# Genomgång cybersäkerhet

## Trelleborgshem

Januari 2020

pwc

# Introduktion

Denna rapport utgör en nulägesanalys som kartlägger nuvarande status inom cybersäkerhetsområdet där styrkor, förbättringsområden och rekommenderade åtgärdsförslag identifieras. Den tar såväl tekniska som organisatoriska säkerhetsåtgärder i beaktande, då båda dessa bör inkluderas i ett systematiskt säkerhetsarbete för att undvika att risker frånses.

Rekommendationerna bygger på PwC:s erfarenhet och expertis inom området och “best practices” inom cybersäkerhetsområdet. Våra slutsatser bygger på intervjuer med nyckelpersoner från den interna organisationen med god insyn i Trelleborgshems cybersäkerhetsarbete samt bolagets huvudsakliga IT-leverantör, Trelleborgs Kommun. Datainsamlingen har varit avgränsad till intervjuer.

Följande funktioner har intervjuats:

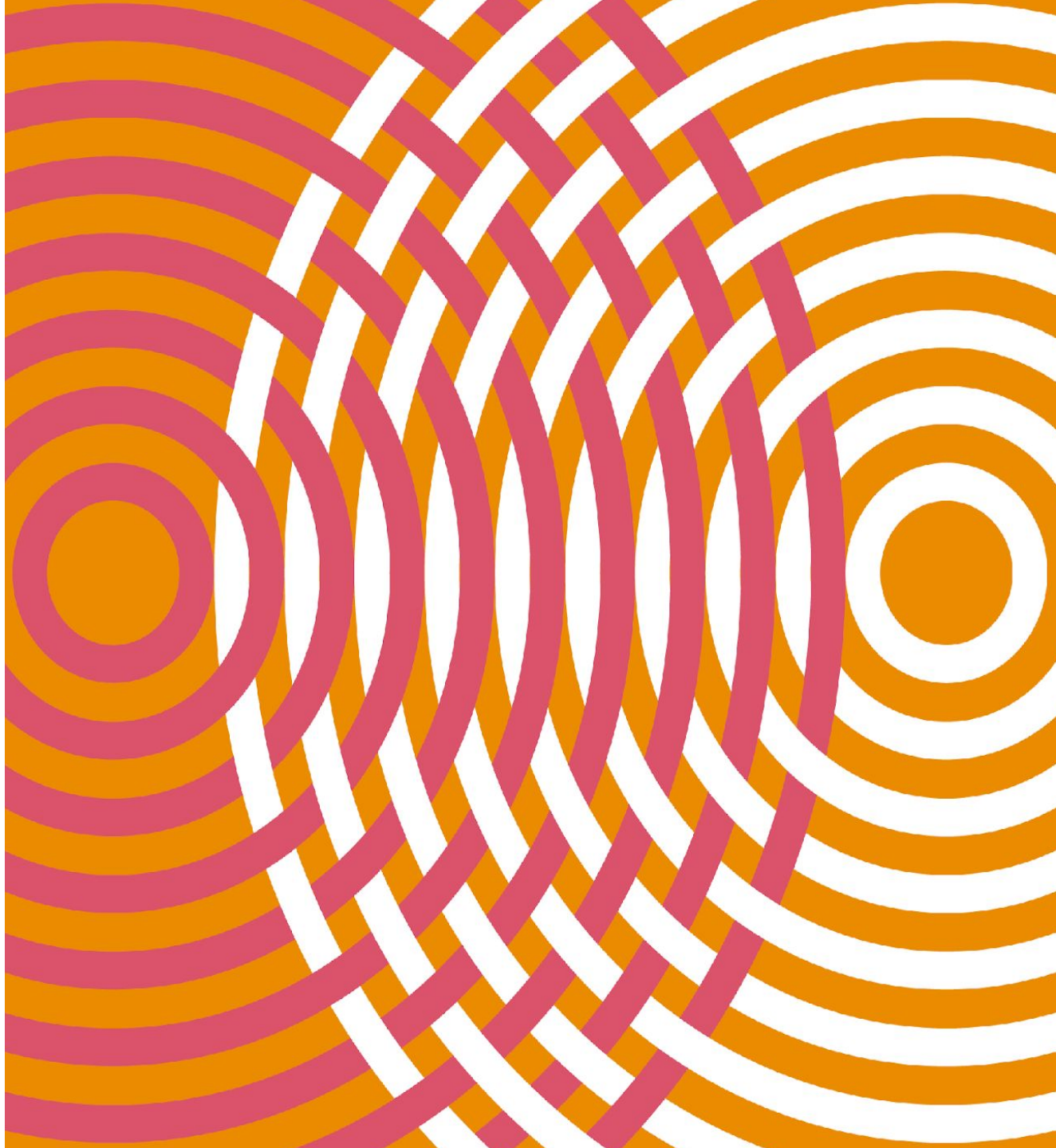
*Teknisk säkerhet:*

- Gunilla Sramek – IT samordnare TrelleborgsHem
- Conny Andersson – Drifttekniker TrelleborgsHem
- Kent Ahlgren – IT Trelleborgs kommun
- Filip Fryklund – IT Trelleborgs kommun

*Organisatorisk säkerhet:*

- Pia Jönsson – VD TrelleborgsHem
- Birgitta Persson – Ekonomichef

Rapporten har även faktagranskats av intervjuade personer.



# Inledande iakttagelser

Trelleborgshem är ett kommunalt bolag inom koncernen Rådhus AB som ägs av Trelleborgs Kommun. Bolaget ansvarar för uthyrning av lägenheter och förvaltning av de fastigheter bolaget äger. I samband med införandet av den nya dataskyddsförordningen (GDPR) genomförde bolaget ett relativt omfattande arbete med processer och rutiner avseende personuppgifter och incidenter kopplade till hanteringen av dessa. Mycket av bolagets arbete med cybersäkerhet har dock avgränsats till just behandlingen av personuppgifter.

Som en del i kommunkoncernen omfattas bolaget av de styrdokument som reglerar IT- och informationssäkerhet på kommunövergripande nivå, för de delar där avtal ingåtts mellan Trelleborgshem och kommunen. Det finns flera system som bolaget använder, vilka förvaltas och driftas av den centrala IT-funktionen i kommunen. I dessa delar innebär koncernplaceringen att även Trelleborgshem omfattas av de styrprocesser, avtal, skydd och andra mekanismer som tillhandahålls centralt. Här är mognaden i stora delar relativt hög. I de delar där Trelleborgshem utövar ett eget ansvar för sin cybersäkerhet, utan styrning från kommunens centrala IT-funktion, är emellertid mognaden lägre. Trelleborgshem har ett antal verksamhetskritiska system (ex. Vitec) där bolaget själv ansvarar för upphandling av lämplig leverantör, dock i samråd med kommunens IT-avdelning. Kommunens IT-avdelning hanterar även behörighetshantering och implementering av system. Trelleborgshem ansvarar själva för inköp av telefoner och läsplattor. Här har bolaget inte genomfört någon riskinventering, informationsklassning eller process för incidenthantering.

Eftersom Trelleborgshem är ett relativt litet bolag som inte har möjlighet att ha specialistkompetens inom IT-frågor förekommer det regelbundna möten med kommunens IT-avdelning i samband med inköp av nya system. Avseende programvaror och applikationer styrs bolagen av det informationssäkerhetsarbete som IT-avdelningen genomför för kommunen i övrigt.

**Ur en strategisk synvinkel är den viktigaste rekommendationen från den översiktliga genomgång som presenteras i denna rapport att gränssnittet mellan Trelleborgshem och Trelleborgs kommun behöver tydliggörs. Detta innebär att Trelleborgshem, tillsammans med Trelleborgs kommuns IT-avdelning, behöver tydliggöra vilka system och applikationer bolaget ensamt är ansvarigt för, vilken information som finns i dessa system och hur informationen ska klassas, samt vilka skyddsmekanismer som är lämpliga att ha på plats för att skydda informationen och säkerställa en robust drift. Detta eftersom ansvaret åvilar Trelleborgshem och inte täcks av det skydd och de processer som gäller för andra delar av cybersäkerheten, och som inryms inom ramen för kommunens centrala IT-funktion. Lämpligtvis bör detta även åtföljas av medvetandehöjande åtgärder och utbildningar, både på ledningsnivå och för de anställda.**

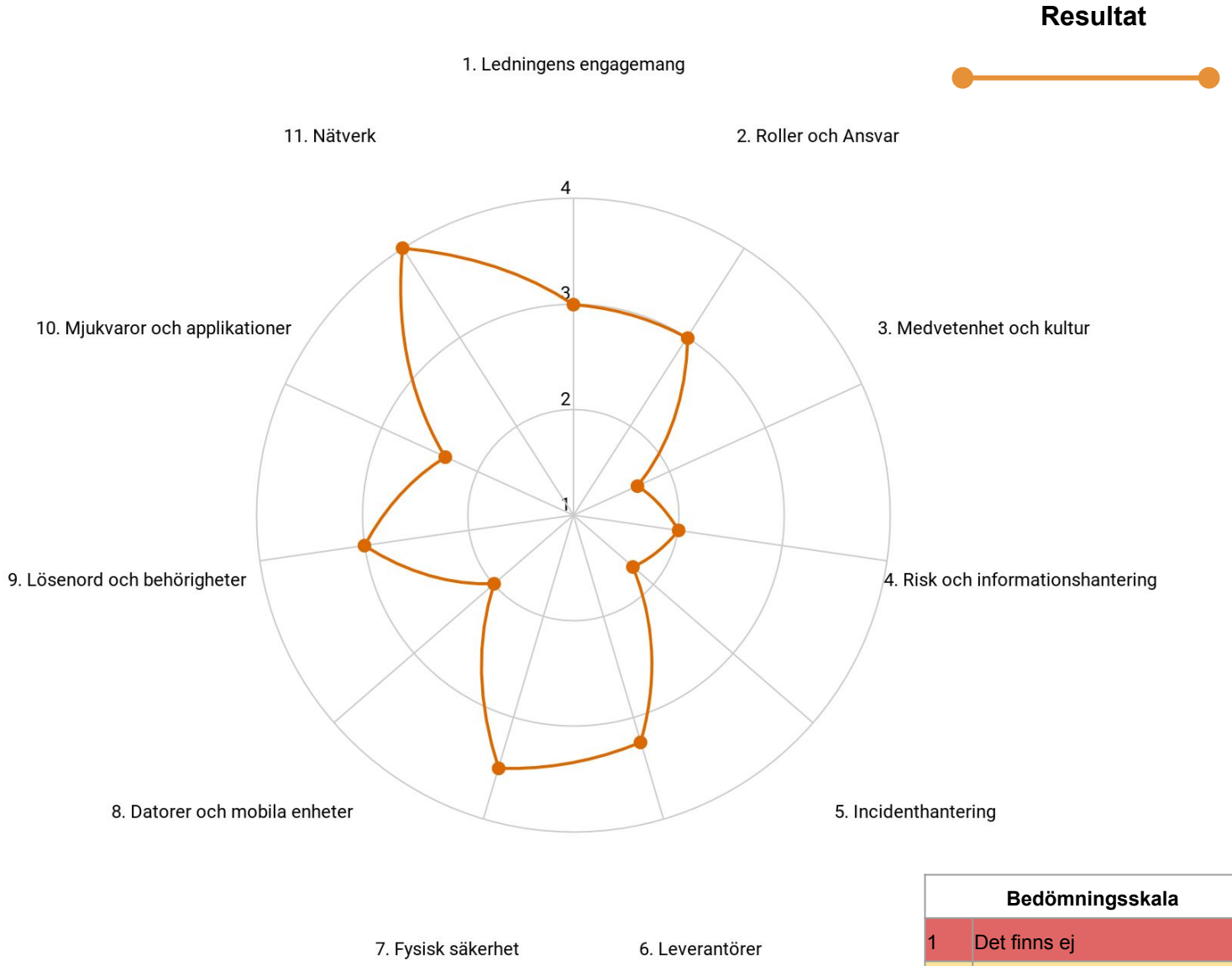
Poängbedömningen i denna rapport har i möjligaste mån haft Trelleborgshem som utgångspunkt, och inte kommunens övergripande IT-processer.

# Sammanfattning

Diagrammet till höger visar resultatet av vår genomgång. Det är baserat på intervjuerna och ger en översiktsbild av samtliga relevanta cybersäkerhetsområden. Skillnaden mellan nivåerna i bedömningsskalan baseras på om det finns dokumenterat, är implementerat och kommunicerat samt övat/testat.

Sammanfattningsvis är viktigaste rekommendationen i denna rapport är att gränssnittet mellan Trelleborgshem och Trelleborgs kommun och förståelsen för konsekvenserna av detta för Trelleborgshems systematiska cybersäkerhetsarbete behöver kartläggas och förstås. Detta innebär att det behöver tydliggöras vilka system och applikationer bolaget ensamt är ansvarigt för, vilken information som finns i dessa och hur den ska klassas, samt vilka skyddsmekanismer som är lämpliga att ha på plats för att säkerställa skydd.

Se vidare i rapporten för detaljerade iakttagelser och rekommendationer för respektive områden.




| Bedömningsskala | |
|---|---|
| 1 | Det finns ej |
| 2 | Det finns i viss utsträckning |
| 3 | Det finns i stor utsträckning |
| 4 | Det finns i full utsträckning |

# Rekommendationer - Organisatorisk säkerhet

| Område | Våra rekommendationer |
|---|---|
| **Ledningens engagemang** | • Säkerställ att cybersäkerhet framöver inkluderas i det löpande, strategiska arbetet genom att exempelvis addera cybersäkerhet som en stående punkt som protokollförs på agendan vid ledningsgruppsmöten.<br>• Inför utbildningar gällande informations- och cybersäkerhet för ledningsgruppen.<br>• Säkerställ en protokollförd dokumentation av de löpande mötena med kommunens IT-avdelning för att säkra att all information når Trelleborgshem. |
| **Roller & ansvar** | • Definiera, dokumentera och kommunicera roller, ansvar och mandat. Säkerställ att dessa är etablerade och kända inom organisationen.<br>• KPI:er och rapporteringsvägar ska vara tydliga och kommunicerade för att undvika otydlighet vid bortfall av nyckelpersoner och liknande situationer.<br>• Implementera och efterfölja kommunens riktlinjer enligt standarden ISO 27000, även i de delar som Trelleborgshem ensamt ansvarar för. |
| **Medvetenhet och kultur** | • Säkerställ att gällande IT-säkerhetsinstruktion samlar det viktigaste att tänka på i det dagliga arbetet gällande cybersäkerhet. Säkerställ efterlevnad genom löpande kontroller.<br>• I samråd med Trelleborgs Kommun, utred och analysera inom vilka områden Trelleborgshem har behov av medvetandehöjande aktiviteter.<br>• Inför syfte och mål för medvetandehöjande aktiviteter, utbildningar och övningar för de anställda.<br>• Säkerställ även att det genomförs uppföljning av övningar och utbildningar för att säkerställa och utvärdera utbildningarnas mål. |
| **Risk- och informationshantering** | • Ta fram en riskanalys och formaliserad process för att revidera denna med avseende på cyberrelaterade risker.<br>• Definiera Trelleborgshems riskaptit.<br>• Genomför en officiell informationsklassning och säkerställ att adekvat skydd finns där det behövs.<br>• Implementera rutiner för att säkerställa att beslutad riskaptit genomsyrar Trelleborgshems verksamhet och att kommunens riktlinjer enligt ISO 27000 efterlevs. |
| **Incidenthantering** | • Utveckla existerande Nödlägesplan så att den även inbegriper incidenthantering gällande informationssäkerhetsrelaterade incidenter och säkerställ att den inkluderar tydliga processer, roller och rutiner. Alternativt, säkerställ att den incidenthanteringsprocess för denna typ av händelser som kan finnas på kommunövergripande nivå även implementeras i bolaget.<br>• Utbilda personal och medarbetare i adekvat hantering av information för att undvika interna incidenter.<br>• Genomför övningar för incidentscenarion för att höja den allmänna medvetenheten kring cyberrelaterade risker. |

# Rekommendationer - Teknisk säkerhet

| Område | Våra rekommendationer |
|---|---|
| **Leverantörshantering** | • Överväg att anlita en tredje part som ser över och granskar avtal med leverantörer av IT-system utifrån de säkerhetsbehov som finns.<br>• Säkerställ leverantörernas incident- och kontinuitetshanteringsförmåga.<br>• Fastställ en rutin och process för att genomföra revisioner av leverantörer, vilket även bör vara ett krav i avtalet (SLA). |
| **Fysisk säkerhet** | • För att förhindra att obehöriga får tillgång till känslig information rekommenderas att Trelleborgshem ser över eventuellt behov av säkra arbetsutrymmen. |
| **Datorer och mobila enheter** | • Öka säkerheten kring mobiler och läsplattor på bolaget med VPN och skyddad information under hela livscykeln.<br>• Reglera användandet av datorer och mobila enheter. Tillåt exempelvis ej okrypterade USB och använd endast mobildata utanför kontoret. |
| **Lösenord & Behörigheter** | • I samråd med kommunens IT-avdelning, inför lösenordskrav för att säkerställa komplexiteten och se till att krav på lösenordsbyte gäller alla system.<br>• Skapa en process för att administrera behörigheter.<br>• Implementera en process för principen om lägsta nödvändiga behörighetsgrad (least privilege). |
| **Mjukvaror och applikationer** | • Begränsa möjligheten att ladda ner mjukvaror/applikationer till mobiler och läsplattor för att undvika skadlig kod.<br>• Utse en dedikerad roll som ansvarar för säkerställande av säkra uppdateringar på mobiler och läsplattor. |
| **Nätverk** | • Inga rekommendationer. |

# Detaljerad rapport

pwc

# 1

# Organisatorisk säkerhet

# Organisatorisk säkerhet
## Ledningens engagemang

Ett lyckat informations- och cybersäkerhetsarbete kräver ledningens engagemang. Ledningen sätter riktningen för informations- och cybersäkerhetsarbetet och säkerställer att arbetet genomsyrar hela verksamheten. Ledningen ska sköta det strategiska arbetet och stötta det operativa arbetet. En del av ledningens arbete inkluderar att författa en policy för informations- och cybersäkerhetsarbetet. En policy är ledningens viljeyttring och anger informations- och cybersäkerhetsarbetets inriktning. Genom en policy (eller liknande styrdokument) dokumenterar ledningen den strategiska riktningen för arbetet. Vidare, en policy och hur den tillämpas kan även vara viktig att kunna presentera för kunder och eventuella tillsynsmyndigheter. För Trelleborgshems vidkommande finns en kommunövergripande Policy för informationssäkerhet (KS 2018/521) som Trelleborgshem indirekt omfattas av. Det finns även en IT-säkerhetsinstruktion för Trelleborgshem. Denna är under omarbetning och vidareutveckling, men är gällande i sin nuvarande form.

| Område | Iakttagelser | Våra rekommendationer |
|---|---|---|
| **Ledningens engagemang** | Ledningen anses ha ett engagemang för informations- och cybersäkerhetsfrågor. Detta manifesteras i att IT-samordnare, VD och Ekonomichef börjat belysa IT-säkerhet genom föreliggande genomgång av cybersäkerheten, samtidigt som de har mandat att fatta beslut om åtgärder och investeringar gällande detta (med hänsyn till budget och andra eventuella restriktioner). Gällande ledningens kunskap om frågor relaterade till informations- och cybersäkerhet är denna i viss utsträckning begränsad.<br><br>Trelleborgshem är ett kommunalt bolag inom koncernen Rådhus AB vilket innebär att de till viss del omfattas av de styrdokument som reglerar IT- och informationssäkerhet på kommunövergripande nivå. År 2006 slöts ett samverkansavtal mellan Trelleborgshem och IT-avdelningen på Trelleborgs kommun. Efter denna tidpunkt har det funnits regelbundna träffar mellan kommunens IT-avdelning och Trelleborgshems Ekonomichef. Mötena har dock inte protokollförs utan rapportering tillbaka till Trelleborgshem sker muntligt. | • Säkerställ att cybersäkerhet framöver inkluderas i det löpande, strategiska arbetet genom att exempelvis addera cybersäkerhet som en stående punkt som protokollförs på agendan vid ledningsgruppsmöten.<br><br>• Inför utbildningar gällande informations- och cybersäkerhet för ledningsgruppen.<br><br>• Säkerställ en protokollförd dokumentation av de löpande mötena med kommunens IT-avdelning för att säkra att all information når Trelleborgshem. |

# Organisatorisk säkerhet
## Roller och ansvar

För att lyckas med informations- och cybersäkerhetsarbetet bör roller och ansvar för arbetet vara definierade och kommunicerade i organisationen. Den funktion som har hand om det övergripande informations- och cybersäkerhetsarbetet bör även ha tillräckligt mandat och resurser för att kunna utföra sitt arbete. Funktionen ska både vara stödjande och strategisk. Funktionen har ansvar för att se till att ledning, verksamhetschefer och medarbetare får stöd och underlag för att fatta beslut avseende informationssäkerheten i verksamheten. Det är viktigt att tillägga att informella roller och beslutsvägar kan resultera i sårbarheter i organisationen på lång sikt. Detta kan dock mitigeras genom att tydliggöra samt definiera roller, ansvar och mandat.

| | Område | Iakttagelser | Våra rekommendationer |
|---|---|---|---|
| | **Roller & ansvar** | Trelleborgshem har ej formaliserat eller dokumenterat roller och ansvar kopplat till cybersäkerhet. Det är IT-samordnaren som just nu ansvarar för inköp av datorer, mobiler, läsplattor, ansvarar för efterföljande av kommunens riktlinjer samt att vara kontaktperson vid IT-frågor. Vidare är IT-samordnarens mandat och resurser inte tydligt kopplat till cybersäkerhetsarbetet. På kommunnivå är dessa roller dock tydligt förankrade i organisationen och genom standarden ISO-27000.<br><br>Vid bortfall av nyckelpersoner är det inte formellt dokumenterat vem som tar över ansvar eller roller, t.ex. vem som i så fall tar över med samma befogenheter och beslutsmandat om ordinarie funktion eller person är borta. | • Definiera, dokumentera och kommunicera roller, ansvar och mandat. Säkerställ att dessa är etablerade och kända inom organisationen<br><br>• KPI:er och rapporteringsvägar ska vara tydliga och kommunicerade för att undvika otydlighet vid bortfall av nyckelpersoner och liknande situationer<br><br>• Implementera och efterfölja kommunens riktlinjer enligt standarden ISO 27000 även i de delar som Trelleborgshem ensamt ansvarar för. |

# Organisatorisk säkerhet
## Medvetenhet och kultur

Utöver att etablera en ändamålsenlig organisation för informations- och cybersäkerhetsarbetet och välja rätt tekniska lösningar behöver en organisation bygga upp en god säkerhetskultur. Säkerhetskulturen syftar till den övergripande attityden och inställningen till säkerhet i organisationen. Medarbetarna ska ha förståelse för informations- och cybersäkerhetsarbetet, de ska känna sig delaktiga och motiverade att delta i det och ta ansvar för att arbetet bedrivs på det sätt som är beslutat.

I arbetet med att utveckla en god säkerhetskultur är det viktigt att informations- och cybersäkerhet genomsyrar hela anställningsprocessen, från nyanställning till och med avslutad anställning, samt att organisationen arbetar med kontinuerlig utbildning för medarbetare i informationssäkerhet.

| | Område | Iakttagelser | Våra rekommendationer |
|---|---|---|---|
| ● | **Medvetenhet och kultur** | Medvetandehöjande aktiviteter såsom utbildningar och övningar genomförs inte i Trelleborgshem med undantag för de insatser som skedde i samband med införandet av GDPR. Det finns ingen långsiktig och definierad plan för att säkerställa ökad kompetens och förmåga inom för Trelleborgshem relevanta områden. Det framkom att Trelleborgshem inte framför vilken typ av kompetens- och medvetandehöjande aktiviteter som krävs för anställda, bortsett från den översiktliga genomgången som sker vid nyanställning.<br><br>Det saknas etablerade rutiner för när och hur medvetandehöjande aktiviteter ska tas fram och genomföras. Bolagets IT-säkerhetsinstruktion saknar i nuläget delvis instruktioner som styr beteende och vardagliga rutiner, exempelvis att internetdelning bör användas snarare än publikt wifi, om inte VPN-lösning finns att tillgå. | • Säkerställ att gällande IT-säkerhetsinstruktion samlar det viktigaste att tänka på i det dagliga arbetet gällande cybersäkerhet.Säkerställ efterlevnad genom löpande kontroller.<br><br>• I samråd med Trelleborgs Kommun, utred och analysera inom vilka områden Trelleborgshem har behov av medvetandehöjande aktiviteter.<br><br>• Inför syfte och mål för medvetande-höjande aktiviteter, utbildningar och övningar för de anställda.<br><br>• Säkerställ även att det genomförs uppföljning av övningar och utbildningar för att säkerställa och utvärdera utbildningarnas mål. |

# Organisatorisk säkerhet
## Risk- och informationshantering

Riskhantering är en central del i informations- och cybersäkerhetsarbetet. Det bör finnas ett arbetssätt för att kunna identifiera, analysera och hantera informations- och cyberrelaterade risker. För att kunna identifiera och analysera risker är det av hjälp att den information som organisationen hanterar är identifierad samt klassificerad. All information som organisationen hanterar är inte i behov av samma skydd och innebär inte samma risk om den skulle förloras, förvanskas eller inte vara tillgänglig. Arbetssättet bör inkludera metoder för att värdera konsekvenser, bedöma risker, hantera och följa upp åtgärder samt rapportera risker och status på åtgärder. Riskbedömningen bör även göras i relation till ledningens uppfattning om vilka konsekvenser som inte kan accepteras, vanligen kallat riskaptit.

| Område | Iakttagelser | Våra rekommendationer |
|---|---|---|
| **Risk- och informationshantering** | Trelleborgshem saknar en riskanalys och en formaliserad process för att revidera och följa upp analysen. Det finns en ambition hos såväl IT-samordnare, VD som Ekonomichef att agera riskbaserat, men det saknas tydliga processer för hur detta ska ske. Trelleborgshem saknar därmed även en definierad riskaptit och risktolerans. Här kan verktyget Draft-it, vilket bolaget redan använder, vara till hjälp för att gå igenom processer och förbättra dataskyddsrutiner.<br><br>På kommungemensam nivå har ISO-27000 införts. Införandet sker även successivt på de delar som berör Trelleborgshem när nya system införs. Stora förändringar går igenom en informationssäkerhetsutvärdering med hänsyn till bl.a. datainspektionens riktlinjer. | • Ta fram en riskanalys och formaliserad process för att revidera denna med avseende på cyberrelaterade risker.<br>• Definiera Trelleborgshems riskaptit.<br>• Genomför en officiell informationsklassning och säkerställ att adekvat skydd finns där det behövs.<br>• Implementera rutiner för att säkerställa att beslutad riskaptit genomsyrar Trelleborgshems verksamhet och att kommunens riktlinjer enligt ISO 27000 efterlevs. |

# Organisatorisk säkerhet
## Incidenthantering

En informationssäkerhetsincident är en händelse som har en direkt påverkan på en informationstillgångar. Exempel på incidenter skulle kunna vara: IT-angrepp/intrång, skadlig kod, oskyddad känslig information och/eller bristande intern hantering av information. Det bör finnas ett konsekvent och effektivt tillvägagångssätt för hantering av informations- och cybersäkerhetsincidenter inklusive kommunikation kring säkerhetshändelser och sårbarheter. Detta är viktigt av flera anledningar, bl.a. för att kunna hantera incidenter på ett effektivt sätt för att på så sätt kunna minska konsekvenserna av dem, men även för att skapa bra underlag för arbetet med riskanalyser och kontinuitetsplanering.

| Område | Iakttagelser | Våra rekommendationer |
|---|---|---|
| **Incident-hantering** | Trelleborgshem har ingen incidenthanteringsplan eller framtagna processer, roller och rutiner vid en informations- och cybersäkerhetsincident förutom för personuppgiftsrelaterade incidenter (utifrån krav i GDPR). Om en incident inträffar är det upp till medarbetarna själva att meddela detta.<br><br>Trelleborgshem genomför inga övningar för incidentsscenarion vilket hänger ihop med avsaknaden av ett strukturerat informationsrisksarbete. Bolaget har dock en Nödlägesplan, vilken dock inte täcker in informationssäkerhetsspektrat av incidenter. VD:n menar att medvetenheten kring risker på bolaget måste höjas på alla nivåer.<br><br>På kommunal nivå finns en process samt monitorering via brandvägg där en resultatrapport genereras veckovis. Det finns även mailfilter, rutin med driftroller där larm omhändertas samt PRTG Network Monitor. | • Utveckla existerande Nödlägesplan så att den även inbegriper incidenthantering gällande informationssäkerhetsrelaterade incidenter och säkerställ att den inkluderar tydliga processer, roller och rutiner. Alternativt, säkerställ att den incidenthanteringsprocess för denna typ av händelser som kan finnas på kommunövergripande nivå även implementeras i bolaget.<br><br>• Utbilda personal och medarbetare i adekvat hantering av information för att undvika interna incidenter.<br><br>• Genomför övningar för incidentscenarion för att höja den allmänna medvetenheten kring cyberrelaterade risker. |

# Organisatorisk säkerhet
## Leverantörshantering

En stor del av de IT-relaterade tjänster som organisationer använder är idag outsourcade. Det kan handla om exempelvis outsourcing av hela IT-driften, förvaltning av IT-tjänster i organisationens lokaler eller utveckling av IT-system. Det är även vanligt att tjänster, system, lagring och hela plattformar körs genom molnet via s.k. molnleverantörer (Software-as-a-Service, SaaS, Platform-as-a-Service, PaaS, Infrastructure-as-a-Service, IaaS osv.) Det finns ett antal säkerhetsutmaningar relaterade till outsourcing i allmänhet och cloudleverantörer i synnerhet. Bland dessa finns förlorad kontroll, avsaknad av inblick och transparens och jurisdiktionproblem. Med anledning av dessa utmaningar är det viktigt att det ställs krav på leverantörer samt att dessa krav följs upp.

| | Område | Iakttagelser | Våra rekommendationer |
|---|---|---|---|
| | **Leverantörs-hantering** | Trelleborgshem har juridiska bindande avtal med sina IT-leverantörer varav alla finns i Draft-it. Detta kan gälla allt från temperaturavläsningar i lägenheter till nyckelsystem och digitala nycklar. För de leverantörer som hanterar personuppgifter har Trelleborgshem skrivit personuppgiftsbiträdesavtal. Det framgår dock att beställning och kravställningen mot leverantörerna inte är fullt kontrollerad eller klarlagd till följd av bristande teknisk kompetens inom Trelleborgshem.<br><br>För de system där kommunen är IT-leverantör tar man hänsyn till cyberrelaterade risker genom ex. GDPR gällande tredjeland. Kommunen har också gått ut med direktiv som kravställer att upphandlade system ska informationsklassas och hänsyn ska tas till CloudAct och tredjeland. | • Överväg att anlita en tredje part som ser över och granskar avtal med leverantörer av IT-system utifrån de säkerhetsbehov som finns.<br><br>• Säkerställ leverantörernas incident- och kontinuitetshanteringsförmåga.<br><br>• Fastställ en rutin och process för att genomföra revisioner av leverantörer, vilket även bör vara ett krav i avtalet (SLA). |

# 2

# Teknisk säkerhet

# Teknisk säkerhet
## Fysisk säkerhet

Informations- och cybersäkerhet ställer krav på den fysiska säkerheten i organisationen. Det räcker inte att endast ha ett gott teknisk skydd, det fysiska skyddet måste också vara ändamålsenligt för att lyckas med god informations- och cybersäkerhet. Det fysiska skyddet har som syfte att förhindra otillåten fysisk åtkomst till, skador på och störningar i tillgången till organisationens information och informationsbehandlingsresurser.

| | Område | Iakttagelser | Våra rekommendationer |
|---|---|---|---|
| | **Fysisk säkerhet** | Utifrån storleken på organisationen så har Trelleborgshem ett väl fungerande skalskydd som styrs via iLock. Lokalerna som Trelleborgshem befinner sig i är inte zonindelade, men de som har en entreprenörsnyckel har emellertid ändå inte tillgång till lägenheter eller andra lokaler.<br><br>När det kommer till rutiner för att säkerställa att personalen arbetar i säkra utrymmen om så kräver är detta inget som finns på plats på bolaget. HR avdelningen har ett låsbart kassaskåp som endast HR/VD/Ekonomichef har tillgång till. Hyresavtal låses in i ett plåtskåp hos Hyresadministratören i Bobutiken. Även hyreskontrakt på lokaler förvaras i ett låsbart plåtskåp.<br><br>Trelleborgshem erbjuder glance-protection till sina anställdas datorer. | • För att förhindra att obehöriga får tillgång till känslig information rekommenderas att Trelleborgshem ser över eventuellt behov av säkra arbetsutrymmen. |

# Teknisk säkerhet
## Datorer och mobila enheter

De datorer och mobila enheter (mobiler och surfplattor) som företaget tillhandahåller till sina anställda bör vara skyddade på ett ändamålsenligt sätt. Det bör finnas tekniska skydd såsom brandvägg och virusskydd, mjukvara och operativsystem uppdaterade, men även rutiner och instruktioner som bestämmer hur användarna ska hantera dessa enheter.

| | Område | Iakttagelser | Våra rekommendationer |
|---|---|---|---|
| | **Datorer och mobila enheter** | Den tekniska säkerheten skiljer sig markant mellan datorer (som tillhandahålls via kommunenes centrala IT) och mobiler och läsplattor (vilka köps in och administreras direkt av Trelleborgshem). Vid borttappande av dator eller uppsägning kan information snabbt rensas från datorn centralt, vilket inte är fallet med telefoner. Det senare är särskilt känsligt då verksamhetskritiska system som exempelvis Vitec även är nåbara via mobil. Kommunen använder sig av VPN och Bitlocker för att skydda information på datorer och det utförs en kontinuerlig monitorering för att upptäcka otillåten utrustning, något som bland annat märktes för en tid sedan då Trelleborgshem införskaffat tre stycken accesspunkter som inte var godkända av kommunen, och som inte mötte de av kommunen centralt uppställda säkerhetskraven.<br><br>För mobiltelefoner och läsplattor finns inget skydd mot förlust, obehörig åtkomst, och stöld. Det finns inget tvingande krav på användning av VPN om man jobbar på distans, och överlag finns ingen säkerhetshantering av mobiler eller läsplattor. | • Öka säkerheten kring mobiler och läsplattor på bolaget med VPN och skyddad information under hela livscykeln.<br><br>• Reglera användandet av datorer och mobila enheter. Tillåt exempelvis ej okrypterade USB och använd endast mobildata utanför kontoret. |

# Teknisk säkerhet
## Lösenord och behörigheter

En god lösenordspolicy och -kultur är vitalt för att förebygga och minska cyberrelaterade hot. Det är dels viktigt att säkerställa att användare använder komplexa lösenord, men samtidigt att de även hanterar lösenordet på ett säkert sätt. Användare bör använda olika lösenord till olika tjänster samt ansvara för att hålla sina lösenord hemliga. En annan grundläggande åtgärd för att minska risken för att information hamnar hos obehöriga är att begränsa åtkomsten. Det bör finnas regler för styrning av åtkomst som innefattar vilka som bör ha behörighet till vilka tjänster, hur denna behörighet tilldelas och när och hur behörigheter ska tas bort.

| | Område | Iakttagelser | Våra rekommendationer |
|---|---|---|---|
| | **Lösenord och behörigheter** | Trelleborgshem använder sig av tvåfaktorsautentisering för Visma och lönesystemet Koncek. Det finns en övergripande policy om lönenordsbyte var tredje månad, men utan tillhörande krav på lösenordskomplexitet. För Vitec finns ingen rutin kring lösenord, utan byte sker endast i de fall då någon glömmer bort sitt lösenord. Vitec är tillgängligt via mobil, vilket utgör en risk då mobilhanteringen inte sker centralt (se bild 17). Det finns ingen dokumenterad rutin för behörighetstilldelning och borttagning, och hanteringen kring detta är spridd beroende på funktion och system.<br><br>Det finns inga rutiner för att säkerställa att konton med administratörsrättigheter/ priviligerade rättigheter i databasen inte används utanför det avsedda användningsområdet, och bolaget har tidigare haft problem med många aktiva priviligierade konton (“superusers”) i Vitec, något som i viss mån lever kvar idag. | • I samråd med kommunens IT-avdelning, inför lösenordskrav för att säkerställa komplexiteten och se till att krav på lösenordsbyte gäller alla system.<br><br>• Skapa en process för att administrera behörigheter.<br><br>• Implementera en process för principen om lägsta nödvändiga behörighetsgrad (least privilege). |

# Teknisk säkerhet
## Mjukvaror, applikationer och nätverk

Mjukvaror och applikationer kan medföra risker och sårbarheter. Det bör finnas någon form av styrning av vilka program medarbetare får ladda ned på sina enheter (både datorer och mobila enheter) för att undvika att skadlig kod eller andra sårbarheter kommer in i systemen. Vidare bör det säkerställas att de mjukvaror och applikationer som laddas ned uppdateras kontinuerligt för att minimera sårbarheten och därigenom öka säkerheten. öka säkerheten och motverka kryphål. Säkerheten är även viktig för alla nätverk, särskilt när det gäller trådlösa nätverk. Trådlös nätverkstrafik kan enkelt avlyssnas eftersom det handlar om vanliga radiosignaler. Om inte trafiken är krypterad går det att extrahera information såsom exempelvis lösenord.

| | Område | Iakttagelser | Våra rekommendationer |
|---|---|---|---|
| | **Mjukvaror och applikationer** | Trelleborgs kommun bistår Trelleborgshem med exempelvis brandvägg- och antivirusskydd på både servrar och klienter, och dessa system uppdateras kontinuerligt. På Trelleborgshems mobiler och läsplattor finns det inga begränsningar i vilka mjukvaror/applikationer som medarbetarna får ladda ner. Detta finns däremot för datorer som driftsätts via Trelleborgs Kommun, och kommunen har en dedikerad tekniker för att säkerställa att mjukvaror och applikationer alltid har den senaste säkra uppdateringen. | • Begränsa möjligheten att ladda ner mjukvaror/applikationer till mobiler och läsplattor för att undvika skadlig kod<br>• Utse en dedikerad roll som ansvarar för säkerställande av säkra uppdateringar på mobiler och läsplattor |
| | **Nätverk** | Trelleborgs Kommun har hårdvarubrandvägg installerad för att skydda all nätverkstrafik mellan det interna nätverket och internet, vilket även inbegriper trafiken till och från Trelleborgshem. För att säkerställa säkerheten finns även på kommunnivå även trådlösa nätverk som är krypterade och skyddade med unika certifikat, vilket även är tillgängligt för Trelleborgshem. | • Inga rekommendationer. |

# Tack!

pwc.com

# Bilaga 1 - Bedömningsskala

De iakttagelser som diskuterats i denna rapport har bedömts utifrån vilken risk de eventuellt utgör för organisationen. Betygsättningen illustreras med hjälp av trafikljus. Det bör noteras att klassificeringen främst fokuserar på graden av behov av ledningens uppmärksamhet.

Ett **rött** ljus används för områden som vi bedömer ska få stor uppmärksamhet. Det innebär att organisationen är långt ifrån att nå upp till en godtagbar säkerhetsnivå.

**Gult** ljus indikerar ett problem som även om det inte är lika allvarligt som ett rött ljus bör ges uppmärksamhet. Det ska tolkas som att organisationen har vidtagit åtgärder men att organisationen för närvarande inte fullt ut når upp till en godtagbar säkerhetsnivå.

Ett **grönt** ljus tilldelas iakttagelser där vår bedömning är att organisationen når upp till de en grundläggande säkerhetsnivå på området som granskats.