Koncern IT
Økonomiforvaltningen

Bilag

Til Økonomiudvalget

Bilag 3: Centrale initiativer til sikring af informationssikkerheden i 2019

26. februar 2020

Den teknologiske udvikling, nye avancerede trusler og et øget fokus bl.a. som følge af persondataforordningens ikrafttrædelse, stiller løbende krav til kommunens arbejde med informationssikkerheden. I 2019 er der gennemført en række initiativer, der kort er skitseret i tabel 1 og 2 nedenfor:

Tabel 1:Styring-, databeskyttelse- og medarbejderindsatser

Initiativområde	Formål
Vedtagelse af fem forretningscirkulærer	At styrke kommunens governance i relation til drift af it og beskyttelse af data, bl.a. ved at: - Fastlægge roller og ansvar på tværs af kommunen - Fastlægge regler i relation til persondatabeskyttelse, informationssikkerhed samt for drift, vedligehold og udfasning af it-systemer.
Undervisning og implementering af forretningsgang for it-anskaffelser	At forbedre den indledende forventningsafstemning om opgaver og roller i en it-anskaffelse på tværs af kommunen. Hermed minimeres tilbageløb og fordyrelser i forbindelse med udvikling og implementering af nye it-systemer.
Oplysning om phishing	At styrke kommunens medarbejdere i at identificere e-mails, der har til hensigt at kompromittere kommunens informationssikkerhed.
Databeskyttelses task-forces	At sikre compliance med databeskyttelsesforordningen og iværksættelse af risikomitigerende tiltag gennem udarbejdelse af databehandleraftaler og gennemførelsen af konsekvensanalyser af kommunens behandlingsprocesser.

Initiativområde	Formål
Styrkelse af cyberforsvar	At styrke kommunens sikkerhed overfor større cybertrusler gennem en række initiativer herunder: - Kommunen har afsluttet segmentering af kommunens datanetværk, der minimerer

Koncern IT
Vejledende Sikkerhed
Borups Allé 177
2400 København NV

EAN-nummer
5798009809308

	skaderne hvis it-kriminelle får adgang til kommunens infrastruktur. - Udarbejdelse af arkitektursikkerhedsstandarder, reducerer kompleksiteten og øger sikkerheden i de løsninger, der anskaffes i kommunen - Øget scanning og overvågning af kommunens infrastruktur gør det muligt at identificere angreb, sårbarheder og øvrige driftsforstyrrelser tidligt.
Oprydning af ældre infrastruktur	At styrke sikkerheden og minimere den driftsmæssige kompleksitet ved bl.a. at udskifte ældre servertyper og lan-switches.
Tværgående løsninger	At minimere den tekniske kompleksitet på tværs af kommunen. Dette er bl.a. sket gennem centralisering af kommunens logningsløsning (SIEM) og udvikling af it-identitetsstyringssystem (IGA).
Datamanagement	At sikre de rette medarbejdere har adgang til de rette datatyper, hvilket bl.a. er sket gennem det tværgående Office365 oprydningsprojekt. Herudover har Sundhedsforvaltningen udviklet et system til håndtering af vikarers it-identiteter.
Beredskab	At sikre kommunen hurtigt kan reetablere sikker drift efter et it-nedbrud samt fortsætte (manuel) drift i den mellemliggende periode. Dette er bl.a. sket ved, at alle forvaltninger har opdateret deres beredskabsplaner og disse planer er testet i en fælles KK-kriseøvelse.
Risikovurdering af it-systemer	At sikre en høj sikkerhed i forvaltningernes individuelle it-systemer. Alle forvaltningerne har arbejdet målrettet med at udarbejde og implementere handleplaner på baggrund af de it-risikovurderinger, der blev udarbejdet i 2018. Gennem dette arbejde har forvaltningerne aktivt taget stilling til de sikkerheds- og lovgivningsmæssige udfordringer i et udsnit af deres systemportefølje.

Videre proces

I 2020 har Databeskyttelsesrådgiveren taget initiativ til at udarbejde et samlet koncept for risikovurderinger på tværs af kommunen, hvilket gennemføres i samarbejde med KIT og forvaltningerne. Herudover vil der være et fortsat fokus på flere af de igangsatte initiativer fra 2019 med bl.a. styrkelsen af cyberforsvaret, beredskabet, datamanagement, risikovurdering af it-systemer og vedligeholdelse af kommunens infrastruktur.