Granskning av it- och informationssäkerhet

Rapport

Varbergs kommun

KPMG AB

2023-12-18

Antal sidor 24

Bilaga 1

Varbergs kommun
Granskning av it- och informationssäkerhet

2023-12-18

Innehållsförteckning

Varbergs kommun
Granskning av it- och informationssäkerhet

2023-12-18

1 Sammanfattning

KPMG har av Varbergs kommuns revisorer fått i uppdrag att granska kommunens arbete för att upprätthålla en god informations- och it-säkerhet.

Syftet med granskningen har varit att bedöma om kommunstyrelse och nämnder bedriver ett systematiskt informationssäkerhetsarbete så att det sker på ett ändamålsenligt sätt.

Vår samlade bedömning utifrån granskningens syfte är att kommunstyrelse och nämnder delvis bedriver ett systematiskt och ändamålsenligt informationssäkerhetsarbete.

Kommunen har upprättat ett ledningssystem med processer, dokument och roller som utgör strukturell grund för ett systematiskt informationssäkerhetsarbete. Ledningssystemet hade inte implementerats fullt ut då granskningen genomfördes, men vi bedömer att kommunen på övergripande nivå har skapat organisation och struktur för ett systematiskt informations- och it-säkerhetsarbete.

Vi ser att det finns behov av att stärka organisationerna inom nämnderna samt erbjuda stöd från centrala funktioner i syfte att informationssäkerhetsarbetet ska genomföras med en högre grad av systematik samt att tillse att styrande dokument efterlevs. Detta då analyser och aktiviteter i verksamheterna krävs för att bedöma vilket skyddsvärde informationstillgångar har som kan utgöra underlag över vilka it-säkerhetsåtgärder som behövs för att skydda informationstillgångar och it-miljö.

Nedan redovisas bedömningar som gäller på övergripande kommunnivå. Bedömningar avseende granskade nämnder återfinns under rapportens olika avsnitt. Rekommendationer till samtliga revisionsobjekt hittas i rapportkapitel 4 *Samlad bedömning och rekommendationer.*

Revisionsfråga	Bedömning: Delvis
Finns aktuella styrande dokument som tydliggör ansvar, vilka krav som ställs och hur arbetet ska bedrivas?	Det finns styrande dokument som tydliggör ansvar och krav på informationssäkerhetsarbetet. Vi ser dock behov av att reglementen eller ansvar ses över i förhållande till nuvarande organisation och på det sätt ansvaret utförs i praktiken samt att detta ska vara samstämmigt mellan reglementen och styrande dokument för informationssäkerhet. Vi konstaterar att kommunen upprättat en strukturell grund för ett systematiskt informations- och it-säkerhetsarbete. Ledningssystemet hade vid tid för granskning inte fullt ut implementerats i den operativa verksamheten varför dokumenten inte är tillräckligt kända.

Revisionsfråga	**Bedömning: Delvis**
Finns en ändamålsenlig organisation för informationssäkerhetsarbetet?	Kommunstyrelsen har stärkt förmågan att leda och vara kravställare i övergripande informationssäkerhetsarbete. Vi ser dock behov av att det ansvar som beskrivs i styrande dokument är samstämmigt med nuvarande organisation samt hur ansvaret upprätthålls i praktiken. Kommunstyrelsen behöver utvärdera organisation och förutsättningar för förskole- och grundskolenämndens respektive utbildnings- och arbetsmarknadsnämndens hantering av elev- och pedagogklienter.
Revisionsfråga	**Bedömning: Nej**
Finns beslutade informationssäkerhetsmål med tillhörande handlingsplaner?	Av rapporten om kommunens samlade informationssäkerhetsarbete framgår kommunens målsättning att systematisera arbetet. För att i ökad omfattning kunna följa upp och styra arbetet anser vi att tydliga mål behöver formaliseras.
Revisionsfråga	**Bedömning: Nej**
Har styrelse och nämnder tillsett att det finns en tillräcklig säkerhetskultur?	Utbildningsinsatser har inte genomförts i tillräcklig omfattning. Vi ser därför en risk att det finns en bristande kunskap och medvetenhet om informationssäkerhet och tillhörande hot och risker.
Revisionsfråga	**Bedömning: Endast delvis**
Finns ett systematiskt arbete med riskanalyser och informationsklassning?	Momenten genomförs inte i den omfattning som styrande dokument kravställer. Det saknas i nuläget en kommunövergripande riskanalys som identifierar risker och hot som kommunens samlade it-miljö är exponerad för.
Revisionsfråga	**Bedömning: I allt väsentligt**
Har tekniska säkerhetsåtgärder vidtagits som står i relation till aktuella hot och risker och utvärderas dessa regelbundet?	Kommunstyrelsen har vidtagit åtgärder som skyddar kommunens it-miljö mot aktuella risker och hot. Tekniska säkerhetsåtgärder utvärderas systematiskt. Kommunen bör överväga att stärka både rutiner och tekniska implementationer avseende åtkomst- och behörighetshantering då användarkonton och lösenord är särskilt utsatta vid externa angrepp. I samma avseende behöver kommunstyrelsen tydliggöra krav för livscykelhantering så att inte it-miljön riskerar att vara föråldrad och hindra att tekniska säkerhetsfunktioner kan nyttjas till fullo.

Revisionsfråga	Bedömning: I allt väsentligt
Finns en etablerad övervakning för att upptäcka hot om intrång eller andra säkerhetsincidenter i it-miljön?	Vi bedömer att det kan finnas behov av att utreda förutsättningarna för beredskap utanför kontorstid i syfte att stärka kommunens robusthet vad gäller förmåga att hantera intrång och andra säkerhetsincidenter.
Revisionsfråga	**Bedömning: Endast delvis**
Finns incidenthanteringsrutiner som inkluderar krav på hur incidenter ska dokumenteras och följas upp tillsammans med tydliggjorda eskaleringsvägar?	Det finns en övergripande incidenthanteringsrutin med tydliga eskaleringsvägar som också reglerar uppföljning av incidenter. It-avdelningen har upprättat erforderliga interna incidenthanteringsrutiner, som också utvärderats i praktiken.
Revisionsfråga	**Bedömning: Nej**
Finns dokumenterade reserv- och återgångsrutiner vid allvarligare störningar och avbrott i it-system? Har dessa testats för att säkerställa att de fungerar ändamålsenligt?	Det saknas kommunövergripande reservrutiner. En övergripande kontinuitetsplan är nödvändig för att säkerställa att väsentlig funktionalitet prioriteras i händelse av större avbrott. För en ändamålsenlig kontinuitetsplan är definierade servicenivåer en god vägledning. Arbetet med återställningsplaner för system följer inte vad som anges av styrande dokument. Vi ser det som en brist i förhållande till att planerna är väsentliga underlag i händelse av avbrott. Avsaknad av nämnda underlag föranleder att tester inte genomförts.
Revisionsfråga	**Bedömning: I allt väsentligt**
Finns en etablerad uppföljning av informations- och it-säkerhetsarbetet och rapporteras denna till styrelse och nämnder med regelbundenhet?	En samlad uppföljning av kommunens informationssäkerhetsarbete finns och har rapporterats till kommunstyrelsen samt till kommunens förvaltningschefer. Med anledning av omvärldsläge och förhöjd risk för cyberhot och it-incidenter bör kommunstyrelsen fortsätta att efterfråga kontinuerlig återrapportering avseende aktuella hot och risker tillsammans med kommunens förutsättningar och beredskap för att hantera allvarliga it-säkerhetshändelser.

2 Bakgrund

KPMG har av Varbergs kommuns förtroendevalda revisorer fått i uppdrag att genomföra en granskning av kommunens arbete för att upprätthålla en god informations- och it-säkerhet. Uppdraget ingår i revisionsplanen för år 2023.

Organisationer i offentlig sektor hanterar ovärderliga informationstillgångar och blir alltmer beroende av sina informationssystem. Ny teknik innebär nya möjligheter men introducerar även nya risker som ställer krav på ett balanserat risktagande och ett väl fungerande säkerhetsarbete.

Informationssäkerhet innebär att all skyddsvärd information ska vara tillgänglig, konfidentiell och spårbar. Den digitala transformationen innebär att det har skapats ett beroende av kontinuerligt fungerande informations- och kommunikationsteknik. Utvecklingen och den förändrade användningen av ny teknik innebär också att hot blir svårare att upptäcka, att riskerna blir mer svårbedömda och att beroenden blir svårare att överskåda. Den digitala utvecklingen måste följas av ett anpassat och balanserat säkerhetsarbete för att säkerställa att inte de system och digitala tjänster som nyttjas för informationshantering och lagring är exponerade och tillgängliga för cyberhot och angrepp. Där tekniken implementeras på ett ogenomtänkt eller otillräckligt sätt uppstår brister som kan utnyttjas av hotaktörer.

Brister i informationshanteringen och säkerhetsarbetet kan få allvarliga konsekvenser, till exempel att integritetskänslig information sprids eller att verksamhetskritiska processer stoppas. Detta kan leda till både ekonomisk skada och förtroendeskada för kommunen. Det är således väsentligt att kommunen har en tillräcklig intern styrning och kontroll av sitt it-säkerhetsarbete så att arbetet sker på ett ändamålsenligt sätt.

Med anledning av ovanstående drar kommunens revisorer slutsatsen i sin riskanalys, att arbetet med informations- och it-säkerhet behöver granskas.

2.1 Syfte, revisionsfrågor och avgränsning

Granskningen har syftat till att bedöma om kommunstyrelse och nämnder bedriver ett systematiskt informationssäkerhetsarbete så att det sker på ett ändamålsenligt sätt.

Granskningen har besvarat följande revisionsfrågor:

- Finns aktuella styrande dokument som tydliggör ansvar, vilka krav som ställs och hur arbetet ska bedrivas?
- Finns en ändamålsenlig organisation för informationssäkerhetsarbetet?
- Finns beslutade informationssäkerhetsmål med tillhörande handlingsplaner?
- Har styrelse och nämnder tillsett att det finns en tillräcklig säkerhetskultur?
- Finns ett systematiskt arbete med riskanalyser och informationsklassning?
- Har tekniska säkerhetsåtgärder vidtagits som står i relation till aktuella hot och risker och utvärderas dessa regelbundet?

- Finns en etablerad övervakning för att upptäcka hot om intrång eller andra säkerhetsincidenter i it-miljön?
- Finns incidenthanteringsrutiner som inkluderar krav på hur incidenter ska dokumenteras och följas upp tillsammans med tydliggjorda eskaleringsvägar?
- Finns dokumenterade reserv- och återgångsrutiner vid allvarligare störningar och avbrott i it-system? Har dessa testats för att säkerställa att de fungerar ändamålsenligt?
- Finns en etablerad uppföljning av informations- och it-säkerhetsarbetet och rapporteras denna till styrelse och nämnder med regelbundenhet?

Granskningen har omfattat kommunstyrelsens övergripande ansvar för informationssäkerhet och it-säkerhet samt kommunstyrelsen och nämndernas verksamhetsansvar för de informationstillgångar som hanteras inom respektive nämnd. Granskningen har avsett kommunstyrelsen, socialnämnden, förskole- och grundskolenämnden samt utbildnings- och arbetsmarknadsnämnden.

Granskningen har avsett år 2023.

2.2 Revisionskriterier

I granskningen utgörs revisionskriterierna av:

- Kommunallagen 6 kap § 6
- Tillämpbara interna regelverk och policyer.

2.3 Metod

Dokumentanalysen har bland annat omfattat övergripande styrdokument fastställda av kommunfullmäktige, kommunstyrelsen och kommundirektör i Varbergs kommun. Exempel på styrande dokument är reglemente för kommunstyrelse och nämnder i Varbergs kommun, policy för informationssäkerhet, Riktlinjer för informationssäkerhet.

Dokumentgranskning har även inkluderat uppföljning av det övergripande informationssäkerhetsarbetet.

Intervjuer har genomförts med:

- Kommunstyrelsens presidium
- Ordförande för socialnämnden, förskole- och grundskolenämnden respektive utbildnings- och arbetsmarknadsnämnden
- Chef för socialförvaltningen, förskole- och grundskoleförvaltningen respektive utbildnings- och arbetsmarknadsförvaltningen
- För informationssäkerhetsarbetet utsedda funktioner per förvaltning

Samtliga intervjuade har getts möjlighet att faktakontrollera rapporten.

3 Resultat av granskningen

3.1 Organisation och styrning av informationssäkerhet

3.1.1 Ledningssystem för informationssäkerhet (LIS)

En kommuns eller ett bolags verksamhet kan identifieras som samhällsviktig och står då under kraven i Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, även kallat NIS-direktivet. I lagen ställs krav på att verksamheter som är identifierade som samhällsviktiga ska ha ett etablerat ledningssystem för informationssäkerhet, ett så kallat LIS.

Varbergs kommuns ledningssystem framgår av instruktionen Ledningssystem för informationssäkerhet/dataskydd[1]. Här anges att ledningssystemet utgår från MSB:s metodstöd och baseras på ISO/IEC 27001-standarden. Dokumentet beskriver roller och ansvar i informationssäkerhetsarbetet, samt de processer och dokument som utgör kommunens samlade informationssäkerhetsarbete.

Vidare har kommunfullmäktige antagit en policy för informationssäkerhet[2] som fastställer övergripande inriktning på arbetet. Av policyn framgår ansvar och roller i informationssäkerhetsarbetet, samt att arbetet ska baseras på etablerade standarder.

Policyns innehåll konkretiseras av en riktlinje för informationssäkerhet[3] samt ytterligare ett antal dokument med syfte att tydliggöra hur informationssäkerhetsarbetet ska gå till väga. I rapporten redovisas vissa av dessa dokument utifrån specifikt användningsområde.

Genom intervjuer har vi fått en bild av att kommunen tillskapat processer, dokument och centrala funktioner som utgör basen i ledningssystemet, men att ledningssystemet ännu inte har fått genomslag i det operativa informationssäkerhetsarbetet. Vi uppfattar att de styrande dokumenten inte fullt ut är kända inom granskade nämnder, liksom att det i dagsläget inom kärnverksamheterna saknas tillräckliga kunskaper för att arbeta i enlighet med ledningssystemet.

3.1.2 Bedömning

Vår bedömning är att det finns styrande dokument som tydliggör ansvar och krav på informationssäkerhetsarbetet, men att dokumenten inte är kända i tillräcklig omfattning.

Vi konstaterar att kommunen upprättat en strukturell grund för ett systematiskt informations- och it-säkerhetsarbete. Ledningssystemet hade vid tid för granskning inte fullt ut implementerats i den operativa verksamheten.

[1] Beslutad 2021-10-15
[2] Beslutad 2018-10-16, ej reviderad
[3] Beslutad 2019-12-17

3.2 Ansvarsfördelning informationssäkerhet

3.2.1 Övergripande ansvar för informationssäkerhet

Kommunstyrelsen har enligt reglementet[4] ansvar för interna säkerhetsfrågor samt för att leda och samordna kommunens informationssäkerhet och IT-strategi.

Av riktlinjer för informationssäkerhet framgår att kommunstyrelsen ansvarar för samordning och uppföljning av arbetet med informationssäkerhet. Informationssäkerhet inom respektive verksamhetsområde ansvarar styrelse och nämnder för.

Kommunen ska därtill utse olika arbetsgrupper för frågor om informationssäkerhet. Vilka dessa grupperingar är klargörs av anvisningar för arbetet med informationssäkerhet[5]. Här framgår att det ska finnas en informationssäkerhetsgrupp med representanter från förvaltningarna. Därtill ska finnas en GDPR-grupp för dataskyddsfrågor.

Enligt policyn ska stöd till kommunens verksamheter ges genom specifika medarbetare som arbetar kommunövergripande med informationssäkerhet och it-säkerhet. Vad som avses förtydligas av riktlinjerna, som säger att det inom kommunstyrelsens förvaltning ska finnas en informationssäkerhetsstrateg för samordning av det övergripande informationssäkerhetsarbetet.

Vi konstaterar att det pågår ett organisatoriskt utvecklingsarbete inom kommunen som syftar till att stärka kommunstyrelsens kontroll och strategiska styrning över övergripande säkerhetsfrågor. Som följd av det flyttades kommunens informationssäkerhetsstrateg för en tid sedan till den förhållandevis nybildade digitaliseringsenheten inom kommunstyrelseförvaltningen. I avsnitt 3.1.3 redogörs ytterligare för organisation och ansvarsfördelning mellan digitaliseringsenheten och it-avdelningen.

Omfördelningen syftar till att informationssäkerhetsstrategen ska få bättre överblick över verksamheternas behov av stöd, samt kunna agera kravställare mot it-avdelningen och nämnderna i fråga om att tillse aktiviteter och arbete som bidrar till ett systematiskt informationssäkerhetsarbete.

3.2.2 Granskade nämnders ansvar för informationssäkerhet

Av policyn för informationssäkerhet framgår att ansvar för informationssäkerhet följer det ordinarie verksamhetsansvaret. Inom varje förvaltning ska det även finnas en informationssäkerhetssamordnare, enligt instruktionen för ledningssystemet för informationssäkerhet. Rollbeskrivning för informationssäkerhetssamordnarna konkretiseras av en särskild arbetsbeskrivning[6] av vilken det framgår att samordnaren är central för förvaltningarnas löpande informationssäkerhetsarbete.

[4] Beslutad 2022-12-13
[5] Beslutad 2019-12.19
[6] Vägledning informationssäkerhetssamordnare, beslutad 2022-02-21

I instruktionen för informationssäkerhet i verksamhetsnära förvaltning[7] beskrivs roller kopplat till kommunens systemförvaltningsmodell. Modellen innebär att det på förvaltningsnivå finns specifika funktioner som genom systemförvaltarskapet har ett informationssäkerhetsansvar kopplat till ett visst verksamhetssystem.

Från intervjuer är vår uppfattning att det linjebaserade verksamhetsansvaret för informationssäkerhet är känt inom samtliga förvaltningar. Samtliga granskade förvaltningar har, i enlighet med styrande dokument, utsett varsin informationssäkerhetssamordnare.

Vi uppfattar dock att förvaltningarnas organisering och utrymme att arbeta med informationssäkerhetsfrågor skiljer sig åt.

Förskole- och grundskoleförvaltningen har två funktioner som arbetar dedikerat med informationssäkerhet respektive systemsamordningen. En av dessa är en heltidsanställd informationssäkerhetssamordnare. Vid tid för granskning pågick uppbyggnad av ett nätverk för informationssäkerhets- och dataskyddsfrågor där administratörer på varje skolenhet ska ingå.

Socialförvaltningen och utbildnings- och arbetsmarknadsförvaltningen har två funktioner som hanterar informationssäkerhetsfrågor vid sidan av andra arbetsuppgifter. Båda förvaltningarna beskrivs vara i en organisationsutvecklingsfas där arbetsformer för informationssäkerhet är del i en större utvecklingsprocess. Det finns också en upplevelse av att tid och kunskap för att arbeta med informationssäkerhet är begränsad, varför centralt stöd ses som nödvändigt.

3.2.3 Ansvarsfördelning it- och cybersäkerhet

Kommunstyrelsens reglemente anger att styrelsen ska fatta beslut om organisationsövergripande it-lösningar samt bevaka att kommungemensamma system är ändamålsenliga. Ansvar för drift av it-system och tjänster, liksom att beslutad nivå avseende it-säkerhet upprätthålls, är enligt reglementet[8], ett ansvar som tillhör servicenämnden. I enlighet med reglementet så är kommunens it-avdelning organiserad inom serviceförvaltningen som lyder under servicenämnden.

Av instruktion för informationssäkerhet i it-nära förvaltning[9] framgår att it-avdelningen har ansvar för den tekniska it-säkerheten för kommunens it-miljö. Det operativa ansvaret för it-säkerhet följer enligt instruktionen ordinarie verksamhetsansvar inom it-avdelningen. Härvid framgår att it-chef är högst ansvarig för verksamhetens leverans avseende it- och informationssäkerhet. Instruktionen konkretiserar även ansvar för funktionen ”driftansvarig”, vilket ligger i taktiskt och operativt driftansvar för it-säkerhet, samt att tillse att den tekniska infrastrukturen är uppdaterad och säker. För rollen it-säkerhetssamordnare framgår av instruktionen att vederbörande samordnar säkerhetsarbetet för den kommungemensamma it-miljön.

Vid tid för granskning består it-avdelningen av drygt 50 medarbetare organiserade i tre enheter: kontaktcenter, it-service där it-drift ingår, samt en enhet för utveckling och

[7] Beslutad 2020-06-29
[8] Beslutad 2022-12-13
[9] Beslutad 2020-06-29

förvaltning. It-säkerhetsarbetet utförs av tio medarbetare inom driftenheten där det finns en driftchef och en it-säkerhetssamordnare. Hela avdelningen leds av it-chef.

Intervjuade företrädare för it-avdelningen menar att sättet som kommunstyrelsens och servicenämnens reglementen formulerats innebär att it-avdelningen blir en utförare av det it-säkerhetsarbete som kravställs av kommunstyrelsen. Från it-avdelningen uppfattas att avdelningen formellt inte har uppdraget att bedriva ett strategiskt it-säkerhetsarbete utan främst ska vara en utförarorganisation. Intervjuade framhåller att avdelningen trots det arbetar aktivt med it-säkerhetsstrategiska insatser då kommunens it-säkerhet annars hade riskerat att försvagas. Det finns en upplevelse från intervjuade att omorganisationen mellan serviceförvaltningen och kommunstyrelseförvaltningen har inneburit vissa otydligheter i ansvar mellan digitaliseringsavdelningen och it-avdelningen. Bland annat lyfts strategiskt ledarskap i olika frågor samt rapporteringsvägar.

I kommunen finns en it-säkerhetsgrupp som leds av it-säkerhetssamordnare, som bland annat följer upp genomförda insatser för att höja den it-tekniska säkerhetsnivån samt beställer utvärdering av etablerade skyddsfunktioner. I gruppen ska it-driftschef, informationssäkerhetsstrateg samt ytterligare funktioner från it-avdelningen ingå. Enligt intervjuade ingår dock inte informationssäkerhetsstrateg regelbundet i gruppen, utan vid behov. För att skapa förutsättningar för framdrift i strategiska informationssäkerhetsfrågor har i stället ett separat forum etablerats där informationssäkerhetsstrateg och it-säkerhetssamordnare träffas månadsvis.

Utöver it-avdelningens ansvar finns funktioner inom förskole- och grundskoleförvaltningen samt utbildnings- och arbetsmarknadsförvaltningen som hanterar pedagogers och elevers klienter samt applikationer som endast nyttjas inom dessa verksamheter och inte av kommunens övriga verksamheter.

Vi redogör för förvaltningarnas hantering av elev- och pedagogklienter nedan, men konstaterar här att den tekniska lösningen innebär att klienterna är uppkopplade mot kommunens nätverk, men i övrigt inte ingår i kommunens gemensamma it-miljö. Klienterna omfattas därmed inte av kommunens gemensamma it-säkerhetslösning, de hanteras heller inte av it-avdelningen i någon utsträckning.

3.2.4 Organisation för pedagog- och elevklienter inom förskole- och grundskoleförvaltningen och utbildnings- och arbetsmarknadsförvaltningen

För cirka tio år sedan införde båda förvaltningarna digitala lärplattformar som ansågs vara bättre anpassade för undervisning än den gemensamma it-plattform som då användes inom kommunen. Förvaltningarna har av samma anledning fortsatt använda separata digitala undervisningsplattformar sedan dess.

Praktiskt innebär det att elever och lärare inom förskoleklass och grundskola samt elever och vissa lärare inom gymnasieskola använder datorer av andra sorter än de som används inom övriga kommunen. Därtill används surfplattor inom förskola och gymnasiet som inte är en del av kommunens gemensamma it-miljö.

Verksamhetsnära funktioner som handhar it-teknisk drift och support av klienterna har utsetts inom respektive förvaltning. Inom förskole- och grundskoleförvaltningen finns sex medarbetare för detta, inom utbildnings- och arbetsmarknadsförvaltningen hanteras klienterna bland annat av lärare samt av en upphandlad leverantör. Anledningen till att klienterna inte driftas av ordinarie it-avdelning uppges vara att kommunen inte ville ansvara för de nya plattformarna då dessa först introducerades. Förvaltningarna tog därför hem driften och har sedan dess fortsatt hantera den. Företrädare för de bägge förvaltningarna anser att upplägget har kostnadsmässiga och verksamhetsmässiga fördelar då klienternas funktion som lärverktyg och drift av dessa effektiviseras genom att hantering och samordning sker av verksamhetsnära stödorganisationer.

Vår bild är att det finns en viss samordning mellan it-avdelningen inom serviceförvaltningen och dessa förvaltningsspecifika funktioner. Samt att samarbetet ses som viktigt från både förvaltningarna och it-avdelningen.

Vi uppfattar dock att det inom kommunen råder delade meningar kring organiseringen och användandet av elev- och pedagogklienter. Obeaktat klienternas funktion som pedagogiska verktyg och deras it-säkerhetsförutsättningar anses upplägget av företrädare för it-avdelningen innebära att förvaltningarna har etablerat parallella it-funktioner, vilket är förenat med risker avseende dubbelarbete och suboptimering. Samt att klienterna varken omfattas av it-avdelningens skyddsåtgärder eller ingår i den strategiska utvecklingen av kommunens gemensamma it-miljö.

3.2.5 Bedömning

Vi gör bedömningen att kommunstyrelsen delvis har tillsett en ändamålsenlig organisation för informationssäkerhetsarbetet. Vår bedömning är att förskole- och grundskolenämnden i allt väsentligt har en ändamålsenlig organisation för informationssäkerhetsarbetet men att socialnämnden och utbildnings- och arbetsmarknadsnämnden delvis har en ändamålsenlig organisation för informationssäkerhetsarbetet.

Vi bedömer att nuvarande formuleringar i kommunstyrelsens och servicenämndens reglementen är otydligt avseende var ansvaret för det strategiska it-säkerhetsarbetet åvilar i jämförelse med hur arbetet genomförs i praktiken. Enligt nuvarande formuleringar uppfattar vi att kommunstyrelsen har det övergripande ansvaret för it-säkerheten men att servicenämnden har ansvar att upprätthålla säkerhetsnivåerna.

I de styrande dokumenten för informationssäkerhet framgår att it-avdelningen har ansvar för kommunens it-säkerhet med it-chef som ansvarig tjänsteperson vilken tillhör serviceförvaltningen. Om ansvar enligt reglementet ska upprätthållas ser vi behov av att det inom kommunstyrelseförvaltningen tillsätts strategisk it-kompetens med ansvar att fastställa övergripande it-säkerhetsnivåer.

Med nuvarande organisering efterlevs inte reglementet avseende ansvar för drift av it-system och tjänster samt att beslutad nivå avseende it-säkerhet inte upprätthålls. Detta då it-avdelningen inom serviceförvaltningen inte ansvarar för klienter och plattform som nyttjas inom förskole- och grundskolenämnden och utbildnings- och arbetsmarknadsnämnden. Vi kan vi inte utesluta att det finns risk för dubbelarbete och

suboptimering samt att implementationer och funktioner för stärkt it-säkerhet inte kan nyttjas fullt ut i hela kommunen. Vi bedömer att kommunstyrelsen behöver utvärdera organisation och förutsättningar för arbetet. Om organisationen anses ändamålsenlig, ser vi behov av att reglementen revideras och att gränsdragning för ansvaret tydliggörs mellan kommunstyrelsen, servicenämnden, förskole- och grundskolenämnden samt utbildnings- och arbetsmarknadsnämnden.

Kommunstyrelsen har i enlighet med rekommendationer från MSB utsett en informationssäkerhetsstrateg med uppdrag att leda och samordna det kommunövergripande informationssäkerhetsarbetet. Vår uppfattning är att nuvarande organisering medfört att kommunstyrelsen stärkt förmågan att leda och vara kravställare i det övergripande informationssäkerhetsarbetet.

Vi uppfattar att nämnderna har behov av stöd för att informationssäkerhetsarbetet ska vara systematiskt, varpå kommunstyrelsen bör utvärdera om nuvarande resurser har förutsättningar att möta de behov som finns. Vidare ser vi att det inom socialnämnden och utbildnings- och arbetsmarknadsnämnden finns risk att nuvarande resurser inte är anpassade efter den omfattning och krav som ställs på informationssäkerhetsarbetet inom respektive nämnd, varför vi bedömer nämndernas organisationer för informationssäkerhetsarbetet som icke ändamålsenliga.

3.3 Informationssäkerhet

3.3.1 Riskbedömning och informationsklassning

Av lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster framgår att leverantör av samhällsviktiga tjänster ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete avseende nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster. Utifrån detta har MSB rekommendationer avseende säkerhetsåtgärder i syfte att öka skyddet mot angrepp eller minimera eventuell skada. Rekommendationerna omfattar bland annat säkerhetsuppdateringar, säkerhetskopiering samt förmågan att upptäcka säkerhetshändelser.

3.3.1.1 Riskanalys

Informationssäkerhetsrisker ska, enligt intervjuuppgifter, ha identifierats inom ramen för den kommunövergripande risk- och sårbarhetsanalysen. Därtill finns enligt utsago ett upprättat dokument där olika informationssäkerhetsrisker sammanställts, dock framgår av intervjuade att det inte är i form av en regelrätt riskanalys.

Gällande riskanalyser för enskilda verksamhetssystem anges av informationssäkerhetsinstruktionen för it-nära förvaltning att it-säkerhetssamordnare ansvarar för att leda eller delta i dessa.

Vår samlade bild från intervjuer med berörda förvaltningar är att det finns en upplevelse att arbetet med riskanalyser behöver utvecklas. Arbetet sker enligt uppgift inte strukturerat och inte heller regelbundet samt så dokumenteras det inte i tillräckligt hög grad i nuläget.

3.3.1.2 *Informationsklassning*

Av informationssäkerhetsinstruktionen för verksamhetsnära förvaltning konstateras att systemägare inom den verksamhet som nyttjar systemet, utifrån genomförd informationsklassning, beslutar om adekvat skyddsnivå. Skyddsåtgärder ska även dokumenteras i en förvaltningsplan och hållas aktuella under hela systemets livscykel.

För genomförandet av informationsklassningar har kommunen en etablerad modell som redovisas i riktlinjen för informationssäkerhet.

Vår bild är att informationsklassningar tidigare genomfördes mer konsekvent och under ledning av it-avdelningens medarbetare. Sedan ansvaret för att tillse informationsklassningar har överförts till systemansvariga inom respektive förvaltning finns en upplevelse att momenten inte genomförs i samma utsträckning. För flera prioriterade system saknas även förvaltningsplaner, det vill säga dokumentation som redogör för viktiga uppgifter om systemet, gällande avtal, förvaltningsansvariga, driftaktiviteter etc.

Det finns en uttalad ambition att informationsklassningar ska genomföras inför upphandling av nya system, vilket ofta sker, men inte alltid. Vi uppfattar också att informationsklassningar inte involverar it-medarbetare konsekvent, och att det medfört att implementering av nödvändiga säkerhetsåtgärder dröjer. Ibland renderar det även extra kostnader då redan inköpta produkter behöver kompletteras med ytterligare skyddsfunktioner efter att it-avdelningen säkerhetsutvärderat produkterna.

Bland granskade nämnder har förskole- och grundskoleförvaltningen informationsklassat befintliga system och utifrån detta vidtagit skyddsåtgärder.

Socialförvaltningen och utbildnings- och arbetsmarknadsförvaltningen har informationsklassat de mest kritiska systemen. Anledningar som nämns till varför inte samtliga system klassats är resursbrist och att berörda inväntar ett nytt klassningsverktyg som ska implementeras. I detta sammanhang ser vi också en variation mellan nämnderna avseende vilken klassningsmodell som används, och vilka funktioner som deltar vid momenten.

3.3.2 Bedömning

Vi bedömer att det inom kommunstyrelsen och granskade nämnder endast delvis finns ett systematiskt arbete med riskanalyser och informationsklassning.

Det finns en beslutad systematik för riskanalyser och informationsklassningar men vi uppfattar att dessa moment inte genomförts i den omfattning som styrande dokument kravställer. Det innebär att det i nuläget inte finns tillräckliga underlag som visar vilka behov av tekniska säkerhetsåtgärder som behövs för att skydda kommunens informationstillgångar.

Kommunövergripande riskanalys som identifierar risker och hot som kommunens samlade it-miljö är exponerad för saknas i nuläget. Vi har inte heller tagit del av några förvaltningsspecifika riskanalyser.

Bland granskade nämnder uppfattar vi att tillvägagångssätt vid informationsklassningar varierar men att förskole- och grundskolenämnden har en högre grad av systematik i

genomförande av informationsklassningar. Vi bedömer att kommunstyrelsen genom en stärkt intern kontroll behöver säkerställa att styrande dokument efterlevs. Dels avseende att beslutad modell för klassning används av samtliga verksamheter, dels gällande att resurs med it-säkerhetskompetens involveras så att it-säkerhetsperspektivet beaktas i tillräcklig utsträckning i samband med riskbedömningar.

3.4 Informationssäkerhetsmål och handlingsplaner

Av instruktionen för ledningssystemet för informationssäkerhet framgår att kommunens informationssäkerhetsgrupp arbetar fram inriktningsmål avseende informationssäkerhet. Dessa fastställs sedan av kommunledningen. Förvaltningarna ska planera för åtgärder i syfte att nå målen. Åtgärderna ska dokumenteras i en handlingsplan.

Vi har tagit del av den senaste LIS-rapporten, en sammanställning över kommunens informationssäkerhetsarbete som rapporteras till kommunstyrelsen och tjänstepersonledningen. Rapporten redovisar inte uttryckligen de mål som satts för arbete, däremot framgår målsättningar med att systematisera informationssäkerhetsarbetet. Intervjuade uppger att målen, från och med 2024, ska presenteras separat och med tillhörande handlingsplaner.

3.4.1 Bedömning

Vår bedömning är att det inte finns beslutade informationssäkerhetsmål med tillhörande handlingsplaner.

Av LIS-rapporten framgår kommunens målsättning att systematisera informationssäkerhetsarbetet. För att i ökad omfattning kunna följa upp och styra arbetet anser vi att tydliga mål behöver formaliseras.

3.5 Säkerhetskultur

Enligt instruktionen för ledningssystemet för informationssäkerhet ska riktade utbildningsinsatser genomföras för olika målgrupper baserat på verksamhetsspecifika behov. Utbildningsinsatserna ska också sammanställas i LIS-rapporten och redovisas i förhållande till utfall av dessa.

I LIS-rapporten konstateras att utbildningar inte genomförts i enlighet med styrande dokument. Hittills har utbildning getts till förvaltningarnas informationssäkerhetssamordnare. Enstaka kunskapshöjande insatser har även gjorts i form av informationskampanjer på intranät och personalmöten samt att it-avdelningen skickat ut fiktiva nätfiskemejl för att testa användarnas säkerhetsmedvetenhet. Uppföljning av testerna har påvisat behov av utbildning och enligt uppgifter i intervju ska kommunen upphandla en extern utbildningstjänst från årsskiftet 2023/2024.

Förskole- och grundskoleförvaltningen har som enda revisionsobjekt genomfört förvaltningsinterna utbildningsinsatser mot rektorer och administratörer på kommunens skolenheter. Generellt beskrivs kunskapsnivån inom granskade nämnder som varierande och minskande ju längre ut i kärnverksamheterna som medarbetarna finns.

3.5.1 Bedömning

Vi bedömer att kommunstyrelsen, socialnämnden och utbildnings- och arbetsmarknadsnämnden inte tillsett en tillräcklig säkerhetskultur. Vi bedömer att förskole- och grundskolenämnden delvis har tillsett en tillräcklig säkerhetskultur.

Styrande dokument ställer krav på riktade utbildningsinsatser för olika målgrupper utifrån verksamhetens behov. Vi konstaterar att det endast är förskole- och grundskoleförvaltningen som har genomfört utbildningsinsatser inom informationssäkerhet men att det inte kan säkerställas att dessa är tillräckliga i syfte att uppnå en tillräcklig säkerhetskultur.

I övriga verksamheter har utbildningsinsatser inte genomförts i enlighet med kraven i styrande dokument. Vi bedömer att de insatser som genomförts på övergripande nivå i form av information inte är tillräckliga för att etablera en säkerhetskultur. Vi ser därför en risk att det finns en bristande kunskap och medvetenhet om informationssäkerhet och tillhörande hot och risker vilket kan innebära en risk att information inte hanteras korrekt och säkert eller att incidenter kan ske.

3.6 It-säkerhet

3.6.1 Implementerade säkerhetsåtgärder

Av instruktionen för informationssäkerhet i it-nära förvaltning regleras it-säkerhetsmässiga åtgärder som ska gälla för it-miljön. Här framgår också att komponenter inom den gemensamma it-miljön ska klassificeras enligt kommunens etablerade modell för informationsklassning i syfte att kunna vidta tillbörliga skyddsåtgärder.

Vi har i granskningen fått en detaljerad beskrivning av de tekniska säkerhetsåtgärder som kommunens it-avdelning har etablerat. Med hänsyn till att alltför detaljerad information om etablerade säkerhetsåtgärder kan utgöra en sårbarhet för kommunen väljer vi att översiktligt konstatera att dessa har etablerats utifrån en prioritering och i förhållande till de krav som ställs i beslutad standard för informationssäkerhet och säkerhetsåtgärder. Vi ser även att nuvarande säkerhetsåtgärder i stort är överensstämmande med åtgärder som Myndigheten för samhällsskydd och beredskaps rekommenderar för stärkt cyberförsvar.

Enligt MSB:s rekommendationer är behörighetshantering ett väsentligt område att prioritera för att upprätthålla cyberförsvar. Intervjuade beskriver att kommunen identifierat vissa sårbarheter i nuvarande behörighetshantering vilket behöver åtgärdas. Dels finns system med konstaterat viktiga informationstillgångar där informationsklassning identifierat behov av multifaktorsautentisering, men där det inte kan införas på grund av att systemet är föråldrat och saknar tekniska förutsättningar. Kommunens lösenordspolicy[10] innehåller inte heller någon konkret kravställning avseende teckenvariation eller längd vilket kan riskera att alltför enkla lösenord används som skulle kunna innebära ökad risk för externa angrepp. Enligt intervjuade

[10] Instruktion för informationssäkerhet till medarbetare, daterad 2021-10-19

pågick vid genomförandet av granskningen arbete med att stärka åtkomst- och behörighetshantering.

Intervjupersoner har beskrivit att it-avdelningen arbetar kontinuerligt med olika vedertagna kontrollsystem för att utvärdera och säkerställa att etablerade åtgärder motsvarar aktuell riskbild gällande it- och cybersäkerhetshot. Ett av verktygen som används är en årlig it-säkerhetsanalys enligt ett internationellt säkerhetsramverk[11] som kravställts i instruktionen för ledningssystemet. Resultatet från mätningen visar nivån på it-säkerhetsåtgärder och dokumenteras och resulterar i handlingsplaner per mätområde.

Vid sidan av ovan nämnda kontroller som har betoning på mer strategisk utvärdering av it-säkerhetsåtgärder genomför it-avdelningen regelbundna penetrationstester i syfte att identifiera eventuella säkerhetsbrister i befintliga säkerhetsåtgärder.

3.6.2 Implementerade säkerhetsåtgärder för elev- och pedagogklienter inom förskole- och grundskoleförvaltningen samt utbildnings- och arbetsmarknadsförvaltningen

Som vi beskrev tidigare i rapporten använder elever och lärare inom grundskola samt elever och vissa lärare inom gymnasieskola personliga datorer i lärandesyfte. Den tekniska lösningen innebär att programvara och datorer är av andra sorter än vad som används i övriga kommunen. Däremot har användarna samma typ av e-postkonto och användaruppgifter för inloggning i program som används inom övriga kommunen, och som administreras av it-avdelningen. Genom detta täcks användarkontona av samma automatiska kontroller som är gällande för samtliga användare inom kommunen. Om säkerhetssystemet upptäcker något avvikande mönster kring ett konto stängs det automatiskt. Utöver detta omfattas klienterna av leverantörernas säkerhetsåtgärder där nivå på detta avtalats särskilt.

Klienterna är uppkopplade mot kommunens gemensamma nätverk, men som nämnts tidigare ingår de i övrigt inte i den gemensamma it-miljön. De nätverk som klienterna är uppkopplade mot har isolerats från kommunens övriga nätverk, vilket innebär att spridning av eventuella virus avgränsas.

Vi har tagit del av en av de årliga it-säkerhetsanalyser[12] som kommunen genomför regelbundet, vilken genomförts med avseende på just elev- och lärarklienterna. Analysen identifierar ett antal säkerhetsrisker, främst kopplat till vissa av de klienter som används inom utbildnings- och arbetsmarknadsförvaltningen. För samtliga typer av klienter konstateras att säkerheten i stor utsträckning är beroende av plattformsleverantörens kontroll.

Intervjuade företrädare för förskole- och grundskoleförvaltningen framför att säkerhetsgenomlysningarna utgör grund för kontinuerlig it-säkerhetsutveckling, och att det begränsade antalet incidenter som inträffar indikerar att lösningen har tillräcklig säkerhet. Vidare uppges att den största risken är säkerheten kring användarkonton eftersom det finns cirka åttatusen elevkonton vilket försvårar arbetet med att

[11] CIS Controls
[12] CIS-analys Varbergs kommun: skola, daterad 2021-10-14

säkerställa att de hanteras korrekt av användarna. Att användarkontona omfattas av it-avdelningens säkerhetslösning ses därför som en avgörande förutsättning.

Företrädare för it-avdelningen framhåller att de externa kontrollerna visar att elev- och pedagogklienterna utgör en it-säkerhetsrisk gällande kommunens samlade it-miljö. När it-avdelningen genomför säkerhetshöjande åtgärder för den gemensamma infrastrukturen konstateras att motsvarande åtgärder inte implementeras på elev- och pedagogklienter.

3.6.3 Bedömning

Vi gör bedömningen att tekniska säkerhetsåtgärder i allt väsentligt har vidtagits som står i relation till aktuella hot och risker, samt att etablerade säkerhetsåtgärder utvärderas regelbundet för att fastställa att de fungerar ändamålsenligt.

Baserat på den redogörelse som vi fått avseende etablerade säkerhetsåtgärder bedömer vi att kommunstyrelsen vidtagit åtgärder som skyddar kommunens it-miljö mot aktuella risker och hot. Vi konstaterar också att tekniska säkerhetsåtgärder utvärderas systematiskt.

Vi ser dock att kommunen bör överväga att stärka både rutiner och tekniska implementationer avseende åtkomst- och behörighetshantering då användarkonton och lösenord är särskilt utsatta vid externa angrepp. I samma avseende bedömer vi att kommunstyrelsen behöver tydliggöra krav för livscykelhantering så att inte it-miljön riskerar att vara föråldrad och hindra att tekniska säkerhetsfunktioner kan nyttjas till fullo.

Avseende förskole- och grundskolenämndens och utbildnings- och arbetsmarknadsnämndens elev- och pedagogklienter konstaterar vi att sårbarheter har identifierats i genomförda säkerhetsanalyser. Därav bedömer vi att nämnderna behöver följa upp resultatet i analyser och utvärdera nuvarande skyddsnivåer. Detta då hanteringen av dessa klienter inte ligger inom kommunstyrelsens ansvarsområde.

3.7 Övervakning och säkerhetsloggar

Grundläggande krav för loggning och övervakning framgår av instruktionen för informationssäkerhet i it-nära förvaltning. Dokumentet reglerar även frekvens för säkerhetskopiering. Däremot framgår inte vilken funktion som ansvarar för loggning.

Vi delges att kommunen har implementerat en teknisk lösning som övervakar den gemensamma it-miljön i syfte att detektera eventuella intrångsförsök. I händelse av intrång larmas it-avdelningen genom kommunens ordinarie ärendehanteringssystem. Inträffade händelser samlas i en händelselogg som it-säkerhetssamordnare har uppsikt över.

En sårbarhet som konstateras är att övervakning endast sker vardagar under kontorstid. En informell överenskommelse har fattats om att tekniker från it-avdelningen kan kontaktas under kvällar och helger, men faktisk beredskap utanför kontorstid saknas.

3.7.1 Bedömning

Vår bedömning är att kommunstyrelsen i allt väsentligt har etablerat en tillräcklig övervakning för att upptäcka hot om intrång eller andra säkerhetsincidenter i it-miljön genom tekniska verktyg och funktioner.

Vi bedömer att det kan finnas behov av att utreda förutsättningarna för beredskap utanför kontorstid i syfte att stärka kommunens robusthet vad gäller förmåga att hantera intrång och andra säkerhetsincidenter.

3.8 Incidenthantering

Av lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster framgår att leverantör av samhällsviktiga tjänster ska vidta lämpliga åtgärder för att förebygga och minimera verkningar av incidenter som påverkar nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster. Åtgärderna ska syfta till att säkerställa kontinuiteten i tjänsterna.

I medarbetarinstruktionen för informationssäkerhet exemplifieras innebörden av informationssäkerhets- och it-säkerhetsincidenter. Här framgår att it-säkerhetsincidenter ska anmälas till it-support samt hur GDPR-incidenter ska anmälas. Informationssäkerhetsincidenter nämns inte.

Vi har tagit del av ett antal instruktioner som reglerar incidenthanteringsprocessen, både på kommunövergripande nivå och internt på it-avdelningen. Genom intervju uppfattar vi att dokumenten används operativt. Av dokumenten framgår att it-avdelningen har uppföljningsansvar för incidenter. Utifrån hantering av en tidigare inträffad incident har rutinerna konstaterats vara i behov av utveckling.

De nämnder som vi har granskat saknar interna incidenthanteringsrutiner, med undantag av socialförvaltningen som har tagit fram rutiner för personuppgiftsincidenter, vilka vi tagit del av, samt skapat en e-tjänst för anmälan av dylika incidenter. Vi uppfattar att medarbetare har god kännedom om personuppgiftsincidenter, men att kunskapen om vad som är en informationssäkerhetsincident är lägre. Nämnderna har också få anmälda informationssäkerhetsincidenter och flera intervjuade förvaltningsrepresentanter uttrycker behov av att klargöra vad som är en incident och hur dessa ska hanteras.

3.8.1 Bedömning

Vi bedömer att det endast delvis finns incidenthanteringsrutiner som inkluderar krav på hur incidenter ska dokumenteras och följas upp.

Vi konstaterar att det finns en övergripande incidenthanteringsrutin med tydliga eskaleringsvägar som också reglerar uppföljning av incidenter. Likaledes bedömer vi att it-avdelningen har upprättat erforderliga interna incidenthanteringsrutiner, som också utvärderats i praktiken.

Beträffande granskade nämnder ser vi att endast socialnämnden har en etablerad incidenthanteringsrutin. Vår bedömning är följaktligen att övriga nämnder behöver

dokumentera motsvarande rutiner, samt att utbildningsinsatser genomförs där informationssäkerhetsincidenter förklaras och anmälningsförfarande tydliggörs.

3.9 Reserv- och återgångsrutiner

Instruktionen för ledningssystemet för informationssäkerhet anger att det finns en kommungemensam plan för kontinuitetshantering och övning ur ett beredskapsperspektiv. Som komplement till den ska it-avdelningen upprätta ett internt dokument för roller och ansvar i händelse av avbrott eller annan störning. Därtill ska återställningsplaner för samtliga system som hanterar information finnas, enligt instruktionen för informationssäkerhet i it-nära förvaltning.

Utifrån intervjuuppgifter har vi uppfattat att nämnda planer saknas. Arbete med att ta fram återställningsplaner per system inleddes för en tid sedan, men har inte slutförts.

Verksamheterna i granskade nämnder har gjort viss kontinuitetsplanering där kritiska system har identifierats och delvis prioriterats utifrån vilka som är viktigast att återstarta vid avbrott. Verksamheterna saknar emellertid dokumentation över prioriterade system, liksom reserv- och återgångsrutiner per system. Flera intervjuade verksamhetsföreträdare anser att både it-avdelningen och förvaltningarna skulle vara betjänta av dokumenterade överenskommelser om servicenivåer som reglerar tidsfrist för återstart av system, då det skulle bidra till samsyn kring behov och driftleverans. Vidare framgår från intervjuade att det behöver tydliggöras var ansvaret för kontinuitetsplaneringen ligger, då det enligt uppgift förekommer en uppfattning att detta ansvar tillhör it-avdelningen, vilket i själva verket åligger berörd verksamhet.

3.9.1 Bedömning

Vi gör bedömningen att det inte finns dokumenterade reserv- och återgångsrutiner vid allvarligare störningar och avbrott i it-system.

Det saknas kommunövergripande reservrutiner, vilket inte heller kravställts i några styrande dokument. Vi anser att en övergripande kontinuitetsplan är nödvändig för att säkerställa att väsentlig funktionalitet prioriteras i händelse av större avbrott. För en ändamålsenlig kontinuitetsplan är definierade servicenivåer en god vägledning.

Vi konstaterar att arbetet med återställningsplaner för system inte följer vad som anges av styrande dokument. Vi ser det som en brist i förhållande till att planerna är väsentliga underlag i händelse av avbrott.

Avsaknad av nämnda underlag föranleder att tester inte genomförts.

Avseende granskade nämnder är vår bedömning att den prioritering av system som nämnderna gjort behöver sammanställas och dokumenteras i förvaltningsinterna prioriteringslistor samt även kommuniceras till it-avdelningen.

3.10 Uppföljning och återrapportering

3.10.1 Uppföljning

Av riktlinjer för informationssäkerhet framgår att samtliga nämnder ska säkerställa lämpliga kontrollpunkter för informationssäkerhetsarbetet. Enligt intervjuuppgifter har granskade nämnder återrapportering av dataskyddsfrågor, men specifik rapportering av informationssäkerhetsfrågor saknas. Kravställda kontrollpunkter för informationssäkerhetsarbetet saknas också.

För att ledningen på strategisk nivå ska få en samlad bild och kunskap om informationssäkerhetsarbetet i organisationen behöver det ske en övergripande uppföljning av arbetet som sedan rapporteras under ledningens genomgång, enligt MSB:s metodstöd. Uppföljningen utgör även underlag för eventuella beslut på strategisk nivå angående åtgärder och resursfördelning. Resultatet från ledningens genomgång ska dokumenteras och bevaras.

I Varbergs kommun ska ledningens genomgång sammanställas en gång om året, enligt instruktionen för ledningssystem för informationssäkerhet. I samband med det ska fastställda inriktningsmål avseende informationssäkerhet följas upp och utvärderas. Utöver ledningens genomgång ska informationssäkerhetsstrategen sammanställa en årlig LIS-rapport som ska delges kommunens förvaltningschefer.

Vi har tagit del av ledningens genomgång som rapporterades till kommunstyrelsen i juni 2023. Genomgången utgjordes av samma LIS-rapport som delges förvaltningschefer. Rapporten ger en överblick över nuläge och gångna årets arbete. Den inkluderar även en redogörelse av it-säkerhetsarbetet och it-säkerhetsincidenter, vilket kravställs av instruktionen för informationssäkerhet i it-nära förvaltning.

Därutöver har informationssäkerhetsarbetet översiktligt rapporterats till kommunstyrelsens arbetsutskott vid något enstaka tillfälle under året. Uppfattningen från berörda tjänstepersoner är att kommunstyrelsen har förtroende för det arbete som görs och för att adekvata beslut fattas av tjänstepersonerna.

Som ytterligare uppföljning av informationssäkerhetsarbetet ska kommunen en gång vart annat år genomföra Myndigheten för samhällsskydd och beredskaps ”Infosäkkollen[13]”, enligt instruktionen för ledningssystemet för informationssäkerhet. Syftet uppges vara att kartlägga aktuell status på informationssäkerhetsarbetet. Resultaten från samtliga aktiviteter ska sammanställas i en rapport vilken också ska innehålla förslag på åtgärder baserat på identifierade förbättringsområden. Vi har tagit del av Infosäkkollen som genomfördes hösten 2023 och konstaterar att den innehåller en analys över status på kommunens informationssäkerhetsarbete.

[13] Ett verktyg för offentlig sektor framtaget av Myndigheten för samhällsskydd och beredskap. Verktyget kartlägger status på informationssäkerhetsarbetet hos den enskilda organisationen och jämför resultatet mot andra offentliga organisationer. Källa: Instruktioner för informationssäkerhet med dataskydd.

3.10.2 Bedömning

Vår bedömning är att det i allt väsentligt finns en etablerad uppföljning av informations- och it-säkerhetsarbetet, och att det rapporteras regelbundet till kommunstyrelsen.

Vi noterar att Ledningens genomgång har genomförts där en samlad uppföljning av kommunens informationssäkerhetsarbete finns och att denna har rapporterats till kommunstyrelsen samt till kommunens förvaltningschefer.

Med anledning av omvärldsläge och förhöjd risk för cyberhot och it-incidenter bör kommunstyrelsen fortsätta att efterfråga kontinuerlig återrapportering avseende aktuella hot och risker tillsammans med kommunens förutsättningar och beredskap för att hantera allvarliga it-säkerhetshändelser.

Vi bedömer att granskade nämnder bör ta fram kontrollpunkter för informationssäkerhetsarbetet, i enlighet med styrande dokument, samt följa upp dessa.

4 Samlad bedömning och rekommendationer

Syftet med granskningen har varit att bedöma om kommunstyrelse och nämnder i Varbergs kommun bedriver ett systematiskt informationssäkerhetsarbete så att det sker på ett ändamålsenligt sätt.

Vår samlade bedömning utifrån granskningens syfte är att kommunstyrelse och nämnder delvis bedriver ett systematiskt och ändamålsenligt informationssäkerhetsarbete.

Kommunen har upprättat ett ledningssystem med processer, dokument och roller som utgör strukturell grund för ett systematiskt informationssäkerhetsarbete. Ledningssystemet hade inte implementerats fullt ut då granskningen genomfördes, men vi bedömer att kommunen på övergripande nivå har skapat organisation och struktur för ett systematiskt informations- och it-säkerhetsarbete.

Vi konstaterar att nämnderna utsett funktioner och i vissa delar en organisation men att det finns en variation över förutsättningar för att bedriva ett operativt informations-säkerhetsarbete på ett systematisk vis. Det finns även behov av stöd och kompetens för att genomföra arbetet vilket behöver anpassas efter de behov som nämnderna har.

Att samtliga verksamheter bedriver ett arbete i enlighet med beslutade styrdokument är väsentligt för att it-säkerhetsarbetet ska kunna utföras korrekt och utifrån tillräckliga underlag. Detta då säkerhetsåtgärder ska baseras på resultatet av riskanalyser och informationsklassningar för de informationstillgångar som hanteras i kommunen och relevanta skydd kan implementeras.

Utifrån resultatet av vår granskning rekommenderar vi kommunstyrelsen att:

- Utvärdera om nuvarande resurser för det informationssäkerhetsarbete som bedrivs inom respektive förvaltning har förutsättningar att möta de behov som finns
- Utvärdera organisation och förutsättningar för förskole- och grundskoleförvaltningens respektive utbildnings- och arbetsmarknadsförvaltningens hantering av elev- och pedagogklienter. Samt om hanteringen anses ändamålsenlig, förtydliga ansvar och gränsdragning i reglementen
- Förtydliga kommunstyrelsens och servicenämndens reglementen avseende ansvar för det strategiska it-säkerhetsarbetet. Samt om ansvar tillfaller kommunstyrelsen, tillse att det finns en samordnande it-säkerhetsfunktion inom kommunstyrelseförvaltningen
- I kommunövergripande riskanalyser inkludera och dokumentera informationssäkerhetsrisker (inklusive it- och cybersäkerhet) och tillse att beslut om åtgärder vidtas för att nå en rimlig riskacceptans
- Stärka den interna kontrollen av att styrande dokument efterlevs i syfte säkerställa att riskbedömningar och informationsklassningar samt upprättande av återställningsplaner genomförs i enlighet med styrande dokument

- Säkerställa att dokumentation från riskbedömningar och informationsklassningar utgör underlag och krav för etablering av kompletterande säkerhetsåtgärder
- Formalisera mål för informationssäkerhetsarbetet
- Tillhandahålla utbildningsinsatser avseende informationssäkerhet
- Se över lösenordspolicyn
- Överväga att stärka rutiner och tekniska implementationer avseende åtkomst- och behörighetshantering
- Förtydliga krav för livscykelhantering
- Utreda förutsättningarna för övervakning av och beredskap för oönskade händelser avseende it-miljön utanför kontorstid
- Ta fram en övergripande kontinuitetsplan

Utifrån genomförd granskning rekommenderar vi förskole- och grundskolenämnden att:

- Säkerställa att informationssäkerhetsrisker för nämnden inkluderas i en årlig riskbedömning då samtliga verksamheter ingår i en gemensam infrastruktur vilket kan innebära en ökad sårbarhet i händelse av allvarligare it-incident
- Följa upp genomförda it-säkerhetsanalyser i syfte att säkerställa en ändamålsenlig hantering av elev- och lärarklienter
- Upprätta en intern incidenthanteringsrutin
- Ta fram kravställda återställningsplaner för verksamhetssystem
- Dokumentera en lista över prioritering av system samt kommunicera denna till it-avdelningen
- Ta fram kravställda kontrollpunkter för informationssäkerhetsarbetet och tillse uppföljning av dessa

Utifrån genomförd granskning rekommenderar vi socialnämnden att:

- Säkerställa att organisation för informationssäkerhetsarbetet motsvarar det arbete som ska genomföras
- Säkerställa att informationssäkerhetsrisker för nämnden inkluderas i en årlig riskbedömning då samtliga verksamheter ingår i en gemensam infrastruktur vilket kan innebära en ökad sårbarhet i händelse av allvarligare it-incident
- Tillse förutsättningar för att genomföra systematiska informationsklassningar av befintliga och kommande verksamhetssystem
- Inkludera informationssäkerhetsincidenter i rutinerna för personuppgiftsincidenter
- Ta fram kravställda återställningsplaner för verksamhetssystem
- Dokumentera en lista över prioritering av system samt kommunicera denna till it-avdelningen
- Ta fram kravställda kontrollpunkter för informationssäkerhetsarbetet och tillse uppföljning av dessa

Utifrån genomförd granskning rekommenderar vi utbildnings- och arbetsmarknadsnämnden att:

- Säkerställa att organisation för informationssäkerhetsarbetet motsvarar det arbete som ska genomföras
- Följa upp genomförda it-säkerhetsanalyser i syfte att säkerställa en ändamålsenlig hantering av elev- och lärarklienter
- Säkerställa att informationssäkerhetsrisker för nämnden inkluderas i en årlig riskbedömning då samtliga verksamheter ingår i en gemensam infrastruktur vilket kan innebära en ökad sårbarhet i händelse av allvarligare it-incident
- Tillse förutsättningar för att genomföra systematiska informationsklassningar av befintliga och kommande verksamhetssystem
- Upprätta en intern incidenthanteringsrutin
- Ta fram kravställda återställningsplaner för verksamhetssystem
- Dokumentera en lista över prioritering av system samt kommunicera denna till it-avdelningen
- Ta fram kravställda kontrollpunkter för informationssäkerhetsarbetet och tillse uppföljning av dessa

5 Bilaga A

Som revisionskriterium i granskningen utgår vi från MSB:s metodstöd och rekommendationer för ett systematiskt informationssäkerhetsarbete och säkerhetsåtgärder med fokus på nedanstående områden.

Standard och krav

Metodstödet bygger på de internationella standarderna för informationssäkerhet i ISO/IEC 27000-serien och då främst på SS-EN ISO/IEC 27001 och SS-EN ISO/IEC 27002 om ledningssystem för informationssäkerhet.

Ledningssystem för informationssäkerhet

Ett ledningssystem för informationssäkerhet (ofta förkortat LIS) är den del av ledningssystemet som styr verksamhetens informationssäkerhet. För att informationssäkerhetsarbetet ska lyckas och vara framgångsrikt är det viktigt att informationssäkerheten integreras med de olika styrformerna, som planering och uppföljning. Det innebär till exempel att ledningen löpande informerar sig om informationssäkerhetsarbetet, gör regelbundna verksamhetsplaneringar och kontroller samt ser över styrdokumenten med jämna mellanrum.

Ledningen bör också se till att organisationen antar en policy för informationssäkerhetsarbetet. I ytterligare styrdokument, riktlinjer och liknande kan sedan den högsta ledningen ge vägledning till chefer och övriga medarbetare om vilka krav som ställs i arbetet. Det är viktigt att alla i en organisation känner till och förstår innehållet i policys och riktlinjer.

Ansvar och organisation

Metodstödet beskriver hur ansvaret för arbetet med informationssäkerhet bör fördelas i organisationen samt tydliggör betydelsen av ledningens förståelse och engagemang i informationssäkerhetsarbetet för att det ska lyckas. Det bör finnas en person inom organisationen med ansvar för att samordna informationssäkerhetsarbetet. Grundprincipen är att ansvaret för informationssäkerhetsarbete ska följa det ordinarie verksamhetsansvaret från ledning ner till enskilda medarbetare. Informationssäkerhetssamordnaren har därmed inget formellt ansvar för informationssäkerheten utan ska verka som ett stöd för att den övriga organisationen innefattande ledning, chefer och medarbetare tar sitt ansvar för informationssäkerhet i verksamheten. Det är viktigt att tydligt klargöra informationssäkerhetssamordnarens roll och vilket mandat och rapporteringsplikt som ska ingå i rollen.

Utbildning och kommunikation

MSB:s metodstöd ställer krav om ständig utbildning och kommunikation för att höja medvetenheten och kunskapen om informationssäkerhet. Utbildning och kommunikation ökar också acceptansen av och förståelsen för de säkerhetsåtgärder som implementeras.

Riskanalys och informationsklassning

Genom en riskanalys ska verksamheten identifiera de hot och oönskade händelser som kan leda till negativa konsekvenser för organisationen. Riskanalyser kan göras verksamhetsövergripande, för en process eller för ett enskilt objekt. Risker och potentiella händelser som kan leda till negativa konsekvenser beskrivs och bedöms sedan avseende sannolikheten att de inträffar samt potentiella konsekvenser.

Metodstödet anger vidare att informationsklassning är en förutsättning för att skapa rätt skydd för informationen som hanteras i respektive verksamhet. Med en gemensam klassningsmodell kan organisationens informationstillgångar skyddas utifrån interna och externa krav på informationens konfidentialitet, riktighet och tillgänglighet. Skyddsnivåerna beskriver säkerhetsåtgärder som informationens värde kräver. Identifierat behov av säkerhetsåtgärder utgör ett viktigt underlag vid exempelvis kravställning av tjänster, som interna och externa it¬-tjänster. De identifierade behoven av säkerhetsåtgärder bör dokumenteras i en åtgärdsplan. It-säkerhetsåtgärder rent tekniskt kan vara en del men klassningen kan även ha identifierat behov av kompletterande risk- och konsekvensanalyser, förbättrade rutiner eller andra åtgärder som bedöms nödvändiga för att säkerställa säkerheten för informationstillgångarna.

Skyddsåtgärder

Informationstillgångar består av information och resurser som används för att hantera information. Själva informationen är den primära tillgången som ska klassas. Resurser som används för att hantera informationen, till exempel it¬-system och fysiska tillgångar, samt rutiner i verksamheten ska sedan utformas enligt skyddsnivåer som matchar klassningens resultat. De resurser som hanterar informationen behöver därför skyddas på lägst den nivå som högst klassad information har.

I MSB:s föreskrift för säkerhetsåtgärder i informationssystem framgår att systemägaren behöver ha en dialog med berörda informationsägare inom organisationens olika verksamheter för att införa de säkerhetsåtgärder som ger rätt nivå av skydd för informationssystemet. Behovet av säkerhetsåtgärder identifieras utifrån de informationsklassningar och riskbedömningar som informationsägaren har genomfört, samt systemägarens egna riskbedömningar för informationssystemet.

MSB:s metodstöd beskriver att övervakning anger status för ett system, en process eller en aktivitet. Övervakning sker ofta kontinuerligt genom exempelvis att loggar i ett it-system övervakas och avvikelser automatiskt rapporteras. Övervakning och mätning görs för att bedöma om implementerade säkerhetsåtgärder har avsedd verkan och fungerar tillfredsställande.

Uppföljning och förbättringsarbete

För att ledningen på strategisk nivå ska få en samlad bild och kunskap om informationssäkerhetsarbetet i organisationen behöver det ske en övergripande uppföljning av arbetet som sedan rapporteras under ledningens genomgång. Uppföljningen utgör även underlag för eventuella beslut på strategisk nivå angående åtgärder och resursfördelning.

Resultatet från ledningens genomgång ska dokumenteras och bevaras.

Interna styrdokument

Enligt MSB bör ledningen se till att organisationen antar en policy för informationssäkerhetsarbetet. I ytterligare styrdokument, riktlinjer och liknande kan ledningen ge vägledning till chefer och övriga medarbetare över de krav och förhållningssätt som gäller i informationssäkerhetsarbetet.

I riktlinjer är det vanligt att det förs in bestämmelser om till exempel:

- användning av internet och e-post
- åtgärder till skydd mot skadlig kod
- fysisk säkerhet
- incidenthantering
- kontinuitetsplanering
- mobilt arbete
- inventarier och licenser
- behörighetsadministration
- loggning

Det är viktigt att alla i en organisation känner till och förstår innehållet i policys och riktlinjer. Erfarenheten visar tydligt vikten av att anställda uppvisar ett säkert beteende i sitt dagliga arbete.

Varbergs kommun
Granskning av it- och informationssäkerhet

2023-12-18

Datum som ovan

KPMG AB

DocuSigned by:
Jenny Thörn
E1872868AB3D4FC...

Jenny Thörn

Verksamhetsrevisor

DocuSigned by:
Sofie Ernerudh
74FAE6583E654B4...

Sofie Ernerudh

Verksamhetsrevisor