?</u>	4
<u>3.2</u>	<u>Finns det en tydlig ansvarsfördelning avseende IT-säkerhetsfrågorna inom landstinget?</u>	6
<u>3.3</u>	<u>Finns tillfredsställande rutiner för inköp, installation och avyttring av PC?</u>	7
<u>3.4</u>	<u>Har landstinget ett tillfredställande viruskydd samt erforderliga rutiner för incidentrapportering?</u>	8
<u>3.5</u>	<u>Har landstinget erforderliga rutiner för säkerhetskopiering?</u>	9
<u>3.6</u>	<u>Är driftsställens (datorrum) fysiska och miljörelaterade säkerhet tillfredställande?</u>	10
<u>3.7</u>	<u>Har landstinget ett erforderligt skydd för obehörigt tillträde till datorer och information?</u>	11
<u>3.8</u>	<u>Är landstingets dokument ”Internet som arbetsredskap” känt inom organisationen och sker uppföljning över tillämpning av policyn?</u>	12
<u>4.</u>	<u>Sammanfattande bedömning</u>	14

Bilaga 1 Resultat webbformulär

1. Inledning

1.1 Bakgrund

Med begreppet IT menas informationsteknik som innefattar teknik för elektronisk framställning, lagring, överföring och presentation av information. Tekniken kan bestå av hårdvara, nät, kommunikation och programvaror av olika slag.

Vår definition av IT-säkerhet menas här alla olika åtgärder som används för att skydda och säkerställa åtkomsten av information samt att interna och externa regelverk följs. Kontrollfunktioner i separata system innefattas här inte av begreppet.

Betydelse av IT ökar allt mer inom landstingets verksamhetsområden och förändringar sker kontinuerligt. Landstinget hanterar många känsliga uppgifter. Brister i säkerheten kan ge allvarliga konsekvenser såväl för landstinget som för enskilda personer.

1.2 Syfte

Granskningen syftar till att översiktligt granska landstingets IT-säkerhet. I granskningen ingår bl a att kontrollera regler och stöddokument, ansvarsförhållanden, behörighetshandtering, backuptagning och förvaring samt driftsäkerhet.

1.3 Metod

Vi har

- intervjuat ansvariga tjänstemän från IT-centrum samt de tre sjukvårdsområdena
- gjort en genomgång av framtagna dokument
- ställt frågor till användare och ansvariga via webbaserade formulär
- använt oss av Komrevs för ändamålet framtagna checklistor
- gjort en fysisk besiktning av datorrum på landstingets fyra driftsenheter

1.4 Avgränsning

Granskningen omfattar i huvudsak de i rapporten redovisade kontrollerna.

Granskningen har inte berört säkerheten i separata system utan inriktats på mer allmänna IT-frågor.

Vi har alltså inte granskat att systemen loggar erforderliga händelser, att personer har rätt behörighet till systemens olika register, att systemens egna kontrollfunktioner fungerar som avsett (att rätt person får ändra i leverantörsreskontra, att kontroll sker av att obligatoriska fält är ifyllda korrekt o.dyl.).

2. Övergripande beskrivning av organisation och systemstruktur

Inom Landstinget i Jönköpings län har landstingsstyrelsen det övergripande ansvaret för IT. Landstingsdirektören är landstingets ytterst ansvariga tjänsteman.

IT-centrum ansvarar för landstingets infrastruktur (kommunikation, datorer samt driften av landstingets olika system). IT-centrum ansvarar även för landstingets gemensamma applikationer intranet, internet och generella program i användarens dator (officepaketet).

Det finns fyra driftsställen;

- Rosenlund
- Ryhov
- Eksjö
- Värnamo

Inom IT-centrum arbetar ca 80 personer. 6 st av dessa är lokaliserade i Eksjö, 6 st är lokaliserade i Värnamo, ca 13 st arbetar på Ryhov samt resterande på Rosenlund. Alla personer som är lokaliserade inom de tre sjukvårdsområdena är antingen nät-, pc- eller systemtekniker.

Centralt på IT-centrum finns IT-direktör, IT-säkerhetsansvarig och administrativ personal.

Centralt på IT-centrum finns även IT-produktion med personal inom drift, kundservice, tekniker samt konsulter som arbetar med utveckling av applikationer m m.

IT-centrum har driftsansvaret för landstingets webbplats. Landstingets informationsavdelning är systemägare och ansvarar för riktlinjer avseende innehåll.

Drift av system sker även vid landstingets vårdcentraler. Vid vårdcentralerna ansvarar vårdcentralens IT-kontaktpersoner för backuptagning. (primärvårdssystemet, journaler m m). Även vissa av Folk tandvårdens kliniker drif tar sitt system vid vårdcentralerna.

Vid förvaltningarna finns IT-ansvariga (IT-planeringschefer, kravställare som beaktar förvaltningarnas krav på ett effektivt IT-stöd) och en IT-säkerhets handläggare med tillsynsansvar för IT-säkerheten inom sin förvaltning.

I landstingets driftsenheter hanteras system som innehåller viktig och känslig information såsom

- olika typer av patientinformation (t ex journaler)
- landstingets hemsida
- befolkningsregister
- lönesystem, ekonomisystem och förrådssystem

Även landstingets intranet och mailsystem hanteras inom landstingets driftsenheter.

Lagring av egna upprättade dokument ska enligt anvisningar ske på centrala servrar i landstingets driftsenheter (dvs olika dokument som användare arbetar med t ex ord och text, kalkyler och presentationer).

3. Granskningsresultat

3.1 Finns det en aktuell och fastställd IT-säkerhetspolicy samt andra styrande riktlinjer inom landstinget?

Iakttagelser:

En informationssäkerhetspolicy fastställdes av landstingsstyrelsen 1993. Landstingsstyrelsen har därefter i ett dokument 2000-06-08 (PM) förtydligat ansvarsfördelning, befogenheter och arbetsinnehåll för bl a rådgivning, uppföljning och utveckling av landstingets informationssäkerhet.

I dokumentet anges att landstingets IT-säkerhetsansvarige

- samordnar, utvecklar och arbetar med uppföljning av att organisationen tillämpar gällande regler och riktlinjer
- årligen ska lämna en rapport till landstingsdirektören avseende IT-säkerhetsrelaterade frågor
- är samordnare för verksamheternas säkerhetshandläggare.

Dokumentet tydliggör även uppgifterna för de säkerhetshandläggare som enligt säkerhetspolicy ska finnas vid respektive förvaltning. Säkerhetshandläggare ska bl a enligt dokumentet arbeta med information, kompetensutveckling och uppföljning avseende IT-säkerheten.

En Internetpolicy upprättades i februari 2003. Dokumentet beskriver vad som är tillåtet och otillåtet för användare då Internet används. I dokumentet tydliggörs även att verksamhetschefen ansvarar för att personalen känner till innebörden av policyn och att IT-centrum ansvarar för bl a brandvägg, programvaror för kommunikation via Internet, support, loggning och felsökning.

IT-centrum ska även, enligt Internetpolicyn, vid behov lämna rapporter till IT-direktören och landstingsdirektören över hur användarna trafikerar olika webbplatser.

Dokument som beskriver ansvar och rutiner för IT-säkerhet finns framtaget 1995.

Centrala riktlinjer för e-post finns.

Centrala riktlinjer för extern åtkomst till landstingets nät finns.

Vid de tre sjukvårdsområdena finns ett dokument som berör ”IT-säkerheten inom sjukvården”. Dokumentet bygger på ÖCB (numera krisberedskapsmyndigheten) FA22 standard och behandlar bl a behörighetshantering, säkerhetskopiering, tillträdes- och brandskydd. Detta dokument är ej generellt utan det gäller vid sjukvårdsförvaltningarna.

Driftavtal (färdiga blanketter) som reglerar IT-centrums ansvar för driften av systemet finns upprättade i olika nivåer.

Förutom ovan nämnda dokument finns även andra förvaltningsspecifika riktlinjer och anvisningar. Det har för oss inte varit helt lätt att bedöma om dokument som vi tagit del av är generella eller förvaltningsspecifika.

Olika typer av stödjande blanketter finns.

Kommentarer och rekommendationer:

- Vi bedömer att landstinget har många tillfredställande styrande och stödjande dokument (säkerhetspolicys, Internetpolicys, olika riktlinjer, rutinbeskrivningar o.dyl). Vi har även funnit goda exempel på förvaltningsspecifika dokument. T ex finns vid de tre sjukvårdsområdena ovan nämnda dokument som bl a innehåller checklistor, organisationsbeskrivning och åtgärdsplanering.
- Vår bild är dock att landstingets samling av dokument är svåröverskådlig och att det därmed finns risker att dokumenten inte fyller sitt syfte. Vi föreslår därför att landstinget ser över de dokument som finns samt i anslutning till detta även ser över hur olika dokument ska kommuniceras till ansvariga och användare. Vi kan t ex konstatera att flera användare i vår webbenkät har angett att de inte tagit del av lanstingets Internetpolicy.

3.2 Finns det en tydlig ansvarsfördelning avseende IT-säkerhetsfrågorna inom landstinget?

Iakttagelser:

IT-säkerhetsansvarig för landstinget finns. Säkerhetsorganisationen har även tydliggjorts i dokument (se 3.1 ovan).

Vid varje förvaltning finns IT-säkerhetshandläggare. Denne arbetar bl a med information och uppföljning inom den egna förvaltningen. Rapportering sker till förvaltningsledningen på varierande sätt. Innehållet i arbetet varierar från förvaltning till förvaltning. Till sjukvårdsledningen i Värnamo rapporteras varje år i dokument vilket säkerhetsarbete som skett under året samt vad som planeras under nästkommande år. I rapporten beskrivs även vilka uppföljningsinsatser som gjorts. Vid vissa förvaltningar sker ej några rutinmässiga rapporteringar till ledningen.

Uppföljning över att vårdcentraler följer gällande rutiner sker på ett varierande sätt inom landstinget (t ex backuptagning). Särskilda checklistor för uppföljning mot vårdcentralerna finns framtagna vid landstingets sjukvårdsområden.

Vissa säkerhetshandläggare har till oss angett att de efterlyser en bättre samordning avseende IT-säkerhetsarbetet inom landstinget. De upplever även att rollen som övergripande IT-säkerhetsansvarig inom landstinget är otydlig.

Ansvariga bedömer de övergripande säkerhetsdokumenten som positiva men de upplever att de inte, i tillräcklig utsträckning, arbetar på det sätt som anges i de övergripande i dokumenten (t ex arbetar IT-säkerhetsansvarig enbart med uppföljning mot IT-centrum, rapportering av IT-säkerhet till landstingsdirektören sker via IT-direktören). Det pågår, enligt uppgift, ett arbete med syfte att tydliggöra roller och ansvar inom IT-säkerheten

Av 81 chefer inom landstinget som svarat på fråga om tydlighet avseende ansvar för IT-säkerhet kan vi konstatera att fler än hälften svarat bra eller mycket bra. Samtidigt konstaterar vi även många chefer svarat ”mycket dåligt”, ”dåligt” och ”varken bra eller dåligt”. (Se bilaga 1 svar från webbaserat formulär).

Kommentarer och rekommendationer:

- Vi bedömer det positivt att det inom landstinget finns särskilt ansvariga för IT-säkerhet och att IT-säkerhetsarbetet beaktas på ett positivt sätt inom landstinget, främst genom att det finns särskilda säkerhetshandläggare vid varje förvaltning.
- Den policy som finns tydliggör även ansvaret för säkerhetsarbetet. Vi kan dock konstatera att policyn inte efterlevs.

- Vi bedömer att rollen som centralt IT-säkerhetsansvarig är otydlig och att det är viktigt att rollen tydliggörs i samspelet mellan säkerhetshandläggare, förvaltningschefer, landstingsdirektör och IT-direktör.
- Det är viktigt att ansvaret (rollen/roller) för kontroll och uppföljning av IT-säkerhet (informationssäkerhet) ytterligare tydliggörs inom landstinget. Vi vill här framför allt peka på rollen "landstingets IT-säkerhetsansvarig". Det är viktigt att landstingsledningen via bl a uppföljning försäkras sig om att organisationen (chefer, systemansvariga, användare m fl) förstår vad vars och ens ansvar innebär och att framtagna policys och instruktioner tillämpas.
- Vi bedömer att den samordning som sker avseende IT-säkerhetsarbetet mellan landstingets förvaltningar är bristfällig. Det är viktigt att resurserna samordnas på ett bättre sätt för ökad säkerhet och ökad effektivitet.

3.3 Finns tillfredsställande rutiner för inköp, installation och avyttring av PC?

Iakttagelser

Övergripande rutin för inköp av pc finns för landstinget. Förvaltningarna hyr utrustningen av IT-centrum som "äger" utrustningen. Vid alla inköp ska en IT-beställning göras på särskilt framtagen blankett, "IT-beställningsblankett".

IT-beställningsblanketten ska skrivas under av IT-kontaktperson, verksamhetschef, IT-samordnare samt av IT-centrum när installation skett.

Allt som ska anslutas till nätverket ska godkännas av IT-centrum.

Även beställning av programvara sker via IT-beställningsrutinen.

All installation av programvara hanteras av IT-centrum. Via behörighetsrutiner begränsas användares möjlighet att använda egna installerade program. Det finns inget "tekniskt" skydd (t.ex låsta diskett- eller cd-stationer) avseende installation eller nerläsning av filer från Internet. Användare får dock skriftliga och muntliga anvisningar om att detta inte är tillåtet.

Anvisningar över var användare ska spara dokument finns. Dokument får ej sparas lokalt i egen dator.

Vid avyttring av pc ska IT-beställningsblanketten fyllas i av samma ansvariga personer som vid ett inköp och överlämnas till IT-centrum.

IT-centrum hämtar sedan pc:n och paketerar den i en låst låda innan den körs till leverantör (avtal finns med denna leverantör, leverantör har avtal med speditör) där hårddisken rensas. Lådorna kan inte öppnas under frakt. Nycklar finns endast hos IT-centrum och leverantör.

Det finns undantag där IT-centrum själva rensar hårddiskarna. Detta gäller enheter som hanterar särskilt känslig information och som ställer högre krav på sekretess. IT-säkerhetsansvarig har tagit fram dokument med riktlinjer kring detta.

Det finns en inventarieförteckning som hanteras av IT-centrum. En gång i månaden får förvaltningarna en lista med den utrustning de hyr av IT-centrum. Inventarieförteckningen styr IT-centrums debitering mot förvaltningarna. IT-centrum ansvarar för uppdateringen av förteckningen.

Kommentarer och rekommendationer:

- Vi bedömer att rutinen är tillfredställande. Det är dock viktigt att ansvariga följer upp att rutinen tillämpas på ett korrekt sätt.
- Vi föreslår att det utarbetas en rutin för uppföljning av att endast godkänd programvara finns installerad i användares pc.

3.4 Har landstinget ett tillfredställande viruskydd samt erforderliga rutiner för incidentrapportering?

Iakttagelser

Inom Landstinget finns en "Antivirusgrupp" som har till uppgift att bevaka och hantera virus. I gruppen finns representanter från landstingets olika verksamheter. Daglig drift och övervakning görs av IT-centrum (via "Driften" och Helpdesk) och utsedda tekniker på de tre sjukhusen.

Landstingets antiviruskydd består idag av fyra olika nivåer;

- Clientskydd
- Serverskydd
- Mailskydd
- Brandvägg

Uppdatering av servrar och pc-clienter sker med automatik 1 gång/vecka och oftare vid behov.

Uppdatering av mailskyddet sker kontinuerligt (och vid behov).

Leverantören av antiviruskyddet bevakar dygnet runt vad som händer. Virus klassificeras på en skala från 1-5 där 5 är det allvarligaste hotet. Om risken når nivå 3 uppdateras skyddet kommande natt, samtidigt skickas larm via e-post och sms till utsedd mobil, vid nivå 4 och 5 skickas utöver ovanstående röstsamtal till mobil.

Vid en virusattack är det i första hand Drift/Helpdesk, eller personal i beredskap som enligt en handlingsplan, tar ställning till vilka åtgärder som behöver göras. Finns det osäkerhet kontaktas virusansvarig/IT-säkerhetsansvarig eller nät/kommunikationstekniker för rådgivning. Det finns också klarlagt hur informationsspridning till verksamheten ska gå till, t.ex. via e-post, fax eller telefon.

Det pågår aktiviteter för att förbättra landstingets skydd mot spam. Ansvariga upplever problem med nuvarande skydd.

Ett arbete med att förbättra skyddet mot sk ”spionprogram” (Spyware) har påbörjats.

Ansvariga vid IT-centrum upplever brister i det nuvarande viruskyddet då användare surfar på Internet. En arbetsgrupp arbetar idag med att ytterligare förbättra detta viruskydd.

Vid incidenter (t ex virus) ska rapportering först ske till utsedda kontaktpersoner inom förvaltningen. Kontaktpersoner ska därefter rapportera till kundservice på IT-centrum.

Kommentarer och rekommendationer:

- Vi bedömer landstingets viruskydd vara tillfredställande och att det är positivt att det pågår aktiviteter för att förbättra skyddet ytterligare. Det är viktigt att ansvariga slutför arbetet med att förbättra skyddet mot spyware.

3.5 Har landstinget erforderliga rutiner för säkerhetskopiering?

Iakttagelser

Rutiner avseende säkerhetskopiering (t ex intervall av backuptagningar, omfattning, kopieringsteknik, förvaring, återläsningskontroller, hur länge kopior sparas) varierar inom landstinget. Backuper tas vid driftsenheter och vid landstingets vårdcentraler. Kontroller sker av vårdcentralernas backuprutiner via IT-säkerhetshandläggare. Uppföljningsarbetet mot vårdcentraler varierar mellan de olika sjukvårdsområdena.

Ett förbättringsarbete pågår för närvarande med syfte att bättre säkerställa att backuper tas, förvaras och kontrolleras på ett tillfredställande sätt. En av målsättningarna med arbetet är att få enhetliga och kvalitetssäkrade rutiner. I samband med detta kommer även dokumentationen att förbättras.

Kommentarer och rekommendationer:

- Vi har i granskningen konstaterat att rutiner för backuptagning är mycket varierande. Det är därför mycket viktigt att det arbete som pågår med att skapa enhetliga och kvalitetssäkrade rutiner genomförs i enlighet med ansvarigas planering.

3.6 Är driftsställens (datorrum) fysiska och miljörelaterade säkerhet tillfredställande?

Iakttagelser

En fysisk besiktning har skett vid landstingets fyra driftställen. Besiktningen har bl a innefattat driftställets

- fysiska konstruktion och placering (t ex motståndskraftiga väggar, dörrar)
- skydd för brand, värme, vatten, damm o.dyl
- skydd för tillträde

Avseende Rosenlund är det planerat att bygga en helt nytt driftställe som ska ersätta det nuvarande. Tidpunkten för detta är beslutat.

Planer finns även att successivt förflytta driften från vårdcentraler till något av landstingets driftställen. Det är även planerat att koncentrera mer av driften till ett par driftställen och i samband med detta öka säkerheten ytterligare.

Kommentarer och rekommendationer:

- Vi bedömer att lokalen för den IT-drift som sker vid Rosenlund inte är tillfredställande för ändamålet. Vi uppfattar det därför positivt att landstinget beslutat att förbättra säkerheten genom att ersätta Rosenlund med nytt driftställe. Vi finner de andra driftställen som tillfredställande. Där vill vi tillägga att vi bedömer att Ryhov är väl anpassat för ändamålet.

3.7 Har landstinget ett erforderligt skydd för obehörigt tillträde till datorer och information?

Iakttagelser

Gemensamma rutiner för behörighetsadministration finns. Rutinerna är dokumenterade. Administrationen av behörigheter hanteras av IT-centrum. Nätverk finns för varje sjukvårdsområde och ansvarig för behörighetshantering finns. Behörigheter administreras på varje driftsenhet. Då anställda slutar ska enligt rutin rapportering via blankett göras av ansvarig chef. Anmälan om att ansvarig slutar fungerar inte alltid som önskvärt.

IT-kontaktpersoner avgör vilken behörighet som ska tilldelas användare. Blankett för beställning finns. Lösenord återrapporteras via telefon till IT-kontaktperson som fysiskt överlämnar meddelande till användare. Vid förändringar av lösenord används samma rutin. Byte av lösenord krävs enligt fastställt intervall. Vid för många inloggningsförsök spärras användarens dator (användarid) för påloggning. Längden på lösenordet är reglerat. Användaren måste byta lösenord ett visst antal gånger innan en repetering av lösenordet kan ske. Information avseende lösenord ges till användare bl a i samband med anställning. Inloggningsförsök loggas. Rutiner för uppföljning av loggar är otydliga. Detta noterades även i en granskningsrapport 2002.

Det förekommer att användare har gemensam behörighet till nätverket (av praktiska skäl delar användare på datorn). Då detta förekommer ska det enligt uppgift alltid förekomma unika användarnamn (ID) till användarens system. När detta förekommer ges anvisningar om att alltid logga ur applikationen (det system som användaren i huvudsak använder). Landstinget arbetar aktivt för att reducera detta förfarande till ett minimalt antal system.

Skärmsläckare med ”lås” finns. Skärmsläckaren måste dock aktiveras av användaren. Via information och utbildning delges användare vikten av att aktivera skärmsläckare. Skärmsläckaren aktiveras ej då flera delar på en dator eftersom det då finns risk att information går förlorad. Vanligtvis har dock de applikationer som används utlåsningsfunktioner.

Anvisningar avseende skrivarens placering saknas. Några användare har i vårt webbformulär angett att de upplever risker att känsliga dokument hamnar hos obehöriga vid utskrift. Strategiskt driver landstinget utvecklingen från egna personliga skrivare mot skrivare som delas av flera användare (nätverksskrivare).

IT-personalen bär ID-kort. Vi har ej funnit några landstingsgemensamma anvisningar avseende vikten av att IT-personal alltid ska legitimera sig innan tillträde till dator ges saknas.

Vid samtliga driftsenheter finns tillträdesskydd till serverrum.

Leverantörer tillåts ej arbeta ensamma enligt rutin. Blankett för sekretessförbindelse finns.

Arbete hemifrån förekommer. Rutiner och skriftliga anvisningar som reglerar hemanvändning finns. Säkerhetsdosa tilldelas användare enligt skriftlig rutin.

Tre brandväggar finns inom landstinget varav en är mot Sjunet. Tester har under året genomförts (på uppdrag av Sjunet) avseende brandväggen mot Sjunet med, enligt uppgift, positivt resultat. 2002 genomfördes tester av Ernst & Young. Vissa brister upptäcktes vilka enligt uppgift är åtgärdade. Landstinget har därefter inte gjort några egna tester utanför eller innanför brandvägg. Rutin för kontinuerlig test och rapportering saknas.

I tidigare granskning (2002) konstaterades att det saknades formella incidenthanteringsrutiner. Förslag till formaliserade incidenthanteringsrutiner lämnades. Ett förbättringsarbete har därefter skett.

I den tidigare granskningen lämnades även förslag till att utreda behovet av ett system för att upptäcka attacker från internet (IDS system, Intrusion Detection System). Landstinget saknar idag denna typ av system.

Kommentarer och rekommendationer:

- Det är viktigt att landstinget för ansvariga chefer tydliggör vikten av att tillämpa den rutin som finns då anställda slutar.
- Det är viktigt att landstinget ser över var centrala skrivare finns placerade idag samt i anslutning till detta vilka risker det finns med att utskrifter kan nås av obehöriga.
- För att säkerställa att landstingets brandväggar och andra resurser fungerar på ett tillfredställande sätt föreslår vi att landstinget på ett mer rutinmässigt sätt genomför tester via sk intrångstest både från insidan och utsidan av landstingets brandväggar.
- Vi bedömer att det är viktigt att landstinget utreder behovet av ett system för att enklare kunna upptäcka attacker från Internet i enlighet med förslag som lämnats i tidigare granskning. (Intrusion Detection System).
- Det är viktigt att landstinget säkerställer att anställda är medvetna om att IT-personal alltid måste legitimera sig innan tillträde ges till datorer.

3.8 Är landstingets dokument "Internet som arbetsredskap" känt inom organisationen och sker uppföljning över tillämpning av policyn?

Iakttagelser

Enligt dokumentet ska verksamhetschefen ansvara för att personalen känner till innebörden av policyn.

Enligt uppgift ges även information till anställda av IT-säkerhetshandläggaren i varierande grad.

IT-centrum ansvarar enligt policyn för avtal med Internetleverantör, uppkoppling, brandvägg, programvaror för kommunikation via Internet, support, loggning och felsökning.

IT-centrum ska enligt policyn lämna rapporter till IT-direktören och landstingsdirektören avseende användares nyttjande av Internet.

Loggning av användarens trafik mot Internet sker. Gallring av loggar sker efter 90 dagar. Det finns i internetpolicyn syftesbeskrivning avseende ändamålet med loggningen, dvs att användning för kontroll kan ske. Stödjer bl a följsamhet mot personuppgiftslagen.

Uppgifter används inte idag för att säkerställa att anställda efterlever Internetpolicyn. Rutiner för uppföljning saknas. I vårt webbformulär har framkommit att många användare ej tagit del av policyn ”internet som arbetsredskap”. (Se bilaga 1 svar från webbaserat formulär).

Det finns ingen landstingsövergripande kontinuerlig utbildning av användare inom IT- och informationssäkerhet. Varje förvaltning har egna rutiner och arbetsätt.

När det gäller skydd mot virus då anställda surfar bedömer ansvariga att det finns vissa brister. En arbetsgrupp arbetar idag med att ytterligare förbättra detta virusskydd.

Kommentarer och rekommendationer:

- Landstingets Internetpolicy är idag inte tillräckligt känd inom organisationen. Det är viktigt att aktiviteter vidtas för detta. Det är otillfredsställande att över 30 % av 81 svarande chefer uppger att de inte tagit del av policyn.
- Rutiner för uppföljning av efterlevnad via den loggning som sker bör utarbetas avseende Internettrafiken. (Rapporter som säkerställer att användarnas tillämpar policyn ”internet som arbetsredskap”).
- Det är positivt att det pågår ett arbete för att ytterligare förbättra landstingets virusskydd i samband med anställdas surfande.

4. Sammanfattande bedömning

Vi vill sammanfatta vår granskning med att vi bedömer resultatet avseende de flesta utförda kontrollerna som tillfredställande. Vi har också konstaterat brister men där det samtidigt pågår förbättringsaktiviteter. Här är det givetvis viktigt att tydliga tidsplaner sätts upp och att arbetet slutförs enligt plan. Vi kan här t ex peka på att

- de backuprutiner som finns kvalitetssäkras och dokumenteras (intervall avseende back-upptagning, förvaring kopior, hur länge kopior sparas, återställningstester o.dyl)
- Rosenlund ersätts som driftställe enligt plan och att driften vid vårdcentraler reduceras.
- skyddet avseende spyware förbättras.
- antalet användare som delar på ett id reduceras enligt plan.

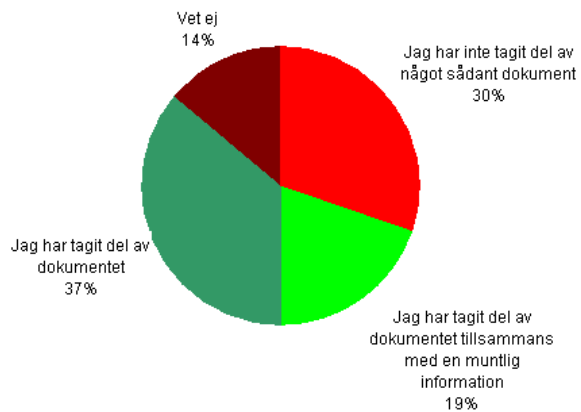
Andra områden som vi bedömer vara otillfredsställande och som är viktiga för landstinget att förbättra sammanfattas i nedanstående punkter.

- Rollen som centralt IT-säkerhetsansvarig är otydlig och det är viktigt att rollen tydliggörs (t ex samspelet mellan säkerhetshandläggare, förvaltningschefer, landstingsdirektör och IT-chef). Det är viktigt att landstingsledningen via bl a uppföljning försäkras sig om att organisationen (chefer, systemansvariga, användare m fl) förstår vad vars och ens ansvar innebär och att framtagna policys och instruktioner tillämpas.
- Den samordning som sker avseende IT-säkerhetsarbetet mellan landstingets förvaltningar är bristfällig. Det är viktigt att resurserna samordnas på ett bättre sätt.
- Landstingets samling av dokument är svåröverskådlig och därmed finns det en risk att dokumenten inte fyller sitt syfte. Vi föreslår därför att landstinget ser över de dokument som finns samt i anslutning till detta även ser över hur olika dokument ska kommuniceras till ansvariga och användare. Vi kan t ex konstatera att flera användare i vår webbenkät har angett att de inte tagit del av landstingets Internetpolicy
- Landstingets Internetpolicy är idag inte tillräckligt känd inom organisationen. Det är viktigt att aktiviteter vidtas för detta. Det är otillfredsställande att över 30 % av 81 svarande chefer uppger att de inte tagit del av policyn. Rutiner för uppföljning av efterlevnad via den loggning som sker bör utarbetas avseende Internettrafiken. (Rapporter som säkerställer att användarnas tillämpar policyn ”internet som arbetsredskap”).
- Det är viktigt att landstinget till ansvariga chefer tydliggör vikten av att tillämpa den rutin som finns då anställda slutar.

- Det är viktigt att landstinget ser över var centrala skrivare finns placerade idag samt i anslutning till detta ser över vilka risker det finns med att utskrifter kan nås av obehöriga.
- Det är viktigt att landstinget säkerställer att anställda är medvetna om att IT-personal måste legitimera sig innan tillträde ges till datorer.
- För att säkerställa att landstingets brandväggar och andra resurser fungerar på ett tillfredsställande sätt föreslår vi att landstinget på ett mer rutinmässigt sätt genomför tester via sk intrångstest (både från insidan och utsidan av landstingets brandväggar).

Bilaga 1 Resultat webbformulär

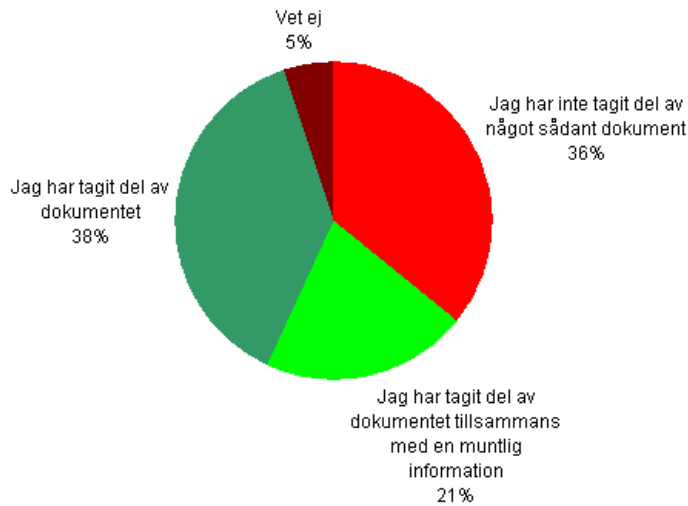
Tagit del av policyn "Internet som arbetsredskap". (234 svar från användare som använder internet dagligen)



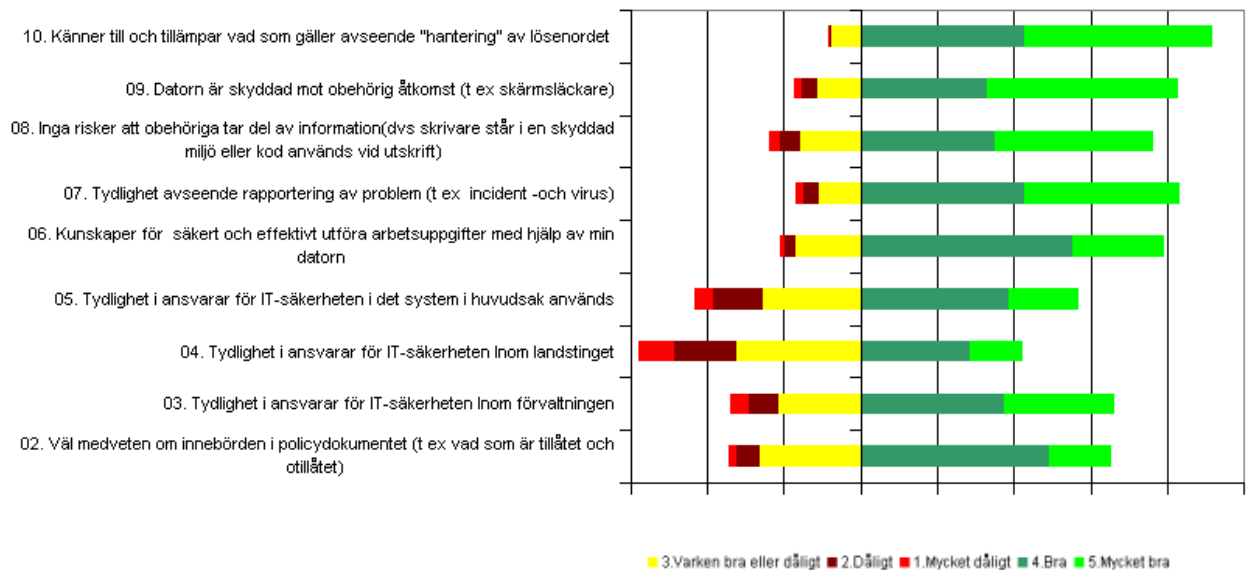
Tagit del av policyn "Internet som arbetsredskap". (Alla 756 svar)



Tagit del av policyn "Internet som arbetsredskap". (81 svar från chefer)



Alla de frågor som ställdes i vårt webformulär (756 svar)



Känner till och tillämpar vad som gäller avseende "hantering" av lösenordet

