Deloitte.

Beslutningsnotat

Københavns Kommune, Koncern IT

Anbefalinger til styrkelse af Københavns Kommunes tekniske cyberforsvar

18. juni 2018

Indhold

1 Ledelsesresume

Deloitte har i perioden marts 2018 til maj 2018 gennemført en analyse af Københavns Kommunes tekniske cyberforsvar. Formålet med analysen har været at klarlægge, om det nuværende sikkerhedsniveau er tilstrækkeligt og effektivt set i forhold til det nuværende og især det fremtidige trusselbillede for kommunen specifikt og samfundet generelt og med baggrund heri opstille anbefalinger til områder, hvor der bør investeres i en yderligere sikring af it-infrastrukturen.

Der er i dag sandsynligt, at Københavns Kommune vil blive udsat for cyberangreb i form af forsøg på berigelse eller aktivisme – og trusselniveauet forventes at være stigende.

Deloitte vurderer, at Københavns Kommune i meget høj grad kan blive udsat for angreb, hvor der er fokus på økonomisk berigelse gennem afpresning, bedrageri eller anden form for økonomisk kriminalitet. Deloitte vurderer endvidere, at kommunen i høj grad kan blive udsat for angreb såsom aktivisme, for eksempel i form af ændring af offentlig hjemmeside eller ved at forstyrre driften i kommunen i en sådan grad, at der skabes omtale eksempelvis ved at påvirke telefonsystemer eller lignende.

Endelig vurderes en væsentlig risiko for kommunen at være såkaldte strejfere: Angreb, der ikke som udgangspunkt er rettet mod Københavns Kommune, men som alligevel rammer kommunen og begår skade her.

Udviklingen indenfor de seneste tre år har vist, at især organiserede kriminelle og statsstøttede hackere har øget kapaciteten markant. I forhold til hensigten er risikoen for angreb, der har til hensigt at opnå økonomisk berigelse og udøve cyberaktivisme og cyberspionage, steget. På øvrige områder vurderes trusselbilledet at være mere eller mindre uændret.

Særligt ondsindede installationer og uautoriseret adgang er angrebsmetoder, der udgør en risiko

Der er på overordnet plan fire metoder, der vil blive anvendt af ondsindede aktører i forbindelse med cyberangreb på Københavns Kommune. Heraf vurderes to metoder at udgøre en stor risiko for kommunen.

Ondsindede installationer udgør en væsentlig risiko for Københavns Kommune, og der er relativt stor sandsynlighed for, at kommunen rammes heraf. En særlig årsag til den store risiko er manglende kontrol med sikkerheden i fagsystemer.

Uautoriseret adgang udgør en middelstor til stor risiko for Københavns Kommune, selvom der er relativt lille sandsynlighed for, at kommunen blive ramt heraf. Dette skal ses i lyset af, at den nuværende sikringspraksis er begrænset, og at skadevirkningen fra et angreb kan være meget stor.

Fire centrale indsatsområder og 12 konkrete anbefalinger til tiltag

Med baggrund i trusselbilledet for Københavns Kommune og de konkrete udfordringer, der er identificeret, vurderer Deloitte, at Københavns Kommune bør styrke sit tekniske cyberforsvar indenfor fire hovedområder for at sikre sig imod det stigende trusselniveau, der er for kommunen.

Samlet set er der 12 anbefalinger til tiltag, der fordeler sig indenfor 4 områder som beskrevet i nedenstående.

Tabel 1. Fire indsatsområder

Indsatsområde	Overordnet beskrivelse	Samlet økonomi
1. Overvågning og detektering	Proaktiv overvågning af infrastrukturen for at opdage eventuelle trusler og øget opmærksomhed på trusselbilledet. Løbende test af eventuelle sårbarheder og styrket it-sikkerheds- og compliancestyring.	**Anbefaling om implementering af 12 konkrete tiltag** **Investering:** 20,5-29,9 mio. kr. **Øget årlig drift:** 11,7-18,4 mio. kr.
2. It-sikkerheds-arkitektur og releasestyring	Etablering af en sikkerhedsarkitektur for kommunen samt yderligere sikring af og styring med sikkerhedspatchning på systemniveau.	
3. Beredskab og hændelses-håndtering	Styrkelse af it-beredskabet både ved at kvalificere det eksisterende beredskab og ved at tydeliggøre mandater, processer, samarbejde og kommunikation.	
4. Infrastruktur-tiltag og genetablerings-kapabilitet	Igangsættelse af en række infrastrukturtiltag, der skal øge den tekniske sikkerhed i forhold til cyberangreb. Sikring af, at kommunen i tilfælde af nedbrud som følge af et cyberangreb bliver funktionsdygtig så hurtigt som muligt for derigennem at mindske skadevirkningen i størst mulig grad.	

De 12 indsatser er blevet prioritet fra 1 til 12 med baggrund i deres vurderede effekt. Der er i prioriteringen ikke taget hensyn til den økonomiske omkostning knyttet til indsatsen.

Tabel 2. Prioritering af indsatser

	Indsats	Investering	Årlig driftsudgift
1	**1.1. Overvågning af it-infrastruktur**	2,0-2,8 mio. kr.	3,8-5,8 mio. kr.
2	**4.1. Segmentering af netværk**	9,6-13,4 mio. kr.	1,2-1,7 mio. kr.
3	**2.1. It-sikkerhedsarkitektur**	-	1,5-2,3 mio. kr.
4	**3.1. Incident response**	1,7-2,3 mio. kr.	0,2-0,4 mio. kr.
5	**4.5. Yderligere sikring af Active Directory**	-	0,1-0,2 mio. kr.
6	**1.2. Gennemførsel af penetration tests**	-	0,9-1,3 mio. kr.
7	**4.6. Leverandørerunderstøttelse ved nedbrud**	0,7-1,1 mio. kr.	0,8-1,5 mio. kr.
8	**4.4 Fysisk sikring af KIT**	0,5-0,6 mio. kr.	-
9	**4.3. Privileged Access Management-løsning**	4,9-7,8 mio. kr.	0,8-1,5 mio. kr.
10	**2.2. Release Management på sikkerhedsområdet**	-	1,1-1,5 mio. kr.
11	**4.2. Cloud Access Security Broker**	1,2-1,9 mio. kr.	0,6-1,0 mio. kr.
12	**2.3. Segregation of duties**	-	0,8-1,1 mio. kr.

Prioritering af genetablering

Skulle Københavns Kommune komme i en situation, hvor et cyberangreb medfører et totalt eller næsten totalt nedbrud på kommunens it, og det således ikke er muligt for brugerne at tilgå kritiske it-services (systemer, data, netværk mv.), så er Koncern IT (KIT) sammen med forvaltningerne nødt til at genetablere adgangen til it-services i en prioriteret rækkefølge.

DCK (Digitaliseringschefkredsen) har identificeret ti kerneopgaveområder i Københavns Kommune og prioriteret disse i forhold til vigtighed for genetablering fra et til fire, hvor et er vigtigst, og fire er mindst vigtig. Områderne med højest prioritet er borgernes sundhed og velvære samt medarbejdernes sikkerhed. Som anden prioritet er services til borgerne, borgernes velfærd og kommunens økonomi.

Med afsæt i prioriteringen af kommunens kerneopgaver er der udarbejdet en indikativ liste over, i hvilken rækkefølge kommunens systemer/systemområder bør genetableres. På tilsvarende vis, med afsæt i prioriteringen af kerneopgaveområderne, bør der udarbejdes en oversigt over, i hvilken rækkefølge en genopretning af kommunens lokationer bør prioriteres, og i hvilken rækkefølge adgang til slutbrugerenheder skal ske til kommunens organisatoriske enheder og medarbejdergrupper.

Den konkrete genopretning i bølger bør i tillæg til prioriteringen af kerneopgaveområderne også bero på fire operationelle principper, der sammen med den forretningsmæssige prioritering skal understøtte KIT og forvaltningerne i forbindelse med det konkrete arbejde med en genetablering.

2 Baggrund og formål

Deloitte har i perioden marts 2018 til maj 2018 gennemført en analyse af Københavns Kommunes tekniske cyberforsvar.

Formålet med analysen har været at klarlægge, om det nuværende sikkerhedsniveau er tilstrækkeligt og effektivt set i forhold til det nuværende og især det fremtidige trusselbillede for kommunen specifikt og samfundet generelt og med baggrund heri opstille anbefalinger til områder, hvor der bør investeres i en yderligere sikring af it-infrastrukturen ud fra en afvejning af investeringsomfanget i forhold til effekten af investeringen.

Analysen har omfattet tre sammenhængende delanalyser, jævnfør nedenfor, og således bygger anbefalingerne til investering på en vurdering af trusselbilledet for København Kommune sammenholdt med de udfordringer, der er knyttet til den nuværende praksis i kommunen i forhold til it-sikkerhed.

Tabel 3. Analysens dele

Delanalyser	Formål/beskrivelse
1. Trusselbillede og -vurdering for Københavns Kommune	Beskrivelse af, hvilke it-sikkerheds- og cybertrusler, Københavns Kommune står overfor p.t., hvordan disse har udviklet sig over de senere år og forventes at udvikle sig fremadrettet. Gennemgang af, hvilke angrebsmetoder der forventes anvendt, og en vurdering af, hvor godt Københavns Kommune er sikret imod disse.
2. Centrale it-sikkerhedsudfordringer	Vurdering af Københavns Kommunes nuværende og fremtidige it-sikkerheds-udfordringer i relation til det foranderlige trusselbillede samt modenheden af de nuværende indsatser, der er igangsat som en del af cyberforsvaret i KIT. De centrale sikkerhedsudfordringer er identificeret med udgangspunkt i Deloittes Cyber Strategy Framework (CSF), som sammenfatter en række it-sikkerhedsstandarder fra ISO, NIST og SANS. Modellen er opdelt i fire hovedområder, som samlet indeholder 34 underområder.
3. Anbefalinger til indsatsområder/investeringer	Opstilling af katalog med anbefalinger til tiltag og eventuelle investeringer, der med det fremtidige trusselbillede for øje kan styrke cybersikkerhedsberedskabet i kommunen. Anbefalingerne tager afsæt i trusselbillede og -vurdering (1) samt en vurdering af Københavns Kommunes nuværende og fremtidige it-sikkerhedsudfordringer (2).

Endvidere har Deloitte bistået med at belyse, hvordan Københavns Kommune kan prioritere, hvordan en genetablering skal foregå i forlængelse af et større nedbrud forårsaget af cyberangreb (disaster recovery).

Der angives i nærværende dokument en række udfordringer/forbedringspotentialer knyttet til den nuværende it-sikkerhedspraksis i kommunen. I forlængelse heraf skal det understreges, at nogle af årsagerne til disse udfordringer/forbedringspotentialer er, at:

- Den teknologiske udvikling har betydet, at der er kommet løsninger på markedet, der kan sikre kommunen yderligere, eller at de eksisterende løsninger har fået nye og forbedrede funktionaliteter.
- Trusselbilledet for kommunen har forandret sig, så det er nødvendigt at iværksætte nye tiltag for at opretholde en tilfredsstillende sikkerhed. Dette kan både ske ved anskaffelse af nye tekniske løsninger og ved ansættelse af yderligere årsværk til eksempelvis at foretage en nærmere analyse af data.
- De tidligere implementerede tiltag har krævet mere arbejde end forventet, og det er derfor nødvendigt at tilknytte yderligere ressourcer for at understøtte effekten af disse.
- Der er områder i kommunen, der er decideret underprioriteret i det eksisterende setup, og at det derfor er nødvendigt at tilføre midler for at få øget den samlede it-sikkerhed.

3 Trusselbilledet for Københavns Kommune

Deloitte har med udgangspunkt i forskellige kendte (offentlige og ikke-offentlige, globale og lokale) kilder og konkrete hændelser udarbejdet en vurdering af trusselniveauet for Københavns Kommune. Der er hertil udarbejdet en vurdering af, hvordan trusselniveauet har udviklet sig i de seneste tre år, og hvordan det forventes at udvikle sig i de kommende tre år.

Med baggrund i trusselniveauet er der foretaget en vurdering af, hvilken sandsynlighed der er for, at kommunen rammes af konkrete angrebsmetoder, og hvilken konsekvens de konkrete angrebsmetoder vil have for kommunen, samt hvor godt kommunen er sikret i dag i forhold til disse angrebsmetoder. Denne vurdering bygger på den samlede gennemgang af det nuværende tekniske sikkerhedssetup i særligt KIT.

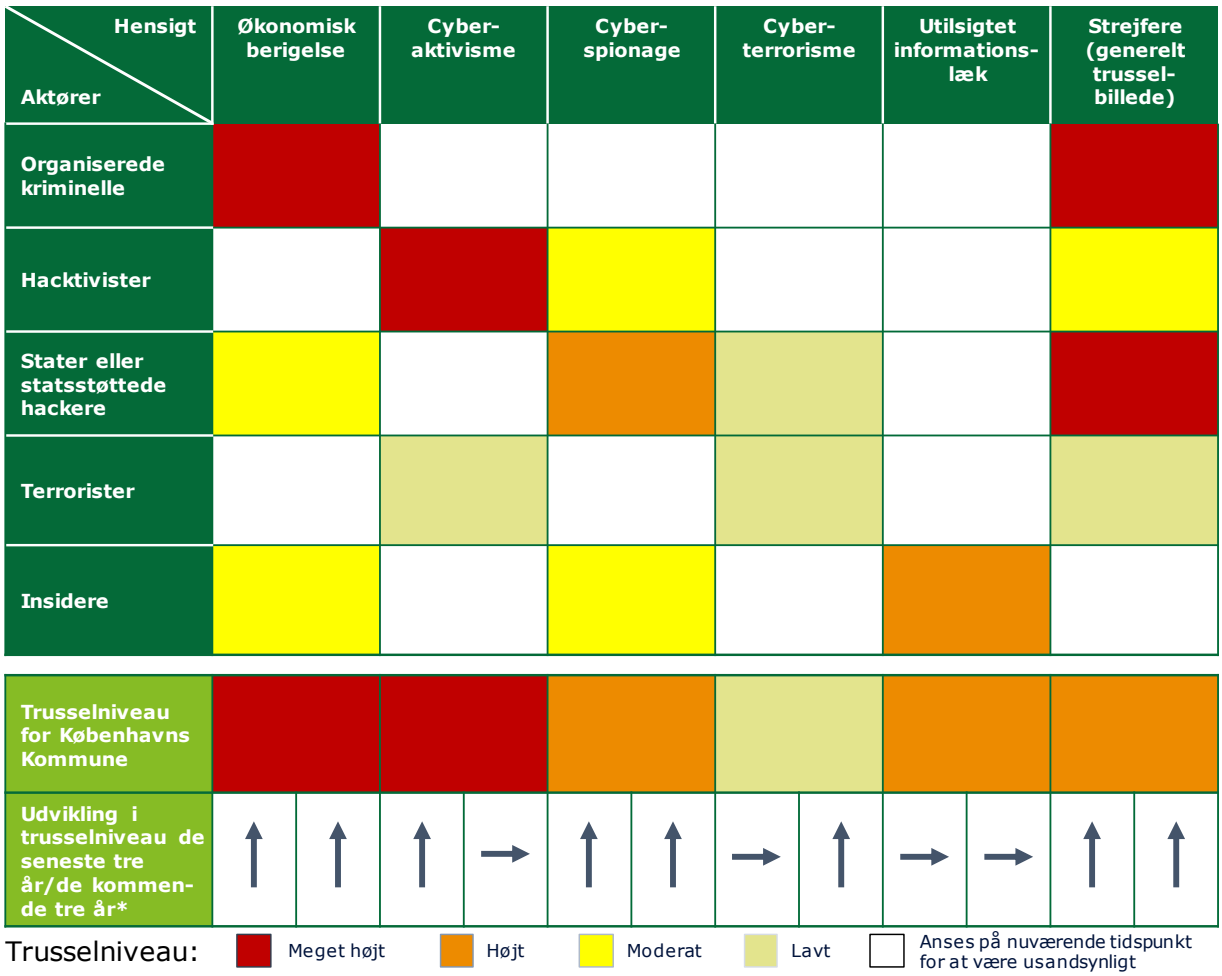
3.1 Trusselniveau og sandsynligheden for cyberangreb mod Københavns Kommune

Der er i dag sandsynligt, at Københavns Kommune vil blive udsat for cyberangreb i form af forsøg på berigelse eller aktivisme

Det er Deloittes vurdering, at Københavns Kommune skiller sig ud fra de øvrige danske kommuner, idet Københavns Kommune er markant større indbyggermæssigt, er hovedstad og således centrum for hovedparten af de statslige institutioner, har flere større virksomheder mv., hvilket betyder, at kommunen alt andet lige vil være et mere interessant mål for cyberangreb end andre kommuner. Endvidere kan kommunen som følge af sin størrelse, politiske beslutningsstruktur og semidecentrale organisering af it-ansvar have svært ved at respondere effektivt på et cyberangreb, hvis der ikke er klare fælles planer og retningslinjer for arbejdet med it-sikkerhed.

Trusselbilledet mod Københavns Kommune er sammensat af en række arketypiske aktører, som kan have onde hensigter rettet mod kommunen. Nedenfor i figur 1 er Deloittes vurdering af trusselbilledet for Københavns Kommune opsummeret. Aktørerne og hensigterne er nærmere beskrevet i bilag.

Figur 1. Trusselbillede for Københavns Kommune



Deloitte vurderer, at Københavns Kommune i meget høj grad risikerer at blive udsat for angreb, hvor der er fokus på økonomisk berigelse gennem afpresning, bedrageri eller lignende. Deloitte vurderer endvidere, at kommunen i høj grad kan blive udsat for angreb i form af aktivisme, der spænder fra ændring af offentlig hjemmeside til at lægge infrastrukturen ned, så kommunens drift påvirkes, og der derigennem skabes omtale.

Endelig vurderes en væsentlig risiko for kommunen at være såkaldte strejfere: Angreb, der ikke som udgangspunkt er rettet mod Københavns Kommune, men som alligevel rammer kommunen og forårsager skade her. Et alment kendt eksempel på en såkaldt strejfer er #NotPetya-angrebet på Mærsk i sommeren 2017, som lagde hele deres it-infrastruktur ned i en længere periode.

Sandsynligheden for cyberangreb er steget over de seneste år – og den forventes fortsat at være høj/stigende

Udviklingen indenfor de seneste tre år har vist, at især organiserede kriminelle og statsstøttede hackere har øget kapaciteten markant. I forhold til hensigten er risikoen for angreb, der har til hensigt at opnå økonomisk berigelse og udøve cyberaktivisme og cyberspionage, steget. På øvrige områder vurderes trusselbilledet at være mere eller mindre uændret.

3.2 Konkrete angrebsmetoder og risici for kommunen

Deloitte vurderer, at der er fire metoder, der vil blive anvendt af ondsindede aktører i forbindelse med cyberangreb på Københavns Kommune.

Tabel 4. Metoder til cyberangreb

Metoder	Eksempler	Vurderet nuværende og fremtidig risiko
Tyveri, manipulation og social engineering	• Phishing • Smishing • Social engineering • CEO fraud • Høst af brugeroplysninger	**Lav**
Ondsindede installationer	• Malware • Ransomware • Botnets • Spyware	**Høj**
Uautoriseret adgang	• Målrettet indtrængen • Opportunistisk målretning • Udnyttelse • Høst af brugeroplysninger	**Middel til høj**
Overbelastning af servere	• DDoS • Botnets	**Lav**

Tyveri, manipulation og social engineering vurderes at udgøre en relativt lille risiko for Københavns Kommune på trods af en høj sandsynlighed for, at kommunen vil rammes heraf. Vurderingen bygger på, at kommunen har gennemført en lang række tiltag, herunder awarenesskampagner, for at minimere risikoen. Tilsvarende vurderes **overbelastning af servere** ligeledes at udgøre en relativt lille risiko for Københavns Kommune på trods af en høj sandsynlighed for, at kommunen vil rammes heraf, idet kommunen har en god perimetersikkerhed og benytter services fra eksterne udbydere, der mitigerer risikoen. Det skal dog nævnes, at DSB, der anvender samme services til mitigering af DDoS, for nylig blev lagt ned af et DDoS-angreb.

Deloitte ser derimod en stor risiko for, at Københavns Kommune vil blive ramt af **ondsindede installationer** eller **uautoriseret adgang**. Dette skal ses i lyset af sandsynligheden for, at der vil forekomme et angreb, den potentielle konsekvens ved et sådant angreb samt den nuværende praksis i særligt KIT, når det drejer sig om at sikre sig imod sådanne angreb. De to mest risikofyldte metoder samt KIT's praksis er nærmere gennemgået nedenfor.

Ondsindede installationer kan nedlægge store dele af kommunens it-infrastruktur

Ondsindede installationer kan være i form af malware, der ødelægger infrastruktur, og ransomware, der så at sige kidnapper dele af infrastrukturen, og hvor der kræves løsepenge for genåbne den. Det kan endvidere være i form af spyware, som gør det muligt for aktører på et senere tidspunkt at hacke systemer, hvor de er svagest. Endelig kan ondsindede installationers målsætning være at anvende den inficerede enhed til angreb på servere; den tidligere nævnte hændelse hos Mærsk var baseret på en ondsindet installation. Kommunen har oplyst, at de også har opdaget ondsindede installationer, men at de indtil nu har været ineffektive.

Københavns Kommune har mange medarbejdere, der anvender teknologi for at udføre deres daglige arbejde, og der er således stor risiko for, at nogen vil komme til at åbne en e-mail eller trykke på et link, som initierer installationen.

Samtidig viser Deloittes analyse af det nuværende it-sikkerhedssetup, at der er en række udfordringer, som gør, at kommunen ikke er tilstrækkelig beredt i forhold til at håndtere angreb baseret på ondsindede installationer. Disse udfordringer er listet nedenfor.

Tabel 5. Udfordringer knyttet til ondsindede installationer

Udfordring	Konsekvens
Kommunens indsats i forhold til analyse af logdata mhp. identifikation af anormale mønstre, der udgør en risiko, bør styrkes.	Det kan gå unødig lang tid, indtil der responderes på et angreb, og der kan ske yderligere spredning imens.
KIT's mandat i forbindelse med håndtering af sikkerhedshændelser er uklart, særligt når det gælder hændelser, der vedrører fagsystemer.	
Uklare retningslinjer og politikker for løbende sikkerhedspatchning af særligt fagsystemer.	Der kan være ukendte sårbarheder i infrastrukturen, hvorigennem installationer kan foretages, ligesom der ikke er viden om senest udviklede metoder.
Der er begrænset arbejde med cyberthreat intelligence og anvendelse af penetrationstest.	
Kommunens netværk er kun segmenteret i begrænset omfang, og er i dag opdelt i en række zoner, som hver indeholder flere hundrede servere og systemer.	Hvis en ondsindet installation er inde på netværket, vil den kunne sprede sig til stort set hele kommunen.
Kommunen har et meget stort antal privilegerede brugere. Endvidere er der meget begrænset styring med disse, og selvom deres aktivitet logges, følges der ikke op på denne	Der anvendes ofte brugeroplysninger fra privilegerede brugere til at trænge ind på netværk eller i systemer, hvorfor begrænset styring heraf medfører øget risiko for, at angreb er succesfulde.
Der er ikke afsat midler til arbejdet med sikkerhedsarkitektur i kommunen.	Manglende politikker for og krav til sikkerhedsarkitektur øger risikoen for, at der findes systemer i kommunen, der ikke er sikret tilstrækkeligt imod angreb.

Gennem uautoriseret adgang til kommunens it-infrastruktur kan der gøres stor skade

Uautoriseret adgang kan opnås via hacking. Når en aktør har opnået adgang til systemet, er denne i stand til at udføre en række ødelæggende aktiviteter, der spænder fra defacement (ændring af det visuelle udtryk) til fuld administrativ kontrol. Advanced persistent threats (længevarende adgang til systemer) udgør en signifikant fare for informationssystemer.

Deloitte vurderer, at risikoen for Københavns Kommune er middel til stor. Dette skyldes, at selvom sandsynligheden for, at Københavns Kommune rammes af hacking, vurderes som mindre, så vil konsekvensen, hvis det skulle ske, potentielt være meget stor, både i forhold til tilgængelighed, integritet og fortrolighed af data. Samtidig viser Deloittes analyse af det nuværende it-sikkerhedssetup, at der er en række udfordringer, som gør, at kommunen ikke er tilstrækkelig beredt i forhold til håndtering af angreb baseret på uautoriseret adgang. Disse udfordringer er listet nedenfor.

Tabel 6. Udfordringer knyttet til uautoriseret adgang

Udfordring	Konsekvens
Københavns Kommunes it-installation er så stor og kompleks, at cyberangreb er meget vanskelige at spore	Det kan tage unødig lang tid at opdage et angreb, og imens vil en ondsindet aktør have mulighed for at agere uden at blive opdaget.
Kommunens indsats i forhold til analyse af logdata mhp. identifikation af anormale mønstre, der udgør en risiko, bør styrkes, ligesom der bør arbejdes med prædefinerede angrebsscenarier for "normal" system- og infrastrukturbrug	
KIT's mandat i forbindelse med håndtering af sikkerhedshændelser er uklart, særligt når det gælder hændelser, der vedrører fagsystemer.	
Der foregår hovedsagelig reaktiv analyse af logfiler, altså sporing efter konstatering af mistænkelige hændelser.	
Der er begrænset arbejde med cyberthreat intelligence og anvendelse af penetrationstest.	Der kan være ukendte sårbarheder i infrastrukturen, hvorigennem

Udfordring	Konsekvens
	uautoriseret adgang kan ske, ligesom der ikke er viden om senest udviklede metoder.
Kommunens netværk er kun segmenteret i begrænset omfang, og er i dag opdelt i en række zoner, som hver indeholder flere hundrede servere og systemer.	Hvis en ondsindet aktør er inde på netværket, vil denne kunne bevæge sig rundt til stort set hele kommunen.
Kommunen har et meget stort antal privilegerede brugere. Endvidere er der meget begrænset styring med disse, og selvom deres aktivitet logges, følges der ikke op på denne	Der anvendes ofte brugeroplysninger fra privilegerede brugere til at trænge ind på netværk eller i systemer, hvorfor begrænset styring heraf medfører øget risiko for, at angreb er succesfulde.
Der er ikke afsat midler til arbejdet med sikkerhedsarkitektur i kommunen.	Manglende politikker for og krav til sikkerhedsarkitektur øger risikoen for, at der findes systemer i kommunen, der ikke er sikret tilstrækkeligt imod angreb.

3.3 Kommunens beredskab ved et cyberangreb med store konsekvenser

Københavns Kommune har i dag ikke en klar plan for håndtering af et cyberangreb med store konsekvenser. Deloittes overordnede vurdering af det nuværende beredskab følger nedenfor.

Tabel 7. Nuværende beredskab

Område	Beredskab	Konsekvens
Systemer	Der findes p.t. ikke en prioriteret oversigt på tværs af forvaltningerne over, hvilke systemer det er vigtigst at få sikret imod et cyberangreb. Der arbejdes i de enkelte forvaltninger på en prioritering og en udarbejdelse af beredskabsplaner. Der er en uklar ansvarsdeling mellem forvaltningerne og KIT. Særligt for kommunens ældre kritiske systemer vides det ikke, om der er en tilstrækkelig solid plan for genetablering.	Der kan gå unødig lang tid, til systemer er genoprettet, hvilket kræver, at der foretages en prioritering på tværs af forvaltninger. Det er uklart, om det er muligt hurtigt at retablere særligt kommunens ældre kritiske systemer. *Der er i regi af nærværende analyse lavet et overordnet udkast til prioritering af opgaveområder og systemer.*
Brugerstyring	Ikke omfattet af analysen, men det er angivet, at der ved en angreb lig det, der skete hos Mærsk, ikke er muligt umiddelbart at retablere kommunens centrale brugerstyringssystem .	Brugerstyringssystemet skal retableres fra bunden, hvilket kan tage meget lang tid.
KIT's datacenter	Se ovenfor ud for systemer.	Se ovenfor ud for systemer.
Outsourcet drift	Se ovenfor ud for systemer.	Se ovenfor ud for systemer.
Netværk	Der er som tidligere nævnt kun begrænset netværkssegmentering. Der er ikke en klar prioritering af, hvilke lokationer i kommunen som skal prioriteres i tilfælde af angreb på kommunens netværksinfrastruktur, som resulterer i, at man på kommunens mange lokationer ikke kan komme på netværket.	Et cyberangreb kan sprede sig til stort set hele kommunen.
Slutbrugerenheder	KIT angiver, at de formodentlig er i stand til at geninstallere cirka 200-300 slutbrugerenheder per døgn. Dette forventes dog at stige til op imod 1.000 fra november.	Skulle kommunen komme i en situation, hvor en stor del af kommunens cirka 22.500 slutbrugerenheder ikke er funktionsdygtige, vil det i værste fald betyde, at der vil være brugere, der står uden enhed i en længere periode.

4 Anbefalede indsatser

Med baggrund i trusselbilledet for Københavns Kommune og de konkrete udfordringer, der er identificeret, vurderer Deloitte, at Københavns Kommune bør styrke sit tekniske cyberforsvar indenfor fire hovedområder for at sikre sig imod det stigende trusselniveau, der er for kommunen.

Tabel 8. Fire indsatsområder

Indsatsområde	Overordnet beskrivelse	Samlet økonomi
1. Overvågning og detektering	Proaktiv overvågning af infrastrukturen for at opdage eventuelle trusler og øget opmærksomhed på trusselbilledet. Løbende test af eventuelle sårbarheder og styrket it-sikkerheds- og compliancestyring.	**Anbefaling om implementering af 12 konkrete tiltag** **Investering:** 20,5-29,9 mio. kr. **Øget årlig drift:** 11,7-18,4 mio. kr.
2. It-sikkerhedsarkitektur og releasestyring	Etablering af en sikkerhedsarkitektur for kommunen samt yderligere sikring af og styring med sikkerhedspatchning på systemniveau.	
3. Beredskab og hændelseshåndtering	Styrkelse af it-beredskabet både ved kvalificering af det eksisterende beredskab og ved tydeliggørelse af mandater, processer, samarbejde og kommunikation.	
4. Infrastrukturtiltag og genetableringskapabilitet	Igangsættelse af en række infrastrukturtiltag, der skal øge den tekniske sikkerhed i forhold til cyberangreb. Sikring af, at kommunen i tilfælde af nedbrud som følge af et cyberangreb bliver funktionsdygtig så hurtigt som muligt for derigennem at mindske skadevirkningen i størst mulig grad.	

I det følgende gennemgås hvert af de fire områder, herunder hvorfor Københavns Kommune skal styrkes på området, hvad bedste praksis er på området, og hvilke tiltag Deloitte anbefaler at igangsætte.

Estimaterne er et udtryk for en vurdering af prisspænd i forhold til foranalyse, anskaffelse, implementering og efterfølgende drift af de enkelte indsatser, og som grundlag for eksekvering på de konkrete indsatser forudsættes blandt andet en omkringliggende (rimeligt) velfungerende infrastruktur samt procesgange.

Hver indsats er vurderet i forhold til, hvilken effekt de vil have ved implementering. Vurderingen bygger på i alt fem parametre (styrker indsigt og læring, styrker perimetersikkerheden, reducerer skadesomfang, reducerer tid fra hændelse til detektion og reducerer genopretningstid), der hver især er vægtet i forhold til vigtigheden for Københavns Kommune set i forhold til det nuværende og fremtidige trusselsbillede samt de eksisterende udfordringer i forhold til it-sikkerheden. Hver indsats er således vurderet fra 0 (slet ikke) til 8 (i meget stor grad) på hver parameter, hvilket har givet dem en samlet score, der er anvendt til at foretage en samlet prioritering af indsatserne.

Endvidere er det vurderet, i hvor høj grad de anbefalede indsatser mindsker den nuværende og fremtidige risiko for kommunen i forhold til de identificerede angrebsmetoder (tyveri, manipulation og social engineering, ondsindede installationer, uautoriseret adgang og overbelastning af servere). For hver indsats er det således vurderet, i hvilken grad de mindsker risikoen. Dette er sket på en skala fra ingen påvirkning til i høj grad.

4.1 Overvågning og detektering

Overvågning og detektering omfatter, at kommunen skal have bedre og mere dybtgående værktøjer og kompetencer til at fastlægge, hvilke trusler der i realtid og nærrealtid er rettet med kommunens it-infrastruktur, så kommunen er bedre i stand til at reagere hurtigt og mere proaktivt – dette både i forhold til forsøg på ondsindede installationer og uautoriseret adgang til systemer mv. Den øgede overvågning skal implementeres gennem både anskaffelse af nye services og it-løsninger samt tilknytning af yderligere årsværk.

Endvidere skal der sikres en bedre forståelse og adressering af de sårbarheder, som er knyttet til såvel systemer som infrastruktur. Dette skal ske gennem en systematisk anvendelse af penetrationstest.

Hvad er gjort, og hvilke problemstillinger er der i dag?

KIT har implementeret en security incident and event management-løsning (SIEM-løsning), som i forhold til en stor del af kommunens systemer og infrastruktur opsamler logdata på aktiviteter. Endvidere er arbejdet med overvågning blevet forankret i en dedikeret enhed for operationel sikkerhed. I forhold til aktuelle trusler er der et samarbejde med Center for Cybersikkerhed, ligesom der abonneres på udvalgte tekniske rapporter, herunder fra CSIS.

Nedenfor følger de centrale udfordringer, som Deloitte ser, og de potentielle konsekvenser, som udfordringerne kan have for kommunen.

Tabel 9. Udfordringer og konsekvenser

Udfordringer – Deloittes observationer	Potentielle konsekvenser af ikke at gøre noget
• Københavns Kommunes it-installation er så stor og kompleks, at cyberangreb er meget vanskelige at spore. • Der er i dag opsat regelbaserede alarmer i den fælles logopsamling, og der foretages sporing efter konstatering af mistænkelige hændelser i kommunens systemer. Deloitte vurderer dog, at kommunens indsats i forhold til analyse af logdata mhp. identifikation af anormale mønstre, der udgør en risiko, bør styrkes ressourcemæssigt, ligesom der i dag ikke er investeret i egentlige it-værktøjer hertil. • Der anvendes kun i begrænset omfang prædefinerede brugsscenarier, der definerer normal og unormal adfærd, og den nuværende teknologi, der anvendes i kommunen, giver i mindre omfang mulighed for at analysere brugermønstre og -adfærd. o • Der foretages i dag løbende sårbarhedsscanninger, men der gennemføres ikke i systematisk omfang penetrationstests (simulerede angreb på systemer eller infrastruktur) for derigennem at opnå yderligere indsigt i, hvilken effekt et angreb ville have i forhold til kommunens sårbarheder.	• Angreb vil først opdages, når angrebet har medført så store skadevirkninger, at den normale drift forstyrres. I praksis kan det være mange timer eller dage efter, at angreb et er påbegyndt. Derudover er det en risiko for, at såfremt angrebet har til formål at stjæle data, så vil man med den overvågning, man har i dag med stor sandsynlighed ikke opdage angrebet, da det ikke medfører driftsnedbrud. • Den komplekse infrastruktur bevirker, at genoprettelsestiden efter et angreb vil være længere end i andre kommuner. Jo længere tid et angreb er uopdaget i infrastrukturen, jo flere services kan potentielt inficeres. Hastighed i opdagelsen af angreb er derfor afgørende for hvor lang nedetid, der kan forventes. o • Der kan eksistere (ukendte) sårbarheder, som ondsindet software eller hackere vil kunne udnytte.

Hvad gør andre, og hvad er god praksis?

Deloitte ser en tendens til, at virksomheder i lyset af det generelt stigende trusselbillede investerer og opnormerer i overvågningsteknologi og -kapabiliteter med henblik på at kunne reagere hurtigere på cyberangreb og dermed begrænse skadevirkninger. Dette omfatter investering i systemer til opsamling og analyse af data, herunder SIEM-løsninger, og etablering af dedikerede enheder – enten internt eller sourcet – der står for overvågning og analyse. Typisk sker disse investeringer og opnormeringer i umiddelbar forlængelse af, at man har været udsat for et større cyberangreb med stor skadevirkning. Eksempler herpå, som Deloitte er bekendt med, er flere forsikrings- og energiselskaber samt statslige institutioner. Det skal dog bemærkes, at adgangen til effektive redskaber til eksempelvis analyse af logs og adfærd baseret på machine learning er forholdsvist nyt, men der er i øjeblikket en stor efterspørgsel efter og fokus på at implementere sådanne løsninger.

På det statslige område etableres der i forlængelse af den nye cyber- og informationssikkerhedsstrategi et døgnbemandet overvågningscenter i Statens It, der vil give alle Statens It's kunder (som *ikke* omfatter de mest udsatte statslige myndigheder såsom Forsvaret, Rigspolitiet og SKAT) muligheden for døgnovervågning af kritiske systemer. Endvidere etableres et døgnbemandet nationalt cybersituationscenter ved Center for Cybersikkerhed for at skabe et nationalt situationsbillede af den aktuelle sikkerhedstilstand for samfundskritiske digitale netværk. Situationscentret skal foretage teknisk monitorering af netværk, scanne efterretningskilder, medier og fora for oplysninger om nye trusler og igangværende potentielt alvorlige cyberangreb og samtidig fungere som nationalt kontaktpunkt i forhold til grænseoverskridende cybersikkerhedshændelser.

Økonomi og effekt

Deloitte anbefaler fire tiltag med underliggende behov for investering og øgede driftsomkostninger.

Tabel 10. Indsatser i forhold til overvågning og detektering

Indsats	Investering	Drift	Vurderet effekt af forslag (fra 0-8)
1.1. Overvågning af infrastruktur	2,0 - 2,8 mio. kr.	3,8 - 5,8 mio. kr.	5,4
1.2. Gennemførelse af penetrationstest	-	0,9 - 1,3 mio. kr.	3,3
Total	4,5 - 6,3 mio. kr.	4,4 - 6,7 mio. kr.	

4.2 It-sikkerhedsarkitektur og releasestyring

It-sikkerhedsarkitektur og releasestyring omfatter, at kommunen tilfører ressourcer til KIT's enterprisearkitekturfunktion og således påbegynder et arbejde med sikkerhedsarkitektur for at understøtte kontinuerlig og struktureret udarbejdelse af en samlet sikkerhedsreferencearkitektur, herunder en fast definition af krav til nye systemer, så de bygges efter en standardiseret og sikker måde. Endvidere skal enterprisearkitekturfunktion stå for at udvikle krav til sikkerhedstest og støtte forvaltninger i dette arbejde. It-sikkerhedsarkitektur bør være en integreret funktion i Københavns Kommune. Den skal sikre, at nye systemer bygges efter en standardiseret og sikker måde.

Endelig anbefales det, at der i regi af KIT etableres en fælles og styret release management-proces/-politik for såvel forvaltningerne som KIT, som dækker alle kritiske it-aktiver (kronjuveler) og sikrer en styret sikkerhedsmæssig opdatering, så forvaltningernes systemer er sikkerhedsmæssigt forsvarligt patchet. Dette skyldes ikke mindst bevægelsen mod cloud samt den øgede digitalisering, der giver flere og flere systemer hos forvaltningerne.

Hvad er gjort, og hvilke problemstillinger er der i dag?

Der findes en række sikkerhedskrav defineret af KIT, der skal anvendes i forbindelse med udvikling og anskaffelse af nye applikationer, ligesom der foretages årlige risikovurderinger af applikationer i kommunen (påbegyndt i 2017). I forlængelse af vurderingen fremsendes en række krav til systemejerne, der skal højne sikkerheden i applikationen. I forhold til patchning, så har de systemansvarlige i KIT formuleret og følger faste procedurer for patchning af kommunens fælles systemer og infrastrukturen.

Kommunen har i dag ikke dedikerede ressourcer, der arbejder med it-sikkerhedsarkitektur. Det er KIT's formodning, at det tidligere har fordyret kommunens projekter, og i dag er der eksempler på, at det har haft sikkerhedsmæssige konsekvenser. Det er vurderingen, at disse konsekvenser vil øges fremover, såfremt der ikke tilføres dedikerede it-sikkerhedsressourcer til KIT's enterprisearkitekturfunktion.

Nedenfor følger de centrale udfordringer, som Deloitte ser, og de potentielle konsekvenser, som udfordringerne kan have for kommunen.

Tabel 11. Udfordringer og konsekvenser

Udfordringer – Deloittes observationer	Potentielle konsekvenser af ikke at gøre noget
• Der er ingen dedikerede ressourcer i KIT, der arbejder med it-sikkerhedsarkitektur, da der aldrig er afsat midler hertil. • Der findes ingen fast sikkerhedsreference-arkitektur, som forvaltningerne og KIT kan anvende som grundlag for udvælgelse, design og udvikling af it-løsninger, der sikrer en høj fortrolighed, integritet, tilgængelighed og robusthed. • Der bliver i mange tilfælde ikke sikkerhedskravstillet korrekt i forvaltningerne i forbindelse med systemanskaffelser, og der mangler konkret viden om, hvad der skal kravstilles i forhold til sikkerhed. • Forvaltningerne efterspørger i stigende grad arkitekturbistand i forbindelse med systemanskaffelser. Rådgivningen fra KIT lider dog under, at den ikke er baseret på fælles standarder o • Kommunen er i en proces, hvor der løbende anvendes flere cloud-løsninger. Kommunen arbejder endvidere med evergreen it, hvor alle komponenter konstant er fuldt patchede. Det betyder, at der er behov for øget styring af en central opfølgning på, om alle forvaltningernes systemer og applikationer er sikkerhedsmæssigt patchet. o • Koncern IT har ikke i fuldt omfang implementeret segregation of duties.	• Ved ikke at have en dedikeret bemanding samt en fast og veldefineret sikkerheds-arkitektur og -politik kan der potentielt blive introduceret sårbarheder igennem usikkerhed i arkitekturen i nye applikationer. o • Uden en central styring af Release Management for sikkerhedsområdet, er det op til den enkelte systemejer at sikre, at deres applikationer er opdaterede. I praksis er dette en nedprioriteret opgave, og det kan betyde, at kommunen udsættes for en risiko. o • Det betyder, at en ondsindet intern medarbejder selvstændigt kan ødelægge større dele af den samlede it-infrastruktur. Der er således risiko for, at en medarbejder bevidst kan udrette omfattende skade. Der er endvidere risiko for, at dette kan ske ubevidst.

Hvad gør andre, og hvad er god praksis?

Det er Deloittes vurdering og erfaring, at et centralt element i at opnå en ordentlig sikkerhed og sammenhængskraft i et setup med en semidecentral organisering af it-ansvar, er en central enhed, der definerer retningslinjer og styring i forhold til it-arkitektur, herunder særligt it-sikkerhedsarkitektur. Disse retningslinjer indbefatter typisk klare politikker samt retningslinjer for sikkerhed og patchning for de systemer, der knyttes til den fælles infrastruktur.

Vigtigheden af en central enhed, der definerer it-sikkerhedsarkitektur ses i såvel større private virksomheder som i større offentlige institutioner samt på tværs af den offentlige sektor; it-sikkerhedsarkitektur spiller for eksempel en afgørende rolle i en lang række offentlige institutioner. KIT

har fået oplyst, at SKAT, DSB, Statens It og Rigspolitiet alle har etableret et it-sikkerhedsarkitektursetup på mellem tre og otte årsværk.

Økonomi og effekt

Deloitte anbefaler to tiltag med underliggende behov for øgede driftsomkostninger.

Tabel 12. Indsatser i forhold til it-sikkerhedsarkitektur og releasestyring

Indsats	Investering	Drift	Vurderet effekt af forslag (fra 0-8)
2.1. It-sikkerhedsarkitektur	-	1,5-2,3 mio. kr.	4,3
2.2 Release management på sikkerheds-området	-	1,1-1,5 mio. kr.	1,9
2.3 Segregation of duties	-	0,8-1,1 mio. kr.	1,0
Total	-	3,4-4,9 mio. kr.	

4.3 Beredskab og hændelseshåndtering

beredskabs- og hændelseshåndtering omfatter processer, roller og ansvar, der er knyttet til håndteringen af større it-sikkerhedshændelser, fra de observeres og inddæmmes, og der foretages en genetablering, til normal drift. Det skal sikres, at der på tværs af kommunen er klarhed over processen, samt over hvem der har ansvar for at definere en større sikkerhedshændelse og igangsætte en respons. Dette omfatter for eksempel beslutninger om, hvornår KIT må beslutte at slukke for hele eller dele af systemporteføljen og it-infrastrukturen, samt hvilke beslutningsfora og eskaleringsveje mv. der skal sammensættes for mest effektivt at håndtere hændelsen og så hurtigt som muligt føre kommunen tilbage til normal driftsstadie.

Endvidere omfatter en styrket beredskabs- og hændelseshåndtering, at der findes planer for genetablering, herunder en prioritering af de kritiske it-aktiver (systemer, brugergrupper, lokationer/netværk mv.), samt et overblik over fysiske it-aktiver.

Hvad er gjort, og hvilke problemstillinger er der i dag?

Der er en formaliseret organisation i KIT (operationel it-sikkerhed) med en dedikeret bemanding, der indenfor normal arbejdstid løbende overvåger it-sikkerhedshændelser og agerer ved hændelser, særligt i forhold til de dele af infrastrukturen, der er KIT's ansvar. Endvidere er forvaltningerne i gang med at revidere deres beredskabsplaner, herunder foretage en prioritering af deres it-aktiver og stillingstagen til, hvordan de forretningsmæssigt håndterer situationer, hvor deres systemer er utilgængelige.

Nedenfor er de centrale udfordringer, som Deloitte ser, og de potentielle konsekvenser, som udfordringerne kan have for kommunen, præsenteret.

Tabel 13. Udfordringer og konsekvenser

Udfordringer – Deloittes observationer	Potentielle konsekvenser af ikke at gøre noget
• Den generelle incident management-proces anvendes som udgangspunkt til registreringen og håndteringen af sikkerhedshændelser. • Eskalationsprocessen er ikke klart defineret, ligesom det ikke er defineret, hvem der har ret til at lukke hele eller dele af systemet og netværket mv. i forbindelse med større hændelser. • Der er ikke udviklet en prioriteret plan på tværs af forvaltninger for, hvad eller hvem der først skal genoprettes i forbindelse med et nedbrud. Ligeledes er det uklart, hvem der beslutter, hvad eller hvem der først skal genoprettes. Der findes dog en samlet beredskabsplan for hovedstaden, der i nogen grad også omfatter cybersikkerhed. • Der gennemføres ikke beredskabstest. Der er dog i regi af Hovedstadens Beredskab ved at blive planlagt en gennemførelse af en beredskabstest.	• Manglen på en defineret incident management-proces kan betyde, at løsningstiden for en sikkerhedshændelse forlænges unødigt. • Manglen på en systematisk behandling af sikkerhedshændelser gør kommunen mindre effektiv i forbindelse med detekteringen og håndteringen af sikkerhedshændelser. • En uklar eskalationsproces kan betyde en forlænget responstid i tilfælde af en hændelse, hvilket kan øge spredning af ondsindede installationer og forlænge løsningstiden. • Manglende klarhed over, hvem der har ret til at lukke ned for systemer mv., betyder, at man potentielt mister muligheden for at inddæmme en ondsindet installation eller en hacker. • Manglende klarhed over, hvad der skal genoprettes først, kan forårsage konflikter mellem de forskellige forvaltninger i forbindelse med en sikkerhedshændelse eller generelle driftsnedbrud.

Hvad gør andre, og hvad er god praksis

Deloitte anbefaler generelt, at man opdeler planlægningen af it-beredskabet i to selvstændige dele. Dette sikrer operationel kapacitet til at reagere på en kritisk hændelse i praksis og compliance med relevante standarder og myndighedskrav. Denne opdeling omfatter følgende:

1. Instruks til it-beredskab: fastlæggelse af it-beredskabets gyldighed, rammer og afgrænsninger og overordnede retningslinjer. Retningslinjerne indeholder ingen følsomme informationer, og må gøres tilgængelig for ansatte samt øvrige myndigheder og tredjeparter.
2. Operationel plan for organisering af it-beredskab: en beskrivelse af proces og organisering af it-beredskabet samt de handlingsorienterede operationelle planer for it-beredskabsorganisationens roller, der finder anvendelse i en aktuel it-beredskabssituation. Endvidere bør den operationelle plan for beredskabet omfatte henvisninger til system- og kontaktinformationer, der finder anvendelse ved aktivering, varsling og kommunikation af it-beredskabet, samt relevante skabeloner til brug i forbindelse hermed. Bilaget kan indeholde følsomme informationer og er klassificeret som fortroligt.

Endelig er det afgørende, at der løbende foretages test og kvalitetssikring af beredskabet og hændelseshåndteringen med henblik på læring og løbende forbedringer.

Økonomi og effekt

Deloitte anbefaler et tiltag med underliggende behov for investering og øget driftsomkostning.

Tabel 14. Indsatser i forhold til beredskab og hændelseshåndtering

Indsats	Investering	Drift	Vurderet effekt af forslag (fra 0-8)
3.1. Incident response	1,7-2,3 mio. kr.	0,2-0,4 mio. kr.	4,1
Total	1,7-2,3 mio. kr.	0,2-0,4 mio. kr.	

4.4 Infrastrukturtiltag og genetableringskapabilitet

Infrastrukturtiltag omfatter en styrkelse af netværkssegmenteringen i kommunen gennem implementering af softwarebaseret løsning, således at det er muligt at begrænse spredningseffekten af et cyberangreb. Endvidere anbefales det, at der anskaffes og implementeres en såkaldt cloud access security broker, som er et stykke software, der sidder mellem kommunens og cloud-leverandørens infrastruktur og sikrer, at kommunens sikkerhedspolitikker overholdes af cloud-leverandøren.

Derudover anbefales det, at der implementeres en såkaldt privileged access management-løsning, der kontrollerer adgange samt logger og analyserer brugeres adfærd, ligesom den sikrer, at der kun gives tidsbegrænsede privilegerede adgange (brugerkonti med udvidede rettigheder). Ydermere bør der ses på, om der kan sikres hurtigere genetablering af kommunens brugerstyringssystem (AD), da dette i dag er centralt for den samlede brugeradgang, og hvis det ikke er tilgængeligt, så vil ingen brugere kunne anvende deres it-systemer.

Hvad er gjort, og hvilke problemstillinger er der i dag?

Der foregår i dag nogen grad af overvågning af netværk og firewalls. Ligeså sikres det, at alle slutbrugerenheder har opdateret antivirus, og med den igangværende migrering til Win10E opnås der her en yderligere sikring af kommunens desktops, herunder i forbindelse med implementering af whitelisting.

Nedenfor er de centrale udfordringer, som Deloitte ser, og de potentielle konsekvenser, som udfordringerne kan have for kommunen, præsenteret.

Tabel 15. Udfordringer og konsekvenser

Udfordringer – Deloittes observationer	Potentielle konsekvenser af ikke at gøre noget
• Kommunens netværk er i dag opdelt i en række zoner, som hver indeholder flere hundrede servere og systemer. Det betyder, at hvis en hacker får adgang til ét system, vil denne have uhindret adgang til at kompromittere alle andre systemer i netværkszonen. o • I dag anvendes over 2000 store og små cloudtjenester. Det kan være fildelingstjenester, konverteringsværktøjer eller usikre sociale medier. KIT har kontrol med de cloud-tjenester, der indmeldes i FISKK, men der er ikke kontrol med de tjenester der i øvrigt købes af forvaltningerne, og der er i dag ingen tekniske begrænsninger for hvilke tjenester, der anvendes. o • Kommunen har et meget stort antal privilegerede brugere. Endvidere er der meget begrænset styring med disse, og selvom deres aktivitet logges, følges der ikke op på denne, da der ikke er afsat midler hertil o • Kommunen har aktivt valgt en 'åben-dør-politik', hvor de fleste af kommunens lokationer er tilgængelige for alle. Dette gør sig også gældende for KITs lokaler hvor det på trods af krav om adgangskort ved indgang er relativt simpelt at komme ind ved at følge efter en medarbejder. o • Kommunens Active Directory (AD) er et centralt angrebsmål i forbindelse med cyberangreb og er et helt centralt element i kommunens it-infrastruktur. Der foretages løbende backup af kommunens AD, men der er ikke iværksat nogle særlige procedurer for yderligere at sikre, at man altid er i besiddelse af en version af AD'et. o • Hvis kommunen rammes af et meget stort cyberangreb, kan ødelæggelserne være så omfattende, at der er behov for ekstern arbejdskraft og kompetencer for at sikre en tilstrækkelig hurtig reetablering af infrastrukturen.	• Manglende segmentering af netværk medfører, at malware, ransomware og hackere mv. har mulighed for at sprede sig uhindret i netværket, ligesom det tager længere tid at genoprette it-systemerne efter et vellykket cyberangreb, fordi kompleksiteten er stor, og fejlsøgning dermed er svær. o • Manglende styring med cloudtjenester kan medføre en række sikkerhedsmæssige risici. Cloudtjenesterne kan eksempelvis udsættes for et DDoS-angreb, ligesom der er eksempler på, at sikkerheden nedprioriteres i forbindelse med genbrug af elementer i SaaS-produkter. o • Manglen på opfølgning på privilegerede brugeres ageren medfører en risiko for, at disse brugere opfører sig destruktivt, uden at kommunen er opmærksom herpå, eller at disse brugeres adgange bliver brugt til installation af ransomware. o • Det er især kritisk for KIT, da mange medarbejdere har udvidede rettigheder, og det er muligt at få fysisk adgang til dele af infrastrukturen. Dermed er der risiko for, at en ondsindet aktør kan anvende denne adgang destruktivt. o • Ved ikke at have adgang til en backup af AD risikeres genopretningstiden at stige signifikant, i det der potentielt skal ske en samlet genopretning af alle brugere. o • Hvis angrebet har ramt mange danske organisationer, kan det reelt være vanskeligt at skaffe disse ressourcer, da mange offentlige og private organisationer vil efterspørge dem på én gang.

Hvad gør andre, og hvad er god praksis?
Deloitte ser generelt, at virksomheder i lyset af det generelt stigende trusselbillede og i lyset af, at flere og flere løsninger leveres via et cloud-setup, investerer i og opnormerer deres it-infrastruktur, særligt når de ligesom Københavns Kommune har en infrastruktur med et decentralt setup med mange brugere og lokationer. I forhold til styring af privilegerede brugeres adgang var manglende styring heraf i Mærsks tilfælde en af årsagerne til, at deres store nedbrud i 2017 blev så omfattende, som det gjorde.

Ved at implementere segmentering sikres det, at et angreb ikke kan sprede sig til andre systemer, da de enkelte systemer og servere bliver isoleret på hvert sit netværk. Det er en tendens i markedet, at store virksomheder implementerer netværkssegmentering. Både Nordea, Mærsk og SIT samt Hillerød, Frederiksberg, Ålborg, Herning m.fl. kommuner anvender segmentering.

I forhold til cloud har for eksempel Stockholm kommune i deres sikkerhedspolitik lagt særlig fokus på sikring af cloud-løsninger ud fra argumentet om, at flere og flere af kommunens løsninger bliver cloud-baseret.

Styring af priviligerede brugere er noget, der er kommet i fokus i løbet af de seneste år, ikke mindst på fordi vigtigheden heraf sås i angrebet mod Mærsk i 2017, hvor manglende styring af privilegerede rettigheder årsagen til, at det gik så galt som det gjorde. Dette har således bevirket, at mange organisationer, herunder Mærsk, i den seneste tid netop har implementeret en Privilege Acces Management-løsning.

I forhold til AD'et ses det i de fleste sammenlignelige organisationer, at der er sket en yderligere sikring heraf, eksempelvis igennem yderligere back-up. Når det drejer sig om kritiske systemer, så er der eksempler på virksomheder, der anvender resilient infrastruktur, som er placeret i et dark center (et datacenter, hvor kritiske systemer kører i dubleret drift) således at der her kan ske en hurtig reetablering. Det vurderes dog ikke som meget relevant for Københavns Kommune, da mange af de kritiske systemer ikke er placeret i kommunens egne driftscentre. I forhold til slutbrugerenheder er der eksempler på, at der anvendes tredjepartsaftaler om standbykapacitet, i forhold til at kunne levere for eksempel præinstallerede pc'er – baseret på et nødberedskabsimage – i tusindvis dagligt. Ligeledes ses det, at der laves en aftale med eksterne leverandører, der kan stille mandskab til rådighed indenfor kort tid.

Økonomi og effekt

Deloitte anbefaler seks tiltag med underliggende behov for investering og øget driftsomkostninger.

Tabel 16. Indsatser i forhold til infrastrukturtiltag og genetableringskapabilitet

Indsats	Investering	Drift	Vurderet effekt af forslag (fra 0-8)
4.1. Segmentering af netværk	9,6 - 13,4 mio. kr.	1,2 - 1,7 mio. kr.	4,5
4.2. Cloud access security broker	1,2 - 1,9 mio. kr.	0,6 - 1,0 mio. kr.	1,5
4.3. Privileged access management-løsning	4,9 - 7,8 mio. kr.	0,8 - 1,5 mio. kr.	2,4
4.4. Fysisk sikring af KIT	0,5 - 0,6 mio. kr.	-	2,4
4.5. Yderligere sikring af Active Directory	-	0,1 - 0,2 mio. kr.	3,3
4.6. Leverandør-understøttelse ved nedbrud	0,7 - 1,1 mio. kr.	0,8 - 1,5 mio. kr.	3,1
Total	16,9 - 24,7 mio. kr.	3,5 - 6,0 mio. kr.	

4.5 Opsummering af anbefalede indsatser

I nedenstående tabel er de gennemgåede tiltag opsummeret og prioriteret i forhold til deres vurderede effekt.

Tabel 17. Samlet prioriteret liste over indsatser

Prioritering	Indsats	Investering	Årlig driftsudgifter	Effekter ved implementering					Samlet effekt af forslag – uvægtet (0-8)	Samlet effekt af forslag – vægtet (0-8)
				Styrker indsigt og læring (0-8)	Styrker perimeter-sikkerheden (0-8)	Reducerer skadesomfang (0-8)	Reducerer tid fra hændelse til detektion (0-8)	Reducerer genopretningstid (0-8)		
				Sandsynlighed	Konsekvens		Genopretning			
				Vægt: 20%	Vægt: 10%	Vægt: 30%	Vægt: 20%	Vægt: 20%		
1	**1.1. Overvågning af it-infrastruktur**	2,0-2,8 mio. kr.	3,8-5,8 mio. kr.	8	3	5	6	4	**4,3**	**5,4**
2	**4.1. Segmentering af netværk**	9,6-13,4 mio. kr.	1,2-1,7 mio. kr.	0	8	7	4	4	**3,8**	**4,5**
3	**2.1. It-sikkerhedsarkitektur**	-	1,5-2,3 mio. kr.	5	4	5	4	3	**3,5**	**4,3**
4	**3.1. Incident response**	1,7-2,3 mio. kr.	0,2-0,4 mio. kr.	2	0	5	5	6	**3,0**	**4,1**
5	**4.5. Yderligere sikring af Active Directory**	-	0,1-0,2 mio. kr.	0	0	7	0	6	**2,2**	**3,3**
6	**1.2. Gennemførsel af penetration tests**	-	0,9-1,3 mio. kr.	6	4	3	4	0	**2,8**	**3,3**
7	**4.6. Leverandørerunderstøttelse ved nedbrud**	0,7-1,1 mio. kr.	0,8-1,5 mio. kr.	0	0	5	3	5	**2,2**	**3,1**
8	**4.4 Fysisk sikring af KIT**	0,5-0,6 mio. kr.	-	0	6	6	0	0	**2,0**	**2,4**
9	**4.3. Privileged Access Management-løsning**	4,9-7,8 mio. kr.	0,8-1,5 mio. kr.	0	6	6	0	0	**2,0**	**2,4**
10	**2.2. Release Management på sikkerhedsområdet**	-	1,1-1,5 mio. kr.	0	4	5	0	0	**1,5**	**1,9**
11	**4.2. Cloud Access Security Broker**	1,2-1,9 mio. kr.	0,6-1,0 mio. kr.	0	5	2	2	0	**1,5**	**1,5**
12	**2.3. Segregation of duties**	-	0,8-1,1 mio. kr.	0	4	2	0	0	**1,0**	**1,0**
Total		**20,5-29,9 mio. kr.**	**11,7-18,4 mio. kr.**							

I nedenstående tabel er det vurderet, i hvor høj grad de anbefalede indsatser mindsker den nuværende og fremtidige risiko for kommunen i forhold til de identificerede angrebsmetoder. Vurderingen er sket ud fra en skala på i alt fire trin, hvoraf den laveste vurdering er, at indsatsen ingen påvirkning har på risikoen, herefter at det mindsker i risikoen i mindre grad, herefter at den mindsker risikoen i nogen grad og som den højeste vurdering, at det mindsker risikoen i høj grad.

	Tyveri, manipulation og social engineering	**Ondsindede installationer**	**Uautoriseret adgang**	**Overbelastning af servere**
Nuværende og fremtidig risiko:	***Lav***	***Høj***	***Middel til høj***	***Lav***
1.1. Overvågning af it-infrastruktur	I mindre grad	I høj grad	I høj grad	Ingen påvirkning
4.1. Segmentering af netværk	Ingen påvirkning	I høj grad	I nogen grad	Ingen påvirkning
2.1. It-sikkerhedsarkitektur	I mindre grad	I nogen grad	I nogen grad	I mindre grad
3.1. Incident response	Ingen påvirkning	I nogen grad	I nogen grad	I nogen grad
4.5. Yderligere sikring af Active Directory	Ingen påvirkning	I høj grad	I nogen grad	Ingen påvirkning
1.2. Gennemførsel af penetration tests	Ingen påvirkning	I nogen grad	I nogen grad	Ingen påvirkning
4.6. Leverandører-understøttelse ved nedbrud	Ingen påvirkning	I mindre grad	I mindre grad	I mindre grad
4.4 Fysisk sikring af KIT	I nogen grad	Ingen påvirkning	I mindre grad	Ingen påvirkning
4.3. Privileged Access Management-løsning	Ingen påvirkning	I mindre grad	I mindre grad	Ingen påvirkning
2.2. Release Management på sikkerhedsområdet	Ingen påvirkning	I mindre grad	I mindre grad	Ingen påvirkning
4.2. Cloud Access Security Broker	Ingen påvirkning	I mindre grad	I mindre grad	Ingen påvirkning
2.3. Segregation of duties	I nogen grad	Ingen påvirkning	Ingen påvirkning	Ingen påvirkning

5 Prioritering af genopretning

Skulle kommunen komme i en situation, hvor et cyberangreb medfører et totalt eller næsten totalt nedbrud af Københavns Kommunes it, og der således ingen mulighed er for, at brugerne kan tilgå kritiske it-services (systemer, data, netværk mv.), så er KIT sammen med forvaltningerne nødt til at genetablere adgangen til it-services i en prioriteret rækkefølge.

Det forretningsmæssige afsæt for prioritering af, hvilke it-services der skal genoperettes først, er drevet af, hvilke af kommunens kerneopgaver, som er de vigtigste at kunne levere. Når det er kendt, hvilke kerneopgaver der bør prioriteres før andre, så kan det – afledt heraf – forretningsmæssigt fastlægges, hvilke organisatoriske enheder/medarbejdergrupper der først skal have adgang til it. Med viden om, hvilke organisatoriske enheder/medarbejdergrupper der skal have adgang til it, kan planlægges, i hvilken rækkefølge følgende handlinger skal foretages:

- Udskiftning/geninstallation af slutbrugerenheder skal tilrettelægges
- Netværksadgang på kommunens lokationer skal tilrettelægges
- Adgang til it-systemer skal genetableres.

5.1 Prioritering af kommunens kerneopgaveområder

DCK (Digitaliseringschefkredsen) har identificeret ti kerneopgaveområder i Københavns Kommune og prioriteret disse på baggrund af vigtighed i forhold til genetableringen fra 1 til 4, hvor 1 er vigtigst, og 4 er mindst vigtig. Syv af de ti områder er overvejende rettet mod borgere i og brugere af Københavns Kommune. De tre øvrige er overvejende internt rettede; det vil sige fokuseret mod kommunens drift som virksomhed. De ti områder, inklusive prioriteringen af disse, er vist på den følgende side.

Borgernes helbred og velvære	Service til borgere	Service til virksomheder	Byens drift, anlæg og miljø	Børnenes trivsel og udvikling	Borgernes velfærd	Kultur- og fritidstilbud til borgere	Kommunens økonomi	Med-arbejdernes sikkerhed	Kommunens ledelse og styring
På en række områder har kommunen ansvar for borgerens helbred, herunder i form af hjemme- og sundhedspleje, tandpleje og håndtering af udsatte grupper og handicappede.	Kommunen har ansvaret for at servicere borgere og hjælpe dem på en række områder, eksempelvis i forbindelse med skat, udstedelse af pas mv.	Kommunen servicerer virksomheder på en række områder, for eksempel i forbindelse med tilladelser, støtte til rekruttering mv.	Kommunen har ansvaret for, at byen fungerer efter hensigten, herunder eksempelvis, at byen er fremkommelig, at der hentes affald, og at byggerier styres og udføres.	Kommunen har ansvaret for, at børnene i kommunen trives og udvikler sig. Dette sker blandt andet igennem institutioner og pasning, folkeskolen og specialunder-visning.	Kommunen støtter borgernes velfærd igennem udbetaling af en række ydelser samt andre former for støtte.	Kommunen har ansvar for at drive en række tilbud på kultur og fritids-området, herunder biblioteker, svømmehaller og idræts-faciliteter.	Kommunen har ansvaret for egen økonomi og budget og er ansvarlig for, at den modtager det, den skal, og at der betales, hvad der skal.	Kommunen har ansvaret for medarbejdernes sikkerhed, når de udfører deres arbejdsopgaver, herunder i forbindelse med håndteringen af udsatte grupper.	Kommunen styres overordnet af Borgerrep-ræsentationen og er herunder opdelt i syv forvaltninger med hver sin borgmester og direktør.
1	2	3	3	3	2	4	2	1	3

Figur 2. Ti prioriterede kerneopgaveområder

5.2 Prioritering af systemgenopretning

Med afsæt i ovenstående prioritering af kommunens kerneopgaver er der lavet nedenstående indikative liste over, i hvilken rækkefølge kommunens systemer/systemområder bør genetableres. Listen er baseret på interview og input fra forvaltningernes digitaliseringschefer og er sandsynligvis ikke fuldt udtømmende. Der bør således fortages en nærmere kvalificering af, hvilke systemer/systemområder, der er. I forbindelse med interviewene er det for systemerne/systemområderne blevet vurderet, hvilke krav der er til tilgængelighed, dataintegritet og datafortrolighed.

Systemgenopretningen er tilrettelagt i tre bølger med afsæt i, 1) hvilket kerneopgaveområde systemet understøtter, og 2) hvilke krav til tilgængelighed der er til systemet.

Figur 3. Prioritering af systemgenopretning

Krav til tilgængelighed	Prioritet 1	Prioritet 2	Prioritet 3	Prioritet 4
Høj	• Sundhedssystemer på ældreplejen (Cura) • Sagsbehandlingssystemer på det sociale område (CSC Social og CSC Omsorg) • Medicinhåndteringssystem (Novax) • Sundhedsplejesystem • Alarm-/kaldesystemer • Telefonisystemer	• Parkeringssystemer • Valgsystemer*	• Vintertjenesten*	
Middel	• Børnetandplejesystem	• Økonomi- og regnskabssystemer • Borgerservicesystemer • Skadedyrsbekæmpelsessystemer • KMD Dagpenge • KMD Aktiv • Øvrige ydelsesudbetalingssystemer • Kommunens hjemmesider • Lønsystemer • Huslejeadministration	• Kirkegårdssystem • Kommunikationssystem i forhold til forældre, lærer og elever • Trafikstyrings- og signalsystem (ITS) • Bygge- og anlægssystemer • Filopbevaringsservices • PPR-systemer • Administrative sags- og journaliseringssystemer • Arbejdsplansystemer	• Biblioteksystemer
Lav	• Visiterings- og indsatssystemer (social og ældre)	• Faglige sagsbehandlingssystemer rettet mod borgere • Jobcentersystemer (Jobcenter planner og Facit) • Kursistadministration • Sprogcentersystemer (Ludus)	• Faglige sagsbehandlingssystemer rettet mod virksomheder • Erhvervshussystemer • Sociale medier • Asset management- og driftssystemer • Facility Management-systemer • Digitale læremidler/-ressourcer • Ledelsesinformationssystemer	• Point-of-sale-systemer (POS) • Booking-/udlejningssystemer • Museumssystemer • Stadsarkivsystemer

**Krav til tilgængelig er kun højt på udvalgte tidspunkter*

Bølge 1 | Bølge 2 | Bølge 3

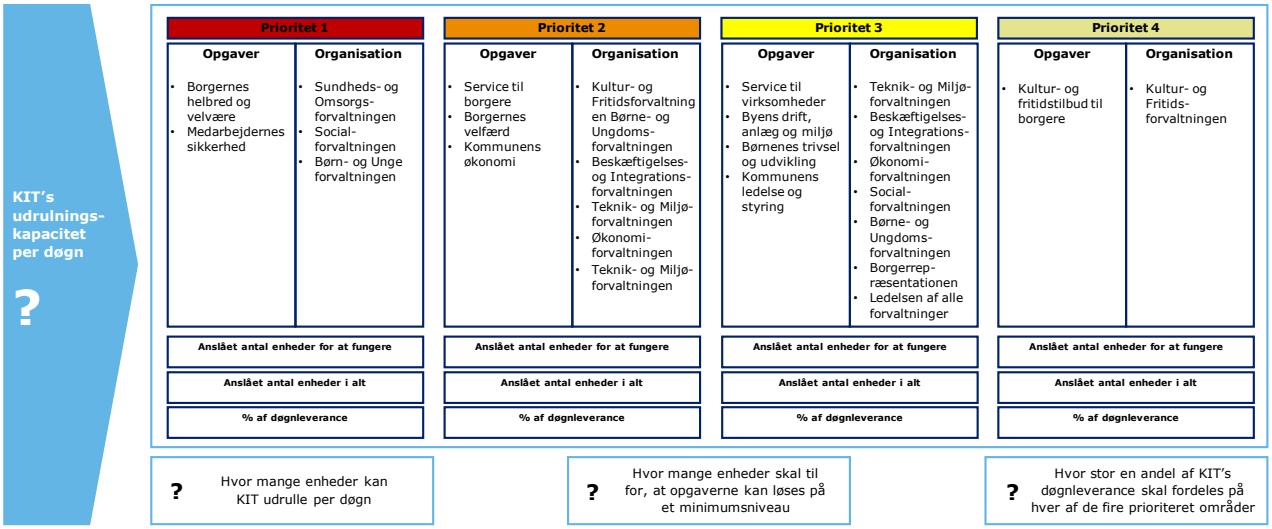
Med afsæt i prioriteringen af kerneopgaveområderne, bør der på tilsvarende vis laves en oversigt over, i hvilken rækkefølge en genopretning af kommunens lokationer bør prioriteres.

5.3 Prioritering af slutbrugerenheder

Princippet for udrulningen af slutbrugerenheder er, at det foregår i rul, hvor hvert område modtager en delmængde af deres samlede slutbrugerenheder per rul. Den konkrete planlægningen heraf bør foretages i et samarbejde mellem forvaltningerne og KIT, hvor det i fællesskab besluttes, hvordan de parate slutbrugerenheder skal fordele sig. Denne beslutning bør dels bero på hvor mange enheder KIT kan udrulle per døgn og dels hvor mange enheder, der skal til for at løse opgaverne på et minimumsniveau.

Til sammen skal disse to spørgsmål således give svaret på, hvor stor en andel af KITs døgnleverance, der skal udleveres til hver af de prioriteret områder, og dermed til de forskellige forvaltninger.

Figur 4. Proces for beslutning om udrulning af slutbrugerenheder



5.4 Operationelle principper for genetablering

Den konkrete genopretning i bølger bør i tillæg til prioriteringen af kerneopgaveområderne også bero på en række operationelle principper. De operationelle principper skal sammen med den forretningsmæssige prioritering understøtte KIT og forvaltningerne i forbindelse med det konkrete arbejde med en genetablering.

De operationelle principper skal ses i lyset af, at der ikke kan laves en fuldt dækkende beskrivelse af potentielle cyberangrebsscenarier og således udarbejdes fulde konkrete genetableringsplaner for forskellige scenarier.

I forbindelse med et nedbrud er det endvidere Deloittes anbefaling, at der i tillæg til de operationelle principper nedsættes et beredskabsforum, der under nedbruddet skal tage stilling til konkrete problemstillinger. Det anbefales, at It-kredsen anvendes hertil.

Princip 1: trinvis genetablering

Såfremt hvert af de ti kerneopgaveområder skal genetableres til fulde, før det næste område kan blive genetableret, kan der potentielt gå meget langt tid, før områderne med prioritet 3 og 4 genetableres.

Således bør planlægningen af genetableringen af hvert af kerneopgaveområderne forgå trinvist således, at der udelukkende genetableres til et minimumsniveau, inden der gås videre til næste område.

Konkret bør det foregå ved, at de forskellige forvaltninger i samarbejde med KIT definerer, hvad minimumsbehovet er for, at kommunen kan levere sin service. Dette gælder således både for hvilke og hvor mange lokationer, der skal være funktionelle, og hvilke systemer, der skal være tilgængelige for, at de konkrete opgaver og services, der ligger under kerneopgaveområderne, kan udføres.

I forlængelse af et nedbrud vil genopretningen således foregå ved, at hvert kerneopgaveområde, startende med prioritet 1, genoprettes til det definerede minimumsniveau, hvorefter genopretningen af næste kerneopgaveområde skal påbegyndes. Dette fortsætter indtil alle kerneopgaveområder har nået sit minimumsniveau, hvorefter kerneopgaveområderne med prioritet 1 vil blive fuldt genoprettet, herefter prioritet 2 og så fremdeles. En nærmere beskrivelse af, hvad minimumsniveauet indbefatter bør tilføjes til kommunens beredskabsplan.

Princip 2: vurdering af beredskabskapabilitet

Der vil være forskel på i hvilken grad de forskellige services kommunen leverer, vil være tilgængelige/mulige at udføre i forbindelse med et nedbrud. Dette forhold bør have indflydelse på den konkrete genetablering af både systemer og organisatoriske enheder/medarbejdergrupper (slutbrugerenheder).

Konkret bør der foretages en vurderingen af de forskellige forvaltningernes beredskabskapabilitet, altså hvor længe de vil kunne fungere uden it-understøttelse. Dette bør gøres i forlængelse af det igangværende arbejde med at lave beredskabsplaner, og bør involvere såvel KIT som forvaltningerne. Hver af de forskellige kerneopgaveområder og de underliggende opgaver bør gennemgås, for at vurdere, hvor længe de kan udføres uden understøttelse af it. Denne vurdering bør efterfølgende være med til at bestemme i, hvilken rækkefølge systemer og slutbrugerenheder genoprettes. Den konkrete rækkefølge bør detaljeres i kommunens beredskabsplan.

Princip 3: særlige tidslige aspekter

Der kan være en række tidslige aspekter, der har indflydelse på i hvilken rækkefølge både systemer, organisatoriske enheder/medarbejdergrupper (slutbrugerenheder) samt lokationer skal genoprettes.

Tidslige aspekter, der bør have indflydelse på prioriteringen kan eksempelvis være tiden på året, idet visse systemer kun relevante i nogle sæsoner (vintertjeneste), deadlines i forhold til løn eller andre udbetalinger samt valghandlinger. I forhold til sidstnævnte skal det understreges, at selvom et valg rent teknisk godt kan gennemføres under et nedbrud, vil det skabe betydelige kaos, skade kommunens omdømme og have store politiske konsekvenser, hvis der er et nedbrud under valghandlingen, hvorfor netop it, der anvendes til valg, bør prioriteres meget højt i forbindelse med valghandlingen.

Konkret bør, der i et samarbejde mellem KIT og forvaltningerne foretages en mapning af alle relevante tidslige aspekter, der kan have indflydelse på prioriteringen. Denne mapning skal herefter anvendes til udarbejdelsen af konkrete scenarier, der anviser tilpassede rækkefølger af genoprettelsen. Disse scenarier bør tilføjes til kommunens beredskabsplan således, at det er klart, hvad der konkret skal gøres, hvis et nedbrud skulle ramme.

Princip 4: teknisk synergi

Der kan være tekniske forhold, der har indflydelse på, hvor effektiv en genoprettelse er. Dette gælder både i forhold til systemer, men også i forhold til lokationer.

Således kan der potentielt være tilfælde, hvor man med fordel kan genetablere et prioritet 2- eller 3-område hurtigt og med en lille indsats, hvor man kan genetablere mange systemer på en gang eller hvor man kan genetablere en lokation med mange medarbejdere, selvom disse ikke løser nogen af de højest prioriterede kerneopgaver. Dette bør af KIT analyseres mere dybdegående, og eventuelle synergier bør efter nærmere aftale med forvaltningerne spille ind i forbindelse med den nærmere beskrivelse af den trinvise genetablering i kommunens beredskabsplan.

Deloitte.

Om Deloitte
Deloitte leverer ydelser indenfor revision, consulting, financial advisory, risikostyring, skat og dertil knyttede ydelser til både offentlige og private kunder i en lang række brancher. Deloitte betjener fire ud af fem virksomheder på listen over verdens største selskaber, Fortune Global 500®, gennem et globalt forbundet netværk af medlemsfirmaer i over 150 lande, der leverer kompetencer og viden i verdensklasse og service af høj kvalitet til at håndtere kundernes mest komplekse forretningsmæssige udfordringer. Vil du vide mere om, hvordan Deloittes omkring 264.000 medarbejdere gør en forskel, der betyder noget, så besøg os på Facebook, LinkedIn eller Twitter.