Granskning av cybersäkerhet
På uppdrag av de förtroendevalda revisorerna
Tyresö kommun

2019-02-14

Granskning av cybersäkerhet Tyresö Kommun

Februari 2019

Innehållsförteckning

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

1. Inledning

1.1. Bakgrund

I en allt mer digitaliserad omvärld blir områden som cybersäkerhet allt viktigare för en organisation. Intrång i IT- och informationssystem blir allt mer vanligt och utgör därför en central risk för en offentlig verksamhet, vilken handhar en mängd känslig information. Vidare föreligger risk att fel uppstår i kritiska processer om information inte är tillförlitlig eller saknas. Brister i det systematiska cybersäkerhetsarbetet innebär därmed risk för att obehöriga antingen kommer över känslig information eller att delar av kommunens verksamhet kan övervakas, skadas eller stängas ner.

De förtroendevalda revisorerna i Tyresö kommun har baserat på rådande riskbild beslutat att en granskning av kommunens arbete relaterat till cybersäkerhet är nödvändig. Med anledning av detta har EY på uppdrag av kommunens förtroendevalda revisorer genomfört en granskning av Tyresö kommuns arbete med cybersäkerhet.

1.2. Syfte

Syftet med granskningen är att ge en *övergripande* bild av Tyresö kommuns mognadsgrad inom området cybersäkerhet genom inhämtning av information, arbetsmöten och analys. Granskningen sker på uppdrag av kommunens förtroendevalda revisorer.

1.3. Avgränsning

De iakttagelser och rekommendationer som presenteras i denna rapport baseras därmed enbart på den information som inhämtats under intervjuer och genom granskning av erhållna dokument, såsom riktlinjer, rutiner och policys. Ingen teknisk analys eller testning har genomförts inom granskningens omfattning.

1.4. Metod

En så kallad Cybersecurity Program Assessment (CPA) har genomförts, vilket är EYs standardiserade ramverk och utarbetade metodologi för granskning och bedömning av mognadsgraden inom organisationers cybersäkerhet. Ramverket är även anpassat för offentlig verksamhet och baseras på den internationella standarden ISO27001. CPA innefattar tre nivåer med varierande detaljrikedom där nivå ett bedöms vara lämplig för övergripande granskning. CPA-ramverket omfattar analys av 20 områden som delas in i fyra huvudkategorier: Organisation och styrning, tekniska plattformar, dagligverksamhet och hotbildshantering. För Tyresö kommun har 18 områden granskats, då två områden bedöms vara utanför granskningens omfattning: mätvärden och rapportering, samt mjukvaruutveckling. Området mätvärden och rapportering är på en högre detaljnivå än vad omfattningen för denna granskning erfordrar och området mjukvaruutveckling bedöms irrelevant då ingen utveckling sker internt av kommunen.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

De 18 områdena som granskats inom uppdraget är:

Organisation och styrning

- Styrning och organisation
- Strategi
- Policy och standards
- IT-arkitektur
- Drift
- Medvetenhet

Tekniska plattformar

- Nätverkssäkerhet
- Serverhostsäkerhet
- Dataskydd

Daglig verksamhet

- Tillgångshantering
- Åtkomsthantering
- Tredjepartshantering
- Kontinuitetsplanering
- Integritet och säkerhet (personuppgifter)

Hotbildshantering

- Incidenthantering
- Hantering av sårbarheter
- Säkerhetsövervakning
- Hotbildsanalys

Mognadsgrad beskrivs på en standardiserad skala enligt nedan:

1. Begynnande – Det finns ingen dokumentation eller uppföljning, händelser hanteras ad hoc.
2. Upprepbar – Viss grundläggande dokumentation finns, men denna kan variera mellan olika enheter och vara bristfällig i sin omfattning och tillämpning.
3. Definierad – Det finns dokumenterade processer och dessa tillämpas i stor mån genom hela organisationen.
4. Förvaltad – Förutom väl dokumenterade processer som tillämpas i hela organisationen, finns det dessutom ett system för uppföljning.
5. Optimerad – Baserat på uppföljningen finns också rutiner för kontinuerlig förbättring och uppdatering av processer och ramverk.

Tyresö kommuns mognadsgrad har jämförts med god praxis, baserat på EYs CPA-ramverk på en definierad (3) nivå för en offentlig verksamhet av liknande storlek och med liknande karaktär som Tyresö kommun.

Inledningsvis har underlag såsom policys, strategi- och styrdokument och dylikt samlats in för att analyseras. Därefter hölls ett arbetsmöte där driftchef och IT-chef från kommunen deltog tillsammans med EYs cybersäkerhetsspecialister. Fokusområden under arbetsmötet var samtliga 18 områden. Efter att EY analyserat resultatet av arbetsmötet sammanställdes ett rapportutkast som diskuterades med kommunen. EY genomförde sedan justeringar och uppdateringar av rapporten,

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

varefter kommunen erhöll en slutlig rapport med övergripande rekommendationer för fortsatt arbete. Tidsplanen för arbetet såg ut enligt följande:

- December 2018 – Förberedelser, planering och insamling av dokumentation.
- Januari 2019 – Dokumentanalys, utförande av arbetsmöte (10e januari) samt granskning av kompletterande dokumentation och uppföljningsfrågor.
- Februari 2019 – Färdigställande av rapport, faktagranskning av kommunen, samt slutgiltig presentation för förtroendevalda revisorer.

1.5. Definitioner

Se bilaga 3.

1.6. Sekretess

Den detaljerade analysen av de 18 undersökta områdena bedöms innehålla känsliga uppgifter som riskerar att omfattas av sekretess. Denna information har förmedlats kommunen i en särskild rapport.

2. Slutsatser

Syftet med granskningen har varit att genomföra en övergripande kartläggning av mognadsgraden i Tyresö kommuns arbete med cybersäkerhet. Kommunen bedöms i relation till andra offentliga organisationer av liknande storlek i förhållande till antal anställda och övergripande verksamhet. Vår övergripande bedömning är att Tyresö kommun har en förhållandevis låg mognadsgrad, med ett snitt på 1,75, på en femgradig skala, men kommunen har ändå vissa tekniska lösningar och processer på plats för att hantera risker i IT-miljön. Mognadsgraden bedöms vara som högst inom drift, tredjepartsupphandling och nätverkshantering. Lägst är mognadsgraden inom hotbildshantering.

Kommunens största och viktigaste förbättringspunkter ligger i organisation, styrning och efterlevnad inom verksamheterna, samt inom hantering av hotbild och angrepp. Vidare finns ett behov av att införa processer för uppföljning inom i stort sett samtliga av de undersökta områdena.

2.1. Övergripande rekommendationer

Organisation och styrning

Tyresö kommun rekommenderas att inleda ett arbete med strategisk cybersäkerhet, som är förankrad från politisk nivå hela vägen ner i verksamheterna. Det bör sättas av pengar specifikt för cybersäkerhet, baserat på rådande situation och hotbild. Från central nivå bör det också följas upp att verksamheten efterföljer de regler och policys som är fastställda. Medarbetares bristande medvetenhet är en mycket vanlig källa till informationssäkerhetsrelaterade incidenter och därför rekommenderas obligatorisk utbildning av nyanställda samt vidareutbildning och uppföljning av

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

befintliga medarbetare. I denna utbildning bör också ingå att ta del av informationssäkerhetspolicyn.

Tekniska plattformar

Det bör implementeras strategier, policys och instruktioner som täcker hela kommunens användande av tjänster som nås via en uppkoppling till internet, så kallade molntjänster, till skillnad från system som ligger internt inom kommunen. Vidare bör ett kommunövergripande system användas för hantering av samtliga mobila enheter som används för att hantera verksamhetsinformation, exempelvis e-post. Detta system bör ha omgivande strategier, policys och instruktioner.

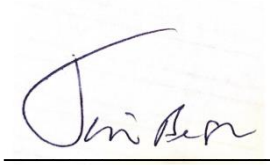
Daglig verksamhet

Åtkomsthanteringen bör kompletteras med regelbundna granskningar av användare, vilket är särskilt viktigt för konton med priviligierad behörighet. Vidare bör en process finnas där närmsta chef godkänner alla behörigheter enligt en formaliserad process med spårbarhet.

Hotbildshantering

Kommunen bör avsätta resurser för att regelbundet analysera hotbilden och upptäcka angrepp. Vissa angrepp kan ha som syfte att synas, men de som inte vill bli upptäckta kan ha långt värre konsekvenser. Vidare bör det planernas för hantering av cyberincidenter och planerna bör också övas i syfte att berörda ska vara väl insatta i sina uppgifter, samt utvärdera och förbättra planen baserat på övningserfarenheterna.

Stockholm den 7 februari



Tim Best, Partner, EY

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

3. Bilaga 1: Förteckning över intervjuade funktioner

- Driftschef
- IT-chef

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

4. Bilaga 2: Dokumentförteckning

- Informationssäkerhetspolicy 2018
- Informationssäkerhet instruktion användare 2018
- Lathund användare infosäk
- Diarieplan
- Handbok för hantering av allmänna handlingar
- Riktlinjer för e-posthantering i Tyresö kommun
- Så här behandlar vi dina personuppgifter (hemsida)
- Så här hanterar vi dina personuppgifter (hemsida)
- Här beskriver vi vad en personuppgiftsincident är
- Information till vårdnadshavare om personuppgiftsbehandling Grundskola
- Riktlinjer för riskhantering och internkontroll
- Riskhantering - gemensamma rutiner för Tyresö kommun 2016
- Tyresö kommun - Årlig utredning 2018
- Riktlinjer för användning av sociala medier i Tyresö kommun

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

5. Bilaga 3: Definitioner

Cybersäkerhet: Används i den här rapporten som ett paraplybegrepp för IT- och informationssäkerhet.

Informationssäkerhet: Berör i huvudsak säkerhetsfrågor som berör information, oberoende av system, eller plattformar.

IT-säkerhet: Säkerhet som huvudsakligen relaterar till IT-infrastruktur, systemfrågor och konfigurering.

Informationsklassning: Klassning av organisationens informationstillgångar enligt i riktlinjer dokumenterade regler med avseende på informationens sekretess, riktighet och tillgänglighet.

Informationsägare: Ansvarar för den verksamhet vars information ska hanteras. Äger och ansvarar för att informationen är riktig och tillförlitlig.

Molntjänster: Tjänster och system som inte drivs lokalt av kommunen och som nås via en internetuppkoppling och inte direkt via det lokala nätverket.

Personuppgiftsombud: Särskilt utsedd person vilken tillser att personuppgifter behandlas på korrekt och lagenligt sätt inom organisationen.

Policy och instruktion: Avser dokumentation av rutiner på ett eller annat sätt. I denna rapporten görs ingen skillnad på om dokumentationen är antagen på politisk eller tjänstemannanivå.

Strategi: Plan eller dokumentation av ett områdes framtida inriktning och prioritering, snarare än praktiska förhållningsregler.